SPECIAL ORDER

DISTRICT OF COLUMBIA

Title
Information Technology Restricted Area Access and Asset Control
Number
11–04
Effective Date
March 30, 2011
Related to:
GO 302.08 (MPDNet Metropolitan Police Department Wide Area Network)

I. BACKGROUND

The Metropolitan Police Department (MPD), Office of the Chief Technology Officer (OCTO), requires that all Information Technology (IT) restricted areas be protected by suitable physical, technical, procedural and environmental security controls. To prevent loss, damage or compromise of assets and interruption to business activities, equipment should be physically protected from security threats or environmental hazards to include unused equipment and equipment that is being disposed.

II. DEFINITIONS

For the purpose of this directive, the following terms shall have the designated meanings:

1. Asset Responsibility Owner – Employee with full-time, permanent status with the MPD who has been assigned technology assets.

2. Director of Operations – Member designated by the Chief Technology Officer (CTO) who serves as the Deputy Director of MPD OCTO.

3. Information Technology Assets (IT assets) – Assets purchased, leased or borrowed by the MPD that consist of, but are not limited to: desktop computers; laptop computers; computer related peripherals (e.g., printers, monitors, external CD drives); hosting equipment and servers; network equipment (e.g., routers, switches, hubs, servers, wireless routers/ bridges, network video recorders/digital video recorders, firewalls); MPD OCTO standard software assets; smart phones, cell phones, pagers, and desk telephones.

4. Primary Users – Temporary or part-time staff (including contractors) who use IT assets for their job.

5. Replacement Program – MPD OCTO's technology program that replaces MPD-owned IT assets that have reached the end of their useful life.

6. IT Restricted Area – Facilities or areas identified by the MPD OCTO that hold or process critical, sensitive or "high-availability" data to include locations where IT assets are stored and inventoried.

7. IT Asset Manager – MPD OCTO member assigned to oversee and track selected IT assets as designed by the CTO.

8. Network Manager – Member designated by the CTO who has oversight responsibility for the MPD network.

9. Technician – Member designated by the CTO who assists with the deployment of technology, usually assigned to the MPD Help Desk.

III. REGULATIONS

A. The CTO shall ensure that all IT restricted areas are protected by suitable physical, technical, procedural and environmental security controls.

B. MPD OCTO members, assigned asset responsibility owners, and primary users shall ensure that all IT assets, to include unused assets and assets that are being disposed, are protected from security threats or environmental hazards to prevent loss, damage or compromise of assets and interruption to business activities.

C. The CTO shall ensure that IT Assets have a MPD asset tag.

1. Asset tags shall be attached by an authorized IT Staff member.

2. Asset tags shall be recorded and tracked by an IT Asset Manager.

D. The CTO shall ensure that all MPD-owned technology assets are assigned to an asset responsibility owner.

1. Assets used by temporary or part-time staff must be assigned to an asset responsibility owner.

2. The asset responsibility owner must indicate when assets will be used by temporary staff. The temporary staff will be identified as the **primary client**.

E. The CTO shall ensure that MPD asset responsibility owner information and primary client information are recorded and tracked.

F. Asset responsibility owners of MPD technology assets cannot exchange, trade or "cascade" assigned equipment without notifying an IT asset manager and receiving approval from the CTO or his/her designee.

G. All MPD owned technology assets shall have a location of record.

1. The location of record shall have an exact address that includes an office number or cubicle number if applicable.

2. Location of record information shall be recorded and tracked by an IT Asset Manager assigned to MPD OCTO.

3. Assets that are intended for MPD related travel or virtual offices are required to have a location of record. The record should indicate the MPD element or location where the asset will be kept most often.

H. Asset responsibility owners shall return any unwanted or unneeded IT assets to an IT asset manager.

1. IT asset managers shall ensure returned assets are placed into secure storage and assigned to inventory in the asset management system.

2. Returned assets shall be assigned and repurposed to other areas of MPD by the MPD OCTO as needed.

I. The CTO shall ensure that all MPD-owned computers, including laptops, have the LANDesk Management Agent installed.

1. The LANDesk agent ensures the Asset Management System is updated with current information.

2. The LANDesk agent operates transparently on the client's computer with no performance impact.

J. The CTO shall ensure that all MPD-owned laptops have the Computrace agent installed. The Computrace agent is a software-enabled recovery service that allows law enforcement to track assigned laptops and provides capabilities to assist in the recovery if stolen.

K. MPD asset responsibility owners of laptops shall connect their computer to the MPD Network at least once a month to receive software security patches and antivirus definition updates.

L. The CTO shall ensure that all IT equipment in general office areas is assigned to a specific asset responsibility owner and location of record. This information shall be recorded and tracked by MPD OCTO.

M. The CTO shall ensure that inventory IT assets **are not** stored in general office areas and are only stored in designated secure asset storage areas.

IV. PROCEDURES

A. Access Control

1. MPD IT personnel shall be granted access to restricted areas only when required and authorized. Where appropriate, IT personnel access shall be restricted and their activities monitored.

2. The CTO or his/her designee shall grant “Controlling Access” to people who require unrestricted access to designated IT restricted areas. Controlling access shall be granted to:

a. The CTO, the Director of Operations, and MPD Network Operations Staff for the MPD Data Center.

b. The CTO, the Director of Operations, the MPD Headquarters IT Asset Manager, the MPD Helpdesk Manger, and their designated back-ups for the MPD Headquarters secure storage area.

c. The CTO, the Director of Operations, the Site IT Asset Manager, and their designated back-ups for other MPD secure storage areas.

3. “Visitor/Escorted Access” shall be granted by the CTO or his/her designee to people who have a legitimate, temporary business-need for access to an IT restricted area.

a. Individuals with “Visitor/Escorted Access” shall not be granted access control cards.

b. People granted “Visitor/Restricted Access” shall be escorted **at all times** within IT restricted areas by IT personnel with “Controlling Access.”

4. MPD OCTO staff shall ensure that all doors to IT Restricted Areas remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

a. Allow officially approved and logged entrance and exit of authorized individuals.

b. Permit the transfer of supplies/equipment as directly supervised by a person with Controlling Access to the area.

c. Prop open a door to the IT Restricted Area **only** if it is necessary to increase airflow into the Data Center in the event of an air conditioning failure. In this case, staff personnel with Controlling Access shall be present at all times and shall limit access to the Data Center to authorized individuals.

5. Under no circumstances may MPD members, sworn or civilian, attempt to bypass a security system to gain access to an IT restricted area for themselves or to permit access to other individuals.

6. The CTO shall ensure that physical entry into IT restricted areas has mechanisms and/or procedures that expressly restrict and monitor access to only authorized persons.

7. Visitors and IT staff who are not part of the Operations Division, MPD-OCTO, must be escorted in Data Centers / Network Closets at all times due to the sensitivity of hardware, software, and information.

B. Requesting Access

1. New requests for access to IT restricted areas will be made through the Network Manager or an IT asset manager to the CTO as appropriate.

a. Requests shall be submitted to the CTO for review and approval/disapproval.

b. If a visitor or other IT staff member needs access to a secure asset storage location, coordination shall be made through a site IT asset manager.

c. If a visitor or other IT Staff needs access to a Data Center or network closet, then coordination shall be made through the Network Manager.

d. Copies of requests for access shall be maintained by the administrative staff of the MPD OCTO.

2. MPD OCTO staff shall not issue control cards to the MPD Data Center for routine access purposes (e.g., cleaning staff, facilities staff). Requests for exceptions shall be considered on a discretionary, case-by-case basis.

3. The Director, Facilities Management Division, shall ensure that permissions for the card control system are administered appropriately and updated when needed.

C. Accessing Restricted Areas

1. Supervised access to data centers/network closets shall be coordinated through the Network Manager.

2. Supervised access to any secure asset storage must be coordinated through that location’s asset manager.

3. The following procedures shall be followed when accessing restricted areas:

a. Each time an individual enters an IT Restricted Area he or she must properly log in on the access control log at the time of entrance.

b. If the person is admitting a visitor, then they must sign the access control log and fill out the appropriate section of the form.

c. Each time an individual with escorted access privileges leaves the area, he or she must properly log out on the access control log at the time he or she leaves (even if only for a short time).

d. The person with controlling access to the area who allows the visitor to leave must fill out the “Log Out” section of the access control log.

4. Equipment stored in a restricted area shall be logged in and out.

a. The Network Manager will log all equipment that is transitioned into or out of the MPD Data Center.

b. The site IT asset manager will log all equipment that is transitioned into or out of secure storage.

D. Revocation of Access Privileges

1. The CTO shall ensure that individuals who no longer have a business need to enter an IT restricted area are immediately removed from the site access control system including, but not limited to, upon receipt of a PD Form 295 (Clearance Record) for the individual.

2. To terminate or revoke MPD Data Center access members shall:

a. Submit a request to Facilities Management Branch to cancel badge access.

b. Collect the individual’s control card.

c. Remove the individual’s name from the authorized access list.

3. Access rights to secure areas shall be revoked immediately for staff that leave MPD employment or are detailed to another assignment.

E. IT Site Security Audits

1. The CTO shall ensure that quarterly reviews are conducted in the following areas:

a. Inspections of door locking mechanisms to provide ensure that hardware cannot be easily manipulated to gain unauthorized access.

b. Review of access permissions to ensure they are accurate and support current business needs. If an individual’s needs no longer justify access, his/her access shall be terminated immediately.

c. Review of access log entries.

2. The CTO shall ensure periodic spot-checks are undertaken to detect unauthorized removal of property. Staff will be informed that these take place, although not when and how.

3. The results of periodic reviews shall be reported to the CTO. The report will include an updated list of those allowed access to the Data Center.

F. Asset Acquisition

1. Purchases of IT assets shall adhere to the regulations of the D.C. Government, the D.C. Office of Contracting and Procurement, and the MPD.

2. Once the procurement process has been completed and a purchase order is created, an email is sent to the IT Asset Manager by the Procurement Automated Source System (PASS) originator.

3. The IT Asset Manager shall coordinate the logistics for delivery and shall be responsible for receiving all the goods in PASS.

4. The IT Asset Manager shall notify the customer that the asset has been received, and forward any documentation required for recordkeeping.

G. IT Asset Inspection, Acceptance, and Distribution

1. Upon receipt, the IT asset manager shall ensure the asset is checked for shipping damages.

   NOTE: This is to ensure that the shipment corresponds with the packing slip and that there are no items that should be returned due to damage during shipping.

2. The IT asset manager shall ensure signatures indicating complete shipments are captured on the manifest receipts.

3. The IT asset manager shall ensure a second signature is captured confirming the amount(s) and type(s) of property received.

4. The IT asset manager shall ensure standard MPD asset tags are affixed to each physical asset, entered into the Asset Management System, placed into a secure MPD inventory facility, and the location in the inventory facility is documented within twenty-four (24) hours of receipt.

5. The IT asset manager shall ensure all purchase documentation is scanned and attached to inventory in the Asset Management System and that original documentation is provided to the IT customer.

   NOTE: This documentation includes, but is not limited to, an email containing the site for downloading the software, software installation instructions, software licensing information and packing slips.

H. Asset Deployment

1. Any item being removed from an inventory facility must be checked out through the Asset Management System and assigned to the appropriate asset responsibility owner by a member of the IT inventory team.

2. The asset responsibility owner’s full name, bureau assigned and location shall be recorded on a PD Form 84 (Property Receipt) and entered into the IT Asset Management System.

3. Upon completion of deployment, the technician shall have the asset responsibility owner complete the Information Technology Release Form (Attachment A.) The technician shall then return the form to the IT Asset Manager for updating in the Asset Management System.

I. Asset Transfer

1. Transfers of IT assets shall be approved by the MPD OCTO and shall be recorded on a PD Form 237 (Violation Notice/Transmittal) signed by the receiving unit.

2. If the asset is identified as relevant for future investigative purposes (e.g., for a litigation hold), MPD OCTO shall ensure that an appropriate label is placed onto the asset.

J. Returned Assets

1. Supervisors of members separating from the MPD shall ensure that computer assets are returned to the appropriate IT asset manager.

2. IT asset managers shall provide a written receipt (i.e., PD Form 84 and/or original receipt stamped “Returned Property”) to the asset responsibility owners upon their separation from MPD.

3. IT Asset Managers shall ensure:

   a. Returned assets are verified in the IT Asset Management System to ensure accountability.

   b. Assets are tested to determine if they can be reused. If they can be reused, IT asset managers shall update the location in the Asset Management System and indicate the location in the inventory facility.

   c. Equipment that is no longer usable is marked for disposal and marked as “surveyed” in the IT Asset Management

System.

d. The PD Form 160 (Requisition for Supplies and Materials) is completed for surplus equipment which will be sent to Property Division for disposal.

K. Loss or Damage to IT Assets

1. Asset responsibility owners shall report all incidents of damage to or loss of IT assets on the PD Form 43 (Report of Damage to or Loss of D.C. Government Property) in accordance with MPD policy and procedures.

2. Asset responsibility owners shall present a copy of the certified PD Form 43 to obtain a replacement cell phone.

L. Asset Retirement / Disposal

1. After a MPD-owned asset reaches the end of its useful life, MPD OCTO shall ensure the asset is properly removed from use and all data contained on the asset is destroyed (i.e., “wiped.”)

2. MPD OCTO shall ensure all retired assets are inventoried in the Asset Management System.

3. Retired assets shall be stored by MPD OCTO for ten (10) business days. During the ten (10) business days, former users may contact the appropriate IT Asset Manager to recover any missing data. However, after ten (10) business days, all data stored will be destroyed unless the asset is subject to retention for investigative or legal purposes (e.g., litigation hold).

4. The IT asset manager shall submit a copy of the purchase order, a certified record of electronic disposal, a copy of the software license and the PD Form 160 to the CTO or his/her designee for approval to be submitted for removal from the fixed asset inventory.

M. IT Asset Verification

1. Every three (3) months, IT asset managers shall provide quarterly capital equipment inventory reports to the CTO.

2. Every six (6) months:

a. IT asset managers shall request that asset responsibility owners review inventory reports to identify assets that may have been moved or disposed of, but not reported. These reports shall be completed and returned to IT asset managers.

b. IT asset managers shall select a rotating 15% of equipment assets for physical inventory. Assets shall be accounted for and explanations for discrepancies between the asset management records and the equipment located must accompany the reports returned. The list shall be updated with any tagged equipment that is not listed.

c. IT asset managers shall conduct spot checks of general work areas to detect unsecured IT assets at their respective sites. Unsecured IT Assets will be verified in the Asset Management System and relocated to a secure storage. MPD members will be informed that these spot checks take place, although not when and how.

3. Every twenty-four (24) months, IT Asset Managers shall account for all capital equipment assets and document in writing any discrepancies between the Asset Management records and the equipment. A report of the findings shall be provided to the CTO. The report shall include updates of any tagged equipment that is not listed in Asset Management records.

V. ROLES AND RESPONSIBILITIES

A. The CTO shall be responsible for developing and maintaining policies, standards, processes, systems and measurements that enable the organization to manage the Information Technology (IT) asset portfolio with respect to risk, cost, control, IT governance, compliance and business performance objectives as established by the Department.

B. The Deputy Technology Officer shall be responsible for defining the physical security standards for all (IT) restricted areas. He/she shall participate in the planning and design of all new IT restricted areas to ensure that IT physical security standards are incorporated in space layouts for offices, buildings and complexes.

C. The Network Manager shall be responsible for conducting on-site reviews of all data centers and network rooms to ensure that all mission-critical, Department-priority and sensitive systems are protected through adequate layered physical security.

D. IT Asset Managers shall be responsible for:

1. Ensuring that IT assets are acquired, recorded, inventoried, and disposed of according to the guidelines provided in this order.

2. Conducting on-site reviews to ensure all inventory assets are properly secured.

VI. ATTACHMENT

A. Attachment A: Information Technology Release Form

Cathy L. Lanier
Chief of Police

CLL:PAB:MOC:CC:GHE

Created December 29, 2009

Metropolitan Police Department

Office of the Chief Information Officer
Information Technology Release Form

Date: ______________________________ **Remedy Ticket Number:** ______________

USER INFORMATION

Desktop User: ______________________ ☆ New ☆ Replacement

Telephone Number: ______________________ E-Mail Address: ______________________

Location: ____________________________ Room Number: ____________

POINT OF CONTACT INFORMATION

FIRST Name: ____________________________ LAST Name: ______________________

Telephone Number: __________________ E-mail Address: ______________________

Issued By: ____________________________ Initials: ______ Date: ______________

Please Print

Received By: ____________________________ Initials: ______ Date: ______________

Please Print

Check If the Employee Listed As the User is No Longer an Employee of MPD ☆

EQUIPMENT INFORMATION

Type of Equipment (Circle One): Laptop Desktop Monitor Toughbook Other ___________

Serial Number: ________________ MPD Asset Tag Number: ______________

Condition: ____ Fair ____ Excellent ____ Bad // Brand: ______________ Model: __________

Type of Equipment (Circle One): Laptop Desktop Monitor Toughbook Other ___________

Serial Number: ________________ MPD Asset Tag Number: ______________

Condition: ____ Fair ____ Excellent ____ Bad // Brand: ______________ Model: __________

Type of Equipment (Circle One): Laptop Desktop Monitor Toughbook Other ___________

Serial Number: ________________ MPD Asset Tag Number: ______________

Condition: ____ Fair ____ Excellent ____ Bad // Brand: ______________ Model: __________

REPLACEMENT EQUIPMENT INFORMATION

Desktop Serial Number: ________________ MPD Asset Tag Number: ______________

Condition: ____ Fair ____ Excellent ____ Bad // Brand: ______________ Model: ________________

Monitor Serial Number: ________________ MPD Asset Tag Number: ______________

Condition: ____ Fair ____ Excellent ____ Bad // Brand: ______________ Model: ________________

OTHER

Serial Number: ________________ MPD Asset Tag Number: ______________

Condition: ____ Fair ____ Excellent ____ Bad // Brand: ______________ Model: ________________