METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 3
SUBJECT: PHYSICAL AND ENVIRONMENTAL SECURITY POLICY	DISTRIBUTION DATE: 1/1/2014 EFFECTIVE DATE: 7/1/2014
ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this Policy is to help ensure that the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) 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 *Metropolitan Government 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, Uninteruptable Power Supply systems, generators, temperature and humidity controls, and fire protection. The protection should be commensurate with the identified risks.

POLICY

1. Generally

Metropolitan Government 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;
1.7. Control and, as necessary, isolate from information processing facilities, access points such as delivery and loading areas, and other points where unauthorized persons may enter the premises;
1.8. Apply security to off-site equipment taking into account the different risks of working outside Metropolitan Government's premises and ensure that equipment, information or software is not taken off-site without prior authorization; and

1.9. Check all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

1.10. Metropolitan Government shall review/update this Policy and accompanying procedures annually.

1.11. As set forth below, Metropolitan Government's secure areas responsibilities are supported through the use of the controls set forth in:

- physical access control (see Section 2);
- physical access authorizations (see Section 3);
- monitoring physical access (see Section 4);
- visitor control (see Section 5);
- visitor access records (see Section 6);
- security awareness and training (see Section 7);
- physical access agreements (see Section 8);
- controlled maintenance and diagnostics activity (see Section 9);
- maintenance tools (see Section 10);
- remote maintenance (see Section 11);
- access control for output devices (see Section 12);
- access control for transmission medium (see Section 13);
- equipment, information, and software transport (see Section 14);
- alternate work site (see Section 15);
- delivery, removal, and media sanitization (see Section 16);
- power equipment and power cabling (see Section 17);
- emergency shutoff (see Section 18);
- emergency power (see Section 19);
- temperature and humidity controls (See Section 20);
- fire protection (see Section 21);
- water damage protection (see Section22);
- information leakage (See Section 23);
- contingency plan (see Section 24);
- Physical Security Incident Management (see Section 25).

2. Physical Access Control

Metropolitan Government shall:

2.1. Enforce physical access authorizations for all physical access points (including designated 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 Metropolitan Government'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, Metropolitan Government 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.
2.10. Maintain, support, and utilize an enterprise access control security system, centrally administered by Metro General Services Department, with the ability, if needed, for decentralized administration to Metro departments requiring access control to their secured areas of responsibility.
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

Metropolitan Government 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 oran information system resides (except for those areas within the facility officially designated as publicly accessible), to include:
3.2.1. Review and approve the access lists, 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 required for the availability of the information systems must follow the principle of least privilege access. Authorized personnel, including full- and part-time staff, 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.
3.5. For facilities or areas involved with information classified as Restricted in the *Metropolitan Government Information Classification Policy*;
3.5.1. For any information processing facilities, areas, or equipment which contain or provide access to restricted information, as defined by the *Metropolitan Government Information Classification Policy,* fingerprint-based background checks must be performed on individuals before granting unescorted access to the facility or area where the information

is processed or resides. Individuals with a "Pass" status may be granted unescorted access, as approved by the Facility Access Manager;

3.5.2. Any individual who is in a "failed" status of a fingerprint-based background check shall not be granted access nor escorted into a secured area which contains or provides access to Restricted information.

4. Monitoring Physical Access

Metropolitan Government 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

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 Metro Government and departmental policies and procedures.

5. Visitor Control

5.1. Metropolitan Government shall control physical access by authenticating visitors before authorizing access to any facility where Confidential or Restricted information resides, other than areas designated as publicly accessible. Individuals (including employees, contract personnel and others) with permanent authorization credentials for the facility are not considered visitors.

5.2. Contractors and vendors, who infrequently need physical access to the facility, must be escorted by authorized personnel at all times.

5.3. Contractors and vendors, who will likely need frequent physical access to any information processing facilities, areas, or equipment which contain or provide access to restricted information, as defined by the *Metropolitan Government Information Classification Policy*, must submit to a fingerprint-based background check to be granted physical access to the facility. Any individual who is in a "failed" status of a fingerprint-based background check shall not be granted access nor shall they be escorted into a secured area where an information system resides which contains or provides access to Restricted information.

5.4. All visitors must display, in plain view, a visitors' badge at all times while in non-public areas of the facility.

5.5. Establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel.

6. Visitor Access Records

Metropolitan Government shall: 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 at least weekly.

7. Security Awareness and Training

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

8. Physical Access Agreements

Metropolitan Government 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, 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 *Metropolitan Government 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, Metropolitan Government 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 into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity).

11. Remote Maintenance

When the maintenance provider of the information systems and supporting infrastructure is not physically present at the information system or information system component, , Metropolitan Government shall:

11.1. Authorize, monitor and control remote maintenance and diagnostic activities;
11.2. Approve, control, and monitor the use of local and remote maintenance and diagnostic tools;
11.3. Employ strong identification and authentication techniques in the establishment of remote maintenance and diagnostic sessions;

11.4. Maintain and review records for all local and remote maintenance and repairs; and
11.5. Terminate all sessions and network connections when remote maintenance is completed.

12. Access Control for Output Devices

Metropolitan Government shall control physical access to information system output devices to prevent unauthorized individuals from viewing or obtaining the output. Monitor, printer and audio devices are examples of information system output devices.

13. Access Control for Transmission Medium

Metropolitan Government shall control physical access to information system distribution and transmission lines within its facilities.

13.1. Protective measures to control physical access to information system distribution and transmission lines shall include security measures such as: disconnected or locked spare 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 the responsible IT network support organization.

14. Equipment, Information and Software Transport

For security of equipment off-premises and removal of property purposes, Metropolitan Government 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.

15. Alternate Work Site

If the Metro Department 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, Metropolitan Government 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

Metropolitan Government 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, Metropolitan Government 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, Metropolitan Government 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 Metropolitan Government or individuals if released for reuse or disposal.

17. Power Equipment and Power Cabling
    Metropolitan Government 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

    Metropolitan Government 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
    - 18.4. Protect emergency power shutoff capability from unauthorized activation.

19. Emergency Power

    Metropolitan Government 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.

20. Temperature and Humidity Controls

    Where applicable, Metropolitan Government 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.

21. Fire Protection

    Metropolitan Government shall employ and maintain fire suppression and detection devices/systems for critical information systems that are supported by an independent energy source.

22. Water Damage Protection

    Metropolitan Government shall protect the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.

23. Information Leakage

    Metropolitan Government shall review the risks of information leakage due to electromagnetic signals emanations and mitigate at a level commensurate with the identified risks.

24. Contingency Plan

    Metropolitan Government shall develop a contingency plan for the information system, as directed by the *Metropolitan Government IT Contingency/Disaster Recovery Planning Policy*, which addresses physical security issues for all recovery strategies and activities.

25. Physical Security Incident Management

    Metropolitan Government shall develop processes for reporting, investigating, resolving breaches or problems with physical security controls, as directed by the *Metropolitan Government Information Security Incident Management Policy*.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300

SIGNATURE

Keith Durbin,
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: section 9
- NIST Special Publication 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*; MA-1 through MA-6, MP-5, MP-6, PE-1 - PE19
- CIS Critical Security Controls 3, 11, 13
- Criminal Justice Information Services Security Policy version 5.6

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	8/1/11	First released version
1.1	12/1/13	Added ISO 27002 section 9.2 (Equipment Security) and renamed policy accordingly
1.2	8/16/2018	Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against. Added review of Center for Internet Security Critical Security Controls. Added review of Criminal Justice Information Services Security Policy version 5.6