

**CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND
DAVIDSON COUNTY**

INFORMATION SECURITY

| | |
|--|---|
| <p>SUBJECT:</p> <p>MUSIC CITY CENTER SCOPE, BACKGROUND, AND GOVERNANCE STATEMENTS FOR INFORMATION SECURITY POLICIES</p> | <p>DISTRIBUTION DATE: 5/18/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EFFECTIVE DATE: 5/18/2018</p> <p>EXPIRATION: UNTIL RESCINDED</p> |

PURPOSE

Music City Center implemented an Information Security Management program per Charles Starks, Preside/CEO of the Music City Center. A core component of this program is a set of information security policies based on international standards. This document provides the scope, background, and governance information common to all of Music City Center’s information security policies. For brevity and clarity, instead of restating this information in every policy, it is referenced; therefore, this information is considered a part of each and every Music City Center information security policy unless specifically noted otherwise.

POLICY

Where applicable, Music City Center will reference the Metropolitan Government of Nashville and Davidson County’s Metropolitan Government Scope, Background, and Governance Statements for Information Security Policies.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.



THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON
COUNTY

KARL DEAN, MAYOR

EXECUTIVE ORDER NO. 038

SUBJECT: Information Security Management Policy and Steering Committee.

I, Karl Dean, Mayor of the Metropolitan Government of Nashville and Davidson County, by virtue of the power and authority vested in me, do hereby find, direct, and order the following:

- I. The Metropolitan Government of Nashville and Davidson County ("Metropolitan Government") is required to maintain the confidentiality and integrity of information systems and high standards of information security; and
- II. Executive Order 004 established two advisory boards, the Information Technology Advisory Board (ITAB) (providing advice on information technology service management and information technology standards and best practices) and the Information Security Advisory Board (ISAB) (providing advice on information security management standards and best practices); and
- III. There is now a need to establish the Metropolitan Government's Information Security Management Policy (ISM Policy) to address the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction now and in the future as changes occur; and
- IV. The Director of Information Technology Services (Director) has recommended an ISM Policy based on the needs of the Metropolitan Government and the advice of the ISAB; and
- V. That ISM Policy, attached as Exhibit A to this Executive Order, is now ordered and established by this Executive Order and shall continue to be in effect until modified by a subsequent Executive Order; and
- VI. There is hereby created an Information Security Steering Committee (Steering Committee) to review and advise the Director on system-wide information security policies, standards, and practices for the Metropolitan Government. The functions, membership and meetings shall be as follows:
 - A. FUNCTIONS
 1. Recommending alterations or changes to the Director of minimum security requirements for Metropolitan Government departments, agencies, and boards.
 2. Recommending to the Director performance measures to determine the effectiveness of Metropolitan Government policies, procedures, plans, standards, guidelines, and controls designed to meet or exceed the objectives identified in the ISM Policy.

RECEIVED

MAR 26 2010

METROPOLITAN
CLERK

METROPOLITAN GOVERNMENT INFORMATION SECURITY MANAGEMENT POLICY

1.0 Definitions of Common Terms

- **Director** – The Director of Information Technology Services.
- **Information Security** – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
 - Confidentiality - Preserving authorized restrictions on access and disclosure including means for protecting personal privacy and proprietary information;
 - Integrity - Guarding against improper information modification or destruction and protecting information nonrepudiation and authenticity; and
 - Availability - Ensuring timely and reliable access to and use of information.
- **Procedures** – The steps that need to be performed to meet standards and comply with this Policy. There are typically many procedures in place to maintain compliance.
- **Standards** – The Metropolitan Government of Nashville and Davidson County's ("Metropolitan Government") minimum requirements for users to assure compliance with this Policy.
- **Systems** - Metropolitan Government information systems.

2.0 Purpose

The purpose of this Information Security Management Policy ("Policy") is to provide consistent direction and support for Information Security.

3.0 Scope

This Policy shall apply to all Metropolitan Government employees and third party users except: employees and users of the Nashville Electric Service, the Metropolitan Nashville Airport Authority, the Metropolitan Hospital Authority, and the Metropolitan Development and Housing Agency. However, these agencies are requested to consider adopting these or similar policies.

4.0 Minimum Standards

Maintaining the confidentiality, integrity, and availability of information, information technology, and critical operational processes in a manner meeting the Metropolitan Government's legal, regulatory and ethical responsibilities on behalf of its citizens is of paramount importance to the Metropolitan Government. The Director, therefore, shall develop, disseminate, review, and update an Information Security management program ("Program") consisting of policies, procedures, plans, standards, guidelines, and controls that are consistent with and meet those responsibilities.

- vi. **Contingency Planning** - establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for information systems and creates the availability of critical information resources and continuity of operations in emergency situations.
- vii. **Identification and Authentication** - developing prerequisites to allowing access to Systems by information system users, processes acting on behalf of users, or devices acting on behalf of users, and authentication (or verification) of the identities of those users, processes, or devices.
- viii. **Incident Response** - (a) establishes incident handling capability for Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (b) that tracks, documents, and reports incidents to Metropolitan Government officials and/or authorities.
- ix. **Maintenance** - (a) performs periodic and timely maintenance on Systems; and (b) provides effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- x. **Media Protection** - (a) protects information system media, both paper and digital; (b) limits access to information on information system media to authorized users; and (c) sanitizes or destroys information system media before disposal or release for reuse.
- xi. **Physical and Environmental Protection** - (a) limits physical access to information systems, equipment, and the respective operating environments to authorized individuals; (b) protects the physical plant and support infrastructure for information systems; (c) provides supporting utilities for information systems; (d) protects information systems against environmental hazards; and (e) provides environmental controls in facilities containing information systems.
- xii. **Planning** - develops, documents, periodically updates, and implements security plans for Systems that describe the security controls in place or plans for the information systems and the rules of behavior for individuals accessing the information systems.
- xiii. **Personnel Security** - (a) requires that individuals occupying positions of responsibility within the Metropolitan Government (and third-party service providers) meet established security criteria for those positions; (b) maintains Metropolitan Government information and information systems protections during and after personnel actions such as terminations and transfers; and (c) employs sanctions for personnel failing to comply with Metropolitan Government security policies and procedures.
- xiv. **Risk Assessment** - periodic assessments of risk to Metropolitan Government operations (including mission, functions, image, or reputation), its assets, and individuals, resulting from the operation of its information systems and the associated processing, storage, or transmission of its information.

- Provides sufficient information about management controls and common controls to enable an implementation that is unambiguously compliant with the intent of this Policy and a determination of the risk to be incurred if the plan is implemented as intended;
- Includes roles, responsibilities, management commitment, coordination among Metropolitan Government entities, and compliance;

In addition, the Director shall review the plan, at least annually, and shall revise the plan to address organizational changes and problems identified during plan implementation or security control assessments.

5.3 Priorities

The Metropolitan Government priorities for Information Security are:

- Complying with applicable federal and state information privacy and security laws, regulations and contractual requirements such as the Health Insurance Portability and Accountability Act, the Red Flags Rule under the Fair and Accurate Credit Transactions Act, the Payment Card Industry Data Security Standard, and the Tennessee Identity Theft Deterrence Act of 1999;
- Developing an Information Security awareness training program for Metropolitan Government employees and third party users as required by Executive Order No. 005;
- Training Metropolitan Government employees and third party users to understand the consequences of security violations and that security violations are subject to discipline, up to and including termination of employment and/or termination of contract, as applicable;
- Utilizing standards, frameworks and controls such as the ISO/IEC 27000 Information Security series, the National Institute of Standards and Technology ("NIST") Federal Information Processing Standards, and NIST Guidelines and the Payment Card Industry Data Security Standard.

6.0 Review

The Director of the Department of Information Technology Services is responsible for the development, review, and evaluation of this Policy. The review shall include assessing opportunities for improvement of this Policy and responding to changes to the Metropolitan Government's environment, business circumstances, legal conditions, or technical environment.

| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 1</p> |
| <p>SUBJECT:</p> <p>ACCEPTABLE USE OF INFORMATION TECHNOLOGY ASSETS POLICY</p> | <p>DISTRIBUTION DATE: 5/15/2018</p> <hr/> <p>EFFECTIVE DATE: 5/15/2018</p> |
| <p>ISSUING AUTHORITY: AMENDED KARL DEAN EXECUTIVE ORDER NO. 015</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

PURPOSE

The purpose of this policy is to inform users of the Music City Center Information Technology Assets of what uses are permissible and what uses are prohibited. Compliance with this policy drives the Music City Center’s ability to protect Convention Center Authority services, Convention Center Authority Team Members and the citizens of Nashville and Davidson County.

POLICY

1. Access and Use

1.1. Team Member Access

All Team Member access to Information Technology Assets:

- shall be approved by the President/CEO or his/her designee,
- shall be limited to the Information Technology Assets necessary and appropriate for the Team Member to perform the job duties and functions assigned to him or her.

2. Sensitive Information

2.1. Team Member Responsibility

Team Members shall be required to know the Classification of the Information of the Music City Center to which they have access, and with which they are permitted to work. Team Members shall understand the appropriate Security Controls that should be applied to that Information.

2.2. Dissemination and Confidentiality

Sending, transmitting or otherwise disseminating Sensitive Information shall be strictly prohibited unless authorized by the President/CEO. Team Members shall not disclose or discuss any Sensitive Information with others, including friends or family. Team Members shall not publish or disclose any Sensitive Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. Team Members shall immediately return any documents or media containing Sensitive Information to the Music City Center upon termination. Team Members shall have no right to any



similarly authorized to gain access to any secure area.

3.4. Virus Protection

A Team Member shall never download files from the Internet from unknown sources, open attachments to email from unknown sources, use Removable Media from unknown sources, or otherwise risk virus infection, except where permitted by the President/CEO or his/her designee. If a Team Member has any reason to suspect material may be infected, a Team Member shall immediately contact the Music City Center Information Technology Services' helpdesk or their Department Director so that the material can be virus-scanned by the Information Technology staff. Team Members shall not knowingly or negligently store, send or create destructive programs, including any virus, self-replicating code or any other program that operates in a similar fashion. Team Members shall not disable or modify the existing Music City Center supported anti-virus software.

3.5. Prohibited Acts

3.5.1. Personal Use

Information Technology Assets are intended for business purposes. Team Members shall not use Information Technology Assets to engage in Internet gambling, post in non-business related chat rooms or on non-business-related Internet Web logs (blogs), or to view pornographic or other inappropriate material as discussed below in 3.5.2. Occasional, limited, reasonable, and appropriate personal use shall be permitted when such use does not:

- Interfere with the Team Member's work performance;
- Interfere with any other Team Member's work performance;
- Unduly impact the operation of Music City Center and/or its Information Technology Assets;
- Violate any law, rule, regulation, or court order; or
- Violate any provisions of this policy, or any other Music City Center policy, standards or practices.

Team Members must use Information Technology Assets in a professional, ethical and legal manner, regardless of whether such use is personal or business-related.

3.5.2. Inappropriate Material

Information Technology Assets shall not be used to upload, download, communicate, create, store, send or intentionally view, access or display material that is fraudulent, libelous, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. The above prohibition shall not apply where such treatment of such material has been explicitly authorized by the President/CEO or his/her designee for preserving evidence, or for other good reason.

Sending messages with derogatory or inflammatory remarks, including, but not limited to, remarks about race, color, national origin, gender, age, religion, sexual orientation or disability may violate federal, state or Metropolitan Government laws, rules and policies on discrimination and sexual harassment. Such messages shall not be transmitted or forwarded using Information Technology Assets except where authorized by the Director of Technology and the Department of Law for the purpose

4. Privacy

4.1. Acknowledgement of and Consent to No Expectation of Privacy

Except as otherwise provided by applicable law, Team Members shall not have an expectation of privacy in any Information they create store, send or receive on Information Technology Assets.

Music City Center retains the right, but not the duty, to monitor any and all aspects of its Information and Information Technology Assets, including, without limitation, monitoring Internet sites visited by Team Members, monitoring chat groups and newsgroups, reviewing materials downloaded or uploaded electronically and reviewing files and Email created, stored or received by a User. Such activity is to be consistent with applicable laws and performed in accordance with any Music City Center/Metropolitan Government policies and procedures governing these actions. Specifically, any correspondence of the Music City Center in the form of email may be a public record under the public records law and may be subject to public inspection. Except for the Music City Center's right to retrieve and read any email message as provided in this policy, email shall be accessed only by the intended recipient. Emails and their content are occasionally visible to the Music City Center/Metropolitan Government Information Technology Services Department employees or Information Technology employees of other Metropolitan Government departments engaged in routine testing, maintenance and problem resolution.

Please note that, prior to use of Information Technology, a Team Member shall execute and enter into *the METROPOLITAN GOVERNMENT ACCEPTABLE USE OF INFORMATION ASSETS POLICY CONSENT AND RELEASE* attached hereto as Signature Page, which is in addition to and not exclusive of the rights granted and obligations imposed herein.

4.2. Passwords and Privacy

Use of a password does not imply that Team Members have an expectation of privacy in the Information they create, store, send, or receive on Information Technology Assets. The Music City Center/Metropolitan Government may utilize global passwords that permit access to any and all Information stored on its Information Technology Assets, regardless of whether access to that Information has been restricted by a requirement that a particular Team Member's password be first entered. Such access may occur with or without notice to the Team Member or the Team Member's written consent.

5. Email Guidelines

5.1. Footer Language

Use of any email footer or signature block requires the approval of the President/CEO. Team Member may be required by the President/CEO to use an approved footer or signature block.

5.2. Mass Email Distribution

Except where necessary for legitimate Music City Center business purposes, the transmission of emails to a general, non-specific audience of the Music City Center is prohibited. Requests to send emails to all Music City Center/Metropolitan Government employees must be approved by the President/CEO, and, where necessary, by the Department of Human Resources. Requests to send Department-wide emails must be approved by the President/CEO or his/her designee.

Removable Media to the issuing Department consistent with Departmental requirements.

8.1. Physical Security

Removable Media shall be secured if not in the possession of the Team Member. Removable Media taken off-site and in transit shall not be left unattended. The theft or loss of any Removable Media containing Sensitive Information shall be reported immediately to the Music City Center's Information Technology Department or the President/CEO.

8.2. Information Storage

Team Members who store Information of the Music City Center/Metropolitan Government on Removable Media shall first ensure that they are fully aware of the content and Classification of that Information.

9. Destroying Information When No Longer Needed

Information of the Music City Center/Metropolitan Government stored on any of the following Devices shall be removed using a Music City Center/Metropolitan Government ITS approved method: hard drives, CDs, DVDs, copiers, computer memory, flash drives, etc. This should be done prior to the Device being retired or disposed of, and in a manner that is consistent with applicable laws and a records retention schedule approved by the Davidson County Public Records Commission, including, without limitation, the General Records Schedule of the Metropolitan Government of Nashville and Davidson County. *See also*, the provisions of paragraph 5.3, above, regarding pending public records requests, or where litigation has commenced or is reasonably anticipated.

10. Approved Cell Phones, PDAs or Blackberries

Any Mobile Device, such as a mobile phone, PDA, Blackberry, etc., that will be used to store or access Information of the Music City Center/Metropolitan Government shall be connected to a Music City Center/Metropolitan Government approved Mobile Device server. These Devices are required to be PIN protected and shall allow remote wiping in the event of theft or loss of the Device. The theft or loss of any Mobile Device used to store or access Information of the Music City Center/Metropolitan Government shall be immediately reported to the Team Member's Department Director, immediate supervisor, or applicable IT Department.

11. Social Media and Social Networking

Social media consists of Internet-based applications including web- and mobile-based technologies that allow for the creation and exchange of user-generated content. Examples of social media include, but are not limited to, Facebook, blogs, Twitter, LinkedIn, YouTube, Flickr, and comments following online news articles. Social networks are communities of people or organizations that share interests and/or activities and use a wide variety of Internet technology to interact. The Music City Center/Metropolitan Government of Nashville and Davidson County use social media and social networking as means of communicating its services, events, and performance to the public.

11.1. Department Use of Social Media

An employee must be authorized by the President/CEO or his/her designee to represent the Department prior to authoring content on a Department's social media. Team Members representing the Music City Center/ Metropolitan Government Department through social media will conduct themselves as a representative of the city. The Music City Center's rules, policies and standards of conduct apply to Team Members who engage in social media/networking

disciplinary action up to and including termination of employment.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
 President/CEO
 Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 7.1.3, 10.8, 11.7.1
- NIST Special Publications 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations: AC-1, AC-6, AC-20, PL-4, MP-4, MP-6,
- NIST Special Publications 800-45, Guidelines on Electronic Mail Security
- NIST Special Publications 800-88, Media Sanitation Guide
- NIST Special Publications 800-46, Guide to Enterprise Telework and Remote Access Security CNSSI Instruction No. 4009 26 April 2010, National Information Assurance (IA) Glossary FIPS 140-2, Security Requirements for Cryptographic Modules
- Metropolitan Government Information Classification Policy
- Music City Center Information Classification Policy

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



| | |
|---|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 1</p> |
| <p>SUBJECT:</p> <p>ACCEPTABLE USE OF INFORMATION TECHNOLOGY ASSETS PLAN</p> | <p>DISTRIBUTION DATE: 5/15/2018</p> <p>EFFECTIVE DATE: 5/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

AUDIENCE

All Team Members

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the accompanying Information Security Policy by providing direction and congruity between it and Music City Center departmental procedures. An Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Acceptable Use of Information Technology Assets Policy.

1. Access and Use

1.1. Team Member Access

All Team Member access to Information Technology Assets:

- *shall be approved by the President/CEO or his/her designee.*
- *shall be limited to the Information Technology Assets necessary and appropriate for the Team Members to perform the job duties and functions assigned to him or her.*

USERS: Team Members, independent contractors, consultants, temporary or part-time employees, leased employees, interns, and other persons or entities to which Music City Center has explicitly granted access to Music City Center/Metropolitan Government's Information Technology Assets, should request, through management, access to the resources required to perform their job duties.

DEPARTMENT AUTHORITY: Data owners and system administrators shall have documented



designee. Note that "stored" means the data resides on the device or media.

DEPARTMENT AUTHORITY: Departments' use of encryption must meet the requirements specified in 12.3 Cryptographic Controls Policy. Music City Center/Metro ITS have solutions in place that Departments can utilize to achieve compliance.

2.4. Access from External Devices

A Team Member shall not access any Sensitive Information from a Device other than one issued to the Team Member by the Music City Center or an Approved Team Member Owned Device. Any exceptions to this rule must be approved by the President/CEO.

USERS: Team Member should check with management to understand how any data they handle is classified. Team Members are responsible for knowing what devices data classified as "sensitive" resides. If sensitive data needs to reside on any device that is not owned by the Team Member or provided by Music City Center/Metro, the Team Member must request an exception.

DEPARTMENT AUTHORITY: Departments are responsible for communicating the Classification of data to their Team Members. To request an exception, Departments can contact the Music City Center Helpdesk.

3. Security

3.1. Use of Passwords or Other Authenticating Information

Team Members shall be responsible for keeping Authenticating Information, including passwords, private and protected. Authenticating Information shall not be printed, kept near the Device in handwritten form, stored online or shared with others, including managers or supervisors. A Team Member shall not use an "AutoComplete" feature that allows a Device to remember usernames or user IDs and passwords to access Sensitive Information.

Team Members shall be responsible for ensuring the proper use of their account and any actions performed with a Team Members account shall be the responsibility of that Team Member. Team Members shall not be permitted to allow other Team Members to have access of their Authenticating Information. Team Member shall not be allowed to use another Team Members Authenticating Information unless explicitly approved by the President/CEO, or as otherwise expressly required by their jobs (e.g. Music City Center or Metropolitan Government Information Technology Services helpdesk, agencies' helpdesks). Team Members shall be responsible for following all standards with regards to Authenticating Information. Immediately following these instances, the Team Members password must be reset.

USERS: Team Members shall ensure that only they have passwords to accounts assigned to them. Team Members shall not share these passwords with anyone and should exercise common sense when dealing with their passwords (not posting them on a monitor, writing them under a keyboard, sending them through email, etc.). Team Members shall ensure that only they use accounts assigned to them.

Team Members should understand that they are responsible for any activity that takes place using their account. Team Members shall receive written approval by the President/CEO or

DEPARTMENT AUTHORITY: Department should contact the applicable IT Department for clarification or questions on how to meet this requirement.

3.5. Prohibited Acts

3.5.1. Personal Use

Information Technology Assets are intended for business purposes. Team Members shall not use Information Technology Assets to engage in Internet gambling, post in non-business related chat rooms or on non-business-related Internet Web logs (blogs), or to view pornographic or other inappropriate material as discussed below in 3.4.2. Occasional, limited, reasonable, and appropriate personal use shall be permitted when such use does not:

- *Interfere with the Team Members work performance;*
- *Interfere with any other Team Members work performance;*
- *Unduly impact the operation of Music City Center/Metropolitan Government and/or its Information Technology Assets;*
- *Violate any law, rule, regulation, or court order; or*
- *Violate any provisions of this policy, or any other Music City Center policy, standards or practices.*

Team Members must use Information Technology Assets in a professional, ethical and legal manner, regardless of whether such use is personal or business-related.

USERS: Team Members should contact their supervisors for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Any violations should be reported to the appropriate authority.

3.5.2. Inappropriate Material

Information Technology Assets shall not be used to upload, download, communicate, create, store, send or intentionally view, access or display material that is fraudulent, libelous, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. The above prohibition shall not apply where such treatment of such material has been explicitly authorized by the President/CEO for the purpose of preserving evidence, or for other good reason.

Sending messages with derogatory or inflammatory remarks, including, but not limited to, remarks about race, color, national origin, gender, age, religion, sexual orientation or disability may violate federal, state or Metropolitan Government laws, rules and policies on discrimination and sexual harassment. Such messages shall not be transmitted or forwarded using Information Technology Assets except where authorized by the President/CEO for the purpose of preserving evidence or for other good reason, or as otherwise expressly required by their job duties (e.g., law enforcement). Team Members encountering or receiving any such prohibited messages or material shall report the incident to a supervisor or a President/CEO.

Music City Center/Metropolitan Government to third-party hosted Network storage areas, such as Microsoft SkyDrive, Google Docs, Dropbox or other cloud storage mechanisms, shall not be allowed without prior approval of the Director of Technology.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Unless absolutely necessary, the primary copy of critical business data must be stored on a Metro Network drive. President/CEO and data owners should be fully aware of where their information resides, including applications, files, email, calendars, etc., and should consult with the Director of Technology for approval on any storage outside the Metro Network. Any violations should be reported to the appropriate authority.

3.5.7. Waste and Abuse

Team Members shall not monopolize or otherwise deliberately perform acts that waste, impair damage or prevent the use by other Team Members of the Information Technology Assets or Information of the Metropolitan Government, or attempt to do any of the above.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement. Such activity includes, but is not limited to, using network to view non-work related streaming media, storing DVD's or music on file and print servers, printing books for personal use with Metropolitan Government printers, etc.

DEPARTMENT AUTHORITY: Any violations should be reported to the appropriate authority.

3.5.8. Unauthorized Distribution of Information on the Internet

Unless specifically authorized by the President/CEO, all Team Members shall be prohibited from making any representations pertaining to or on behalf of Music City Center/Metropolitan Government or from distributing or utilizing in any manner Information of the Metropolitan Government on the Internet.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Any violations should be reported to the appropriate authority.

4. Privacy

4.1. Acknowledgement of and Consent to No Expectation of Privacy

Except as otherwise provided by applicable law, Team Members shall not have an expectation of privacy in any Information they create store, send or receive on Information Technology Assets.

5. Email Guidelines

5.1. Footer Language

Use of any email footer or signature block requires the approval of the President/CEO. Team Members may be required by their President/CEO to use an approved footer or signature block.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement. Signature blocks should be limited to contact information. It should not include personal information, philosophies, jokes, images, etc.

DEPARTMENT AUTHORITY: It is recommended that any information that is used as disclaimers or departmental footers is approved by the legal counsel. Departments should have a documented example of acceptable signature blocks and a process for approving signature blocks, including who is authorized to approve them.

5.2. Mass Email Distribution

Except where necessary for legitimate Music City Center business purpose, the transmission of emails to a general, non-specific audience of Music City Center Team Members is prohibited. Requests to send emails to all Music City Center/Metropolitan Government employees must be approved by the President/CEO, and, where necessary, by the Department of Human Resources. Requests to send Department-wide emails must be approved by the applicable President/CEO.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Any requests to send "bulk" email, or emails sent to a general, non-specific audience, such as "all Metro employees" or "all police officers", etc., can be sent to the Director of Technology.

5.3. Actions Upon Commencement of Litigation or Investigation

Automatic deletion or manual deletion by Team Members of emails with potentially relevant information shall be suspended to preserve responsive records once a formal investigation or litigation is reasonably anticipated or has commenced, upon receipt of a notice of litigation hold, or upon receipt of a public records request with regard to records responsive to it while it is pending.

The obligation to preserve such records may be imposed by request of the Director of ITS, the President/CEO, or by the appropriate legal counsel. Even in the absence of such a request, Team Members aware of litigation, that litigation is reasonably anticipated, or of a pending public records request should not delete any potentially relevant information.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: President/CEO should contact their legal representatives for advice or questions regarding litigation holds or public records requests.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Departments should contact their applicable IT helpdesk for guidance on meeting this requirement.

8. Removable Media

Team Members shall only use Removable Media that has been supplied by the Music City Center/Metropolitan Government. Any Removable Media that is used for the storage of Sensitive Information shall be encrypted with encryption software approved by the Music City Center/Metropolitan Government ITS Department. The Team Member shall return the Removable Media to the issuing Department consistent with departmental requirements.

8.1. Physical Security

Removable Media shall be secured if not in the possession of the Team Member. Removable Media taken off-site and in transit shall not be left unattended. The theft or loss of any Removable Media containing Sensitive Information shall be reported immediately to the Music City Center's Information Technology department or the President/CEO.

USERS: Team Member should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Departments should ensure that employees take appropriate safeguards commiserate with the Classification of the data stored on the media. For more information, refer to the 7.2.1 Music City Center Information Classification Policy.

8.2. Information Storage

Team Members who store Information of the Music City Center/Metropolitan Government on Removable Media shall first ensure that they are fully aware of the content and Classification of that Information.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Departments should refer to the 7.2.1 Music City Center Information Classification Policy.

9. Destroying Information When No Longer Needed

Information of the Music City Center/Metropolitan Government stored on any of the following Devices shall be removed using a Music City Center/Metropolitan Government ITS approved method: hard drives, CDs, DVDs, copiers, computer memory, flash drives, etc., This should be done prior to the Device being retired or disposed of, and in a manner that is consistent with applicable laws and a records retention schedule approved by the Davidson County Public Records Commission, including, without limitation, the General Records Schedule of the Metropolitan Government of Nashville and Davidson County. See also, the provisions of paragraph 5.3, above, regarding pending public records requests, or where litigation has commenced or is reasonably

- *Information that may compromise the safety or security of the public, Music City Center Team Members, or those in the care of the Music City Center;*
- *Personal agendas or opinions;*
- *Any other content protected and confidential under the law.*

USERS: Team Members should contact their Department Director/manager/HR for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Departments should contact their applicable IT helpdesk for guidance on meeting this requirement.

11.2. Employee Personal Use of Social Media

In general, Team Members who participate in social media and social networking are free to publish their own personal information without censorship by the Music City Center/Metropolitan Government. Team Members who choose to identify themselves as the Music City Center Team Members through social media must state in clear terms that their expressed views are theirs alone and do not reflect the views of the Music City Center. Except as authorized, Team Members are prohibited from representing the Music City Center through their personal use of social media.

Just as Team Members behavior outside of work could constitute a failure of good behavior which reflects discredit upon themselves, the Department and/or the Music City Center, their contribution to social media and social networking can do the same. In situations where a Team Member's social media contribution causes an issue which is substantially related to an important government interest, or which has the effect of creating a disruption in the workplace (e.g., such as where the usage is tied to threatening, discriminatory, harassing, or retaliatory behavior directed at the Music City Center/Metropolitan Government or an employee of the Music City Center), disciplinary action up to and including termination may be merited.

Except where authorized, employee's social media content will not include Intellectual property of the Music City Center (e.g., drawings, designs, software, ideas and innovation) or the Music City Center's logo.

USERS: Team Members should contact their Department Director/manager for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Departments should contact their applicable IT helpdesk for guidance on meeting this requirement.

12. Miscellaneous

This policy shall supersede all previous Music City Center/Metropolitan Government acceptable use policies including but not limited to the "Comprehensive Internet and Electronic Mail Use Policy" formerly attached to Executive Order 15. This policy may be amended or revised at any time. Team Members are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions. This policy does not supersede any departmental policies that address areas not defined in this policy as long as the requirements of such departmental policies equal or exceed the minimum requirements set forth in this policy. This policy does not waive the Team Member's responsibility to follow all applicable legal and/or regulatory requirements.

REVISION HISTORY

| REVISION | DATE | CHANGES |
|-----------------|-------------|-----------------------|
| 1.0 | 5/15/2018 | First Release Version |
| | | |

MCC Standard
Administrator-Level Access Practices

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Team Members

PURPOSE

Enhance Information Security, reduce the risk of security incidents and help ensure compliance to Music City Center/Metro's ACCEPTABLE USE OF INFORMATION ASSETS POLICY by limiting high level, administrator access to assets.

SUMMARY

Accounts with administrator level access to an asset, such as a PC, laptop, server, etc. has full rights to all areas of that asset. Administrator-level account users have the ability to modify settings on the device, install/un-install software, install/un-install hardware, etc. Administrator-level accounts are created to justify business needs and will be restricted to specific use to reduce the risks associated with these accounts.

Risks of an account with administrator access include:

1. System files can be accessed or changed.
2. Program files or program configurations could be modified.
3. Software that is not approved could be installed, and won't be maintained.
4. Malicious code can be installed with unlimited rights.
5. New, unapproved user accounts could be added to the system.
6. Password policies could be subverted.
7. Security controls such as anti-malware, firewalls, removable media controls, could be disabled.
8. Installation of illegal, unauthorized or unlicensed software.
9. Access to other users' data that may be stored on the device.
10. Access to other systems or devices connected to the Metro network. These systems or servers can host large databases of sensitive data.

Advantages of limiting access include:

1. **Threat Protection:** Running with reduced privileges can mitigate a majority of software vulnerabilities in software products. Any vulnerability has the potential to be a zero-day: meaning it is exploited before the vendor or security vendors know about it and have a chance to stop exploits with patches or antivirus \ intrusion prevention signatures. Running software with reduced privileges protects most software from being exploited by vulnerabilities that take advantage of the privileges of the running user.
2. **Regulatory Compliance:** When an organization does not remove administrator rights, users can change system settings, which affect compliance to regulatory standards. Failure in compliance may result in more audits and remediation work.
3. **System Stability:** Every time a user adds a new piece of software, installs a driver, or changes a setting, the stability of the system is affected. Forrester Consulting published a paper in 2009 finding that 1 out of 7 helpdesk calls were due to users corrupting their system with unauthorized software (2009, Forrester).



MCC Standard
Administrator-Level Access Practices

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 3 |

Administrative Accounts Monitoring

Groups providing administrative privileges (Domain Admins, Builtin Administrators, Enterprise Admins, etc.) will be audited periodically. Group membership will be monitored for any security groups providing high level administrative privileges and alerts shall be configured for changes in group membership.

Additional Administrative Rights Requirements

Administrative rights are non-transferrable. Users with administrative rights are not allowed to grant other users administrative rights. Each user is required to go through the process of requesting, and getting approval, for those rights. Administrative rights do not automatically transfer to staff replacing a user who has already been approved for these rights. This type of situation requires a separate request.

Before deploying any new device or application, all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems shall be changed and have values consistent with administrative-level accounts.

Administrators shall access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

Administrative rights to databases and applications should be limited to those with a business need to have those rights. Accounts with administrative rights to databases and applications shall be limited to administrative accounts and shall not be granted to standard accounts.

ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



**MCC Standard
Passwords**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Team Members

PURPOSE

Enhance Information Security by using strong passwords for access to Information Technology Assets

SUMMARY

Passwords represent the primary means for authentication to Music City Center/Metropolitan Government systems. As such, it is imperative that technical and administrative controls are in place enforcing a minimum standard that should be followed when creating and when using passwords. **All passwords used to access Music City Center/Metropolitan Government Information Technology Assets are to be treated as Sensitive, Confidential Information of the Music City Center/Metropolitan Government.**

DETAILS

Password Construction Standard

- Blank passwords shall **not** be permitted.
- Passwords shall be at least ten (10) characters long for standard passwords and fourteen (14) characters long for administrative passwords. Passwords in excess of ten (10) or fourteen (14) characters are preferred.
- Passwords shall include characters from a minimum of three (3) of the following four (4) categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphanumeric characters (Special characters. For example: !, \$, #, %)
- Passwords shall **not** contain significant portions of the user's account name or full name.
- Passwords shall **not** contain a word in any language, slang, dialect, jargon, etc.
- Passwords shall **not** contain four (4) or more repeating characters or a predictable pattern.
 - AAAA12345 is not allowed ('A' repeated; '12345' is predictable).
 - ABCD11111E is not allowed ('1' repeated; 'ABCD' is predictable).

Password Protection

Protecting the confidentiality of a password is vital. A password authenticates a user. The user should be the only one to know the password. If someone demands a password, refer them to the Music City Center/Metropolitan Government *Acceptable Use of Information Technology Assets Information Security Policy*.

Additional Password Governance, Storage and Handling

Additional baseline password requirements are listed below.

1. Passwords shall not be stored using reversible encryption.
2. Passwords shall expire, and have to be changed, at least every sixty (60) days.



MCC Process
Mass Email Approval

| | |
|----------------------------|----------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 1 |

AUDIENCE

Team Members

PURPOSE

This process is designed to minimize the amount of unsolicited email sent to employees and ensure that email sent from internal users is for approved work.

SUMMARY

Except where necessary for legitimate business purposes, the transmission of emails to a general, non-specific audience of Music City Center Team Members is prohibited. Any requests to send this type of "bulk" email to lists such as "MCC Building Distribution Group", "MCC Technology", etc. should be sent to Management for approval.

DETAILS

1. Emails requested to be sent to all Music City Center Team Members should come from the President/CEO or his/her designee.
2. Emails requested to be sent to all Music City Center Team Members should be approved by the Department Director prior to the message being sent.
3. Emails requesting to be sent to individual groups or interdepartmental should be approved by the President/CEO or his/her designee.

ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



**MCC Standard
Mobile Device and Removable Media Physical
Security Requirements**

| | |
|----------------------------|---------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Public Information |
| Page No. | Page 1 of 1 |

AUDIENCE

Team Members and Metropolitan Government Users

PURPOSE

The following outlines the minimum security requirements for any media that stores Music City Center/Metropolitan Government Information which is taken outside Music City Center/Metropolitan Government's facilities.

SUMMARY

In order to maintain the confidentiality, integrity and the availability of the Music City Center/Metropolitan Government network and its resources, users should be cautious when handling any media which is taken outside the Music City Center/Metropolitan Government's facilities. The requirements below should reduce the risk of a security incident involving media taken outside Music City Center/Metropolitan Government's facilities.

DETAILS

1. All mobile devices, such as laptops, phones, BlackBerrys, PDAs, etc., and any removable media must be physically secured (locked in the trunk of vehicle or glove box, cable locked to a secured structure, locked in drawers, etc.) if not in the possession of the user or in any location where third parties could easily gain physical access to the devices, such as vehicles, hotels, conferences, Music City Center/Metropolitan Government offices, etc. Steps must be taken to ensure that any mobile device and removable media storing Music City Center/Metropolitan Government Information kept inside the User's residence is secured against theft.
2. Users should diligently protect against the disclosure of Music City Center/Metropolitan Government Information in public areas by ensuring that the display of the device is not viewable by any unauthorized persons, also known as "shoulder surfing".
3. Immediately following a loss or theft of any mobile device or removable media, the Department Director/Agency Head and the Music City Center Technology Department/ITS Technical Service Support Center should be notified.

ADDITIONAL INFORMATION (optional)

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



MCC Procedure
Running On Demand Scan with Trend Micro
OfficeScan

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Team Members and all Metro users

PURPOSE


Reduce the possibility of malware infection by doing manual scans prior to access a resource

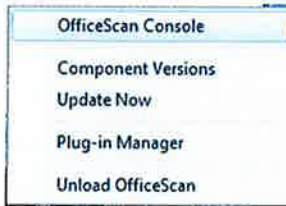
SUMMARY

In order to maintain the confidentiality, integrity and the availability of the Music City Center/Metropolitan Government network and its resources, users should be cautious when accessing any files from any sources. Even files from known, trusted sources can be sources of malware. This document will provide instructions on doing a manual scan of the entire system, as well as a scan on individual files using Metro’s anti-virus application, Trend Micro.

DETAILS

Performing a Manual System Scan with Trend Micro OfficeScan AV:

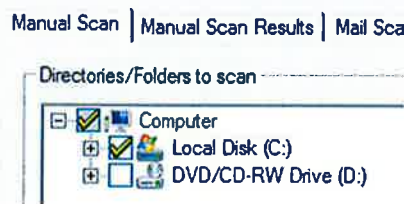
1. Right click on the Trend Icon  in the system tray at the lower right hand corner of the screen to open a context menu.
2. Select the “OfficeScan Console” from the context menu.



3. Select the “Manual Scan” tab on the Trend Micro OfficeScan console



4. Select what Hard Drive/directory you would like to scan



5. Press the Scan Button



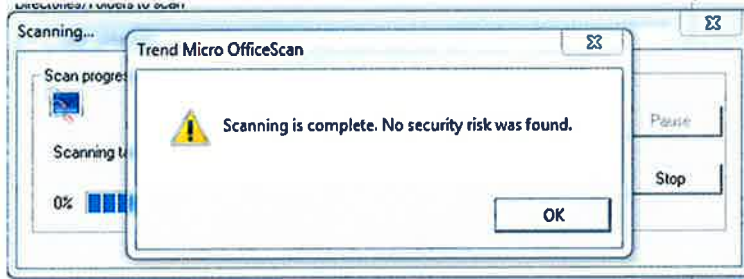
MCC Procedure
Running On Demand Scan with Trend Micro
OfficeScan

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 3 |

4. Wait for the scan to finish then address any issues that may have been found



5. Wait for the scan to finish then address any issues that may have been found.



ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |

**MCC Guidance
Password Creation**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 1 |

AUDIENCE

Team Members and Metro users

PURPOSE

Provide recommendations and guidance on proper password management, including creation and handling. This document supports the *Music City Center/Metropolitan Government Acceptable Use of Information technology Assets Information Security Policy*.

SUMMARY

Passwords represent the primary means for authentication to Music City Center/Metropolitan Government systems. As such, it is imperative that technical and administrative controls are in place enforcing a minimum standard that should be followed when creating and when using passwords. All passwords used to access Music City Center/Metropolitan Government Information Technology Assets are to be treated as Sensitive, Confidential Information of the Music City Center/Metropolitan Government.

DETAILS

Proper password creation should contain the following characteristics:

- At least 10 characters long
- Contain a mix of upper and lowercase letters, numbers, and special characters (!, @, \$, etc.)
- Does not contain words, names birthdates, phone numbers, or other guessable information
- Use Mnemonics to create a password
 - Example: "I like to eat at Red Lobster" becomes Ilike2e@RL

Proper password handling should adhere to the following characteristics:

- Do not write passwords down
- Do not use Metro passwords for other accounts (Facebook, YouTube, etc.)
- Do not tell anyone your password
- Change your password regularly

ADDITIONAL INFORMATION (optional)

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



**MCC Guidance
Password Management**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 4 |

AUDIENCE

Team Members and Metro users

PURPOSE

Provide recommendations and guidance on proper password management, including creation and handling. This document supports the *Music City Center/Metropolitan Government Acceptable Use of Information technology Assets Information Security Policy*.

SUMMARY

Passwords represent the primary means for authentication to Music City Center/Metropolitan Government systems. As such, it is imperative that technical and administrative controls are in place enforcing a minimum standard that should be followed when creating and when using passwords. All passwords used to access Music City Center/Metropolitan Government Information Technology Assets are to be treated as Sensitive, Confidential Information of the Music City Center/Metropolitan Government.

DETAILS

Background

An unauthorized person who obtains a password can:

- Hijack a computer to run his/her illegal activities
- Access sensitive information
- Destroy records or cause network or system outages
- Steal identity information
- Approve or authorize things other users are responsible for
- Send damaging e-mails in another user's name

Passwords are an important aspect of computer security. They are the front line of protection for user accounts and are meant to protect Music City Center/Metropolitan Government data and systems from unauthorized access or use. A poorly chosen password may result in the compromise of Music City Center/Metropolitan Government's entire network. As such, all Music City Center/Metropolitan Government users (including contractors and vendors with access to Music City Center/Metropolitan Government systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Creating Strong Passwords

Anyone who is entrusted with a Metropolitan Government account should be aware of how to select strong passwords. Poor, weak passwords have the following characteristics:

- The password contains less than ten characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.



**MCC Guidance
Password Management**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 4 |

“one”; uppercase “W” replaces “way”; numeric “2” replaces “to”; “r” replaces “remember”; “m” replaces “my”; “*” replaces “password”; “!” on the end for emphasis

Example 2:

“I have a girl who is 17 and a boy who is 12”

Can become: Ig#17b#12!

Uppercase “I”; “g” replaces “have a girl”; “#17” replaces “who is 17”; “b” replaces “and a boy”; “#12” replaces “who is 12”; “!” on the end for emphasis

Example 3:

“I like to eat at Red Lobster”

Can become: Ilik2e@RL!

Uppercase “I”; “lik” replaces “like”; numeric “2” replaces “to”; “e” replaces “eat”; “@” replaces “at”; uppercase “RL” replaces “Red Lobster”; “!” on the end for emphasis

NOTE: Do not use any of these examples as actual passwords!

The following example shows how not to use mnemonics to create a strong password:

“Always assert an ambiguous axiom and argue aggressively”

Should **not** become: Aaaaaaaa

(does not contain at least 10 characters; 4 or more repeating characters;
does not contain either numeric or special characters)

Additional Password Protection Guidance

Protecting the confidentiality of a password is vital. A password authenticates a user. The user should be only one to know the password. As such:

- Don't reveal a password over the phone to ANYONE. ITS staff has the ability to reset passwords. They do not need to know what a password is to gain access.
- Don't reveal a password in an email message that is not encrypted.
- Don't reveal a password to your supervisor. IT staff can reset a password at the supervisor's request.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my children").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.

ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY



MCC Process
Remote Access Request Process

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Team Members

PURPOSE

This process is designed to reduce the risk of security issues arising from the use of non-approved remote access into the Music City Center/Metropolitan Government (Metro) network.

SUMMARY

The use of remote access solutions to connect to the Music City Center/Metro network increases the risk of compromising the confidentiality, availability and integrity of the Music City Center/Metro network and impacting all Music City Center/Metro departments. External access into the Music City Center/Metro network shall utilize a Music City Center/Metro approved Virtual Private Network (VPN), except for information technology assets specifically configured for external access, such as applications accessible outside the network, email, etc. Dial-up access, remote PC connection applications such as Skype, LogMeIn, PC Anywhere, GoToMyPC, etc., are not allowed. All requests for VPN access into the network shall be approved by the President/CEO or his/her designee.

DETAILS

1. Team Members requesting remote access to the Music City Center/Metro network must fill out a "Remote Access Request Form".
2. Request for remote access to the Music City Center/Metro network must be approved by the President/CEO or his/her designee. This signer is responsible for Team Member's actions while on the Music City Center/Metro network. Access will not be granted unless form is signed or emailed from the President/CEO or his/her designee's account.
3. Return all forms to the Metro ITS TSSC.
4. The Team Member signing the form signifies that they have read, understood and accepted all Music City Center/Metro security policies, including the *Acceptable Use of Information Technology Assets* and *Teleworking and Mobile Computer* policies.
5. The use of split-tunneling is not allowed. Split tunneling allows a VPN user to access a public network and the Music City Center/Metro network at the same time, using the same physical network connection.
6. Generic user accounts are not acceptable. Each Team Member requiring access must be assigned an account.
7. Vendor VPN accounts are active for only 6 months from the date of request. Signer is responsible for contacting the Metro ITS TSSC to request an extension.
8. Support of the VPN client is limited to Music City Center/Metro owned assets.
9. Team Members must notify the Music City Center Technology Department of any suspected account compromise.

ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY



MCC FAQ
Secure Configuration Benchmarks

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Team Members

PURPOSE

Benchmarks provide a baseline for systems to test against. Benchmarks should be used only from trusted entities.

SUMMARY

Systems can be configured many ways, and having systems adhere to a predetermined baseline gives administrators guidance on configuring the system to best practices if practical. Benchmarks give a standard for the system to adhere to.

DETAILS

Why benchmarks?

A key method of ensuring that appropriate security is in place is the use of a logical, methodical way of provisioning operating systems and applications in such a way that they are secure from the start. Most operating systems and applications are not configured with security in mind “out of the box”. Ad-hoc processes for securing these devices can cause misconfigurations that may introduce vulnerabilities. By standardizing on an industry acceptable benchmark and configuring to that benchmark, the risk of those vulnerabilities being introduced is reduced.

Furthermore, the use of secure configurations has been recognized as a component to ensuring security. It supports the PROTECT (PR) critical function of the NIST Cyber Security Framework and is called out specifically as a Critical Security Control.

Why the Center for Internet Security benchmarks?

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Resources include secure configuration benchmarks, automated configuration assessment tools and content, security metrics and security software product certifications.

This program is recognized as a trusted, independent authority that facilitates the collaboration of public and private industry experts to achieve consensus on practical and actionable solutions. Because of the reputation, these benchmarks are recommended as industry-accepted system hardening standards and are used by organizations in meeting compliance requirements for FISMA, PCI, HIPAA, and other security requirements.

Configuring IT systems in compliance CIS Benchmarks has been shown to eliminate 8-95% of known security vulnerabilities. The CIS Benchmarks are globally used and accepted as the de facto user-originated standard for IT security technical controls.



MCC FAQ
Secure Configuration Benchmarks

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 3 |

Within Music City Center/Metro ITS, the use of any benchmark or standard must be approved by the Music City Center Directory of Technology/Metro Assistant Director for that area prior to its adoption.

ADDITIONAL INFORMATION *(optional)*

More information about these can be found here: <https://benchmarks.cisecurity.org/>

Full list of what they have developed benchmarks on can be found here:

<https://benchmarks.cisecurity.org/downloads/latests/>

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



**MCC Procedure
Securing Non-Music City Center/Metro
Government Issued Devices**

| | |
|----------------------------|---------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Public Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Team Members and Metro users

PURPOSE

In order to maintain the confidentiality, integrity and the availability of the Music City Center/Metropolitan Government network and its resources, Team Members should ensure that any device used to access Music City Center/Metropolitan Government information technology is secure.

SUMMARY

This document provides a list of Music City Center/Metropolitan Government minimum security requirements to secure any non-Music City Center/Metropolitan Government issued device that is used to access Music City Center/Metropolitan Government resources not allocated for general public use. This document covers any non-Music City Center/Metropolitan Government issued device connecting to the Music City Center/Metropolitan Government network via VPN or connecting on-site to any Music City Center/Metropolitan Government network that is not allocated for general public use.

DETAILS

Below is the list of Music City Center/Metropolitan Government minimum security requirements to secure any non-Music City Center/Metropolitan Government issued device that is used to access Music City Center/Metropolitan Government resources not allocated for general public use.

1. Software Updates

Team Members must ensure that updates are applied regularly to the software on their PCs. In addition to the operating system, updates should include, but not be limited to, the following types of software: (1) web browsers; (2) e-mail clients; (3) instant messaging clients; (4) antivirus software; (5) antispyware software; (6) personal firewalls; (7) word processing and spreadsheet software; and (8) other utilities (such as Java, Silverlight, Acrobat, Flash, etc.).

2. Logical Locks

Team Members should configure the device with a password or a PIN to restrict who can use the system. The Team Member must maintain security by keeping the device locked when not in use or after a period of inactivity to prevent access by unauthorized personnel. Locks should also be enabled when the device resumes from hibernation or sleep state.

3. Attack Prevention

Team Members should use a combination of software and software features that will stop attacks; such software includes antivirus and antispyware software, personal firewalls, spam and Web content filtering, and popup blocking. Team Members should practice safe computing habits including not opening and executing files from unknown or untrusted sources. Other people with access to the device must also be made aware of safe computing habits.

4. Application Configuration

Team Members should disable unneeded features and capabilities from applications,



**MCC Procedure
Securing Non-Music City Center/Metro
Government Issued Devices**

| | |
|----------------------------|---------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Public Information |
| Page No. | Page 3 of 3 |

| | | |
|--|--|--|
| | | |
|--|--|--|



MCC Procedure
Setup of Outlook Signature Block Steps for
Outlook 2010 and 2016

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Team Members

PURPOSE

Provide step-by-step instructions for configuring common Outlook clients to use custom signatures that will appear at the bottom of every message sent, forwarded or replied to.

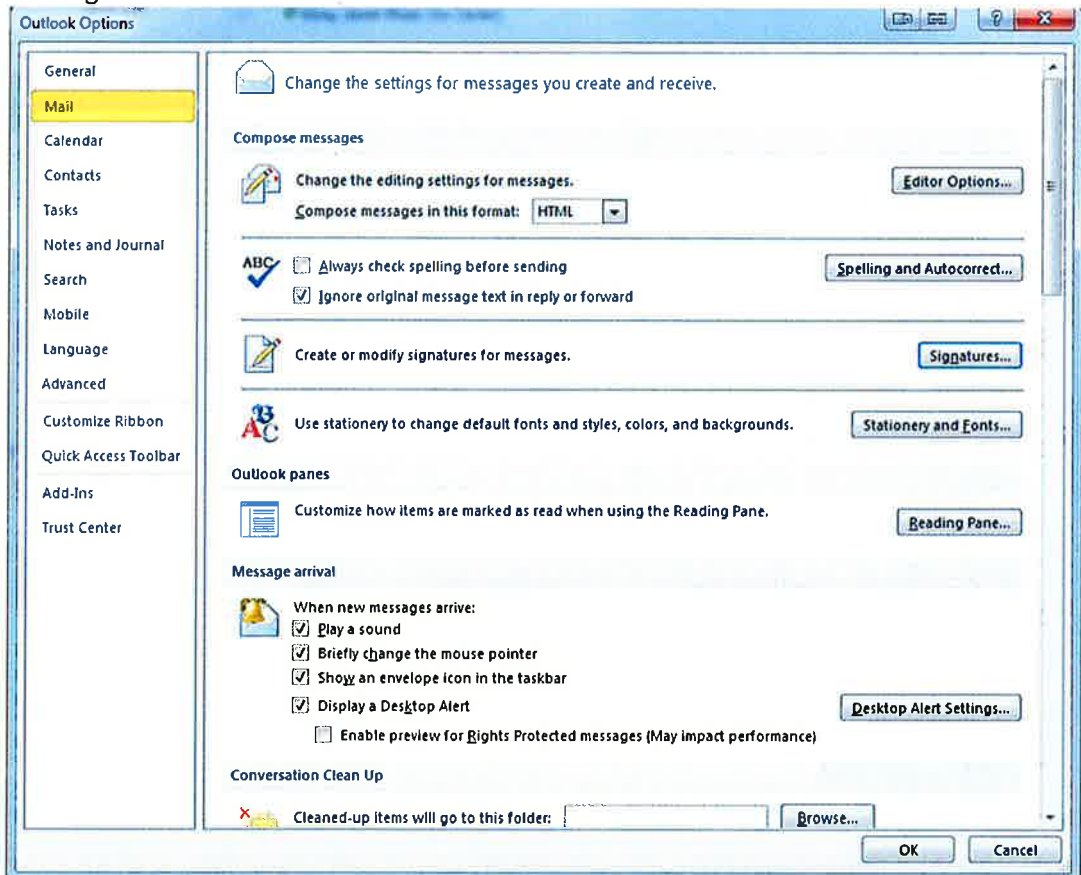
SUMMARY

Note that when done at the Outlook client level, as these instructions describe, each version of Outlook used on each PC used will need to be separately configured, following these instructions. The changes are at the client level and do not transfer automatically to other systems logged into by the Team Member.

DETAILS

Microsoft Outlook 2010/2016:

1. From the main Outlook menu, choose: "File / Options / Mail". From the resulting screen shown below select the "Signatures..." button to the right of the line "Create or modify signatures for messages."



**MCC Procedure
Setup of Outlook Signature Block Steps for
Outlook 2010 and 2016**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 3 |

gave to the new signature block (i.e. "standard1"), then choose "OK" and "OK" in the following screens.

5. Compose and send yourself a message to test and make sure the signature block works/appears properly.

ADDITIONAL INFORMATION *(optional)*

None.

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



MCC Procedure
Setting Up a Screensaver with a Password
Challenge in Windows 7

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Team Members

PURPOSE

Provide step-by-step instructions for setting up a screensaver with a password challenge.

SUMMARY

Screensavers have many selectable options for style and length before activation. These instructions cover only the basics for setup.

DETAILS

Windows 7

1. From the main desktop screen, using your mouse, left-click the Windows Start button on the taskbar. The taskbar can be set to appear in different places on your desktop screen, but most PCs have it on the bottom and the Start button will appear in the left-hand corner, looking something like this:

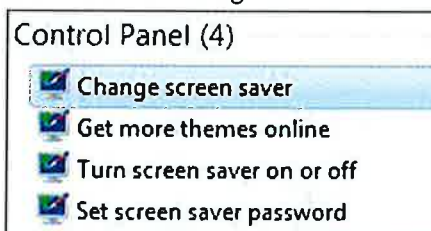


↑
Windows "Start" button

2. Type the word "screensaver" in the resulting "Search programs and files" box as shown below. (you do not need to hit the "Enter" after the word):



3. This will bring up a list of programs and files with the word "screensaver" in them, including the program you want to use in Control Panel. Choose the option labeled "Change screen saver" in the listing under "Control Panel" that will look like the below:



**MCC Procedure
Setting Up a Screensaver with a Password
Challenge in Windows 7**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 3 |

REVISION HISTORY

| REVISION | DATE | CHANGES |
|-----------------|-------------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



**MCC Standard
Smartphone and Blackberry Support**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Team Members with Metro e-mail on their smartphone(s)

PURPOSE

To set a baseline set of security settings for mobile devices to help ensure the security of Metro's information resources.

SUMMARY

This document describes the default security settings applied to ActiveSync connected and BlackBerry Enterprise Server (BES) connected devices.

DETAILS

The Music City Center/Metropolitan Government of Nashville (Metro) continues to work to ensure the confidentiality, integrity and availability of its information resources, including the data Music City Center/Metro employee work with daily. Security policies, standards and processes are continually being developed and defined as the security landscape changes and new threats and risks are discovered. One area that continues to evolve is the use of mobile devices, specifically smartphones and BlackBerrys, within Music City Center/Metro.

The new, ever growing capabilities of these devices offer opportunities to improve productivity and efficiency. However, these same capabilities can also increase the change of Music City Center/Metro data being compromised, leaked or stolen. Due to these risks, Music City Center/Metro has implemented policies that would better secure these devices.

As stated in the *Acceptable Use of Information Technology Assets Policy*: "Any Mobile Device, such as a mobile phone, PDA, BlackBerry, etc., that will be used to store or access Information of the Music City Center/Metropolitan Government shall be connected to a Music City Center/Metropolitan Government approved Mobile Device server."

The default security settings pushed to these devices, for ActiveSync and BlackBerry Enterprise Server (BES) connected devices, are:

- PIN required
- Require encryption on device
- Require encryption on storage cards
- Minimum PIN length: 6 characters
- Time without user input before PIN must be re-entered (in minutes): 5 minutes

Note for BlackBerry Users: Music City Center/Metro employees who would like to use Outlook on their BlackBerry device need to purchase an additional BlackBerry Enterprise (BES) license, which is the plan required by carriers to allow the phone on a BES. Music City Center/Metro ITS does not support the device.



MCC Procedure
Turning Off AutoComplete Functionality in
Windows Server 2008, Windows Server 2012R2,
Windows 7 and Windows 10

| | |
|----------------------------|---------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Public Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Administrators responsible for any non-domain joined devices

PURPOSE



Reduce the chance of data breach by exploiting AutoComplete functionality

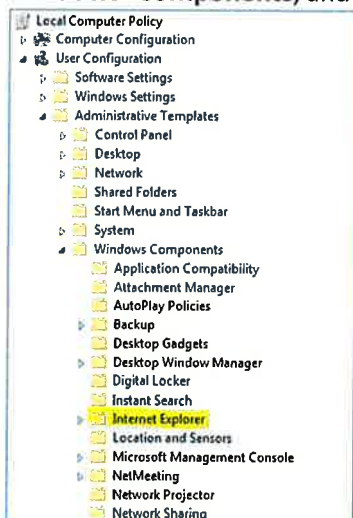
SUMMARY

The AutoComplete feature in Internet Explorer can save Web addresses, form data, and access credentials such as usernames and passwords. This Information will then be automatically entered every time you visit the site again. This presents the potential for another Team Member to access those same sites using the previous Team Member's credentials. It defeats the purpose of having usernames and passwords if they are already automatically entered by your computer. While AutoComplete makes it easier to automatically fill in forms and logon to secure sites, it also makes it easier for Trojans and hackers to gain access to personal data and logon credentials. For these reasons, the use of AutoComplete has been disabled for Nashville \MCC domain joined devices. Below are instructions for disabling this on non-domain joined devices.

DETAILS

Windows Server 2008, 2012R2, Windows 7, Windows 10

1. Click **Start**  , type **Gpedit.msc** in the **Start Search** box, and then press ENTER.
 If you are prompted for an administrator password or for confirmation, type the password, or click **Allow**.
2. Under **Local Computer Policy**, **User Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Internet Explorer**.



3. Click **Enabled** in the **Disable AutoComplete for forms**.

MCC Procedure
Turning Off AutoRun Functionality

| | |
|----------------------------|---------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Public Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Administrators of any non-domain joined devices.

PURPOSE

Reduce the possibility of malware infection by removing a common vector used by malware to propagate.

SUMMARY

Malware increasingly uses AutoRun functionality as a spreading mechanism. In order to address this concern and take steps to ensure the confidentiality, integrity and the availability of the Music City Center/Metropolitan Government network and its resources, this functionality should be disabled on the device. On all MCC\Nashville controlled domains, this is done using group policy. However, any resource not connected to the domain will need to use local security policy to disable this functionality.

DETAILS

The difference between AutoRun and AutoPlay:



AutoRun

AutoRun is a technology used to start some programs or enhanced content (such as video content on a CD) automatically when you insert a CD or another media type into your computer. This is different from AutoPlay, but the result is often the same: when inserted, the CD starts automatically, using a particular program. AutoRun is incorporated into the media types that use it, and you can't modify it.

AutoPlay

AutoPlay is a Windows feature that lets you choose which program to use to start different kinds of media, such as music CDs, or CDs, or DVDs containing photos. For example, the first time you try to play a music CD, AutoPlay asks which media player you want to use, if you have more than one installed on your computer. You can change AutoPlay settings for each media type.

Windows Server 2008, Windows Server 2012R2, Windows 7, Windows 10

1. Click **Start**  , type **Gpedit.msc** in the **Start Search** box, and then press ENTER.
 If you are prompted for an administrator password or for confirmation, type the password, or click **Allow**.
2. Under **Local Computer Policy, Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.



MCC Process
Team Member Owned Device Approval Process

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Team Members

PURPOSE

This process is designed to reduce the risk of security issues arising from the use of devices owned by Music City Center Team Members but not supplied by Music City Center.

SUMMARY

The use of non-Music City Center owned personal devices connecting to the Music City Center/Metro network increases the risk of compromising the confidentiality, availability and integrity of the Music City Center/Metro network and impacting all Music City Center/Metro Departments. Music City Center/Metro is limited to the type of security controls that can be placed on personal devices. As such, the Team Member is required to ensure and maintain the security of their device. This document covers personal devices connecting to the Music City Center/Metro supported network, wired or wireless, except when specifically provided for public use.

DETAILS

An "Approved User Owned Device" is defined as any device owned by a Team Member, where connection to the non-public Music City Center/Metro network by the Team Member using that device has been proved by the President/CEO or his/her designee. The President/CEO or his/her designee shall accept all responsibility for any activity or issues stemming from the use of approved Team Member owned devices. Access to approved Team Member owned devices shall be provided to Music City Center Technology staff when deemed necessary by the President/CEO or his/her designee. All approved Team Member owned devices connecting at work to the network shall meeting Music City Center/Metro ITS minimum security requirements and Team Members shall maintain their approved Team Member owned devices' security on an ongoing basis.

Prior to any Team Member, including but not limited to, employees, independent contractors, consultants, temporary or part-time employees, leased employees, interns, etc. connecting at work to the Music City Center/Metro wired or wireless network, excluding the public network, they must complete and return to Music City Center Technology/Metro ITS Technical Support Center, an "Approved User Owned Device Form". One form per device is required. Requests for approval of Team Member-owned devices can only be initiated by Music City Center personnel. Access will not be granted unless form is signed by the President/CEO or his/her designee.

ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |





Metropolitan Government of Nashville and Davidson County
 700 2nd Avenue South, Suite 301, PO Box 196300, Nashville, TN 37219-6300
 Tech Support Center - P:615-862-6222 F:615-313-9300 E:

Approved User Owned Device Form

Complete and Return to the ITS Tech Support Center. One form per device.

Requests for approval of user-owned devices can only be initiated by Metropolitan Government personnel. Any questions concerning this document should be sent to the ITS TSSC (metroitshelpdesk@nashville.gov).

Date: _____

Metropolitan Government Requestor Name: _____

Metropolitan Government Department/Division: _____

Contact Phone: _____ Email: _____

Device Owner Name (if different): _____

Company/Department (if non-Metropolitan Government): _____

Device Owner Contact Phone: _____ Email: _____

Metropolitan Government Department Director\Agency Head Name:

Windows Login Name for User (Metropolitan Government assigned, if applicable): _____

Employee ID (Metropolitan Government assigned, if applicable): _____

Briefly describe the business need that requires a non-Metropolitan Government supplied device to have access to the Metropolitan Government network (this information is required, use a separate sheet or include diagrams if necessary):

Device Information:

| | |
|---|--|
| *Make and Model | |
| Operating System | |
| *Serial Number | |
| *Media Access Control Address (MAC address) | |
| Name of Anti-virus Software Installed | |
| Primary Internet Provider | |
| Other Security Features (hard drive encryption, firewall, etc.) | |

* Denotes required fields. Please fill out the rest of the information if applicable and as accurately as possible.



Metropolitan Government of Nashville and Davidson County
700 2nd Avenue South, Suite 301, PO Box 196300, Nashville, TN 37219-6300
Tech Support Center - P:615-862-6222 F:615-313-9300 E: metroitshelpdesk@nashville.gov

Shall immediately notify the Department Director\Agency Head or the Director of Information Technology Services when the device is lost or stolen,

Allows Metropolitan Government to delete all data on the device if it is lost, stolen, gifted or if the owner is no longer employed or contracted by Metropolitan Government,

Shall maintain this device's security on an on-going basis, and

Shall abide by all applicable Metropolitan Government policies, standards, requirements, procedures, etc., including but not limited to the *Acceptable Use of Information Technology Assets* and *Teleworking and Mobile Computing* policies.

Failure to adhere may result in disciplinary action, up to and including termination and, where applicable, can result in civil damages and criminal penalties, including fines and imprisonment, as well as Metropolitan Government's attorney's fees and costs.

Device Owner Signature: _____ Date: _____

**MCC Procedure
Using BitLocker**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 05/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 8 |

AUDIENCE

Team Members

PURPOSE

Reduce the possibility of security incidents resulting from data loss

SUMMARY

In order to maintain the confidentiality, integrity and the availability of the Music City Center/Metropolitan Government network and its resources, Team Members should be cautious when handling any media which is taken outside Music City Center/Metropolitan Government's facilities. Removable media, such as thumb drives, CDs, DVDs, external storage, etc. should use Music City Center/Metro ITS approved encryption to protect the data residing on that media. BitLocker is one of the approved solutions provided to meet this need. Below are instructions on the use of this application.

DETAILS

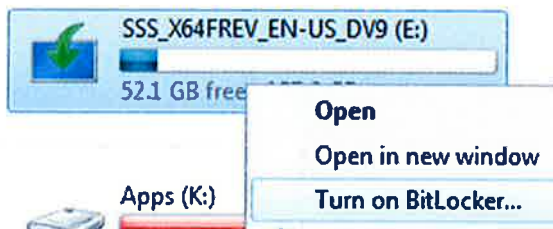
Encrypt a Device

1. Insert a USB device into the computer.
2. Open File Explorer, the inserted USB should appear.

▾ **Devices with Removable Storage (2)**



3. Right click on the inserted USB, select **Turn On Bitlocker**



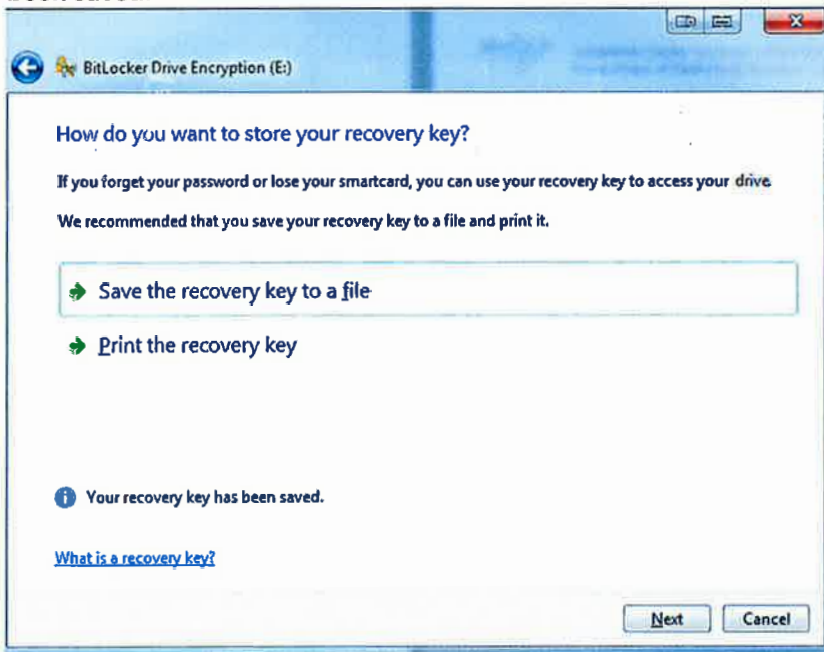
4. Select the box, **Use a password to unlock the drive**

MCC Procedure
Using BitLocker

| | |
|---------------------|----------------------|
| Document ID | ID |
| Effective Date | 05/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 8 |



8. After saving the file, an blue informational message is displayed saying **Your recovery key has been saved.**



9. Hit **Next.**
10. Confirm you want to encrypt the drive, by selecting **Start Encrypting.**

MCC Procedure Using BitLocker

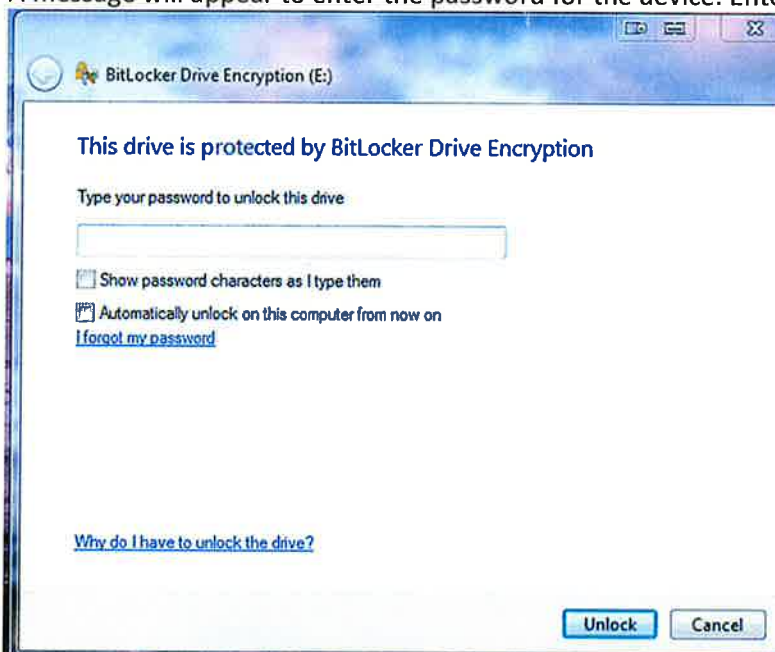
| | |
|---------------------|----------------------|
| Document ID | ID |
| Effective Date | 05/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 5 of 8 |



3. Select any of the option if necessary.
4. Hit **Unlock**. You should be able to access this device now.

Forgot BitLocker Password

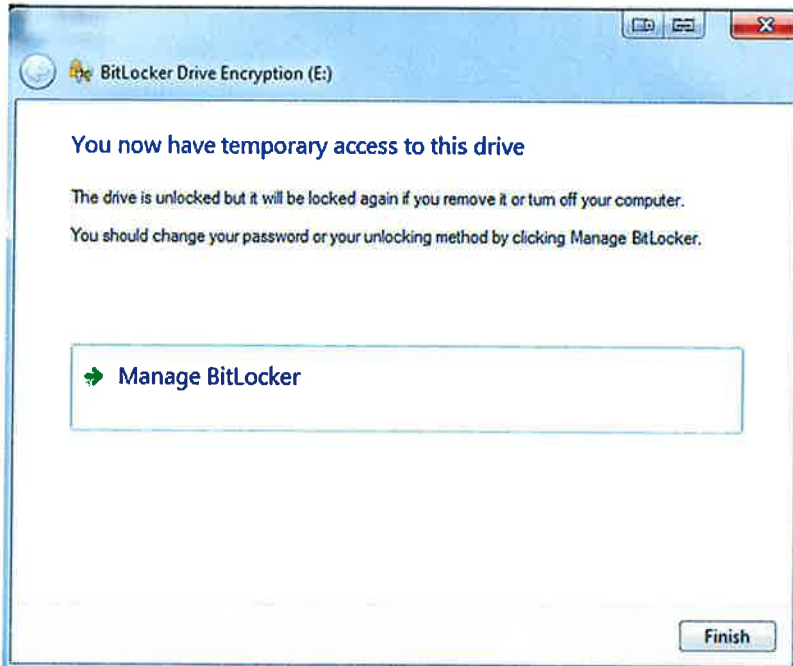
1. Insert the device to a computer
2. A message will appear to enter the password for the device. Enter the password.



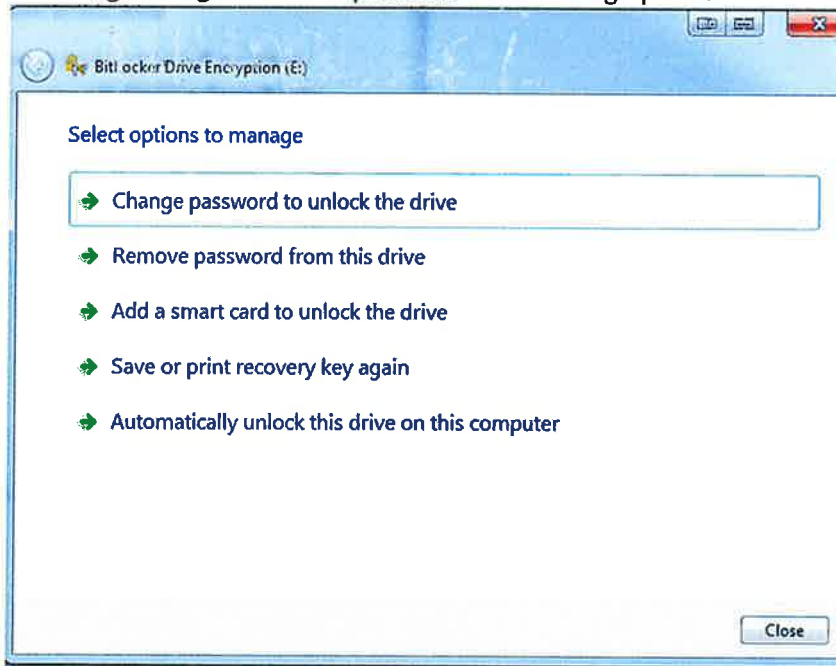
3. Select **I forgot my password**

**MCC Procedure
Using BitLocker**

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 05/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 7 of 8 |



7. Select **Manage BitLocker** for more options or **Finish** for temporary access.
8. Selecting **Manage BitLocker** presents the following options:



ADDITIONAL INFORMATION (optional)
None



MCC Standard
Workstation Security Baseline

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 2 |

AUDIENCE

MCC-Technology and All Metro IT support staff

PURPOSE

To better protect the confidentiality, integrity and availability of the services and Information used by Music City Center/Metro by better managing (inventory, track, and correct) workstations on the network so that only secured, authorized workstations are given access and unauthorized and unmanaged workstations are found and prevented from gaining access.

SUMMARY

The scope of this standard extends to all Metro owned workstations (desktops, laptops, tablets, etc.) on the Music City Center/Metro supported networks.

Asset management and security of workstations are key to helping ensure the security of the Music City Center/Metro network. The standards below are being adopted to better secure workstations, better track workstations and better identify rogue workstations in the Music City Center/Metro network.

DETAILS

All Metro owned and managed workstations (devices running non-server operating systems) must meet the following criteria:

- Use an approved, fully licensed and supported operating systems.
- Be joined to a Metro managed Active Directory domain.
- Utilized approved device encryption.
- Be hardened using an industry recognized security baseline.
- Use a functioning, up-to-date anti-malware application.
- Be configured to use a patch management solution.
- Be configured so that any application that is not centrally patched should be set up auto-update.
- Deploy an application level protection solution.
- Use an asset tracking and management (software and hardware) solution.
- Utilize a host base firewall.
- Be inventoried in an asset tracking solution.

The current solutions used to meet these criteria can be found in Appendix A.

ADDITIONAL INFORMATION *(optional)*

Center for Internet Security Critical Security Controls for Effective Cyber Defense Version 6.0 – CSC 1

APPENDIX A

The solutions listed below are currently being used by Music City Center/Metro ITS to meet the requirements in this standard:



MCC Process
Time Synchronization Policy

| | |
|----------------------------|----------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 1 |

AUDIENCE

System Administrators and Information System Users.

PURPOSE

The purpose of this policy is to define the requirement that all systems in the Music City Center technology ecosystem deploy a time synchronization service to ensure consistent usage of time for logging.

SUMMARY

See Purpose.

DETAILS

1. All systems covered by the scope of this policy must deploy clock synchronization technology to ensure consistent and usable timestamps for activity logging where possible.
2. At present, this means that all systems should use Network Time Protocol (NTP) to synchronize each server's clock with the NTP server at the host level of the MCC Cluster or the primary MCC router.
3. All Active Directory connected systems may synchronize time from their domain controllers if those domain controllers are synchronized to the primary MCC router.

POLICY COMPLIANCE

1. Compliance Measurement
 - a) The Technology team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.
2. Exceptions
 - a) Any exception to the policy must be approved by the Technology team in advance.
3. Non-Compliance
 - a) An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

ADDITIONAL INFORMATION *(optional)*

None

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



MCC Process
Firewall, Router and Switch Management Policy

| | |
|----------------------------|----------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 1 of 3 |

AUDIENCE

Music City Center Department Directors, Information Owners, System Administrators, and Information System Users.

PURPOSE

This document describes a required minimal security configuration for all firewalls, routers, and switches connecting to a production network or used in a production capacity at or on behalf of the Music City Center.

SUMMARY

See Purpose.

DETAILS

Every firewall, router, and switches must meet the following configuration standards:

1. No local user accounts with username "admin" or "administrator" shall be enabled on the firewall, switch, or router. Local accounts must be encrypted. Firewalls, routers, and switches prefer to use TACACS+ for all user authentication when available.
2. The enable password on the firewall, switch, or router must be kept in a secure encrypted form. The firewall, switch, or router must have the enable password set to the current production firewall/router/switch password from the device's support organization.
3. The following services or features must be disabled when applicable:
 - a. IP directed broadcasts
 - b. Incoming packets at the firewall/router/switch sourced with invalid addresses such as RFC1918 addresses
 - c. TCP small services
 - d. UDP small services
 - e. All source routing and switching
 - f. All web services running on router
 - g. Cisco discovery protocol on Internet connected interfaces
 - h. Telnet, FTP, and HTTP services
 - i. Auto-configuration
4. The following services should be disabled unless a business justification is provided:
 - a. Cisco discovery protocol and other discovery protocols
 - b. Dynamic trunking
 - c. Scripting environments, such as the TCL shell
5. The following services must be configured:
 - a. Password-encryption
 - b. NTP configured to a corporate standard source
6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol



MCC Process
Firewall, Router and Switch Management Policy

| | |
|----------------------------|-----------------------------|
| Document ID | ID |
| Effective Date | 5/15/2018 |
| Owner | ISM Committee |
| Info Classification | Internal Information |
| Page No. | Page 3 of 3 |

REVISION HISTORY

| REVISION | DATE | CHANGES |
|-----------------|-------------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 2

SUBJECT:

HUMAN RESOURCES SECURITY POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this Policy is to ensure that the Convention Center Authority of the Metropolitan Government of Nashville and Davidson County (Music City Center) and its Team Members:

- Understand their responsibilities and are suitable for their Roles, in order to reduce the risk of theft, fraud or misuse of Information and Information Technology Assets;
- Aware of Information Security threats and concerns and liabilities and are equipped to support Information Security in the course of their normal work in order to reduce the Risk of human error; and
- Understand their responsibilities so Team Members may exit the Music City Center/Metropolitan Government or change employment in an orderly manner.

POLICY

1. Generally

Music City Center shall:

- 1.1. Define and document security Roles and responsibilities of Team Members;
- 1.2. Require Team Members to apply security in accordance with Music City Center/Metropolitan Government policies and procedures;
- 1.3. Define and assign responsibilities for performing employment termination or change of assignment or duties to include removing access rights to Information and Information Technology Assets;
- 1.4. Ensure individuals requiring access to Music City Center/Metropolitan Government information and information systems sign appropriate confidentiality and/or non-disclosure agreements prior to being granted access; and
- 1.5. Review and update confidentiality and/or non-disclosure agreements annually.



Information and Information Technology Assets.

Screening and rescreening shall be consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The screening criteria shall include explicit information security role appointment requirements (e.g., training, security clearance). Music City Center shall define different rescreening conditions and frequencies for personnel accessing Information and Information Technology Assets based on the type of information processed, stored or transmitted.

2.3. Security Awareness and Training

Music City Center shall provide basic security awareness training to all information system users (including Department, agency and board directors, heads and chairs, and contractors) as part of initial training for new users, and as required by system changes. As all Team Members have responsibility for some degree of physical security, information security, and information technology security, all employees and third party contractors are required to complete this basic security awareness training upon initial employment and maintain that training periodically.

As part of its security awareness program, Music City Center shall:

- Include practical exercises in security awareness training that simulate actual cyber-attacks; and
- Address awareness of the need for operations security as it relates to Music City Center's information security program

Music City Center shall provide Role-based security-related training:

- Before authorizing access to the Information of the Music City Center and/or Information Technology Assets;
- Before performing assigned duties;
- Whenever there are significant changes to the Information System or environment of operation (including identification of new threats and vulnerabilities;
- When any other conditions occur that may impact the security state; and
- As required by applicable regulations.

Music City Center shall determine the appropriate content of security training based on assigned Roles and responsibilities based on the Information of the Music City Center and Information Technology Assets to which personnel have authorized access.

Adequate security-related technical training shall be provided to Information System managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software to perform their assigned duties.

Music City Center security training shall address management, operational and technical responsibilities covering physical, personnel and technical safeguards and countermeasures.

4. External Information System Services

Music City Center/Metropolitan Government shall, among other things, require that providers of external information system services comply with Music City Center/Metropolitan Government information security requirements and employ appropriate security controls, including required confidentiality and/or non-disclosure agreements for service providers, their employees and contractors, in accordance with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards and guidance.

5. Metrics

Suggested metrics to monitor compliance and policy effectiveness include:

- *Percentage of Team Members who are required and have signed the Acceptable Use of Information Technology Assets Policy;*
- *Percentage of Team Members who are required and have successfully completed the Basic Security Awareness Training;*
- *Percentage of Team Members whose access has been assessed based on defined roles and responsibilities;*
- *Number of user accounts that exist for Team Members that have separated from employment;*
- *Number of security incidents resulting in corrective or disciplinary action.*

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO
Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 6.1.6, 12.6, 10.10.5, 12.5.2, 13.1.1, 13.1.2
- NIST Special Publication 800-40, Creating a Patch and Vulnerability Management Program
- NIST Special Publication 800-51, Guide to Using Vulnerability Naming Schemes

**CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

INFORMATION SECURITY

POLICY NUMBER:
ISM 2

SUBJECT:

HUMAN RESOURCES SECURITY PLAN

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Music City Center Department Directors, supervisors, managers, departmental human resources, and IT personnel

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Human Resources Security Policy.

1. Generally

Music City Center shall:

- 1.1. Define and document security Roles and responsibilities of Team Members;*
- 1.2. Require Team Members to apply security in accordance with Music City Center/Metropolitan Government policies and procedures;*
- 1.3. Define and assign responsibilities for performing employment termination or change of assignment or duties to include removing access rights to Information and Information Technology Assets;*
- 1.4. Ensure individuals requiring access to Music City Center/Metropolitan Government information and information systems sign appropriate confidentiality and/or non-disclosure agreements prior to being granted access; and*
- 1.5. Review and update confidentiality and/or non-disclosure agreements annually.*

2.3. Security Awareness and Training

The Music City Center Human Resources Department, with the assistance of the Music City Center Technology Department and Metro Information Technology Services, with regards to information security awareness and training will:

The Department of Human Resources, with the assistance of Information Technology Services (ITS) and General Services, with regard to information security awareness and training will:

- *Identify information training requirements;*
- *Develop curriculum;*
- *Implement training through Metro –Wide training systems; and*
- *Improve curriculum and requirements to adjust to changing threat models, vulnerabilities, risks, and identified gaps and deficiencies.*

Music City Center has training initiatives based on business operation or applicable regulation. For example, HIPAA training requirements for covered entities. These additional training resources may be developed by individual departments and/or Human Resources depending on scope.

Music City Center will centrally track individual and departmental training.

2.4. Security Training Records

Reference HR

2.5. Incident Response Training

Reference HR

3. Termination or Change of Employment

As roles change or terminations occur, the following items must be considered:

- *Determination of changed assets and access;*
- *Termination or change of access;*
- *Retrieval of all Music City Center/Metropolitan Government provided property; and*
- *Assurance that Music City Center/Metropolitan Government can still access assets formerly accessible by the employee (e.g., files on servers).*

These policy items should be included as part of the overall Music City Center process for personnel transfer and/or termination. All appropriate departments and/or groups need to be a part of these processes. Examples may include Music City Center management of physical locations and Information Technology Services management of network access.

3.1. Personnel Termination

3.2. Personnel Transfer

3.3. Access Rights

4. External Information System Services

| | | |
|-----|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 3

SUBJECT:

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

DISTRIBUTION DATE:
05/15/2018

EFFECTIVE DATE:
05/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this Policy is to help ensure that the Convention Center Authority of the Metropolitan Government of Nashville and Davidson County (Music City Center) prevents loss, theft, unauthorized physical access, damage, and interference to its premises, Information, and Information Systems and interruption to its activities.

Although this policy is primarily focused on Information Systems, it applies to all Information in any medium or form, as are defined in the *Music City Center Information Security Glossary*.

Critical or Sensitive Information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. This applies to where the Information Systems are housed, as well as any supporting infrastructure required, including but not limited to, emergency power, cabling, uninterruptable power supply systems, generators, temperature and humidity controls, and fire protection. The protection should be commensurate with the identified risks.

POLICY

1. Generally

Music City Center shall:

- 1.1. Locate or protect equipment to reduce the risks from physical and environmental threats and hazards, as well as opportunities for unauthorized access;
- 1.2. Use security perimeters (such as walls, card controlled entry gates or manned reception desks) to protect areas that contain Information and Information processing facilities;
- 1.3. Protect secure areas by appropriate entry controls to ensure that only authorized personnel are allowed access;
- 1.4. Design and apply physical security for offices, rooms and facilities;
- 1.5. Design and apply physical protection against damage from fire, flood, earthquake, explosion, civil unrest, power failures, and other forms of natural or man-made disaster;



- mechanisms and/or security officers;
- 2.3. Control access to areas officially designated as publicly accessible in accordance with Music City Center's assessment of risk;
 - 2.4. Any Information System (such as kiosks, computers, etc.) that have been deemed necessary in a publicly accessible area, shall be adequately secured, such as by least privileged access, network segmentation, cameras, physically securing all access cables/jacks, and other hardware/software security measures.
 - 2.5. For equipment siting and protection purposes, Music City Center shall position equipment within its facility to minimize potential damage from physical and environmental threats and hazards and to minimize the opportunity for unauthorized access.
 - 2.6. Verify individual access authorizations and credentials before granting access to the facility;
 - 2.7. Secure all keys, combinations and other physical access credentials;
 - 2.8. Routinely inventory and perform physical inspections of all access control mechanisms to ensure proper operations of all electronic, mechanical, and procedural components, and verify the effectiveness of the security controls;
 - 2.9. Change combinations and key cores when keys are lost, combinations are compromised or individuals are transferred or terminated as budget permits or as risks dictate.
 - 2.10. Maintain, support, and utilize an enterprise access control security system, centrally administered by Music City Center's Security Department.
 - 2.11. Restricted areas and facilities which contain Information Systems must be clearly marked. Signage should contain enough Information to be practical, but present minimal discernible evidence as to the nature of the importance of the location.

3. Physical Access Authorizations

Music City Center shall:

- 3.1. Issue appropriate access rights and related physical access credentials;
- 3.2. Develop and keep current a record of personnel with authorized access to the facility or area where Information or an Information System resides (except for those areas within the facility officially designated as publicly accessible), to include:
 - 3.2.1. Review and approve Team Member access, system administrators, and authorization lists at least annually, removing personnel no longer requiring access;
 - 3.2.2. Perform physical audits at least annually to verify that personnel are in possession of all issued credentials (e.g. identification cards, badges, access cards, keys, combinations, codes);
 - 3.2.3. Perform timely termination of physical access rights and recovery of physical security credentials for voluntary termination of employment, job transfers, and reassignment of duties; and
 - 3.2.4. Perform immediate change of physical access rights associated with an involuntary termination of employment and recover physical security credentials.
- 3.3. Ensure that no maintenance or support activities are performed in such a way to compromise security of any Information, Information System, or network;
- 3.4. Access to facilities which contain Information, Information Systems or infrastructure

Music City Center shall:

- 6.1. Maintain visitor access records to the facility where the Information System which contains or can provide access to Restricted Information resides (except for areas within the facility officially designated as publicly accessible); and
- 6.2. Review visitor access records as needed.

7. Security Awareness Training

Physical Security education shall be included as part of all Music City Center/Metropolitan Government Security awareness training in accordance with applicable Metro Government and Music City Center policies and procedures.

8. Physical Access Agreements

Music City Center shall:

- 8.1. Ensure that individuals requiring physical access to its Information and Information Systems sign appropriate access agreements prior to being granted access, which shall include the rules that describe their responsibilities and expected behavior with regard to the physical security; and
- 8.2. Review and update, if necessary, the access agreement form at least annually.

9. Controlled Maintenance and Diagnostics Activity

For Information Systems and supporting infrastructure equipment maintenance purposes, Music City Center/Metropolitan Government shall:

- 9.1. Schedule and perform maintenance and repairs on equipment in accordance with manufacturer or vendor specifications and/or requirements;
- 9.2. Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- 9.3. Provide timely maintenance support and/or spare parts for all critical equipment.
- 9.4. Require that a designated official approve the removal of the equipment from facilities for off-site maintenance or repairs;
- 9.5. Sanitize equipment to remove all confidential and restricted Information, as defined by the *Music City Center's Information Classification Policy*, from associated media prior to removal from its secure area for off-site maintenance or repairs; and
- 9.6. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

10. Maintenance Tools

For equipment maintenance purposes, Music City Center shall approve, control, monitor the use of, and maintain on an ongoing basis, Information System maintenance tools. The intent of this control is to address the security-related issues arising from the hardware and software brought

15. Alternate Work Site

If the Music City Center has established programs for allowing employees to work at home or at geographically convenient satellite offices, then in order to protect equipment and Information at alternate work sites, Music City Center shall:

- 15.1. Employ appropriate management, operational, and security controls at alternate work sites;
- 15.2. Assess, as feasible, the effectiveness of security controls at alternate work sites; and
- 15.3. Provide a means for employees to communicate with Information security personnel in case of security incidents or problems.

16. Delivery, Removal, and Media Sanitization

Music City Center shall authorize, monitor and control Information System-related components entering and exiting a facility and maintain records of those items, except, as approved by the Facility Access Manager, mobile devices which remain in the possession of their owners at all times. Effectively enforcing authorizations for entry and exit of Information System components shall require restricting access to delivery areas and possibly isolating the areas from the Information System and media libraries.

For secure disposal or re-use of equipment purposes, Music City Center shall sanitize media, both digital and non-digital, prior to disposal, release out of its control, or release for reuse. This requirement shall apply to all equipment and media subject to disposal or reuse, whether or not considered removable. In addition, Music City Center shall employ sanitization mechanisms with the strength and integrity commensurate with the classification or sensitivity of the Information residing on the equipment or media. It also shall use its discretion on the employment of sanitization techniques and procedures for equipment and media containing Information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on Music City Center or individuals if released for reuse or disposal.

17. Power Equipment and Power Cabling

Music City Center shall protect power equipment and power cabling for the Information System from damage and destruction. Physical access controls to power equipment and power distribution locations should include; cardkey readers or physical locks, physical walls, and secure doors/gates.

18. Emergency Shutoff

Music City Center shall:

- 18.1. Provide the capability of shutting off power to the Information System or individual system components in emergency situations;
- 18.2. Place emergency shutoff switches or devices in a secure location near the Information System that facilitates safe and easy access for authorized personnel;
- 18.3. Inspect and test functionality of the emergency shutoff switches and devices; and

Information Security Policies.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary.*

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO
Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: section 9
- NIST Special Publication 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*; MA-1 through MA-6, MP-5, MP-6, PE-1 - PE19

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|------------|------------------------|
| 1.0 | 05/15/2018 | First released version |
| | | |

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 3

SUBJECT:

PHYSICAL AND ENVIRONMENTAL SECURITY PLAN

DISTRIBUTION DATE:
05/15/2018

EFFECTIVE DATE:
05/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Music City Center Department Directors, Information Owners, Facility Access Authorities, Facility Security Managers, and Facility Managers

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Physical and Environmental Security Policy.

1. Generally

Music City Center shall:

- 1.1. *Locate or protect equipment to reduce the risks from physical and environmental threats and hazards, as well as opportunities for unauthorized access;*
- 1.2. *Use security perimeters (such as walls, card controlled entry gates or manned reception desks) to protect areas that contain Information and Information processing facilities;*
- 1.3. *Protect secure areas by appropriate entry controls to ensure that only authorized personnel are allowed access;*
- 1.4. *Design and apply physical security for offices, rooms and facilities;*
- 1.5. *Design and apply physical protection against damage from fire, flood, earthquake, explosion, civil unrest, power failures, and other forms of natural or man-made disaster;*
- 1.6. *Design and apply physical protection and guidelines for working in secure areas;*



- entry/exit points) to any facility where an Information System resides (excluding those areas within the facility officially designated as publicly accessible);
- 2.2. Control entry to the facility containing the Information System using physical access control mechanisms and/or security officers;
 - 2.3. Control access to areas officially designated as publicly accessible in accordance with Music City Center's assessment of risk;
 - 2.4. Any Information System (such as kiosks, computers, etc.) that have been deemed necessary in a publicly accessible area, shall be adequately secured, such as by least privileged access, network segmentation, cameras, physically securing all access cables/jacks, and other hardware/software security measures.
 - 2.5. For equipment siting and protection purposes, Music City Center shall position equipment within its facility to minimize potential damage from physical and environmental threats and hazards and to minimize the opportunity for unauthorized access.
 - 2.6. Verify individual access authorizations and credentials before granting access to the facility;
 - 2.7. Secure all keys, combinations and other physical access credentials;
 - 2.8. Routinely inventory and perform physical inspections of all access control mechanisms to ensure proper operations of all electronic, mechanical, and procedural components, and verify the effectiveness of the security controls;

PRESIDENT/CEO or his/her designee: To ensure the effectiveness of the physical access controls, inventories and inspections should be documented and the frequency determined by the associated risks, the type of physical access control mechanism used, and area being secured. The frequency of performing these functions is recommended to be no longer than yearly for physical and procedural mechanisms, and where possible, proactively monitored electronically.

- 2.9. Change combinations and key cores when keys are lost, combinations are compromised or individuals are transferred or terminated as budget permits or as risks dictate.

PRESIDENT/CEO or his/her designee: Notification of employment transfers or terminations should be communicated to the appropriate personnel responsible for terminating access such as facility security managers, facility managers, and facility access authorities within at least a 24 hour time period prior to effective date.

FACILITY MANAGEMENT: Upon notification, facility management personnel should change combinations and/or replace key cores immediately, or within an acceptable timeframe as budgets permits or as risks dictate.

- 2.10. Maintain, support, and utilize an enterprise access control security system, centrally administered by Music City Center's Security Department.
- 2.11. Restricted areas and facilities which contain Information Systems must be clearly marked. Signage should contain enough information to be practical, but present minimal discernible evidence as to the nature of the importance of the location.

USERS: Maintain doors are closed and locked. Prevent persons from accessing restricted areas.

contractors, vendors, and service staff, should be granted access only to facilities, rooms, and systems that are necessary for the fulfillment of their job responsibilities.

1.3. For facilities or areas involved with Information classified as Restricted in the Music City Center's *Information Classification Policy*;

3.5.1. Any individual must be escorted at all times or pre-approved by the President/CEO or his/her designee.

3.5.2. Any individual who is not authorized shall not be granted access nor escorted into a secured area which contains or provides access to Restricted Information unless approved by the President/CEO or his/her designee.

USERS: Shall abide to areas granted and should not proceed into unrestricted areas unless otherwise granted prior permission from management.

DEPARTMENT AUTHORITY: Shall review access periodically.

4. Monitoring Physical Access

Music City Center shall:

4.1. *Monitor physical access to the Information System to detect and respond to physical security incidents;*

4.2. *Ensure that all employees, contractors, and vendors display, in plain view, a current picture ID at all times while in non-public areas of the facility;*

4.3. *Maintain and frequently review physical access logs; and*

PRESIDENT/CEO or his/her designee: Log files should be maintained to include the appropriate event types and errors to effectively identify and analyze security events or error conditions. Documentation should include procedures for the appropriate response to suspicious activity or an anomaly identified in physical access logs. The frequency of log review and analysis should be documented and should occur at least every 1 to 7 days depending on the level of security impact of the system or facility.

Retention of log files should be set based on the level of security impact of the system or facility, to meet legal or regulatory requirements, and in support of incident handling or investigation processes.

4.4. *Investigate and respond to detected physical security incidents, including apparent security violations or suspicious physical access activities. Security Incidents shall be handled in accordance with applicable Music City Center's policies and procedures.*

USERS: Ensure proper identification is displayed at all times.

DEPARTMENT AUTHORITY: Periodically review logs and respond to incidents.

5. Visitor Control

5.1. *Music City Center shall control physical access by authenticating visitors before authorizing*

retraining will be administered periodically through Human Resources and Security Departments. Team Members should be aware of their environment.

TEAM AUTHORITY: Schedule Team Members appropriate to conduct security awareness training. Remind Team Members of risks and related training methods.

8. Physical Access Agreements

Music City Center shall:

- 8.1. *Ensure that individuals requiring physical access to its Information and Information Systems sign appropriate access agreements prior to being granted access, which shall include the rules that describe their responsibilities and expected behavior with regard to the physical security; and*
- 8.2. *Review and update, if necessary, the access agreement form at least annually.*

USERS: Verify authorization of individuals.

DEPARTMENT AUTHORITY: Verify and grant authorization to individuals.

9. Controlled Maintenance and Diagnostics Activity

For Information Systems and supporting infrastructure equipment maintenance purposes, Music City Center/Metropolitan Government shall:

- 9.1. *Schedule and perform maintenance and repairs on equipment in accordance with manufacturer or vendor specifications and/or requirements;*
- 9.2. *Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;*
- 9.3. *Provide timely maintenance support and/or spare parts for all critical equipment.*
- 9.4. *Require that a designated official approve the removal of the equipment from facilities for off-site maintenance or repairs;*
- 9.5. *Sanitize equipment to remove all confidential and restricted Information, as defined by the Music City Center's Information Classification Policy, from associated media prior to removal from its secure area for off-site maintenance or repairs; and*
- 9.6. *Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.*

USERS: Team Members shall update Information Systems accordingly. Team Members shall review any CVE prior to installation.

DEPARTMENT AUTHORITY: Shall approve maintenance and coordinate with other Departments.

10. Maintenance Tools

For equipment maintenance purposes, Music City Center shall approve, control, monitor the use

jacks; and protection of cabling by conduit or cable trays.

13.2. Wiring closets shall be secured areas.

13.3. For all wiring closets and any other location where network distribution cables or equipment resides, physical access shall be authorized and controlled by President/CEO or his or her designee.

USERS: Team Members should report broken jacks or face plates to the Technology Department. Team Members shall request the Technology Department for access to an area that contains distribution and transmission lines. Technology Department staff shall verify and escort Users to and from the facility. Technology Department staff shall disconnect the patch panel and corresponding switch connection inside the appropriate telecom room. The Technology Department staff shall also set the corresponding switch port to an unused VLAN.

DEPARTMENT AUTHORITY: Verify and approve access to Users who need access to the area.

14. Equipment, Information and Software Transport

For security of equipment off-premises and removal of property purposes, Music City Center shall:

14.1. Protect and control equipment, Information and software during transport outside of controlled areas;

14.2. Maintain accountability for equipment, Information and software during transport outside of secured areas; and

14.3. Restrict the activities associated with transport of such equipment, Information and software to authorized personnel.

USERS: Team Members should be aware of the Information Classification in their possession and the potential risks.

DEPARTMENT AUTHORITY: Ensure selected personnel are aware of the Information Classification policy and the risks associated with the Information.

15. Alternate Work Site

If the Music City Center has established programs for allowing employees to work at home or at geographically convenient satellite offices, then in order to protect equipment and Information at alternate work sites, Music City Center shall:

15.1. Employ appropriate management, operational, and security controls at alternate work sites;

15.2. Assess, as feasible, the effectiveness of security controls at alternate work sites; and

15.3. Provide a means for employees to communicate with Information security personnel in case of security incidents or problems.

USERS: Team Members should keep alternate work site secure and use an approved VPN tunnel to access Music City Center/Metropolitan Government resources.

- 18.2. *Place emergency shutoff switches or devices in a secure location near the Information System that facilitates safe and easy access for authorized personnel;*
- 18.3. *Inspect and test functionality of the emergency shutoff switches and devices; and*
- 18.4. *Protect emergency power shutoff capability from unauthorized activation.*

USERS: Notify Technology Department of the emergency outage of the Information System.

DEPARTMENT AUTHORITY: Ensure selected personnel are aware of their duties and provide adequate training for the system.

19. Emergency Power

Music City Center shall provide an adequate uninterruptible power supply to facilitate an orderly shutdown of critical Information Systems in the event of a primary power source loss and employ and maintain automatic emergency lighting for the equipment that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

USERS: Notify Engineering Department of power outage or disturbances.

DEPARTMENT AUTHORITY: Ensure selected personnel are aware of their duties and provide adequate training for the system.

20. Temperature and Humidity Controls

Where applicable, Music City Center shall:

- 20.1. *Maintain temperature and humidity levels within the facility where the equipment resides at acceptable levels; and*
- 20.2. *Monitor temperature and humidity levels at an appropriate frequency.*

USERS: Notify Engineering Department of HVAC temperature and humidity within the building.

DEPARTMENT AUTHORITY: Ensure selected personnel are aware of their duties and provide adequate training for the system.

21. Fire Protection

Music City Center shall employ and maintain fire suppression and detection devices/systems for critical Information Systems that are supported by an independent energy source.

USERS: Notify Security Department of fire damage.

DEPARTMENT AUTHORITY: Ensure selected personnel are aware of their duties and provide adequate training for the system.

22. Water Damage Protection

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO
Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: section 9.1
- NIST Special Publication 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*; PE-1 - PE19

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|------------|------------------------|
| 1.0 | 05/15/2018 | First released version |
| | | |

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 4

SUBJECT:

EXTERNAL PARTY SECURITY POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to define the rules for maintaining the security of the Music City Center’s information, Information Technology Assets and information processing facilities that are accessed, processed, communicated to, or managed by external parties or where external parties add products or services to information processing facilities.

POLICY

Generally, Music City Center shall:

- Identify the security risks to Music City Center’s Information, Information Technology Assets and information processing facilities from business processes involving external parties and implement appropriate controls before granting access;
- Address all identified security risks before giving vendors access to Music City Center’s information or assets; and
- Have agreements in place with external parties addressing relevant security requirements, as applicable, for access, process, communication with, or management of Music City Center’s Information, assets, or information processing facilities.

1. Identification of Risks Related to External Parties

1.1 Music City Center shall identify and manage the security risks, including regulatory compliance considerations, related to information, Information Technology Assets and information processing facilities for any external party who:

- Has access to an information processing facility;
- Has approved unescorted physical access to Music City Center assets such as offices, computers, file cabinets;
- Has logical access to Music City Center’s databases or information systems;
- Has approved connectivity between a vendor network and Music City Center’s network; and/or



SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO
Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 4, 6.2
- NIST Special Publication 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations: AC-8, AT-2, CA-3, PL-4, PM-9, PS-7, RA-3, SA-1, SA-9, SC-7

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2015 | First released version |
| | | |

| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 4</p> |
| <p>SUBJECT:</p> <p>EXTERNAL PARTY SECURITY PLAN</p> | <p>DISTRIBUTION DATE: 5/15/2018</p> <p>EFFECTIVE DATE: 5/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

AUDIENCE

Music City Center Team Members

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the External Party Security Policy.

Generally, Music City Center shall:

- *Identify the security risks to Music City Center’s Information, Information Technology Assets and information processing facilities from business processes involving external parties and implement appropriate controls before granting access;*
- *Address all identified security risks before giving vendors access to Music City Center’s Information or assets; and*
- *Have agreements in place with external parties addressing relevant security requirements, as applicable, for access, process, communication with, or management of Music City Center’s Information, assets, or information processing facilities.*

1. Identification of Risks Related to External Parties

1.1 Music City Center shall identify and manage the security risks, including regulatory compliance considerations, related to Information, Information technology assets and information processing facilities for any external party who:



and other applicable security requirements.

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Music City Center Department Directors, with the assistance of Music City Center's Director of Technology, will address identified security risks in accordance with the Music City Center Risk Assessment and Treatment Policy and Plan and using the results obtained in the Vendor Risk Assessment Questionnaire.

As needed, Information Security Exception Forms will be completed in accordance with the official process per the Music City Center Scope, Background, and Governance Statement for Information Security Policies.

3. Vendor Agreements

Music City Center shall implement agreements with external parties who provide products or services involving access to, processing of, communication with, or managing Music City Center's Information, Information Technology Assets and information processing facilities.

External party providers shall include, for example, vendors/contractors and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The President/CEO shall assign a designated individual to manage vendor relationships and this person will ensure that information security requirements are included where applicable.

Music City Center, in vendor agreements, shall:

- *Require vendors to report perceived security incidents that may impact the confidentiality, integrity or availability of Music City Center data immediately or no more than 24 hours after incident discovery;*
- *Explicitly include vendor personnel security requirements in acquisition-related documents;*
- *Require compliance with applicable Music City Center's information security policies and processes and require appropriate parties to sign agreements stating they will comply with applicable Music City Center information security policies, associated processes, and supporting standards;*
- *Require primary vendors to require their sub-contractors to abide by Music City Center policies and security requirements, as applicable;*
- *Require vendors to employ confidentiality agreements, as applicable;*
- *Address appropriate security controls in accordance with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance;*
- *Define and document information security oversight and user roles and responsibilities with regard to vendors information system services; and*
- *Ensure monitoring and review of vendors that includes adherence to Music City Center information security policies, monitoring service level agreements, and review all security incidents reported by vendors.*

USERS: Seek Department Authority.



CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

POLICY NUMBER:
ISM 5

INFORMATION SECURITY

SUBJECT:

INFORMATION SECURITY INCIDENT
MANAGEMENT CRYPTOGRAPHIC
CONTROLS POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to ensure that security events, weaknesses, and incidents associated with Information Systems are managed in a consistent, effective, and timely manner, to include evaluation and improvement of information security procedures, processes, and controls based on lessons learned.

POLICY

Music City Center shall promptly address Information Security Incidents with consistent and effective management. Such response shall include the Business Owner and the Information Owner and be coordinated by the Chief Information Officer/Director of Technology. Other personnel may be required based on the type and severity of the incident.

1. Reporting Information Security Events, Vulnerabilities, and Incidents

Music City Center Team Members shall expeditiously report to the Technology Department any observed or suspected Information Security Events, Information Security Vulnerabilities, and Information Security Incidents, including any loss and/or theft of Information Technology Assets.

Music City Center shall report any observed or suspected Information Security Events and Incidents to law enforcement or other regulating agencies if laws are suspected to have been broken.

Information Security Events, Vulnerabilities and Incidents, including incident response plans shall be classified as Confidential. Music City Center/Metropolitan Government shall protect incident response plans from unauthorized disclosure and modification.

2. Management of Information Security Incidents



4.2.5. Implement the resulting changes accordingly.

5. Incident Response Training

Music City Center shall provide training to personnel in their Information Security Incident response roles and responsibilities as needed.

6. Loss or Theft

Team Members shall be required to immediately report the loss or theft of Information Technology Assets.

7. Breach Notification

Music City Center shall comply with all applicable federal and state security breach notification laws and regulations, including all requirements to provide notification of an Information Security Breach.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO

Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: section13, 6.1.6
- Title 2, Chapter 140 of the Metropolitan Code of Laws, Karl Dean Executive Order No. 35
- NIST Special Publication 800-53 Rev4, Recommended Security Controls for Federal Information Systems and Organizations: AU-6, AU-9, IR-1-8, PL-4, SI-2, SI-4, SI-5, CP-2
- NIST Special Publication 800-61 Rev2, Computer Incident Handling Guide
- NIST Cybersecurity Framework: PR.IP-9, DE.AE-5, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2

REVISION HISTORY

**CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

POLICY NUMBER:
ISM 5

INFORMATION SECURITY

SUBJECT:

**INFORMATION SECURITY INCIDENT
MANAGEMENT CRYPTOGRAPHIC
CONTROLS PLAN**

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Team Members, Information Owners, System Administrators, and Information System Users

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Information Security Incident Management Cryptographic Controls Policy.

1. Reporting Information Security Events, Vulnerabilities, and Incidents

Music City Center Team Members shall expeditiously report to the Technology Department any observed or suspected Information Security Events, Information Security Vulnerabilities, and Information Security Incidents, including any loss and/or theft of Information Technology Assets.

Music City Center shall report any observed or suspected Information Security Events and Incidents to law enforcement or other regulating agencies if laws are suspected to have been broken.

Information Security Events, Vulnerabilities and Incidents, including incident response plans shall be classified as Confidential. Music City Center/Metropolitan Government shall protect incident response plans from unauthorized disclosure and modification.

USERS: Team Members should expeditiously report to the Technology Department any observed

severity. The severity level may be upgraded or downgraded as more information becomes available.

- Teams are activated and notifications are made as appropriate.
- Actions are taken to mitigate risks and damages.

5. Any department personnel may be required to participate in the CSIRT.

3 Prioritization or Severity Ratings of Incidents

Music City Center shall establish thresholds for determining when an incident is triggered. Music City Center shall prioritize incidents based on two factors:

- .1. Current and potential impact of the incident; and*
- .2. Criticality of affected or potentially affected resources.*

USERS: Shall work with Department Authority to determine impact of implications.

DEPARTMENT AUTHORITY: Shall determine impact of the implications.

4 Information Security Incident Handling

4.1. *Music City Center shall quantify and monitor Information Security Incidents based on:*

- 4.1.1. Classification of the Information Security Incident within defined categories;*
- 4.1.2. The impact of the Information Security Incident; and*
- 4.1.3. The cost of the Information Security Incident.*

4.2. *Music City Center shall:*

- 4.2.1. Coordinate Information Security Incident handling activities with contingency planning activities;*
- 4.2.2. Categorize incidents consistent with response plans;*
- 4.2.3. Focus on containment and mitigation of incident;*
- 4.2.4. Incorporate lessons learned from ongoing Information Security Incident handling activities into Information Security Incident response procedures and training; and*
- 4.2.5. Implement the resulting changes accordingly.*

USERS: Seek Department Authority and abide by Information Security Incident plan. All Information is classified as Sensitive Information and should not be dispersed unless identified as such.

DEPARTMENT AUTHORITY: Determine Classification of Information, set contingency plans into action, and follow up on incident aftermath.

5. Incident Response Training

Music City Center shall provide training to personnel in their Information Security Incident response roles and responsibilities as needed.

USERS: Shall apply training to their active roles.

- Title 2, Chapter 140 of the Metropolitan Code of Laws, Karl Dean Executive Order No. 35
- NIST Special Publication 800-53 Rev4, Recommended Security Controls for Federal Information Systems and Organizations: AU-6, AU-9, IR-1-8, PL-4, SI-2, SI-4, SI-5, CP-2
- NIST Special Publication 800-61 Rev2, Computer Incident Handling Guide
- NIST Cybersecurity Framework: PR.IP-9, DE.AE-5, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |

| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 6</p> |
| <p>SUBJECT:</p> <p>TELEWORKING AND MOBILE COMPUTING POLICY</p> | <p>DISTRIBUTION DATE: 5/15/2018</p> <p>EFFECTIVE DATE: 5/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

PURPOSE

The purpose of this policy is to ensure the Team Members of the Music City Center achieves and maintains information security when using mobile computing and teleworking devices or facilities.

POLICY

1. Access and Use

All acceptable access and use of Music City Center/ Metropolitan Government information technology is defined in ISM 1 Acceptable Use of Information Technology Assets Policy. Team Members will comply with all aspects of that policy in addition to the requirements of this policy.

2. Permitted Forms of Remote Access

All permitted forms of remote access are defined in ISM 1 Acceptable Use of Information Technology Assets Policy.

3. Types of Access Granted for Telework Devices

3.1. Telework PC Access

Team Members working on devices either owned by Music City Center or Team Member-owned devices for the purposes of working off-site shall access resources only as approved by the President/CEO or his/her designee.

3.2. Third Party Owned Computers and Devices

Computers not owned by Music City Center or by the teleworking (e.g., hotel computers, public kiosks, conference computers, friends' PCs) and other devices (e.g., cell phones, PDAs) may access only publicly accessible web-based applications, such as web-based email. Music City Center/Metropolitan Government approved VPN clients shall be prohibited from being installed on any of these external devices.

4. Sensitive Information and Teleworking

Sensitive Information that is stored on or sent to or from telework devices shall be protected with Music City Center/Metropolitan Government Information Technology Services (ITS) Department



Wherever possible, encryption shall be configured and activated on the wireless access point (AP). Music City Center Technology Department does not provide support to user's home network.

7.4. External Networks

Teleworkers shall be aware that networks other than their home networks are unlikely to provide much protection for their network devices and communications, such as a laptop using third-party provided wireless hotspot. Teleworkers shall use a remote access solution provided by Music City Center and they shall activate the secure remote access solution (e.g., establishing a VPN session) immediately after connecting to the third-party network.

8. Securing Non-Music City Center Issued Teleworker-Owned PCs

Team Members shall take necessary precautions against compromising the confidentiality, integrity and availability of all Music City Center information technology by meeting Music City Center minimum security requirements to secure any non-Music City Center issued device that is used to access Music City Center/Metropolitan Government information technology.

9. Miscellaneous

This policy supersedes all previous Music City Center teleworking and mobile computing policies written or communicated. Team Members are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions. This policy may be amended or revised at any time by Music City Center. This policy does not supersede and departmental, agency or board policies that address areas defined in this policy as long as the requirements of such departmental, agency or board policies equal or exceed the minimum requirements set forth in this policy. This policy does not waive the responsibility of the Team Member from following all applicable legal and/or regulatory requirements.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO

Convention Center Authority of Metropolitan Government of Nashville and Davidson County

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 6

SUBJECT:

TELEWORKING AND MOBILE COMPUTING PLAN

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Team Members

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Teleworking and Mobile Computing Policy.

1. Access and Use

All acceptable access and use of Music City Center/ Metropolitan Government information technology is defined in ISM 1 Acceptable Use of Information Technology Assets Policy. Team Members will comply with all aspects of that policy in addition to the requirements of this policy.

USERS: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

DEPARTMENT AUTHORITY: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

2. Permitted Forms of Remote Access

All permitted forms of remote access are defined in ISM 1 Acceptable Use of Information Technology Assets Policy.

USERS: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

requirements. These are defined in the Mobile Device and Removable Media Physical Security Requirements standard.

USERS: Team Members should contact their Department Director for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Department should contact the applicable IT department for clarification or questions on how to meet this requirement.

5.1.2. Removable Media Use

Removable media use is addressed in ISM 1 Acceptable Use of Information Technology Assets Policy.

USERS: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

DEPARTMENT AUTHORITY: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

5.2. Backing Up Information

Proper storage of Music City Center/Metropolitan Government Information, including critical business information, is addressed in ISM Acceptable Use of Information Technology Assets Policy.

USERS: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

DEPARTMENT AUTHORITY: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

5.3. Destroying Information When No Longer Needed

Proper disposal of Music City Center Information is addressed in ISM 1 Acceptable Use of Information Technology Assets Policy.

USERS: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

DEPARTMENT AUTHORITY: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

6. **Approved Smart Phones, Blackberries, etc.**

The use of any mobile device, such as a mobile phone, Blackberry, etc., that will be used to store Music City Center data is addressed in ISM 1 Acceptable Use of Information Technology Assets Policy.

USERS: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

DEPARTMENT AUTHORITY: See ISM 1 Acceptable Use of Information Technology Assets Policy for more information.

DEPARTMENT AUTHORITY: Department should contact the applicable IT department for clarification or questions on how to meet this requirement.

8. Securing Non-Music City Center Issued Teleworker-Owned PCs

Team Members shall take necessary precautions against compromising the confidentiality, integrity and availability of all Music City Center information technology by meeting Music City Center minimum security requirements to secure any non-Music City Center issued device that is used to access Music City Center/Metropolitan Government information technology.

USERS: Team Members should contact their Department Director for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Department should contact the applicable IT department for clarification or questions on how to meet this requirement.

9. Miscellaneous

This policy supersedes all previous Music City Center teleworking and mobile computing policies written or communicated. Team Members are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions. This policy may be amended or revised at any time by Music City Center. This policy does not supersede and departmental, agency or board policies that address areas defined in this policy as long as the requirements of such departmental, agency or board policies equal or exceed the minimum requirements set forth in this policy. This policy does not waive the responsibility of the Team Member from following all applicable legal and/or regulatory requirements.

USERS: Team Members should contact their Department Director for clarification or questions on how to meet this requirement.

DEPARTMENT AUTHORITY: Department should contact the applicable IT department for clarification or questions on how to meet this requirement.

| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 7</p> |
| <p>SUBJECT:</p> <p>INFORMATION CLASSIFICATION POLICY</p> | <p>DISTRIBUTION DATE: 5/15/2018</p> <p>EFFECTIVE DATE: 5/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

PURPOSE

The purpose of this policy is to ensure that the Information of the Convention Center Authority of the Metropolitan Government of Nashville and Davidson County (Music City Center) receives an appropriate level of protection.¹

POLICY

1. Generally

Music City Center shall classify Information of the Music City Center in terms of their value, legal requirements, sensitivity, and criticality to the business and operations of the government and those it serves or as specified by any superseding state or federal law or regulation. Such legal requirements shall include applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance. This policy and accompanying procedures shall be reviewed at least annually.

2. Information Classifications

The following classifications shall be used by Music City Center to assign potential risk and to provide guidelines for Information of the Music City Center:

| | |
|--|--|
| <p>Public Information (no risk)</p> | <p>Public Information is Information of the Music City Center that Music City Center must provide for access to Tennessee residents. Public Information is shared publicly to facilitate Music City Center operations. <i>Examples of public Information include Information provided on the Music City Center Web site and reports meant for public distribution.</i></p> |
| <p>Internal Information (lowest risk)</p> | <p>Internal Information is non-sensitive Information of the Music City Center that is used in daily business operations. If Internal Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, little or no loss would be incurred. <i>Examples of internal Information include staff phone numbers building address.</i></p> |



SIGNATURE



Charles L. Starks,
 President/CEO
 Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 7.2, 7.2.1, 14.1.2
- Title 2, Chapter 140 of the Metropolitan Code of Laws, Karl Dean Executive Order No. 35
- NIST Special Publication 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations: RA-2, CC-9
- Tennessee Public Records Act, T.C.A. § 10-7-503 Tennessee Code Annotated 10-7-101 et seq.

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 3/15/2018 | First released version |
| | | |

¹In addition to this policy, care should be taken to ensure compliance with other applicable federal, state and local laws and authorities including but not limited to Title 2, Chapter 140 of the Metropolitan Code of Laws, Karl Dean Executive Order No. 35, and the Tennessee Public Records Act, T.C.A. § 10-7-503.



| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 7</p> |
| <p>SUBJECT:</p> <p>INFORMATION CLASSIFICATION PLAN</p> | <p>DISTRIBUTION DATE: 3/15/2018</p> <p>EFFECTIVE DATE: 3/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

AUDIENCE

Team Members, Data Owners, Confidential and Restriction Information Users of the Music City Center and Metropolitan Government of Nashville and Davidson County

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Information Classification Policy.

1. Generally

Music City Center shall classify Information of the Music City Center in terms of their value, legal requirements, sensitivity, and criticality to the business and operations of the government and those it serves or as specified by any superseding state or federal law or regulation. Such legal requirements shall include applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance. This policy and accompanying procedures shall be reviewed at least annually.

USERS: Understand the classification types.

DEPARTMENT AUTHORITY: Music City Center shall develop procedures that appropriately classify their Information of the Music City Center assets. This classification is necessary for determining the proper controls to apply based on the following levels:

- Public Information-no risk
- Internal Information-lowest risk



Department of Homeland Security.

All Information of the Music City Center regardless of physical form or characteristics shall be assigned a classification by the Information Owners in accordance with the requirements set forth within this section in order to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification, or destruction.

Music City Center shall comply with the Tennessee Public Records Act (the "TPRA") default presumption that all Music City Center records are available for inspection and copying unless they are protected by a specific exception under the TRPA. Any Metropolitan Government department, agency or entity that disseminates Information in response to a TPRA request shall ensure that the appropriate classification is applied when that Information is released from their department.

When Information of the Music City Center with multiple classifications is stored, transmitted, or destroyed together, Information handling requirements for the higher classification shall apply.

USERS: Understand the classification types.

DEPARTMENT AUTHORITY: When implementing the *Information Classification Policy*, departments should realize and account for the following:

1. The information owners have the best understanding on how their Information of the Music City Center should be classified and are most likely to understand the particular regulations that their Information of the Music City Center may fall under. Therefore, they:
 - a. need to thoroughly understand the risk of not classifying the Information of the Music City Center correctly,
 - b. need to classify Restricted Information of the Music City Center first followed by Confidential Information of the Music City Center,
 - c. are responsible for determining what of their other Information of the Music City Center is the most critical to classify and protect,
 - d. need to make the users aware of the classification, and
 - e. need to ensure that the appropriate classification is applied when the Information of the Music City Center is released from their department.
2. There is considerable risk in collecting and storing Information, and the magnitude of the risk depends on the classification. If there is little or no need for collecting and storing Information, it should be eliminated. Each department should evaluate their business processes to determine if the risk of collecting and storing the Information is worth the resources for applying necessary and required controls.
3. If it is determined that Information of the Music City Center is no longer needed, departments need to ensure the Information of the Music City Center is disposed of in a manner consistent with its classification. If no Records Disposition Authorization (RDA) is in place, the Public Records Commission needs to review and approve disposal.

SCOPE, BACKGROUND AND GOVERNANCE

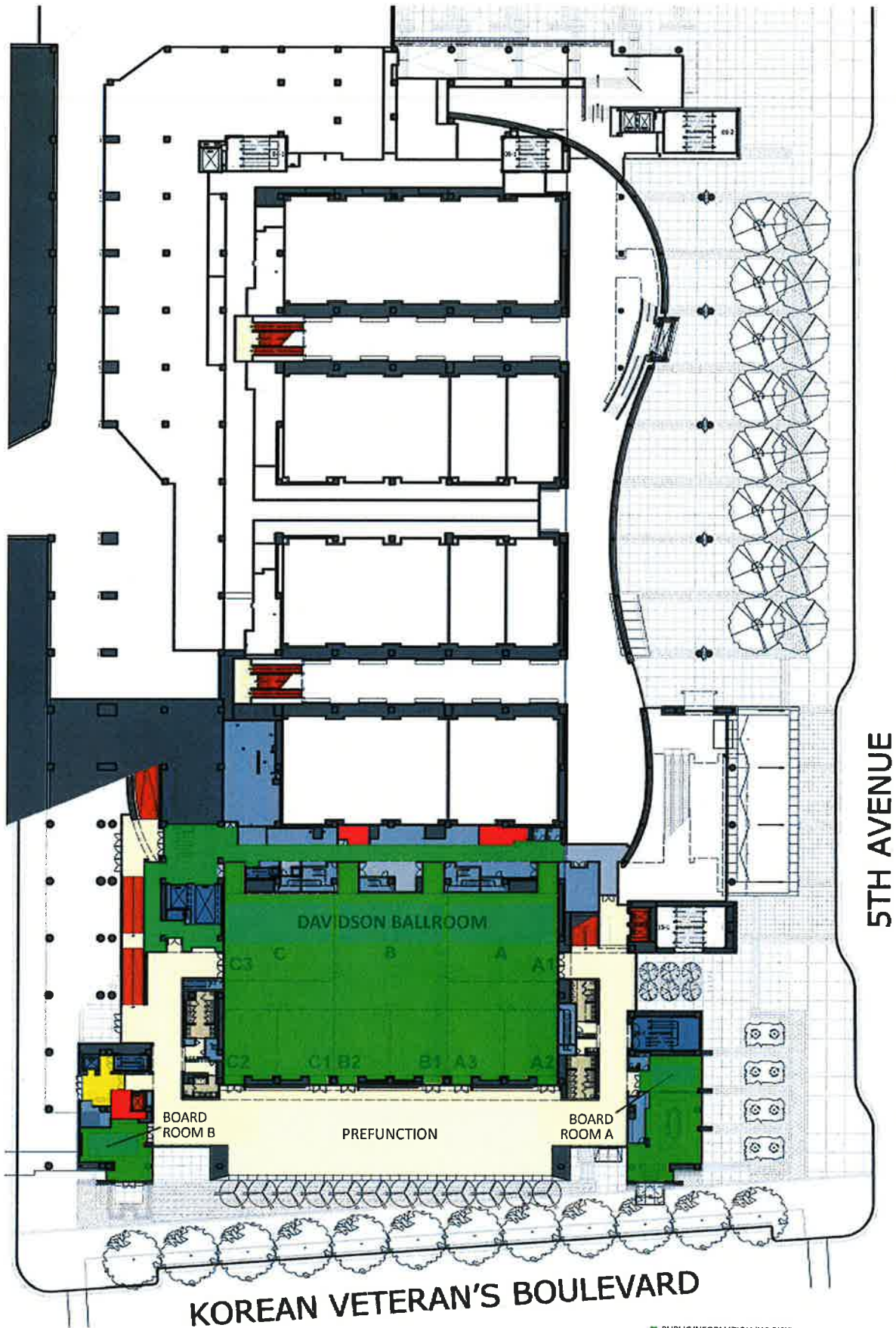
This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

LEVEL 1

INFORMATION SECURITY

MUSIC CITY CENTER

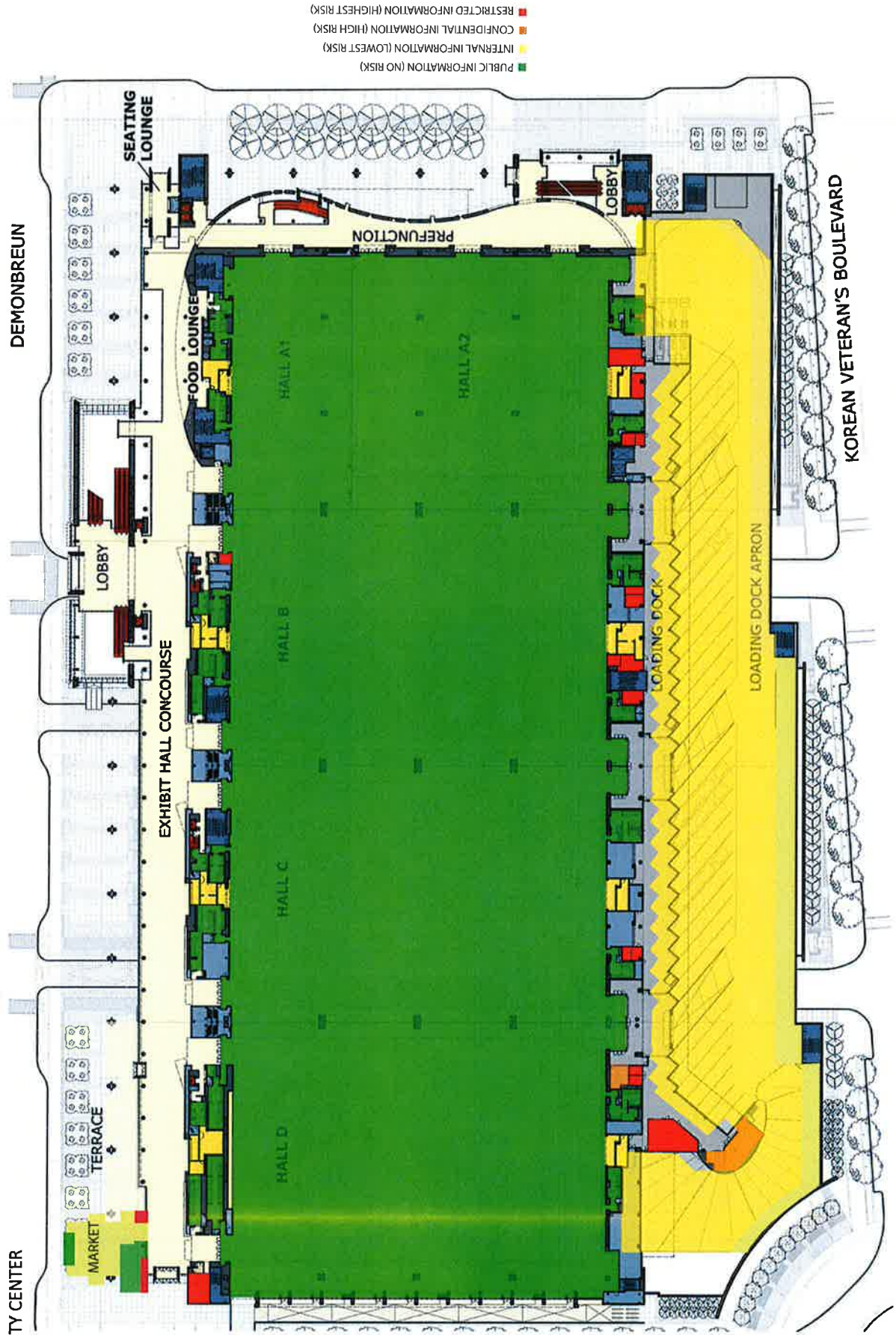




- PUBLIC INFORMATION (NO RISK)
- INTERNAL INFORMATION (LOWEST RISK)
- CONFIDENTIAL INFORMATION (HIGH RISK)
- RESTRICTED INFORMATION (HIGHEST RISK)

LEVEL 3 INFORMATION SECURITY

MUSIC CITY CENTER

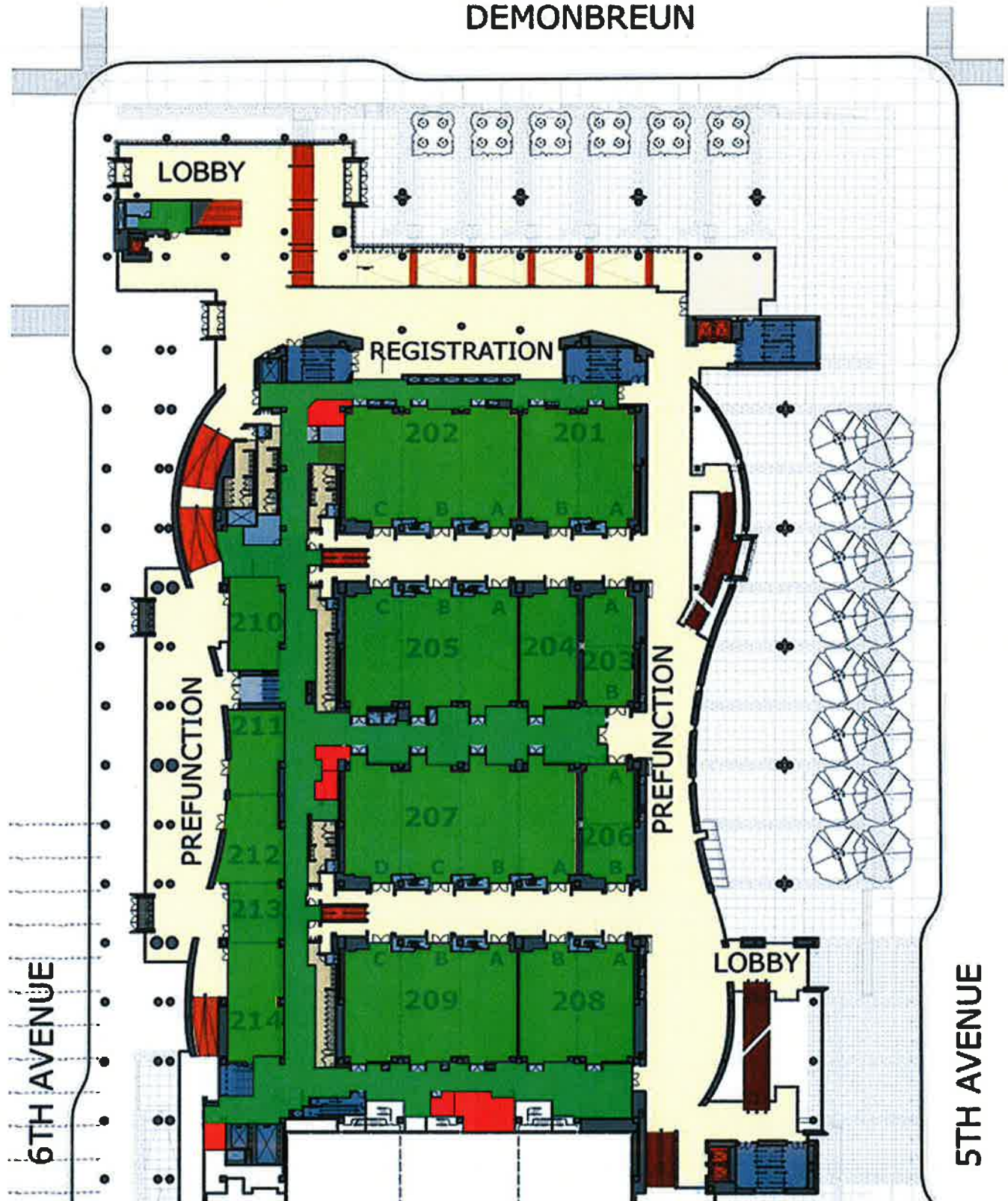


LEVEL 2

MUSIC CITY CENTER

INFORMATION SECURITY

DEMONBREUN

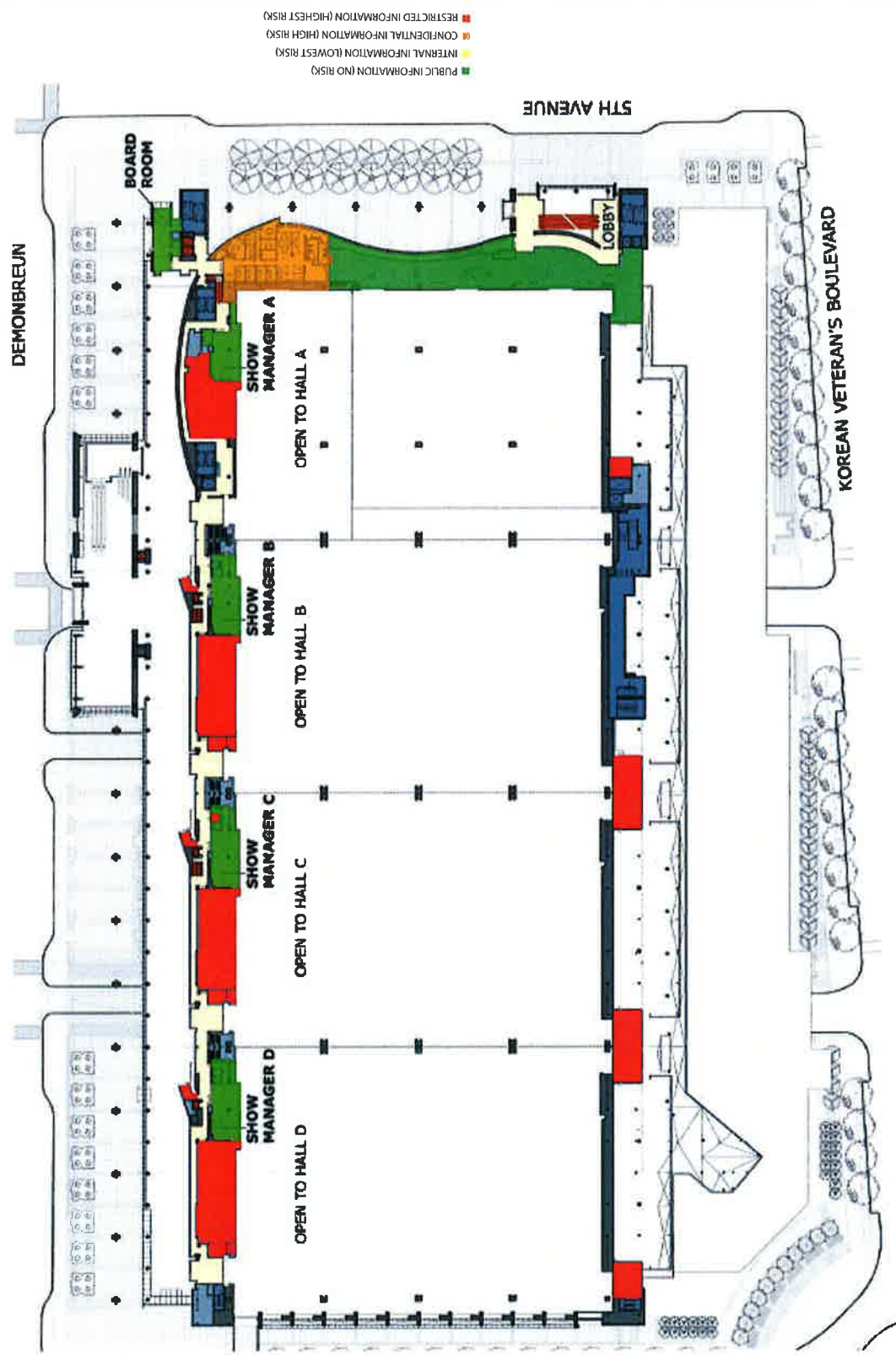


- PUBLIC INFORMATION (NO RISK)
- INTERNAL INFORMATION (LOWEST RISK)
- CONFIDENTIAL INFORMATION (HIGH RISK)
- RESTRICTED INFORMATION (HIGHEST RISK)

LEVEL 3M

MUSIC CITY CENTER

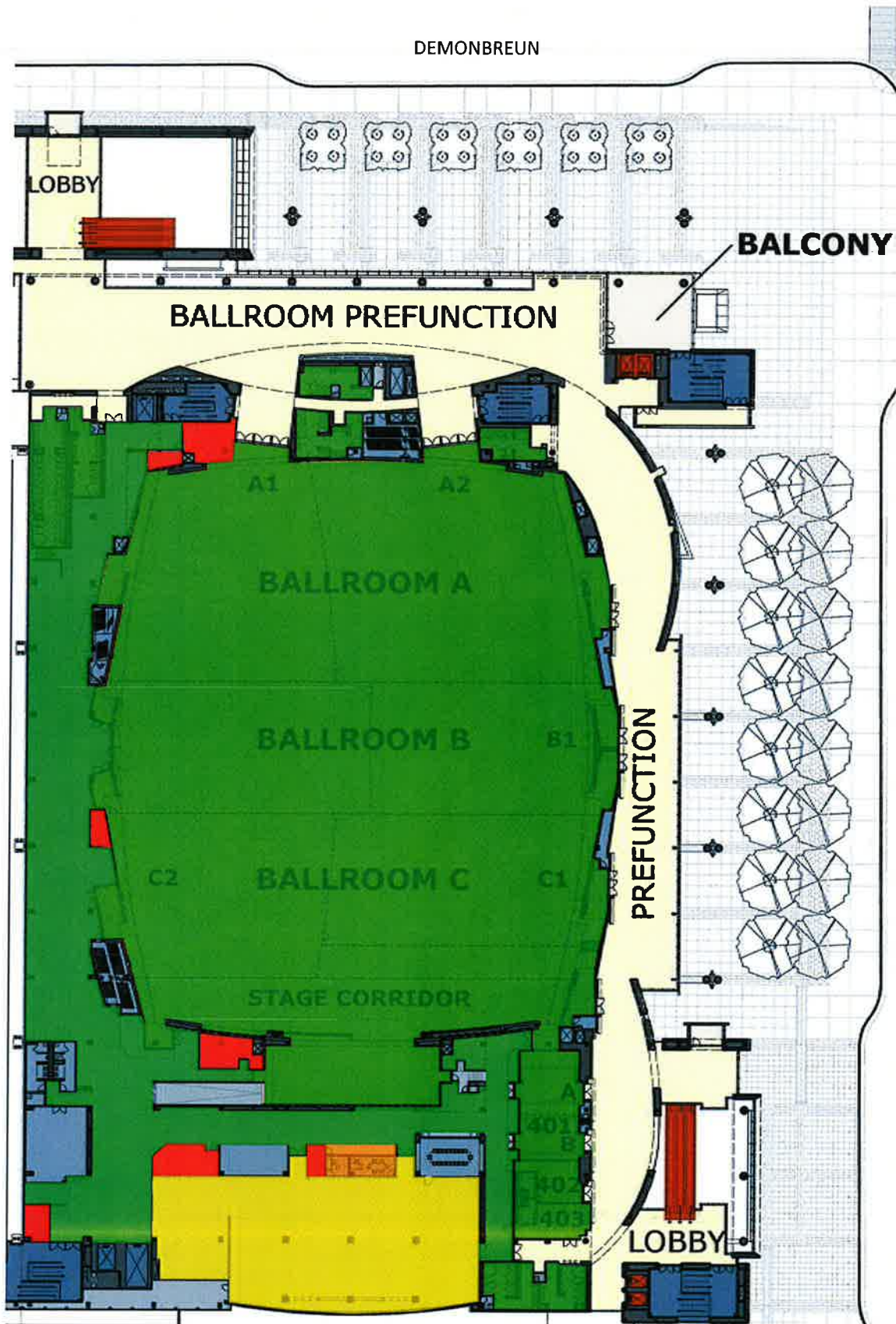
INFORMATION SECURITY



LEVEL 4
MUSIC CITY CENTER

INFORMATION SECURITY

DEMONBREUN



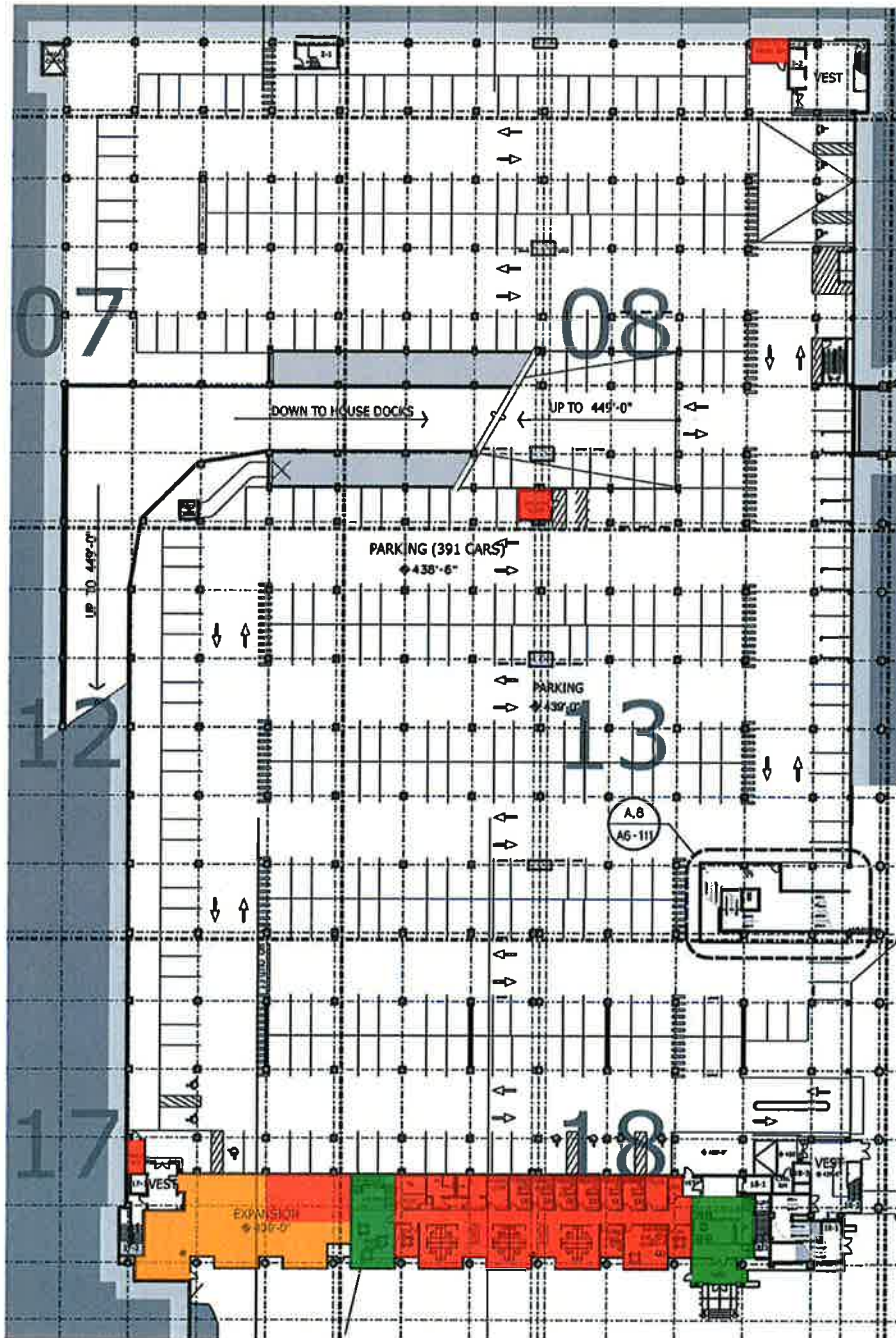
- PUBLIC INFORMATION (NO RISK)
- INTERNAL INFORMATION (LOWEST RISK)
- CONFIDENTIAL INFORMATION (HIGH RISK)
- RESTRICTED INFORMATION (HIGHEST RISK)

LEVEL 1 PARKING GARAGE

MUSIC CITY CENTER

INFORMATION SECURITY

DEMONBREUN



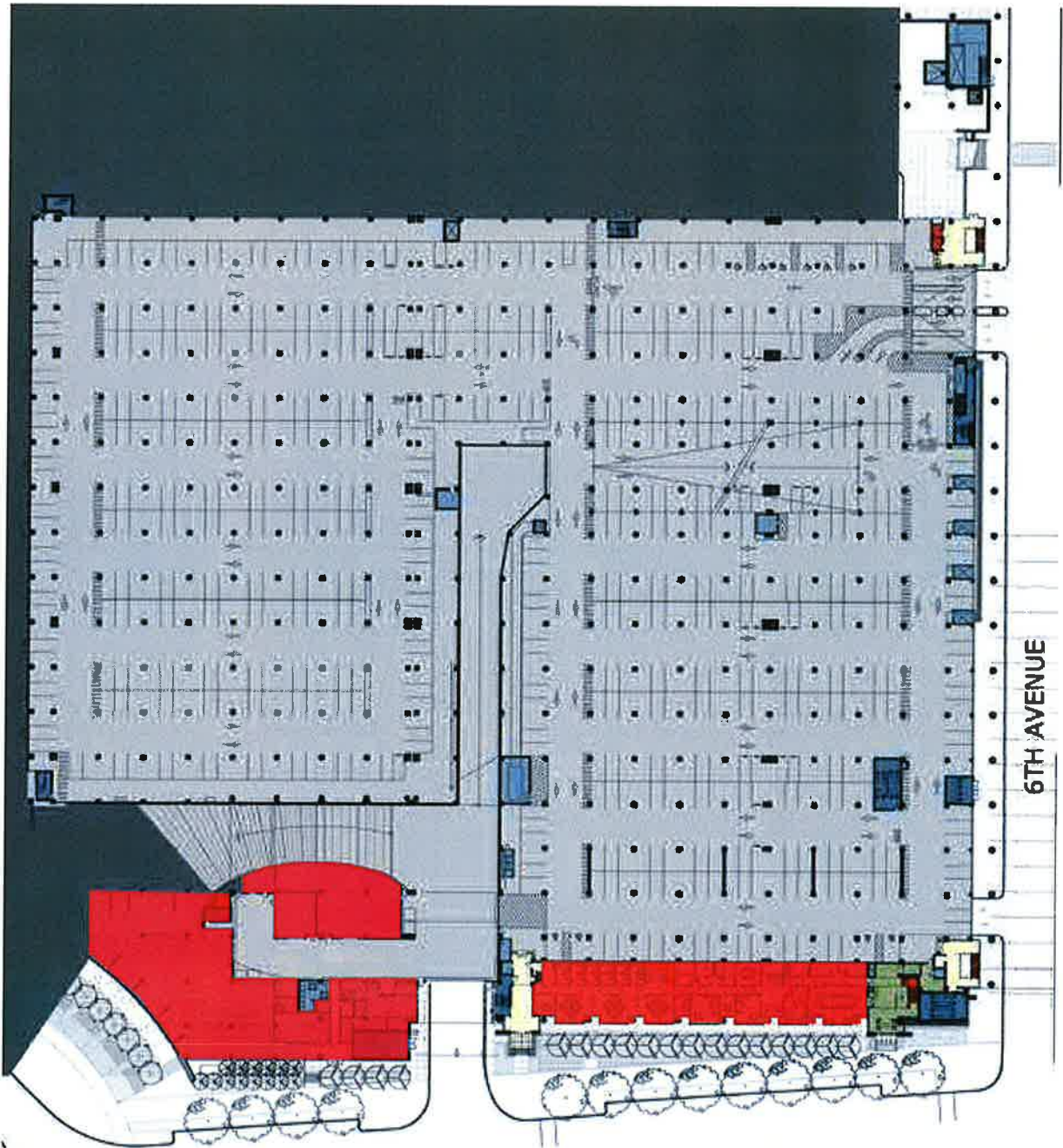
- PUBLIC INFORMATION (NO RISK)
- INTERNAL INFORMATION (LOWEST RISK)
- CONFIDENTIAL INFORMATION (HIGH RISK)
- RESTRICTED INFORMATION (HIGHEST RISK)

KVB

LEVEL 2 PARKING GARAGE

MUSIC CITY CENTER

INFORMATION SECURITY



- PUBLIC INFORMATION (NO RISK)
- INTERNAL INFORMATION (LOWEST RISK)
- CONFIDENTIAL INFORMATION (HIGH RISK)
- RESTRICTED INFORMATION (HIGHEST RISK)

LEVEL P3 PARKING GARAGE

MUSIC CITY CENTER

INFORMATION SECURITY



DEMONBREUN

P3

03

06

07

08

11

12

13

16

18

KOREAN VETERANS BOULEVARD

- PUBLIC INFORMATION (NO RISK)
- INTERNAL INFORMATION (LOWEST RISK)
- CONFIDENTIAL INFORMATION (HIGH RISK)
- RESTRICTED INFORMATION (HIGHEST RISK)

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 8

SUBJECT:

IT CONTINGENCY/DISASTER RECOVERY PLANNING POLICY

DISTRIBUTION DATE:
05/15/2018

EFFECTIVE DATE:
05/15/2018

ISSUING AUTHORITY:

PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this Policy is to ensure that the Music City Center/Metropolitan Government of Nashville and Davidson County (Metropolitan Government) establishes, maintains and implements plans for emergency response, backup operations and post-disaster recovery for systems.

POLICY

1. Generally

Music City Center/Metropolitan Government's IT contingency/disaster recovery planning capability must meet applicable (and agreed to with customers) service levels supporting critical operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal IT contingency/disaster recovery plan ("Plan"). Music City Center/Metropolitan Government personnel shall be trained to execute IT contingency/disaster recovery planning procedures. The Plan shall meet the requirements of applicable federal, state and local laws and regulations. This policy and the accompanying Plan shall be reviewed/updated at least annually. This policy shall only apply to Music City Center/Metropolitan Government departments, agencies and boards, with their own data centers and/or significant IT capabilities.

Music City Center/Metropolitan Government's IT contingency/disaster recovery planning is supported through the use of the controls set forth below.

2. Integration with Business Continuity Plans

The Plan shall represent a broad scope of activities designed to sustain and recover critical IT services following an emergency. Ultimately, Music City Center/Metropolitan Government shall use a suite of plans to properly prepare response, recovery and continuity activities for disruptions affecting its IT systems, business processes and facilities. Because there is an inherent relationship between an IT system and the business processes it supports, there should be coordination between each Plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

6. Alternate Storage Site

Each Music City Center/Metropolitan Government department, agency or board shall establish an offsite secure storage site including necessary agreements to permit the storage and retrieval of information system backup information.

7. Alternate Processing Site

Each Music City Center/Metropolitan Government department, agency and board shall:

- 7.1. Establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the agreed upon time period as described in the service level agreement with the applicable department, agency or board when the primary processing capabilities are unavailable; and
- 7.2. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the Music City Center/Metropolitan Government-defined time period for resumption.

8. Telecommunications Services

Each Music City Center/Metropolitan Government department, agency and board shall establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable.

9. Information System Backup

Each Music City Center/Metropolitan Government department, agency and board shall comply with the *Information Backup Policy*.

10. Information System Recovery and Reconstitution

Each Music City Center/Metropolitan Government department, agency and board shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise or failure. It shall also protect backup and restoration hardware, firmware and software.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.



| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <h2>INFORMATION SECURITY</h2> | <p>POLICY NUMBER: ISM 8</p> |
| <p>SUBJECT:</p> <h2>IT CONTINGENCY/DISASTER RECOVERY PLAN</h2> | <p>DISTRIBUTION DATE: 05/15/2018</p> <p>EFFECTIVE DATE: 05/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

AUDIENCE

System Administrators, Data Owners, Emergency Response Team, Backup Operators

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the IT Contingency/Disaster Recovery Planning Policy.

1. *Generally*

Music City Center/Metropolitan Government's IT contingency/disaster recovery planning capability must meet applicable (and agreed to with customers) service levels supporting critical operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal IT contingency/disaster recovery plan ("Plan"). Music City Center/Metropolitan Government personnel shall be trained to execute IT contingency/disaster recovery planning procedures. The Plan shall meet the requirements of applicable federal, state and local laws and regulations. This policy and the accompanying Plan shall be reviewed/updated at least annually. This policy shall only apply to Music City Center/Metropolitan Government departments, agencies and boards, with their own data centers and/or significant IT capabilities.

Music City Center/Metropolitan Government's IT contingency/disaster recovery planning is supported through the use of the controls set forth below.

USERS: Seek Department Authority

DEPARTMENT AUTHORITY: A Disaster Recovery Plan is a written plan that focuses on recovering Information Technology systems that support business functions, in the event of a disaster.

Departments should:

- Identify Plan managers (the role of administering the Plan) and Plan owners (the role of ensuring Plans are created, updated, tested, and are sufficient to support the business);
- Identify regulatory requirements for Plans, if any (for example, HIPAA requires a Plan for covered entities);
- Develop the Plan;
- Review and revise the Plan biannually; and
- Test their Plan annually.

Plan managers should identify all of the department's or agency's critical business processes as part of an overall Business Continuity Plan. This may be accomplished through a departmental Risk Assessment and subsequent Business Impact Analysis. If assistance is needed with these items, requests should be directed to Metro's CISO listed below.

Business Continuity and Disaster Recovery plans may be loaded into the Living Disaster Recovery Planning System (LDRPS). These plans should be reviewed at minimum as stated above and whenever there are significant changes in processes, hardware, software, and/or facilities.

All personnel required to ensure the successful implementation of a Plan (be it a disaster recovery exercise or an actual situation) should be trained in their specific duties and responsibilities. Disaster recovery exercises should be varied in scope and type and should be viewed as opportunities to discover potential weaknesses (and therefore risks) in the Plan, allowing for proper Risk Treatment.

METRICS

Suggested metrics to monitor compliance and policy effectiveness include:

- Percentage of organizational units with disaster recovery plans developed
- Percentage of disaster recovery plans that have successfully completed a tabletop exercise or other test within the past year
- Percentage of personnel trained in their specific duties and responsibilities in plan implementation
- Percentage of disaster recovery plans that have been reviewed and updated if necessary within the past two years
- Percentage of departmental budget allocated to disaster recovery operations (this may be measured against the cost of lost business during recovery as a function of time)
- Mean Time to Incident Recovery, calculated as the sum of the time for recovery of critical operations divided by number of incidents

4. Plan Training

DEPARTMENT AUTHORITY: Establish secondary hot/warm/cold site.

8. Telecommunications Services

Each Music City Center/Metropolitan Government department, agency and board shall establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable.

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Establish secondary services.

9. Information System Backup

Each Music City Center/Metropolitan Government department, agency and board shall comply with the Information Backup Policy.

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Establish and disseminate the Information Backup Policy.

10. Information System Recovery and Reconstitution

Each Music City Center/Metropolitan Government department, agency and board shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise or failure. It shall also protect backup and restoration hardware, firmware and software.

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Establish baseline for recovery.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

Disaster Recovery Planning Checklist

Items on this checklist are suggested areas of focus for your disaster recovery plans. This checklist should be used as a guideline where applicable and added to, per your department specific needs.

| CHECK | DUE DATE | WHAT | EMPLOYEE RESPONSIBLE | PROGRESS |
|-------|----------|--|----------------------|----------|
| | | Scope – listing of department functions included and excluded from the DR plan | | |
| | | Assumptions – description of what assumptions you made in developing the plan | | |
| | | Overview | | |
| | | Strategies | | |
| | | Internal Department Contacts – who from your department is directly involved in implementing the plan | | |
| | | Supporting Metro Contacts – who from other Metro departments could be called on to implement your plan | | |
| | | Vendor Contacts – listing of the vendors that will provide support or materials to restore your systems | | |
| | | Vendor Contract Information | | |
| | | Application or Hardware Dependencies | | |
| | | Documented, step-by-step recovery procedures | | |
| | | Defined, periodic backups taken – mapping of critical data to backup frequency, type, and backup location | | |
| | | Mission critical systems identified –listing of all critical applications for each department function included in the scope | | |
| | | Recovery Time Objective (Acceptable downtime) – how long can each function included in the scope be down before the department’s operations are negatively impacted or contractual obligations are not met | | |
| | | Recovery Point Objective (How current does the backup have to be?) | | |
| | | Business Continuity Plan (Outage workaround) – documented manual processes to keep department functions operational until systems are restored | | |

Notes

**MCC Standard
Disaster Recovery Planning Checklist**

| | |
|---------------------|----------------------|
| Document ID | ID |
| Effective Date | DATE |
| Owner | OWNER |
| Info Classification | Internal Information |
| Page No. | Page 1 of 2 |

AUDIENCE

Team Members

PURPOSE

Checklist for recovery from an event

SUMMARY

Music City Center faces adversaries and might need to recover applications or services. The following checklists helps plan the course of actions required to re-establish the necessary applications or services.

DETAILS

Disaster Recovery Planning Checklist

Items on this checklist are suggested areas of focus for your disaster recovery plans. This checklist should be used as a guideline where applicable and added to, per your department specific needs.

| CHECK | DUE DATE | WHAT | EMPLOYEE RESPONSIBLE | PROGRESS |
|-------|----------|---|----------------------|----------|
| | | Scope – listing of department functions included and excluded from the DR plan | | |
| | | Assumptions – description of what assumptions you made in developing the plan | | |
| | | Overview | | |
| | | Strategies | | |
| | | Internal Department Contacts – who from your department is directly involved in implementing the plan | | |
| | | Supporting Metro Contacts – who from other Metro departments could be called on to implement your plan | | |
| | | Vendor Contacts – listing of the vendors that will provide support or materials to restore your systems | | |
| | | Vendor Contract Information | | |
| | | Application or Hardware Dependencies | | |
| | | Documented, step-by-step recovery procedures | | |
| | | Defined, periodic backups taken – mapping of critical data to backup frequency, type, and backup location | | |



| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM 9</p> |
| <p>SUBJECT:</p> <p>ACCESS CONTROL AND MANAGEMENT SECURITY POLICY</p> | <p>DISTRIBUTION DATE: 05/15/2018</p> <p>EFFECTIVE DATE: 05/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

PURPOSE

The purpose of this policy is to ensure Convention Center Authority of the Metropolitan Government of Nashville and Davidson County (Music City Center) along with the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) reduces risks to information security by managing accounts that provide access, limiting access to authorized Team Members and preventing unauthorized access to Information Systems.

POLICY

1. General

Music City Center/Metropolitan Government shall develop procedures for the effective implementation of security controls covering access control and information system account management. Information system accounts are used to provide access to information technology assets and physical access, in cases where physical access is tied to information system accounts.

Information system account types include, for example, individual, shared, group, system, guest/anonymous, and service. As set forth below, Music City Center /Metropolitan Government’s access control processes are supported through the use of the controls set forth in: (i) business requirements (Section 2.1 below); (ii) user access management (see Section 2.2 below); (iii) user responsibility (see Section 2.3 below); (iv) system and application access control (see Section 2.4 below); (v) segregation of duties (see Section 2.5 below); and (vi) additional security controls (see Section 2.6 below).

2. Detailed

2.1. Business Requirements of Access Control

2.1.1. Music City Center/Metropolitan Government shall:

- a. provide access based on business and information security requirements;
- b. determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks;



2.2.3. Management of Privileged Access Rights

Music City Center/Metropolitan Government shall implement processes for restricting and controlling the allocation and use of “privileged access rights”. These privileged access rights are generally referred to as “administrative rights”. Inappropriate use of administrative rights (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

2.2.4. Management of Secret Authentication Information of Team Members

Music City Center/Metropolitan Government shall implement processes that control the allocation of any secret authentication information. Passwords are a commonly used type of secret authentication information and are a common means of verifying a user’s identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

2.2.5. Review of User Access Rights

Music City Center/Metropolitan Government shall include a review of Team Members’ access rights at regular defined intervals as part of access control procedures.

2.2.6. Removal or Adjustment of Access Rights

2.2.6.1. Removal

Music City Center/Metropolitan Government shall confirm that the access rights of all Team Members to information assets be removed upon termination of their employment, contract or agreement, or adjusted upon change. Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended.

2.2.6.2. Modifications

Music City Center/Metropolitan Government shall confirm that changes of Team Member’s employment or role is reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

2.2.6.3. Additional Considerations

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

- enforce regular password changes and as needed;
- maintain a record of previously used passwords and prevent re-use;
- not display passwords on the screen when being entered;
- store password files separately from application system data;
- and transmit passwords in protected form.

2.4.4. Use of Privileged Utility Programs

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

2.4.5. Access Control to Program Source Code

Access to program source code shall be restricted. Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries.

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) shall be considered.

2.5. Segregation of Duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Music City Center/Metropolitan Government shall work to implement segregation of duties, where applicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision shall be considered.

2.6. Additional Security Controls

Music City Center/Metropolitan Government shall, where applicable:

- 2.6.1. Access and impose additional usage restrictions to further limit access;
- 2.6.2. Identify parameters that define typical account usage and notify when use is outside those parameters;
- 2.6.3. Enforce a limit of invalid logon attempts and automatically lock account for a specified period of time;
- 2.6.4. Display to Team members a message banner that identifies acceptable use;
- 2.6.5. Display to Team Members data and time of last logon (access);
- 2.6.6. Institute session lock and termination settings for a determined period of inactivity;

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 9

SUBJECT:

ACCESS CONTROL AND MANAGEMENT SECURITY PLAN

DISTRIBUTION DATE:
05/15/2018

EFFECTIVE DATE:
05/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Team Members, Information Owners, System Administrators, and Information System Users

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Access Control and Management Security Policy.

1. General

Music City Center/Metropolitan Government shall develop procedures for the effective implementation of security controls covering access control and information system account management. Information system accounts are used to provide access to information technology assets and physical access, in cases where physical access is tied to information system accounts.

Information system account types include, for example, individual, shared, group, system, guest/anonymous, and service. As set forth below, Music City Center /Metropolitan Government's access control processes are supported through the use of the controls set forth in: (i) business requirements (Section 2.1 below); (ii) user access management (see Section 2.2 below); (iii) user responsibility (see Section 2.3 below); (iv) system and application access control (see Section 2.4 below); (v) segregation of duties (see Section 2.5 below); and (vi) additional security controls (see Section 2.6 below).

USER: Comply with ISM 1.



- data or services;
- e. management of access rights in a distributed and networked environment which recognizes all types of connections available;
- f. segregation of access control roles, e.g. access request, access authorization, access administration;
- g. requirements for formal authorization of access requests;
- h. requirements for periodic review of access rights;
- i. removal of access rights;
- j. process for monitoring account usage to determine dormant accounts including notification to the user or user's manager;
- k. archiving of records of all significant events concerning the use and management of user identities and secret authentication information; and
- l. roles with privileged access.

Furthermore, access controls rules shall:

- a. be established based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";
- b. consider changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
- c. identify rules which require specific approval before enactment and those which do not; and
- d. be supported by formal procedures and defined responsibilities.

2.1.2. Access to Networks and Network Services

Music City Center/ Metropolitan Government shall provide Team Members with only the access to the network and network services that they have been specifically authorized to use. Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to Team Members in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control. Music City Center/ Metropolitan Government shall utilize appropriate technical controls to protect the internal Music City Center/ Metropolitan Government network from external networks.

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: Music City Center shall develop, document and implement procedures concerning the use of networks and network services and shall cover:

- a. separation of internal network from external network utilizing a demilitarized zone implemented via firewalls;
- b. authorization procedures for determining who is allowed to access which networks and networked services;
- c. management controls and procedures to protect access to network connections and network services;
- d. the means used to access networks and network services (e.g. use of

responsible for their actions; the use of shared, generic IDs should only be permitted where they are necessary for business or operational reasons and shall be approved and documented via the security exception request process;

- b. immediately disabling or removing user IDs of Team Members who have left Metropolitan Government;
- c. periodically identifying and removing or disabling redundant User IDs;
- d. ensuring that redundant User IDs are not issued to other users; and
- e. ensuring that User IDs that are not in use for over 90 days are disabled and tagged for deletion.

2.2.2. User Access Provisioning

Music City Center/Metropolitan Government shall implement formal user access provisioning to assign or revoke access rights for all user types to all systems and services. Ideally, consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles.

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: Music City Center shall develop, document and implement procedures for assigning or revoking access rights granted to user IDs. These procedures shall address, at a minimum:

- a. obtaining authorization from the owner of the information system or service for the use of the information system or service. Separate approval for access rights from management may also be appropriate;
- b. verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties;
- c. ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed;
- d. maintaining a central record of access rights granted to a user ID to access information system and services;
- e. adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization; and
- f. periodically reviewing access rights with owners of the information systems or services.

2.2.3. Management of Privileged Access Rights

Music City Center/Metropolitan Government shall implement processes for restricting and controlling the allocation and use of "privileged access rights". These privileged access rights are generally referred to as "administrative rights". Inappropriate use of administrative rights (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

- information;
- d. temporary secret authentication information shall be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages shall be avoided;
- e. temporary secret authentication information shall be unique to an individual and shall meet Metropolitan Government minimum requirements;
- f. users shall acknowledge receipt of secret authentication information;
- g. default vendor secret authentication information shall be altered following installation of systems or software;
- h. all account usernames and authentication credentials are transmitted across networks using encrypted channels; and
- i. all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges.

2.2.5. *Review of User Access Rights*

Music City Center/Metropolitan Government shall include a review of Team Members' access rights at regular defined intervals as part of access control procedures.

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: Music City Center shall develop, document and implement procedures for the review of user access rights. These procedures will include that user access rights:

- a. be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment;
- b. be reviewed and re-allocated when moving from one role to another within the same organization;
- c. have authorizations for privileged access rights be reviewed at more frequent intervals;
- d. include check of privilege allocations at regular intervals to ensure that unauthorized privileges have not been obtained;
- e. ensure that changes to privileged accounts should be logged for periodic review.

2.2.6. *Removal or Adjustment of Access Rights*

Music City Center shall develop, document and implement procedures for handling the removal of access rights, including under what circumstances those rights are removed and procedures for expediting the removal of rights when necessary. Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to Metropolitan Government operations and assets, individuals, other organizations, etc. . Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement.

dismissed, they may be tempted to collect information for future use.

2.3. *Use of Secret Authentication Information*

Music City Center/Metropolitan Government Team Members shall be required to follow all applicable policies, procedures and standards, including, but not limited to, Metropolitan Government's Acceptable Use of Information Technology Assets Policy, with regards to the use of secret authentication information.

USERS: Follow ISM 1.

DEPARTMENT AUTHORITY: Music City Center shall ensure all Team Members have reviewed and signed off on Metropolitan Government's Acceptable Use of Information Technology Assets Policy.

2.4. *System and Application Access Control*

Music City Center/Metropolitan Government shall develop and documents processes to prevent unauthorized access to systems and applications.

2.4.1. *Information Access Restriction*

Access to information and application system functions shall be restricted in accordance with this policy and shall be restricted based on individual business application requirements.

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: In order to restrict access, Music City Center should require the following capabilities for any application:

- a. providing menus to control access to application system functions;
- b. controlling which data can be accessed by a particular Team Member;
- c. controlling the access rights of Team Members, e.g. read, write, delete and execute;
- d. controlling the access rights of other applications;
- e. limiting the information contained in outputs; and
- f. providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

2.4.2. *Secure Log-on Procedures*

Access to systems and applications shall be controlled by a secure log-on procedure. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: Where strong authentication and identity verification is required, additional authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

- b. allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- c. enforce a choice of strong passwords;
- d. force users to change their passwords at the first log-on;
- e. enforce regular password changes and as needed;
- f. maintain a record of previously used passwords and prevent re-use (password history);
- g. not display passwords on the screen when being entered;
- h. store password files separately from application system data; and
- i. transmit passwords in protected form.

2.4.4. *Use of Privileged Utility Programs*

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

USERS: Refer to ISM 1.

DEPARTMENT AUTHORITY: The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be followed:

- a. use of identification, authentication and authorization procedures for utility programs;
- b. segregation of utility programs from applications software;
- c. limitation of the use of utility programs to the minimum practical number of trusted, authorized users;
- d. authorization for ad hoc use of utility programs;
- e. limitation of the availability of utility programs, e.g. for the duration of an authorized change;
- f. logging of all use of utility programs;
- g. defining and documenting of authorization levels for utility programs;
- h. removal or disabling of all unnecessary utility programs;
- i. not making utility programs available to users who have access to applications on systems where segregation of duties is required.

2.4.5. *Access Control to Program Source Code*

Access to program source code shall be restricted. Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries.

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) shall be considered.

USERS: Seek Department Authority for assistance.

applicable, implemented Music City Center shall review these additional security controls and apply where possible.

Music City Center/Metropolitan Government shall, where applicable:

- 2.6.1. *Access and impose additional usage restrictions to further limit access;*
Music City Center can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time within the applicable information system or application.
- 2.6.2. *Identify parameters that define typical account usage and notify when use is outside those parameters;*
Music City Center should attempt to monitor information system accounts for atypical usage and investigate such usage. Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in the department.
- 2.6.3. *Enforce a limit of invalid logon attempts and automatically lock account for a specified period of time;*
Music City Center should configure authentication systems to automatically lock accounts for a short period of time after a number of invalid logon attempts. Care should be taken when configuring these settings so as not to create a denial of service vulnerability. Account lockouts should include notifications to appropriate information or application owners.
- 2.6.4. *Display to Team members a message banner that identifies acceptable use;*
Music City Center should utilize message banners to inform users of appropriate use of the information system and repercussions of inappropriate use.
- 2.6.5. *Display to Team Members data and time of last logon (access);*
Music City Center should configure the information system or application to notify the user, upon successful logon (access) to the system, of the date and time of the last logon Institute session lock and termination settings for a determined period of inactivity.
- 2.6.6. *Institute session lock and termination settings for a determined period of inactivity; and*
Music City Center should configure information systems and applications to either terminate sessions or lock sessions after a defined period of inactivity. Terminating a session results in a complete disconnect of a user from a system, including any processes the user had initiated. Locking a session means all user initiated processes continue, but user must re-authenticate to access the processes.
- 2.6.7. *Require the creation and use of any "generic" account, an account used by multiple Team Members and whose activity cannot be tracked to a unique user,*

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 10

SUBJECT:

INVENTORY AND OWNERSHIP OF ASSETS POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to ensure that the Music City Center achieves and maintains appropriate protection of its assets as they relate to the collection, processing and storage of Information.

POLICY

1. Generally

The Music City Center shall clearly identify all of its assets and shall develop and maintain an inventory of all important assets that, in the event of loss, disclosure or unauthorized access, could pose a risk to the Music City Center/Metropolitan Government. Such assets shall include hardware, software, Information, services, people, and intangibles. As applicable, ownership for hardware, software, and Information as well as parties responsible for services, personnel, and intangibles shall be designated and documented for each asset and shall be reviewed/updated at least annually.

Music City Center's compilation of its inventory and ownership of assets is supported through the use of the controls set forth in the sections below.

2. Configuration Management Plan

Music City Center shall develop, document and implement a configuration management plan for its inventory of assets, otherwise referred to as configuration items, that:

- 2.1. Addresses roles, responsibilities and configuration management processes and procedures;
- 2.2. Defines the configuration items and at what point in the system development life cycle the configuration items are placed under configuration management; and
- 2.3. Establishes the means for identifying configuration items throughout the system development life cycle and a process for identifying and managing the relationships of the configuration items.

and air-conditioning), and other general services (e.g., security, shredding services, janitorial, etc.). Those roles responsible for the provisioning of such services shall be identified.

8. People

Music City Center shall develop and maintain an inventory of its personnel, contractors and other essential individuals. The inventory for personnel shall include their qualifications, skills, experience and supervisor.

9. Intangibles

Music City Center shall develop and maintain an inventory of its intangibles. The inventory for intangibles shall include Music City Center reputation and image.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO
Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 7.1.1, 7.1.2
- Center for Internet Security Controls 1,2,3
- NIST Cyber Security Framework ID.AM-1, ID.AM-2
- NIST Special Publications 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*: CM-8, CM-9, PM-5
- Music City Center *Information Classification Policy*

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |



CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 10

SUBJECT:

INVENTORY AND OWNERSHIP OF ASSETS PLAN

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Team Members and Data Owners

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

The objective of this plan is to provide a guideline to clearly identify all of a department's assets and develop and maintain an inventory of all important assets that, in the event of loss, disclosure or unauthorized access, could pose a risk to the Music City Center / Metropolitan Government. Each heading matches with the applicable heading found in the Inventory and Ownership of Assets Policy.

1. Generally

The Music City Center shall clearly identify all of its assets and shall develop and maintain an inventory of all important assets that, in the event of loss, disclosure or unauthorized access, could pose a risk to the Music City Center/Metropolitan Government. Such assets shall include hardware, software, Information, services, people, and intangibles. As applicable, ownership for hardware, software, and Information as well as parties responsible for services, personnel, and intangibles shall be designated and documented for each asset and shall be reviewed/updated at least annually.

Music City Center's compilation of its inventory and ownership of assets is supported through the use of the controls set forth in the sections below.

USERS: Report any stolen or missing Information Technology Asset to Management. Understand

- 3.1. *Be the responsibility of the Director of the Department to which the asset is assigned;*
- 3.2. *Be current and accurate;*
- 3.3. *Identify the owner of and/or individual responsible for the asset;*
- 3.4. *Be at a level of granularity deemed necessary for tracking and reporting;*
- 3.5. *Include information deemed necessary to achieve effective property accountability;*
- 3.6. *Be available for review and audit by designated Music City Center/Metropolitan Government officials;*
- 3.7. *Include information designed and/or required to ensure business continuity.*

USERS: See Department Director. Team Members should leave all identifiers intact.

DEPARTMENT AUTHORITY: Ensure assets are accounted for.

Selection of Configuration Items

When determining which configuration items to include in an inventory, the Department should consider the critical nature of the asset or service it supports, the classification of any data that is stored on the asset and the risk posed to Music City Center should the asset become lost, stolen or compromised.

Consideration should also be given to the cost and resources involved in managing and maintaining the inventory versus any contractual obligations or compliance with laws or regulations. For example, it would be resource and cost intensive to track computer mice in an inventory when there is minimal risk to Music City Center/Metropolitan Government if they are lost and no legal or regulatory requirement to do so.

Information to Record

Each department should determine the level of detail deemed necessary to achieve effective property accountability and business continuity. At a minimum, the following information should be included in each configuration item record:

- Unique identifier
- Type of configuration item (hardware, software/application/system, service, documentation, etc.)
- Status of the configuration item (production, surplus, active, etc.)
- Classification (restricted, critical, etc.)
- Location of configuration item
- Owner responsible
- Department responsible
- Relationship with other configuration items
- Dependencies to other configuration items

Additional information specific to the type of configuration item should include:

- Hardware inventory specifications (manufacturer, type, model, serial number, physical location)
- Software license information
- For a networked component/device, the machine name, network address, etc.

configurations, approved deviations and any mission critical applications. The inventory of software and applications shall be updated as an integral part of installations, removals and information system updates.

Music City Center shall develop a process to alert on the installation of any unapproved software.

All software and applications must be fully licensed and supported. Any software or applications that have reached end of life/end of support must be tracked as security exceptions.

USERS: Understand and accept ISM 1 – Acceptable Use Policy.

DEPARTMENT AUTHORITY:

- **A standard shall be developed to define and document a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses and develop a process for monitoring for software installations outside of authorized software list.**
- **Music City Center shall deploy the use of software inventory process throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it.**

6. Information

Music City Center shall develop an inventory of its Information. Electronic Information shall be mapped to the hardware (including servers, workstations and laptops) on which such Information resides. The physical location of non-electronic Information, including paper records, shall be identified as part of the inventory. Music City Center will identify owner(s) of such information (Information Owner) shall be identified, recorded and tracked. Such information shall be classified as set forth in the Music City Center Information Classification Policy.

USERS: Team Members should be aware of the Information Classification Policy.

DEPARTMENT AUTHORITY: Ensure Team Members and managements are aware of the Information Classification Policy.

7. Services

Music City Center shall develop and maintain an inventory of its essential services. The inventory for both internally and externally provided and/or required services shall include, but is not limited to, computing, communications services, general utilities (e.g., heating, lighting, power, and air-conditioning), and other general services (e.g., security, shredding services, janitorial, etc.). Those roles responsible for the provisioning of such services shall be identified.

USERS: Team Members should understand what services are provided they provide internally and externally are operational.

DEPARTMENT AUTHORITY: Ensure services are maintained and operational.

- NIST Special Publications 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*: CM-8, CM-9, PM-5
- Music City Center *Information Classification Policy*

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |



CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

POLICY NUMBER:
ISM 11

INFORMATION SECURITY

SUBJECT:

PROTECTION AGAINST MALICIOUS CODE POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to reduce the risk to Music City Center/Metropolitan Government of Nashville and Davidson County assets by protecting against malware.

POLICY

Music City Center/Metropolitan Government of Nashville and Davidson County shall:

- (i) Identify, report, and correct information and system flaws in a timely manner;
- (ii) Provide protection from malicious code at appropriate locations within systems;
- (iii) Monitor system security alerts and advisories and take appropriate actions in response.

1. Malicious Code Protection

1.1. In General

Music City Center/Metropolitan Government of Nashville and Davidson County shall use a variety of controls in order to prevent such threats from exploiting any vulnerability on its Information Systems.

1.2. Enterprise Controls

1.2.1. Principal Risk Mitigation Methods

Music City Center/Metropolitan Government shall:

- a) Employ malicious code protection mechanisms at Information System entry and exit points, including network based anti-malware tools, and at workstations, servers, or mobile devices, where possible, located on the network to detect and eradicate malicious codes that may be:



determine if the exceptions are still needed. Exception requests processing is defined in the *Music City Center/Metropolitan Government Scope, Background and Government Statement for Information Security Policies*.

1.2.2. Additional Risk Mitigation Methods

Information System entry and exit points include firewalls, e-mail servers, web servers, proxy servers, and remote-access servers. A variety of technologies and methods exist to help the Music City Center/Metropolitan Government limit or eliminate the effects of malicious code attacks.

Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect the Music City Center/Metropolitan Government missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, Music City Center/Metropolitan Government shall rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Metropolitan Government shall deploy network access controls (NAC) tools, if available or use another methodology, to verify security configuration and patch level compliance before granting access to a network.

1.2.3. Use of Honeypots

The Music City Center/Metropolitan Government Information Technology System shall include components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. The Music City Center/Metropolitan Government Information Technology System shall include components that proactively seek to identify web-based malicious code. Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots, honey clients or tar pits.

1.2.4. Management of Malicious Code Prevention

Music City Center/Metropolitan Government shall:

- a. Centrally manage malicious code protection mechanisms;
- b. Configure malicious code protection to prevent non-privilege Team Members from circumventing malicious code protection capabilities;
- c. Confirm that the Music City Center/Metropolitan Government Information System updates malicious code protection mechanisms only when directed by a privilege user;
- d. Configure laptops, workstations, and servers so that they will not run auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external SATA devices, mounted network shares, or other Removable Media and configure real-time scanning of files so that an anti-malware scan of content from

2. Mobile Code

2.1. Decisions regarding the employment of mobile code within Music City Center/Metropolitan Government Information Systems are based on the potential for the code to cause damage to the system. Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restriction and implementation guidance shall apply to both the selection and use of mobile code installed on Music City Center/Metropolitan Government servers and mobile code downloaded and executed on individual devices including, but not limited to, workstations, laptops, mobile devices. Policy and procedures related to mobile code shall address preventing the development, acquisitions, or introduction of unacceptable mobile code within the Metropolitan Government Information System(s).

Music City Center/Metropolitan Government shall:

- a. Define acceptable and unacceptable mobile code and mobile code technologies; or block any use of mobile code;
- b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;
- c. Make sure the acquisition, development, and/or use of mobile code to be deployed in Information Technology Systems meet the definitions as set forth in 2.1.a.;
- d. Authorize, monitor, and control the use of mobile code within the Music City Center/Metropolitan Government Information Technology System(s) by:
 - i. Considering protection against mobile code performing unauthorized actions through the use of cryptographic controls to uniquely authenticate mobile code;
 - ii. Preventing the download and execution of prohibited mobile code and the automatic execution of any mobile code. (e.g., Actions required before executing mobile code shall include prompting users prior to opening e-mail attachments.);
 - iii. Implementing detection and inspection mechanisms to identify unacceptable/unauthorized mobile code and take corrective action, when necessary. Such corrective action shall include, but not be limited to, blocking, quarantine, and alerting the appropriate administrator(s); and
 - iv. Disabling Information System functionality that provides the capability for automatic execution of code on mobile devices without user direction.

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 11

SUBJECT:

PROTECTION AGAINST MALICIOUS CODE PLAN

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Team Members, Music City Center and Metropolitan Government of Nashville and Davidson County system administrators, Metro ITS anti-malware solutions administrators, developers, and Information System users.

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the *Protection Against Malicious Code Policy*.

Music City Center/Metropolitan Government of Nashville and Davidson County shall:

- (i) *Identify, report, and correct information and system flaws in a timely manner;*
- (ii) *Provide protection from malicious code at appropriate locations within systems;*
- (iii) *Monitor system security alerts and advisories and take appropriate actions in response.*

1. Malicious Code Protection

1.1. In General

Music City Center/Metropolitan Government of Nashville and Davidson County shall use a variety of controls in order to prevent such threats from exploiting any vulnerability on its



- d) *Send all malware detection events to enterprise wide anti-malware administration tools and event log servers;*
- e) *Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with Music City Center/Metropolitan Government's configuration management policy and procedures and:*
 - i) *Employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis;*
 - ii) *After applying an update, verify that each system, which is automated, has received its signature update;*
 - iii) *Provide method of retrieving signatures form an external source if system does not have access to internal update source;*
 - iv) *Provide a backup of all anti-malware software and signatures for efficient and rapid disaster recovery.*
- f) *Configure malicious code protection mechanisms to:*
 - i) *Perform weekly scheduled scans of Music City Center/Metropolitan Government desktops, laptops and servers and real-time scans of all files on Music City Center/Metropolitan Government systems and external sources as the files are downloaded, created or modified in accordance with the Music City Center/Metropolitan Government security policy; and*
 - ii) *Attempt to clean any detected malicious code from files or infected devices. Unsuccessful attempts to clean will result in deletion of infected file. All malicious code detection will be logged on the client device and be reported to anti-malware technicians; and*
 - iii) *Allow clients to do manual scans of files; and*
 - iv) *Allow clients to manually update anti-malware signatures.*
- g) *Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the Music City Center/Metropolitan Government Information System.*
- h) *Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc.*
- i) *Provide a mechanism for requesting exceptions to the anti-malware scanning settings. These exceptions will be documented and periodically visited to determine if the exceptions are still needed. Exception requests processing is defined in the Music City Center/Metropolitan Government Scope, Background and Government Statement for Information Security Policies.*

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Metro shall use defense in depth when securing all IT resources. End point security is not limited to the anti-malware solutions, but also includes the use of patch management tools and processes. Metro's *Patch and Vulnerability Management Policy* defines how to address patch management. Access controls around the network and data will be based on least privilege, as laid out in the *Acceptable Use of Information Technology Assets Policy*.

- a. Centrally manage malicious code protection mechanisms;
- b. Configure malicious code protection to prevent non-privilege Team Members from circumventing malicious code protection capabilities;
- c. Confirm that the Music City Center/Metropolitan Government Information System updates malicious code protection mechanisms only when directed by a privilege user;
- d. Configure laptops, workstations, and servers so that they will not run auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external SATA devices, mounted network shares, or other Removable Media and configure real-time scanning of files so that an anti-malware scan of content from removable media is done when content is accessed;
- e. Test malicious code protection mechanisms, using the EICAR anti-virus test file monthly on all anti-malware applications. This will be done in order to verify that both detection of the test case and associated incident reporting occur, as required;
- f. Configure protections so that e-mail file attachments, including compressed files, are scanned at the SMTP gateway and that any attachments are not scannable, including encrypted messages and password protected compressed files, are quarantined and e-mail administrator and recipient is notified;
- g. Protect against the sending or receipt of certain types of files (e.g., .exe files) via e-mail from external sources;
- h. Prepare appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements;
- i. Implement procedures to verify Information relating to malicious code and other "warning bulletins" are accurate and informative. Music City Center/Metropolitan Government anti-malware managers shall use qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, to differentiate between hoaxes and real malicious code. All users shall be made aware of the problem of hoaxes and what to do upon receipt of them.

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Metro shall configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external SATA devices, and mounted network shall. Metro shall deploy application level malicious code protection such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply anti-exploitation protections to a broader set of applications and executables.

1.2.5. Team Members Related Requirements

Common malware prevention related policy considers for Team Members include the following:

- a. Team Members are required to scan all media from outside of Music City Center/Metropolitan Government for malware before they can be used;
- b. Team Members are restricted from the use of unnecessary software, such as user applications that are often used to transfer malware (e.g., personal use of external instant messaging, desktop search engine, and peer-to-peer file sharing services), and

- any use of mobile code;*
- b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;*
 - c. Make sure the acquisition, development, and/or use of mobile code to be deployed in Information Technology Systems meet the definitions as set forth in 2.1.a.;*
 - d. Authorize, monitor, and control the use of mobile code within the Music City Center/Metropolitan Government Information Technology System(s) by:*
 - i. Considering protection against mobile code performing unauthorized actions through the use of cryptographic controls to uniquely authenticate mobile code;*
 - ii. Preventing the download and execution of prohibited mobile code and the automatic execution of any mobile code. (e.g., Actions required before executing mobile code shall include prompting users prior to opening e-mail attachments.);*
 - iii. Implementing detection and inspection mechanisms to identify unacceptable/unauthorized mobile code and take corrective action, when necessary. Such corrective action shall include, but not be limited to, blocking, quarantine, and alerting the appropriate administrator(s); and*
 - iv. Disabling Information System functionality that provides the capability for automatic execution of code on mobile devices without user direction.*

USERS: Understand the behavior of malware and how actions can trigger malicious code. Report all suspicious activities to appropriate IT Department.

DEPARTMENT AUTHORITY: Mobile code development, including, but not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, VBScript, and etc. must follow the same guidelines as all application development, as documented in Metropolitan Government security policies.

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

POLICY NUMBER:
ISM 12

INFORMATION SECURITY

SUBJECT:

PATCH AND VULNERABILITY MANAGEMENT POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to ensure Music City Center/Metropolitan Government of Nashville and Davidson County reduces risks resulting from exploitation of published technical vulnerabilities.

POLICY

1. Generally

Music City Center/Metropolitan Government shall:

- a. Ensure all applications are fully supported by the manufacturer;
- b. Maintain all support and maintenance agreements for the lifetime of the application;
- c. Include language in contracts requiring timely updates of applications;
- d. Obtain timely Information about technical vulnerabilities of Information Systems and applications being used;
- e. Evaluate its exposure to such vulnerabilities;
- f. Take appropriate, timely measures to address the associated risk, including patching vulnerabilities.

As set forth below, Music City Center/Metropolitan Government management of technical vulnerabilities is supported through the use of the controls set forth in:

- i) Risk assessment (see Section 2.0 below);
- ii) Vulnerability scanning (see Section 3.0 below);
- iii) Patch management (see Section 4.0 below); and
- iv) Security alerts, advisories and directives (see Section 5.0 below).

2. Vulnerability Risk Assessment

Music City Center/Metropolitan Government shall:



adversaries;

- i. Include privilege access authorization for selected vulnerability scanning activities to facilitate more scanning;
- j. Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in Information System vulnerabilities; and
- k. Employ an independent penetration agent or penetration team to periodically conduct a vulnerability analysis on the Information System as deemed necessary.

Due to the interdependency of the Music City Center/Metropolitan Government network and resources, any vulnerability assessment scan shall be performed in cooperation with the Music City Center/Metropolitan Government Information Technology Services Department and shall follow defined and approved procedures for running such scans.

4. Patch Management and Flaw Remediation

Music City Center/Metropolitan Government shall:

1. Identify, report and correct Information System flaws;
2. Test software updates and patches related to flaw remediation for effectiveness and potential side effects on the Music City Center/Metropolitan Government Information Systems before installation;
3. Incorporate flaw remediation and patch management into its configuration and change management processes;
4. Develop processes for assessing the success and extent of patch management efforts;
5. Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe; and
6. If automated tools cannot be used, develop process for provisioning updates and ensuring updates are deployed.

5. Security Alerts, Advisories and Directives

Music City Center/Metropolitan Government shall:

- a. Receive Information System security alerts, advisories and directives from designated external organizations on an ongoing basis;
- b. Generate internal security alerts, advisories and directives as deemed necessary;
- c. Disseminate security alerts, advisories and directives to appropriate personnel; and
- d. Implement security directives in accordance with established time frames.

6. Miscellaneous

This policy shall supersede all previous Music City Center/Metropolitan Government technical vulnerability management policies. This policy may be amended or revised at any time. Users are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for*

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

POLICY NUMBER:
ISM 12

INFORMATION SECURITY

SUBJECT:

PATCH AND VULNERABILITY MANAGEMENT PLAN

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Music City Center/Metropolitan Government Department Heads, supervisors, information owners, system administrators, and Information System users.

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Patch and Vulnerability Management Policy.

1. Generally

Music City Center/Metropolitan Government shall:

- a. Ensure all applications are fully supported by the manufacturer;*
- b. Maintain all support and maintenance agreements for the lifetime of the application;*
- c. Include language in contracts requiring timely updates of applications;*
- d. Obtain timely Information about technical vulnerabilities of Information Systems and applications being used;*
- e. Evaluate its exposure to such vulnerabilities;*
- f. Take appropriate, timely measures to address the associated risk, including patching vulnerabilities.*

As set forth below, Music City Center/Metropolitan Government management of technical vulnerabilities is supported through the use of the controls set forth in:



Music City Center/Metropolitan Government shall:

- a. *Conduct an assessment of risk from technical vulnerabilities and the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the Information System and the Information it processes, stores or transmit;*
- b. *Update the risk assessment on a defined schedule or whenever there are significant changes to the Information System or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the System; and*
- c. *Establish expected patching timelines based on the risk assessment.*
 - 1) *Patching of security vulnerabilities should be completed as soon as adequate testing has been done to ensure risk of adverse impact due to patch deployment is less than risk of impact from vulnerability exploit.*
 - 2) *Patching of security vulnerabilities should preferably occur within two weeks of patch release.*
 - 3) *Patching addressing vulnerabilities that are being actively exploited should be tested and deployed within forty eight (48) hours.*
 - 4) *Non-security related patches, such as ones that provide additional functionality or address performance issues, should be completed as soon as adequate testing has been done if the issue the patch addresses is being experienced and/or if the additional functionality is desired.*

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Conduct the risk assessment for systems and weigh the risks and associated impact of the risks and determine appropriate course of action.

3. Vulnerability Scanning

Music City Center/Metropolitan Government shall:

- a. *Scan for vulnerabilities in its Information System and hosted applications in accordance with a defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported;*
- b. *Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:*
 - *Enumerating platforms, software flaws and improper configurations; and*
 - *Measuring vulnerability impact using a defined method; and*
 - *Reporting and providing clearly document and defined results; and*
 - *Looks for code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposure entries); and*
 - *Looks for configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).*
- c. *Analyze vulnerability scan reports and results from security control assessments;*
- d. *Remediate legitimate vulnerabilities in accordance with its assessment of risk;*
- e. *Share Information, when appropriate, obtained from the vulnerability scanning processes and security control assessments with designed personnel throughout Music City*

updates are deployed.

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Remediation of technical vulnerabilities involves updates to software, modifications of configurations, etc. These changes to production systems should be treated like any other changes, which should be tested and approved through a change management process. The need to address critical vulnerabilities in a timely manner may shorten the testing time and expedite the change control process.

Remediation attempts should:

- a. Adequately test and evaluate patches before they are installed;
- b. If not patch is available, then use an appropriate combination of the following:
 - i. Turning off services or capabilities;
 - ii. Adapting or adding new controls such as firewalls;
 - iii. Increasing monitoring;
 - iv. Raising awareness of vulnerability;
 - v. Keeping audit logs;
 - vi. Addressing systems at high risk first; and
- c. Be viewed as a sub-function of change management and use change management process procedures.

The use of automated and centrally managed patch management tools and software update tools for operating system and software/applications should be the preferred method of handling patches. This type of infrastructure would provide the ability to test patches prior to deployment, control when patches are deployed, and report of success or failure of patch installation.

If a centrally managed process is not available, then the use of any auto updating capability within the application should be used. Application and system owners should be aware of the risk of auto updating applications and plan accordingly.

If centralized patching and automating are not possible, then a documented process for updating the application should be developed.

5. Security Alerts, Advisories and Directives

Music City Center/Metropolitan Government shall:

- a. *Receive Information System security alerts, advisories and directives from designated external organizations on an ongoing basis;*
- b. *Generate internal security alerts, advisories and directives as deemed necessary;*
- c. *Disseminate security alerts, advisories and directives to appropriate personnel; and*
- d. *Implement security directives in accordance with established time frames.*

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Periodically review approved external organizations list and approve all

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 13

SUBJECT:

CHANGE MANAGEMENT POLICY

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to ensure Music City Center/Metropolitan Government of Nashville and Davidson County (Metropolitan Government) reduces risks to information security caused by changes to information assets and systems. Inadequate control of changes to information assets and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications.

POLICY

1. Generally

Changes to the organization, business processes, information assets and systems that affect information security shall be controlled by the use of formal change control procedures.

Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all applicable changes. When applicable changes are made, an audit log containing all relevant information should be retained.

As set forth below, Music City Center/Metropolitan Government change management processes are supported through the use of the controls set forth in:

- (i) Baseline configuration (see Section 2.1 below);
- (ii) Change control (see Section 2.2 below);
- (iii) Security impact analysis (see Section 2.3 below);
- (iv) Access restrictions for change (see Section 2.4 below);
- (v) Configuration settings (see Section 2.5 below);
- (vi) Least functionality (see Section 2.6 below); and
- (vii) Configuration management plan (see Section 2.7 below).

shall:

- a. Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions, where applicable;
- b. Conduct audits of information assets changes, and when indications so warrant, determine whether unauthorized changes have occurred;
- c. Limit developer/integrator privileges to change hardware, software and firmware components and system information directly within a production environment; and
- d. Review and reevaluate developer/integrator privileges annually.

2.5. Configuration Settings

Music City Center/Metropolitan Government shall:

- a. Establish and document mandatory configuration settings for applicable information technology products using security configuration checklists that reflect the most restrictive mode consistent with operational requirements;
- b. Implement the configuration settings;
- c. Identify, document and approve exceptions from the mandatory configuration settings for individual components based on explicit operational requirements; and
- d. Monitor and control changes to the configuration settings in accordance with Metropolitan Government policies and procedures;
- e. Employ, where possible, automated mechanisms to centrally manage, apply and verify configuration settings;
- f. Employ, where possible, automated mechanisms to respond to unauthorized changes to defined configuration settings;
- g. Incorporate detection of unauthorized security-relevant configuration changes into its incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historically purposes;
- h. Demonstrate conformance to security configuration guidance (i.e., security checklists), prior to change being introduced into a production environment.

2.6. Least Functionality

Music City Center/Metropolitan Government shall configure information assets to provide only essential capabilities and specifically prohibit or restrict the use of designated and documented functions, ports, protocols, and/or services. It shall:

- a. Review information assets to identify and eliminate unnecessary functions, ports, protocols, and/or services; and
- b. Employ automated mechanisms, where possible, to prevent program execution.

2.7. Configuration Management Plan

Music City Center/Metropolitan Government shall develop, document and implement a configuration management plan for information assets that:

- a. Addresses roles, responsibilities and configuration management processes and procedures;

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 13

SUBJECT:

CHANGE MANAGEMENT PLAN

DISTRIBUTION DATE:
5/15/2018

EFFECTIVE DATE:
5/15/2018

ISSUING AUTHORITY:

PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

System Administrators, Data Owners

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Change Management Policy.

1. Generally

Changes to the organization, business processes, information assets and systems that affect information security shall be controlled by the use of formal change control procedures.

Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all applicable changes. When applicable changes are made, an audit log containing all relevant information should be retained.

As set forth below, Music City Center/ Metropolitan Government change management processes are supported through the use of the controls set forth in:

- (i) Baseline configuration (see Section 2.1 below);*
- (ii) Change control (see Section 2.2 below);*
- (iii) Security impact analysis (see Section 2.3 below);*
- (iv) Access restrictions for change (see Section 2.4 below);*

- d. *Retain and review records of controlled changes to the assets and/or system;*
- e. *Audit activities associated with controlled changes to the assets and/or system; and*
- f. *Coordinate and provide oversight for configuration change control activities through a change management committee or change approval board, which convenes weekly.*

USERS: Specify changes and document controls. Give due diligence on affected systems (scheduled maintenance, service outage, etc.)

DEPARTMENT AUTHORITY: Review control documentations and approve changes.

2.3. Security Impact Analysis

Music City Center/Metropolitan Government shall include as part of change control a consideration for any potential security impacts prior to change implementation. Individuals conducting a security impact analysis shall have the appropriate skills and technical expertise to analyze and identify the associated security ramifications.

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Ensure technician has proper skills and expertise. Review and renew training periodically.

2.4. Access Restrictions for Change

Music City Center/Metropolitan Government shall define, document, approve and enforce physical and logical access restrictions associated with changes to the information assets. It also shall:

- a. *Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions, where applicable;*
- b. *Conduct audits of information assets changes, and when indications so warrant, determine whether unauthorized changes have occurred;*
- c. *Limit developer/integrator privileges to change hardware, software and firmware components and system information directly within a production environment; and*
- d. *Review and reevaluate developer/integrator privileges annually.*

USERS: See Department Director for assistance.

DEPARTMENT AUTHORITY: Periodically review access for personnel and modify as necessary with least privileges. Review logs as necessary.

2.5. Configuration Settings

Music City Center/Metropolitan Government shall:

- a. *Establish and document mandatory configuration settings for applicable information technology products using security configuration checklists that reflect the most restrictive mode consistent with operational requirements;*
- b. *Implement the configuration settings;*

USERS: Follow change management plan.

DEPARTMENT AUTHORITY: Implement a change management plan.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
 President/CEO
 Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 10.1.2(ISO 207002 A.12.1.2) (A.14.2.2)
- NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST Special Publication 800-53 rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*: Control numbers – CA-2, CA-7, RA-5, SC-34, SI-4, SI-7, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9
- Center for Internet Security Critical Security Benchmark #4

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|-----------|------------------------|
| 1.0 | 5/15/2018 | First released version |
| | | |

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 14

SUBJECT:

CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING POLICY

DISTRIBUTION DATE:
06/28/2018

EFFECTIVE DATE:
06/28/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this policy is to help the Music City Center/Metropolitan Government improve its security posture by the sharing of cyber threat information within the Music City Center/Metropolitan Government, consuming and using cyber threat information received from external sources, and producing cyber threat information that can be shared with other organizations. This policy also defines specific considerations for participation in information sharing communities.

POLICY

1. Generally

The Music City Center/Metropolitan Government shall develop processes to facilitate the dissemination of cyber threat intelligence and the sharing of cyber threat information with external entities and partners in an effort to improve the security postures of the cyber community as a whole. By exchanging cyber threat information within a sharing community, Metropolitan Government can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats Metropolitan Government may face. Using this knowledge, Music City Center/Metropolitan Government can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies.

2. Detailed

2.1. Music City Center/Metropolitan Government shall identify and document resources to be used to keep informed about information security threats. This cyber threat information should include: indicators of compromise; tactics, techniques, and procedures (TTPs) used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents.

2.2. Music City Center/Metropolitan Government shall identify and document resources to be used to keep informed about information security vulnerabilities and obtain timely information about technical vulnerabilities of information systems and applications being used.



REVISION HISTORY

| REVISION | DATE | CHANGES |
|-----------------|-------------|------------------------|
| 1.0 | 06/28/2018 | First released version |
| | | |

CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 14

SUBJECT:

CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING PLAN

DISTRIBUTION DATE:
06/28/2018

EFFECTIVE DATE:
06/28/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

Music Center Department Directors, Supervisors, Managers, Team Members, and IT Personal

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Cyber-Threat Intelligence and Information Sharing Policy.

1. Generally

The Music City Center/Metropolitan Government shall develop processes to facilitate the dissemination of cyber threat intelligence and the sharing of cyber threat information with external entities and partners in an effort to improve the security postures of the cyber community as a whole. By exchanging cyber threat information within a sharing community, Metropolitan Government can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats Metropolitan Government may face. Using this knowledge, Music City Center/Metropolitan Government can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies.

2. Detailed

2.1. Music City Center/Metropolitan Government shall identify and document resources to be used to keep informed about information security threats. This cyber threat information should include: indicators of compromise; tactics, techniques, and procedures (TTPs) used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from

types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organization. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

- **Tool configurations** are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

After identifying these resources, departments should document who is responsible for monitoring these resources, how often these resources are monitored and how this information should be shared with any IT service providers. Department should develop processes to:

- receive information system security alerts, advisories and directives from designated external organizations on an ongoing basis;
- generate internal security alerts, advisories and directives as deemed necessary; and
- disseminate security alerts, advisories and directives to appropriate personnel.

The Metropolitan Department of Information Technology Services (ITS) will share information they collect from partners to users designated as IT Community Contacts. Departments are responsible for communicating to ITS any additional recipients.

- 2.2. *Music City Center/Metropolitan Government shall identify and document resources to be used to keep informed about information security vulnerabilities and obtain timely information about technical vulnerabilities of information systems and applications being used.*
- 2.3. *Music City Center/Metropolitan Government shall develop methods for producing and sharing threat information internally. This information should be used to remediate risk and respond to threats.*

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: Metropolitan Government will establish a central location to host cyber threat intelligence and provide access to appropriate Metropolitan Government staff.

- 2.4. *Music City Center/Metropolitan Government shall identify appropriate contacts with special interest groups or other specialist security forums and maintain professional associations as a source of security information. External information sharing agreements should be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information. Sensitive Information shall not be shared as part of any information sharing agreements.*

USERS: Seek Department Authority for assistance.

DEPARTMENT AUTHORITY: Departments should identify and take advantage of memberships

exchange of cyber threat information. As internal cyber threat information sources and capabilities are identified, Departments should determine how information from these sources currently support cybersecurity and risk management activities. Departments should identify threat information that is available and suitable for sharing with outside parties.

- Specify the scope of information sharing activities. Information sharing efforts should focus on activities that provide the greatest value to Metropolitan Government and its sharing partners. The scoping activity should identify types of information that Metro authorize for sharing, the circumstances under which sharing of this information is permitted, and those with whom the information can and should be shared.
- Establish information sharing rules. Sharing rules are intended to control the publication and distribution of threat information, and consequently help to prevent the dissemination of information that, if improperly disclosed, may have adverse consequences for an organization, its customers, or its business partners. Information sharing rules should take into consideration the trustworthiness of the recipient, the sensitivity of the shared information, and the potential impact of sharing (or not sharing) specific types of information.
- Proactively establish cyber threat sharing agreements. Rather than attempting to establish sharing agreements during an active cyber incident, Departments should plan ahead and have agreements in place before incidents occur. Such advanced planning helps ensure that participating organizations establish trusted relationships and understand their roles, responsibilities, and information handling requirements.
- Protect the security and privacy of sensitive information. Sensitive information such as personally identifiable information (PII) may be encountered when handling cyber threat information. The improper disclosure of such information could cause financial loss; violate laws, regulations, and contracts; be cause for legal action; or damage an organization's or individual's reputation. Accordingly, organizations should implement the necessary security and privacy controls and handling procedures to protect this information from unauthorized disclosure or modification.
- Provide ongoing support for information sharing activities. Departments should establish an information sharing plan that provides for ongoing infrastructure maintenance and user support. The plan should address the collection and analysis of threat information from both internal and external sources and the use of this information in the development and deployment of protective measures. A sustainable approach is necessary to ensure that resources are available for the ongoing collection, storage, analysis, and dissemination of cyber threat information.

Consuming and Responding to Security Alerts

An information sharing community may publish security alerts notifying community members of emerging vulnerabilities, exploits, and other security issues. Fields that commonly appear in security alerts such as US-CERT alerts, NVD vulnerability

- analysts and slows down prioritization and categorization actions.
- **Accuracy.** Indicators should be correct, complete, and unambiguous. Inaccurate or incomplete information introduces uncertainty and may prevent critical action, stimulate unnecessary action, result in ineffective responses, or instill a false sense of security. Recipients should be made aware of any uncertainty or caveats regarding the accuracy of an indicator.
 - **Specificity.** Indicators should provide clear descriptions of observable events that recipients can use to detect threats while minimizing false positives/negatives.
 - **Actionable.** Indicators should provide enough information and context to allow recipients to develop a suitable response. Possible responses to externally and internally-generated indicators include:
 - Add or modify rules or signatures used by firewalls, intrusion detection systems, data loss prevention systems, and/or other security controls to block or alert on activity matching the indicators (for example, connections involving IP addresses on a blacklist);
 - Configure security information and event management solutions or other log management-related systems to help with analysis of security log data;
 - Scan security logs, systems, or other sources of information, using indicators as search keys, to identify systems that may have already been compromised;
 - Find matching records when investigating an incident or potential incident to learn more about a threat, and to help hasten incident response and recovery actions;
 - Provide additional information to security team;
 - Educate staff on threat characteristics; and
 - Identify threat trends that may suggest changes to security controls are needed.

Music City Center/Metropolitan Government should carefully consider the characteristics of indicators and should take a risk-based approach to determining how indicators can be most effectively used.

**CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

INFORMATION SECURITY

POLICY NUMBER:
ISM 15

SUBJECT:

AUDIT, MONITORING AND LOGGING POLICY

DISTRIBUTION DATE:
06/28/2018

EFFECTIVE DATE:
06/28/2018

ISSUING AUTHORITY:

**PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this Policy is to help the Music City Center/Metropolitan Government provide accurate and comprehensive audit logs in order to detect and react to inappropriate and unauthorized activities. This document addresses the creation, protection, and retention of Information System audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity within the Information and how the actions of individual Information System users can be uniquely traced to those users so they can be held accountable for their actions. The level of logging, auditing and monitoring shall be commiserate to the security required for the Information System.

POLICY

1. Generally

Music City Center/Metropolitan Government shall, where applicable:

- 1.1. Assess the Information System and determine the appropriate level of logging, auditing and monitoring that shall be in place, as commiserate to the classification of the data collected, stored or processed, to the criticality of the service provided by the Information System and to meet any regulatory or legal requirements;
- 1.2. Produce audit logs recording user activities, exceptions and information security events and keep them for an agreed period to assist in future investigations and access control monitoring;
- 1.3. Establish procedures for monitoring use of information processing facilities and regularly review results of the monitoring activities;
- 1.4. Protect logging solutions and log information against tampering and unauthorized access;
- 1.5. Log system administrator and system operator activities;
- 1.6. Log, analyze and take appropriate action regarding faults; and



The Music City Center/Metropolitan Government shall assess Information Systems capability of producing necessary audit logs based on business need.

5. Audit Storage Capacity

Music City Center/Metropolitan Government shall allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded. It also shall consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

6. Response to Audit Processing Failures

The Information System shall, if possible:

- 6.1. Alert designated Music City Center/Metropolitan Government staff in the event of an audit processing failure; and
- 6.2. Take the appropriate, applicable additional action, including, but not limited to: shut down Information System, overwrite oldest audit records, and stop generating audit records.

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

7. Audit Review, Analysis and Reporting

Music City Center/Metropolitan Government shall:

- 7.1. Review and analyze Information System audit records for indications of inappropriate or unusual activity, and report findings to designated Metropolitan Government officials; and
- 7.2. Adjust the level of audit review, analysis, and reporting within the Information System when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Music City Center/Metropolitan Government shall, if possible, integrate/correlate:

- a. Audit review, analysis and reporting processes to support organizational processes for investigation and response to suspicious activities; and
- b. Analyze audit records of vulnerability scanning information, performance data and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

8. Time Stamps

The Information System shall use internal system clocks to generate time stamps for audit records. Those clocks shall be configured to use a Music City Center/Metropolitan Government approved time source.

9. Audit Record Retention

Music City Center/Metropolitan Government shall retain audit records for an appropriately

where capable.

15. Flaw Remediation

Music City Center/Metropolitan Government shall, among other things, expeditiously address flaws discovered during security assessments, continuous monitoring, incident response activities, or Information System error handling.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Music City Center Information Security Glossary*.

CONTACT

Questions should be directed to (615) 401-1479 or by email at mcchelpdesk@nashvillemcc.com, or by mailing them to Director of Technology, Music City Center, 201 5th Avenue South, Nashville, TN 37203.

SIGNATURE



Charles L. Starks,
President/CEO
Convention Center Authority of Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 10.10.1-6, 10.3.1, 15.1.3
- NIST Special Publication 800-92, *Guide to Computer Security Log Management*
- NIST Special Publication 800-53 rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*: Control numbers – SI-1,AU-1, AU-4, AU-5, PE-6, PE-8, SC-7, AU-9, SI- 2, AU-2(4), AU-3(1, 2), AU-12(2), AU-6(1), AU-6(5), AU-7, AU-8, SI-4(1), SI-4(8), SI-4(11), SI-4(14), SI-4(4), SI-4(5)

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|------------|------------------------|
| 1.0 | 06/28/2018 | First released version |
| | | |



CONVENTION CENTER AUTHORITY OF THE METROPOLITAN
GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY

POLICY NUMBER:
ISM 15

SUBJECT:

AUDIT, MONITORING AND LOGGING PLAN

DISTRIBUTION DATE:
06/28/2018

EFFECTIVE DATE:
06/28/2018

ISSUING AUTHORITY:

PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

EXPIRATION: UNTIL
RESCINDED

AUDIENCE

[CONTENT]

PURPOSE

The purpose of this Information Security Plan is to promote compliance of the referenced Information Security Policy by providing direction and congruity between it and multiple Music City Center departmental procedures. The Information Security Plan acts as a bridge between one enterprise policy and one or more departmental procedures and provides guidance for creation of departmental policies if none exist.

PLAN

Each heading matches with the applicable heading found in the Audit, Monitoring and Logging Policy.

1. Generally

Music City Center/Metropolitan Government shall, where applicable:

- 1.1. *Assess the Information System and determine the appropriate level of logging, auditing and monitoring that shall be in place, as commiserate to the classification of the data collected, stored or processed, to the criticality of the service provided by the Information System and to meet any regulatory or legal requirements;*
- 1.2. *Produce audit logs recording user activities, exceptions and information security events and keep them for an agreed period to assist in future investigations and access control monitoring;*
- 1.3. *Establish procedures for monitoring use of information processing facilities and regularly review results of the monitoring activities;*
- 1.4. *Protect logging solutions and log information against tampering and unauthorized access;*
- 1.5. *Log system administrator and system operator activities;*
- 1.6. *Log, analyze and take appropriate action regarding faults; and*

Items Departments must address for audit logs include:

- Access to Information Systems and data, as well as significant system and security events, must be logged by the Information System.
- Audit logs must be protected from unauthorized access or modification.
- Audit logs must be retained for an appropriate period of time, based on any document retention schedules, such as approved Records Disposition Authorizations, legal, regulatory or business requirements. Audit logs that have exceeded this retention period should be destroyed.
- Logging should include creation, access, modification and deletion activities.
- Log files should be regularly examined for access control discrepancies, breaches, and policy violations.
- Departments are responsible for developing appropriate processes for monitoring and analyzing their logs.
- System activity review cycles should include review of audit logs at a defined period and may include daily review based on departmental needs.
- For servers, audit logs/records should be backed up no less than weekly onto a different Information System or media than the system being audited and logs should be deleted at the appropriate time.
- System administrators should not have the ability to modify audit trails.
- Departmental system administrators and Information Owners should work together to identify opportunities to automatically alert to suspicious activity that is logged.

2. Security Auditable Events

Music City Center/Metropolitan Government shall:

- 2.1. *Determine, based on a risk assessment and mission/business needs, that the Information System must be capable of auditing the appropriate events as deemed necessary;*
- 2.2. *Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;*
- 2.3. *Determine, based on current threat information and ongoing assessment of risk, that the appropriate events are to be audited within the Information System;*
- 2.4. *Review and update the list of auditable events on a periodic basis or as required by changes to the Information System; and*
- 2.5. *Include execution of privileged functions in the list of events to be audited by its Information System.*

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Audit information (what to audit, where to store, how long to store) should be identified and documented at the initiation of any IT based project. The purpose of security audit logging is for Departments to identify events which need to be

requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

At a minimum, an audit record should include:

- Date and time of the event
- Component of the Information System (e.g., software component, file, hardware component) where the event (i.e., accessed, modified, or deleted) occurred
- Source or location of event, if applicable
- Destination of event, if applicable
- Type of event
- User identity
- Outcome (success or failure) of the event
- Any attempt to clear the audit logs

The level and content of security monitoring, alerting and reporting needs to be set during the requirements and design stage of projects, and should be proportionate to the information security risks. This can then be used to define what should be logged. There is no one size fits all solution, and a blind checklist approach can lead to unnecessary "alarm fog" that means real problems go undetected. Where possible, always log:

- Input validation failures e.g. protocol violations, unacceptable encodings, invalid parameter names and values
- Output validation failures e.g. database record set mismatch, invalid data encoding
- Authentication successes and failures
- Authorization (access control) failures
- Session management failures e.g. cookie session identification value modification
- Application errors and system events e.g. syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection, configuration changes
- Application and related systems start-ups and shut-downs, and logging initialization (starting, stopping or pausing)
- Use of higher-risk functionality e.g. network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads
- Legal and other opt-ins e.g. permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Logging functionality and systems should be included in code review, application testing and security verification processes. To meet this control, Departments should:

- Ensure the logging is working correctly and as specified
- Check events are being classified consistently and the field names, types and lengths are correctly defined to an agreed upon standard by the Department and any service provider
- Ensure logging is implemented and enabled during application security, fuzz, penetration and performance testing
- Test the mechanisms are not susceptible to injection attacks by attempting to modify the logs outside of normal processes
- Ensure there are no unwanted side-effects when logging occurs, such as resource exhaustion, which can occur when debug logging is turned on
- Check the effect on the logging mechanisms when external network connectivity is lost (if this is usually required)
- Ensure logging cannot be used to deplete system resources, for example by filling up disk space or exceeding database transaction log space, leading to denial of service
- Test the effect on the application of logging failures such as simulated database connectivity loss, lack of file system space, missing write permissions to the file system, and runtime errors in the logging module itself
- Verify access controls on the event log data
- If log data is utilized in any action against users (e.g. blocking access, account lock-out), ensure this cannot be used to cause denial of service (DoS) of other users
- Configure systems to alert the appropriate staff in the event of an audit failure.

7. Audit Review, Analysis and Reporting

Music City Center/Metropolitan Government shall:

- 7.1. *Review and analyze Information System audit records for indications of inappropriate or unusual activity, and report findings to designated Music City Center/Metropolitan Government officials; and*
- 7.2. *Adjust the level of audit review, analysis, and reporting within the Information System when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.*

Music City Center/Metropolitan Government shall, if possible, integrate/correlate:

- a. *Audit review, analysis and reporting processes to support organizational processes for investigation and response to suspicious activities; and*
- b. *Analyze audit records of vulnerability scanning information, performance data and*

ensuring those records are retained appropriately and disposing of records securely when records are no longer required.

10. Protection of Audit Information

The Music City Center/Metropolitan Government shall take necessary steps to protect audit logs, including limiting access to appropriate personnel, backing up logs and alerting to log deletion/clearing.

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Audit records, audit settings, and audit reports must be protected from unauthorized access, modification, and deletion.

Access to audit information must be restricted to appropriate staff, including those authorized to perform IT Security Audits and/or investigate security incidents. Audit information must not be accessible for modification by end-users of the resource.

Regular backup and archival processes should be defined for audit files in order to protect historical log data and collect new log data processed by the server.

11. Non-repudiation

Music City Center/Metropolitan Government Information System shall:

- 11.1. *Protect against an individual falsely denying having performed a particular action; and*
- 11.2. *Associate the identity of the information producer with the information.*

USERS: Seek Department Authority.

DEPARTMENT AUTHORITY: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Logs generated should have the ability to track activity to a specific entity, such as a user account.

12. Monitoring for Information Disclosure

Music City Center/Metropolitan Government shall identify and monitor intelligence sources, including open source information, for evidence of unauthorized exfiltration or disclosure of organizational information.

USERS: Seek Department Authority.

includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications.

The granularity of the information collected is determined by Departments based on its monitoring objectives and the capability of the Information System to support such activities.

Music City Center/Metropolitan Government should purchase, configure and deploy intrusion detection tools where possible and minimally at the network perimeter. Music City Center/Metropolitan Government should employ automated tools to support near real-time analysis of events and checks for unusual/unauthorized activities. Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an Information System or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or Information System components.

Departments should ensure that information systems are capable of providing near real-time alerts when indications of compromise or potential compromise occur. Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

Metropolitan Government should analyze outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.

Metropolitan Government should employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

In addition to the above, Departments should develop procedures and assess and configure monitoring and alerting functions within information systems to:

- Monitor inbound and outbound communications for unusual or unauthorized activities or conditions, such as users being added to administrative groups or services being disabled;
- Alert appropriate personnel of suspicious events;
- Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- Test/exercise monitoring capabilities at a defined, documented frequency;

SI- 2, AU-2(4), AU-3(1, 2), AU-12(2), AU-6(1), AU-6(5), AU-7, AU-8, SI-4(1), SI-4(8), SI-4(11), SI-4(14), SI-4(4), SI-4(5)

REVISION HISTORY

| REVISION | DATE | CHANGES |
|----------|------------|------------------------|
| 1.0 | 06/28/2018 | First released version |
| | | |

| | |
|--|--|
| <p>CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> <p>INFORMATION SECURITY</p> | <p>POLICY NUMBER: ISM</p> |
| <p>SUBJECT:</p> <p>MUSIC CITY CENTER INFORMATION SECURITY GLOSSARY</p> | <p>DISTRIBUTION DATE: 5/15/2018</p> <p>EFFECTIVE DATE: 5/15/2018</p> |
| <p>ISSUING AUTHORITY:</p> <p>PRESIDENT/CEO OF THE CONVENTION CENTER AUTHORITY OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY</p> | <p>EXPIRATION: UNTIL RESCINDED</p> |

PURPOSE

Music City Center/Metropolitan Government has implemented an Information Security Management program per Executive Order No. 038. A core component of this program is a set of information security policies based on international standards. This document provides specific definitions for information security terminology used in Music City Center/Metropolitan Government’s information security policies.

CONTENT

The glossary was created initially with those terms deemed common to the Music City Center/Metropolitan Government Information Security Management program policies, plans, and other documents. The definitions are taken from a variety of industry standard sources, as indicated at the end of each definition.

As policies and plans are developed by work groups, new definitions may be added. These definitions may also come from industry standard sources, or may be fashioned by the work group or the Music City Center Technology Department, for which the work group or Department is credited as the source at the end of the definition.

Definitions added by work groups are voted on for inclusion to this document by the Metropolitan Government Information Security Steering Committee or agreed upon by Music City Center Technology Department.

SCOPE, BACKGROUND AND GOVERNANCE

This information is set forth in the *Music City Center Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Access –Ability to make use of any information system (IS) resource. SOURCE: SP 800-32 Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system



Alternate Work Site – Organization-wide, program allowing employees to work at home or at geographically convenient satellite offices for part of the work week (e.g., telecommuting). SOURCE: CNSSI-4009

Antivirus Signatures - A catalog of data that describes the current Malicious Software threats (e.g., virus, worms, spyware) and how Antivirus Software is to detect and remove the threat from the given system, message or file. SOURCE: SP 800-83

Antivirus Software – A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. SOURCE: SP 800-83

Application – The use of information resources (information and information technology) to satisfy a specific set of user requirements. SOURCE: SP 800-37 Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. SOURCE: CNSSI-4009

Application Developer - manage all aspects of the application development process for those business applications that support the administrative or operational functions of the company or the applications needed to serve customers effectively. SOURCE: Separation of Test, Development, and Production Environments workgroup (added per ISSC July 8, 2011)

Application Tester - uses and tests software for the purpose of locating and eliminating bugs in the product. Performing specific tests, they examine all aspects of a product from an end-user's perspective. SOURCE: Separation of Test, Development, and Production Environments workgroup (added per ISSC July 8, 2011)

Approved User Owned Devices – any Device owned by a User, where connection to the non-public Network by the User using that Device has been approved by the President/CEO. SOURCE: Acceptable Use Policy Work Group

Archived Data - Information that is retained solely for backup or archival purposes in accordance with backup policies. SOURCE: SP 800-83

ASP - "Application Service Provider". SOURCE: SP 800-83

Asset - Any item that is purchased by, owned by, leased to, contracted by, operated by, used by, controlled by, given to, supplied by, or in any other matter connected to Metropolitan Government. This includes everything from information on paper to enterprise computing systems, databases and networks. SOURCE: Acceptable Use Policy Work Group

Attack – Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. SOURCE: CNSSI-4009

Audit – Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. SOURCE: CNSSI-4009

Audit Log – A chronological record of system activities. Includes records of system accesses and

Banner – Display on an information system that sets parameters for system or data use. SOURCE: CNSSI-4009

Baseline – Hardware, software, databases, and relevant documentation for an information system at a given point in time. SOURCE: CNSSI-4009

Board – A board of Metropolitan Government.

Boundary – Physical or logical perimeter of a system. SOURCE: CNSSI-4009

Boundary Protection – Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). SOURCE: CNSSI-4009

Buffer Overflow – A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. SOURCE: SP 800-28; CNSSI-4009

Business Associate Agreement (BAA) - A Business Associate Agreement is a written contract or other document between a Covered Entity and an individual or corporate “person” that: performs on behalf of the covered entity any function or activity involving the use or disclosure of Protected Health Information (PHI); and is not a member of the covered entity’s workforce. A BAA *does not* apply to disclosures by a covered entity to a health care provider for treatment purposes disclosures to the plan sponsor by a group health plan, or a health insurance issuer or HMO with respect to a group health plan, nor to the collection and sharing of PHI by a health plan that is a public benefits program and an agency other than the agency administering the health plan, in order to determine eligibility or enrollment.

The Business Associate Agreement (BAA) must detail permitted activities and disclosures for all Protected Health Information (PHI), and must also provide that the business associate will: not use or further disclose the PHI other than as permitted by the contract or as required by law; use appropriate safeguards to prevent unauthorized use or disclosure of the PHI, report to the covered entity any unauthorized use or disclosure of which it becomes aware; ensure that any agents, including subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to the business associate and ; on termination of the contract, return or destroy all PHI in its possession, or where that is not possible, extend the protections of the contract for as long as the information is retained.

Business Continuity Plan (BCP) – The documentation of a predetermined set of instructions or procedures that describe how an organization’s business functions will be sustained during and after a significant disruption. SOURCE: SP 800-34; CNSSI-4009

Cardholder Data - Data as defined by the Payment Card Industry (PCI) Security Standard Council, which is the full magnetic stripe, or the Primary Account Number (PAN) plus any of the following:

- Cardholder name,
- Expiration date, or
- Service Code (Capitalized terms in this definition have the meanings set forth in the PCI Data

Contractor Managed System - Any system, device or application which is owned, leased or rented by Metro Government or its Affiliates, which is managed or administered by Contractor on behalf of Metro Government or its Affiliates, and, any Contractor-owned systems which reside on the Metro Government IT Network and managed or administered by Contractor. SOURCE: Metro Government Legal Department

Cookie – A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. SOURCE: SP 800-28

Countermeasure – Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. SOURCE: CNSI-4009

Critical Business Information – vital Information, without which Music City Center could suffer serious financial, legal or other damages or penalties and/or incur a disruption of services. SOURCE: Acceptable Use Policy Work Group

Critical Security Patch - Security Patch that mitigates or remedies a Critical Vulnerability.

Critical Vulnerability - Vulnerability that would allow an individual or system without access rights or proper credentials to gain administrative-like access to a IT Product or Service or to data contained therein or whose exploitation could allow code execution without user interaction. For example, a compromise that would allow authorized unfettered or administrative-like access, include without limitation, administrative access to the IT Product or Service, full access or control of a data store, and/or the ability to alter Audit Logs. Determination of “Critical” is determined by the vendor’s assessment of the vulnerability or of a Common Vulnerability Scoring System base score of “high”. SOURCE: SP 800-83

Cryptographic – Pertaining to, or concerned with, cryptography. SOURCE: CNSI-4009

Cryptographic Controls - A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the control. SOURCE: Policy 10.4

Cryptographic Key – A parameter used in conjunction with a cryptographic algorithm that determines (1) the transformation of plaintext data into ciphertext data; (2) the transformation of ciphertext data into plaintext data; (3) a digital signature computed from data, (4) the verification of a digital signature computed from data; (5) an authentication code computed from data; or (6) an exchange agreement of a shared secret. SOURCE: FIPS 140-2

Cryptographic Module – The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. SOURCE: FIPS 140-2

Cryptography – Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. SOURCE: CNSI-

capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). SOURCE: CNSSI-4009

Distribution Date – The date of policy release to department heads. SOURCE: ISSC

Domain – A set of subjects, their information objects, and a common security policy. SOURCE: SP 800-27 An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See also security domain. SOURCE: CNSSI-4009; SP 800-53

Education (Information Security) – Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and strive to produce IT security specialists and professionals capable of vision and proactive response. SOURCE: SP 800-50

Effective Date – The date employees and departments are responsible for full policy compliance and accountable for deviations. SOURCE: ISSC

Electromagnetic Signals Emanation – Unintentional signal or noise appearing external from equipment that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any information processing equipment. SOURCE: Secured Areas Policy Work Group

Electronic Protected Health Information - “E PHI” means PHI as defined in 45 C.F.R. 160.103 of the HIPAA regulations in electronic form. SOURCE: Metro Government Legal Department

Electronic Signature – The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature. SOURCE: CNSSI-4009

Email - Any means of electronic communication transmitted under Simple Mail Transfer Protocol (SMTP), or a similar protocol, in which (a) usually text and/or attachments are transmitted, (b) operations include sending, storing, processing, and receiving information, (c) Users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee. SOURCE: Acceptable Use Policy Work Group

Emanations Security (EMSEC) – Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system. See TEMPEST. SOURCE: CNSSI-4009

Encryption – Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. SOURCE: FIPS 185

Enterprise Architecture (EA) – The description of an enterprise’s entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture. SOURCE: CNSSI-4009

Exception - Any approved action that does not normally comply with Metropolitan Government policies, standards and practices. SOURCE: Acceptable Use Policy Work Group

Hardware – The physical components of an information system. See software and firmware. SOURCE: CNSSI-4009

Head – A head of a Metropolitan Government department or agency.

HIPAA - Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations related thereto. SOURCE: Metro Government Legal Department

Honeypot - A mechanism set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems, generally consisting of a computer, data, or a network site that appears to be part of a network, but is actually isolated, unprotected, and monitored, and which seems to contain information or a resource of value to attackers. SOURCE: Policy 10.4

IAAS - “Infrastructure As A Service.” SOURCE: SP 800-83

Identification – The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. SOURCE: SP 800-47

Identifier – Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers. SOURCE: FIPS 201

Identity – The set of physical and behavioral characteristics by which an individual is uniquely recognizable. SOURCE: FIPS 201

Inappropriate Usage – A person violating acceptable computing use policies. SOURCE: SP 800-61

Important Security Patch - A Security Patch that mitigates or remedies an Important Vulnerability.

Important Vulnerability - A Vulnerability in the IT Product or Service that would allow a user who already had access to the IT Product or Service to obtain unauthorized access rights or compromise the IT Product or Service in some way or whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. Determination of “Important” is determined by the vendor’s assessment of the vulnerability or of a Common Vulnerability Scoring System base score of “medium”. SOURCE: SP 800-83

Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. SOURCE: FIPS 200; SP 800-53; SP 800-53A

Incident Handling – The mitigation of violations of security policies and recommended practices. SOURCE: SP 800-61

Information – An instance of an information type. SOURCE: FIPS 200; FIPS 199; SP 800-60; SP 800-53. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. SOURCE: CNSSI-4009

Interconnection Security Agreement (ISA) – A document that regulates security-relevant aspects of an intended connection between a department, agency or board and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal memorandum of understanding/agreement that defines high-level roles and responsibilities in management of a cross-domain connection. SOURCE: CNSSI-4009

Interface – Common boundary between independent systems or modules where interactions take place. SOURCE: CNSSI-4009

Internet – The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). SOURCE: CNSSI-4009

Intrusion – Unauthorized act of bypassing the security mechanisms of a system. SOURCE: CNSSI-4009

Intrusion Detection Systems (IDS) – Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.) SOURCE: CNSSI-4009

Intrusion Prevention System - A network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. SOURCE: Policy 10.4

Key – A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. SOURCE: SP 800-63

Key Management – The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. SOURCE: FIPS 140-2; CNSSI-4009

Layered Protection – See Defense in Depth. SOURCE: Security in Development and Support Processes Work Group

Least Privilege – The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. SOURCE: CNSSI-4009

Logical Locks - The prevention of User access to data that is provided through the use of software, as opposed to physical locks. SOURCE: NIST SP800-43

Malicious Code and Software - A program that is written intentionally to carry out annoying or harmful actions, which includes Trojan horses, viruses, and worms. SOURCE: Policy 10.4

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of

Network Access – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). SOURCE: SP 800-53; CNSSI-4009

NIST - National Institute of Standards and Technology. SOURCE: SP 800-83

Non-repudiation – Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. SOURCE: SP 800-53; SP 800-53A; SP 800-60; SP 800-18

Off-the-Shelf Software or “OTS” – An item that is (1) sold, leased, or licensed to the general public; (2) offered by a Contractor trying to profit from it; (3) supported and developed by the Contractor who retains the underlying intellectual property rights; (4) available in multiple, identical copies; and (5) used without modification of the internal code.

Open IT Network - Any open, unsecured or untrusted network such as the Internet. SOURCE: SP 800-83

Open Source Software - Software that is licensed pursuant to the provisions of any "open source" license agreement including, without limitation, any version of any software licensed pursuant to any GNU General Public License (GNU GPL) or GNU Lesser/Library Public License (LGPL), or Mozilla Public License (MPL), or any other license agreement that requires source code be distributed or made available in connection with the distribution of the licensed software in object code form or that limits the amount of fees that may be charged in connection with sublicensing or distributing such licensed software. SOURCE: SP 800-83

Organization – An entity of any size, complexity, or positioning within an organizational structure. SOURCE: SP 800-53

Packet Sniffer – Software that observes and records network traffic. SOURCE: SP 800-61; CNSSI-4009

Password – A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. SOURCE: CNSSI-4009

Patch Management – The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. SOURCE: CNSSI-4009

Peer-to-Peer File Sharing Software -

- Means a program, application, or software that is commercially marketed or distributed to the public and that enables a file or files on the computer on which such program is installed to be designated as available for searching and copying to one or more other computers;
 - the searching of files on the computer on which such program is installed and the copying of any such file to another computer;
 - at the initiative of such other computer and without requiring any action by an owner or authorized user of the computer on which such program is installed; and
 - without requiring an owner or authorized user of the computer on which such program is installed to have selected or designated another computer as the recipient of any

Principle of Least Privilege - The principle that security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. SOURCE: SP 800-83

Privilege – A right granted to an individual, a program, or a process. SOURCE: CNSSI-4009

Privileged User – A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform. SOURCE: SP 800-53; SP 800-53A; CNSSI-4009; Confidential Agreements Work Group

Product - Any software, hardware, system, computer equipment or product provided by Contractor to Metro Government. SOURCE: Metro Government Legal Department

Product and Service Inventory - A complete, accurate and current inventory of all IT Products and Services provided by Contractor to Metro Government. SOURCE: Metro Government Legal Department

Protected Health Information or “PHI” - Shall have the meaning set forth at 45 C.F.R. 160.103 of the HIPAA regulations.

Procedures – The steps that need to be performed to meet standards and comply with the Metropolitan Government Information Security Management Policy. There are typically many procedures in place to maintain compliance. SOURCE: Executive Order No. 038

Program – The Metropolitan Government Information Security Management Program. SOURCE: Executive Order No. 038

Protocol – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information. SOURCE: CNSSI-4009

Proxy – An application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. SOURCE: CNSSI-4009

Purchasing Agreement - Any agreement between Contractor and any Metro Government for the purchase, lease, licensing, acquisition, or servicing of an IT Product or provision of Services, regardless whether Metro Government has any payment obligations under the agreement. SOURCE: Metro Government Legal Department

Remediation – The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. SOURCE: SP 800-40 The act of mitigating a vulnerability or a threat. SOURCE: CNSSI-4009

Remote Access – Access to an organizational information system by a user (or an information system

Risk Tolerance – The level of risk an entity is willing to assume in order to achieve a potential desired result. SOURCE: SP 800-32 The defined impacts to an enterprise’s information systems that an entity is willing to accept. SOURCE: CNSSI-4009

Risk Transfer – Sharing with another party the burden of loss or benefit of gain from a particular risk. NOTE In the context of information security risks, only negative consequences (losses) are considered for a risk transfer. SOURCE: ISO/IEC 27002

Risk Treatment - Process of selection and implementation of measures to modify risk. SOURCE: ISO/IEC 27002

Role – A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. SOURCE: CNSSI-4009

SaaS - “Software as a service” or “software on demand”. SOURCE: SP 800-83

Safeguards – Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. SOURCE: SP 800-53; SP 800-53A; SP 800-18; FIPS 200; CNSSI- 4009

Sanitization (Sanitize) – Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. SOURCE: FIPS 200

Secure Area – A facility, or an area, room, or group of rooms within a facility with both the physical and personnel security controls sufficient to protect information systems, equipment, and/or information. SOURCE: Adapted from the Criminal Justice Information Services Security Policy

Security – A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. SOURCE: CNSSI-4009

Security Assessment – The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. SOURCE: SP 800-53A

Security Attribute – An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy. SOURCE: SP 800-53; CNSSI-4009

Service(s) - Any service provided by Contractor (or its Contractor Agents) to Metro Government, including but not limited to, maintenance and support service, program development service, consulting service, outsourcing service, or other professional service. SOURCE: CNSSI-4009

Session Timeout - A security control or function that automatically logs a user off and ends the current use session of the IT Product after a defined period of inactivity. SOURCE: SP 800-83

Spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system.
2. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating masquerading, piggybacking, and mimicking are forms of spoofing. SOURCE: CNSSI 4009

Social Engineering – A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. SOURCE: SP 800-114

Software – Computer programs and associated data that may be dynamically written or modified during execution. SOURCE: CNSSI-4009

Software Development Life Cycle – See System Development Life Cycle. SOURCE: Security in Development and Support Processes Policy Work Group

Software Owner – See System Owner. SOURCE: Security in Development and Support Processes Policy Work Group

Split Tunneling - A technology that allows a VPN User to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. SOURCE: Acceptable Use Policy Work Group

Spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating masquerading, piggybacking, and mimicking are forms of spoofing. SOURCE: CNSSI 4009

Spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. SOURCE: SP 800-53; SP 800-53A; CNSSI-4009

Standards – The Metropolitan Government minimum requirements for users to assure compliance with the Metropolitan Government Information Security Management Policy. SOURCE: Executive Order No. 038; Acceptable Use Policy Work Group

Steering Committee – The Metropolitan Government Information Security Steering Committee. SOURCE: Executive Order 38

Store – Act of backing up, saving, keeping, recording or otherwise writing or storing any data or information in any type of permanent media or permanent storage device. For the avoidance of doubt, this excludes temporarily storing information to a dynamic and volatile RAM.

system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. SOURCE: SP 800-53; SP 800-53A; SP 800-18; FIPS 200

Telecommunications – Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. SOURCE: CNSSI-4009

Telework - Ability for Metropolitan Government's employees and contractors to perform work from locations other than Metropolitan Government's facilities. Teleworkers use various client devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDA), to read and send E-mail, access Web sites, review and edit documents, and perform many other tasks. Most Teleworkers use remote access, which is the ability for Metropolitan Government's Users to access its non-public computing resources from external locations other than Metropolitan Government's facilities. SOURCE: Acceptable Use Policy Work Group

Teleworker – Means a user who teleworks. SOURCE: Acceptable Use Policy Work Group

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-61; SP 800-18; CNSSI-4009

Threat - A potential cause of an unwanted incident, which may result in harm to a system or organization. SOURCE: ISO/IEC 27002

Training (Information Security) – Training strives to produce relevant and needed (information) security skills and competencies. SOURCE: SP 800-50

Transmission – The state that exists when information is being electronically sent from one location to one or more other locations. SOURCE: CNSSI-4009

Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. SOURCE: CNSSI-4009

Trustworthiness – The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. SOURCE: SP 800-79. The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. SOURCE: CNSSI-4009 Security decisions with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities. SOURCE: FIPS 201

Unauthorized Access – Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. SOURCE: FIPS 191

- 44 U.S.C Section 3542
- CNSSI 4009, *National Information Assurance (IA) Glossary*
- FIPS 140-2, *Security Requirements for Cryptographic Modules*
- FIPS 185, *Escrowed Encryption Standard*
- FIPS 191, *Guideline for the Analysis of Local Area Network Security*
- FIPS 199, *Standards for Security Characterization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- Karl Dean Executive Order No. 38
- OMB Circular No. A-130 Appendix III
- NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*
- NIST Special Publication 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST Special Publication 800-27 Rev A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
- NIST Special Publication 800-28 Version 2, *Guidelines on Active Content and Mobile Code*
- NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
- NIST Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*
- NIST Special Publication 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems (Errata Page – Nov 11, 2010)*
- NIST Special Publication 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST Special Publication 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program*
- NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*
- NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST Special Publication 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-53A Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems*
- NIST Special Publication 800-60 Rev 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST Special Publication 800-61 Rev 1, *Computer Security Incident Handling Guide*
- NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication Guideline*
- NIST Special Publication 800-66 Rev 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
- NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification(PIV) Card Issuers (PCIs)*
- NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*
- NIST Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*
- NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*
- Metropolitan Information Security Management Program Work Group *Acceptable Use of Information Technology Assets*