DISTRICT OF COLUMBIA
DEPARTMENT OF CORRECTIONS

Program Statement

OPI: **OMITS**
Number: **2420.2**
Date: **December 15, 2003**
Subject: **Information Security**

1. **PURPOSE AND SCOPE.** To establish standard procedures for the security, management and control of the DC Department of Corrections (DOC) electronic data and information systems.

2. **POLICY.** It is the policy of the DOC to control access to mission-critical information while ensuring accuracy, the privacy of government documents, inmates and staff, and minimizing the risk of loss for any reason.

3. **APPLICABILITY.** This policy applies to all DOC's entities and to all employees, agents, consultants, contractors, volunteers and vendors involved in the use and/or development, implementation and maintenance of information systems.

4. **PROGRAM OBJECTIVES.** The expected results of this program are:

   a. Access to information shall be granted and controlled based on the requirements of official duties and achievement of departmental goals and objectives, or as stipulated by the DC Freedom of Information Act (FOIA) and the Health Information Portability and Accountability Act (HIPAA) of 1996.

   b. Information security procedures shall comply with applicable security laws, regulations and policies, both federal and local.

   c. DOC's data and information systems assets shall be provided adequate security commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information.

   d. DOC data and information systems shall be protected from loss and unauthorized disclosure.

   e. Standard procedures and instructions shall be employed for computer systems operators and operations. These procedures define both required and prohibited activities, retention of department records, and specify controls and documentation to be used.

5. **DIRECTIVES AFFECTED**

a. **Directives Rescinded.** None

b. **Directives Referenced**

1) PS 1280.2C "Notification of Significant Incidents and Extraordinary Occurrences", (9/15/00)

2) PS 1300.1B "District of Columbia Freedom of Information Act (FOIA)", (12/15/03)

3) PM 1300.3 "Health Information Privacy", (12/15/03)

4) PS 2000.2 "Retention and Disposal of Department Records", (2/26/01)

5) PS 2420.4A "Email & Internet", (9/30/03)

6) PS 2420.8 "Recovery Disaster Plan", (12/15/03)

6. **AUTHORITY**

a. The Computer Security Act of 1987, Public Law 100-235 (January 8, 1988)

b. Defense Authorization Act P.L. 106-398 (Government Information Security Reform)

c. D.C. Code § 24-211.02 Powers; Promulgation of Rules [Formerly § 24-442]

d. OMB CIR A-130 Security of Federal Automated Information Resources

e. DC Code §§2-531 through 2-539 (2001) Freedom of Information Act

f. OCTO Information Security Policy (10/15/01)

g. OCTO User Password Protection Procedure (10/15/01)

h. OCTO Desktop Security Standard (10/15/01)

i. 45 Code Federal Regulations Parts 160 and 164 (Privacy Rules)

j. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) DC Privacy Rules

k. 45 Code Federal Regulations Parts 160 and 164 (Privacy Rules)

l. HIPAA DC Guide on Preparing Contingency Plans, HIPAA DC Program Management Enterprise Compliance Implementation Project (June 2003)

7. **NOTICE OF NON-DISCRIMINATION** In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Code section 2.1401.01 et seq., (Act) the District of Columbia does not discriminate on the basis of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, matriculation, political affiliation, disability, source of income, or place of residence or business. Sexual harassment is a form of sex discrimination that is also prohibited by the Act. Discrimination in violation of the Act will not be tolerated. Violators will be subject to disciplinary action.

8. **STANDARDS REFERENCED**

   a. American Correctional Association (ACA) 2nd Edition Standards for Administration of Correctional Agencies: 2-CO-1E-01, 2-CO-1E-06, 2-CO-4E-47, 2-CO-1F-01, 2-CO-1F-03 and 2-CO-1F-06.

   b. American Correctional Association (ACA) 3rd Edition Standards for Adult Local Detention Facilities: 3-ALDF-1E-01, 3-ALDF-1F-01 and 3-ALDF-1F-02.

9. **RESPONSIBILITIES**

   a. **Director** shall approve or disapprove external requests for data access to inmate population or departmental programs and operations.

   b. **DOC Data Access Review Committee (DARC)** shall determine, or when required, recommend action to the Director for the release of information regarding inmates or agency operations or for the conduct of research by external sources.

   c. **Office of Management Information and Technology Services (OMITS) Manager** shall administer the Information Security Program.

   d. **DOC Information Security Officer (ISO)** shall monitor and document compliance with DOC Information Security Program procedures, and identify and correct known deficiencies.

   e. **OMITS Technical Staff** shall provide oversight, including inventory control, system performance monitoring, and technical assistance for the operation and maintenance of DOC computer rooms.

   f. **OICCA** shall conduct annual audits for compliance with this directive.

   g. **Warden/Administrators/Office Chiefs** shall ensure that the IT data, access privileges, and equipment under their responsibility comply with this directive.

   h. **DOC Employees** are responsible for assisting in the protection of DOC's automated correspondence, data, IT systems and equipment they are authorized to use by complying with the security procedures outlined in this directive.

10. **GENERAL REQUIREMENTS**

a. **Data Security**. All employees shall safeguard all electronic data they create, collect or maintain commensurate with the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access to or modification of information.

b. **Data Confidentiality**

1) Sensitive information shall be protected from unauthorized disclosure.

2) Data classification categories, designation criteria, and markings shall be employed consistently.

3) Copying, handling, movement, and disposal of sensitive material, including media used to store sensitive material shall be controlled in accordance with DOC policy.

c. **Data Integrity.** Information shall be protected from intentional or unintentional destruction or modification. OMITS will ensure that the source of data transmitted is known and not modified in transit.

d. **Information Systems Data Availability**

1) Critical information shall be accessible when needed to support the DOC mission.

2) A system of access controls shall be employed and enforced to limit access to systems and data to those with a valid need to know.

e. **Monitoring.** OMITS shall employ automated tracking for monitoring system operations and user activity and for detection of computer crime or abuse.

f. **Telecommunications Security**

1) **Establishment of Access Paths and Systems.** OMITS shall employ flow control systems, including Firewalls, to protect information system resources. The establishment, modification, and termination of network connections shall be centrally managed and controlled by OMITS on an ongoing basis.

2) **Dial-Up Communications.** OMITS shall control access to and from information systems via dial-up connections. OMITS shall enforce standard policies and procedures governing both the location and employment of telephone modems.

3) **Downloaded Data.** The download of DOC data, other than that intended for public dissemination to internal and external sites, shall be restricted. Exceptions require prior written authorization by DOC Director.

4) **E-mail, Internet/Intranet Systems.** OMITS shall control and regulate use of the DOC electronic mail (E-mail) system and the Internet/Intranet.

g. **Workstation Security**

1) Personal computers and workstation equipment shall be "locked-down" with secure devices to safeguard against theft.

2) Security control requirements shall be used in evaluating new hardware and equipment as part of the overall acquisition process.

h. **IT Systems Security.** Adequate security shall be provided for application systems, databases, automated information system facilities (mainframes, minicomputer, and/or microcomputer platforms), Local Area Networks (LANs), Wide Area Networks (WANs), and major applications and general support systems.

i. **Computer Room Security.** Access to computer rooms shall be tightly controlled. Computer rooms are areas that contain controllers, communications servers, or local area network (LAN) file servers used to process or store DOC data and any areas with LAN gateways or tape backup units.

11. **PROCEDURES**

a. **Authorized users of DOC Computer Systems shall:**

1) Comply with all other policies and procedures related to information security, e-mail, and Internet use.

2) Access systems and data only by means of their personally assigned user IDs and passwords.

3) Adhere to software installation protocol and shall not install unauthorized software on personal computers and workstations.

4) Ensure that unattended personal computers and workstations are either logged off or that the security screen features are engaged.

5) Terminate communication links when they are not in use (e.g., Internet, e-mail).

6) Ensure confidential and/or sensitive information is handled by secure electronic mail and/or use of confidentiality notice(s).

7) Ensure sensitive information that is stored on hard-disk drives or other internal components is protected by either password access or encryption.

8) Ensure that sensitive information that is stored on computer media (floppy diskettes, CD’s) are maintain in a locked storage compartment when they are away from their workstation.

9) Ensure that portable laptops, notebooks, PDA's and other transportable computers are not left unattended and device and storage media protection is used.

b. **Warden/Administrators/Office Chiefs shall:**

1) On an annual or as needed basis, identify and provide OMITS with a list of sensitive and operationally critical systems that meet the requirements of "major applications". Major applications are those where critical or significant harm to DOC operations would result from the loss, misuse or unauthorized access to, or modification of, the information in the application.

2) Provide OMITS with a listing of data, files, and systems requiring special backup and controls.

3) Under OMITS leadership, develop appropriate levels of risk assessment and accessibility for each employee under their management or supervision.

4) Notify OMITS of all personnel changes, i.e., reassignments, changes in job responsibilities/titles, terminations, and any other changes affecting data/systems "access" privileges. (Attachment A)

5) Maintain records on assigned keys and personnel approved for entry into computer rooms.

6) Notify OMITS in the event of any confirmed or suspected security violations, including virus infections, unauthorized access, or attempt to access, computer rooms or data in accordance with PS 1280. "Notification of Significant Incidents and Extraordinary Occurrences" (9/15/00).

7) Include special provisions in Duty Officer and/or Post Orders for notification and access to computer rooms in the event of emergencies or disaster.

c. **OMITS Information Security Officer (ISO) shall:**

1) **Risk Assessments**

a) In coordination with Administrators/Managers/Office Chiefs, develop and maintain an information risk assessment that is appropriate and applicable to all IT systems.

b) Conduct a risk assessment survey quarterly, or when there are modifications made to any IT system.

c) Review and update the information risk assessment annually to ensure that protection methods, procedures, and tool sets are current and appropriate to the threats and vulnerabilities involved.

2) **Data Access and Security**

a) Process requests, from external parties for data access, through the DOC Director and the DARC. (Attachment B and C)

b) Ensure appropriate training and certification is obtained before access to a system is permitted.

c) Ensure that prompt notification is made regarding personnel changes that affect access privileges, or revocation of access when employees are separated or are terminated.

d) Process all requests for NCIC access via the Metropolitan Police Department WALES/NCIC Computer Access Request Form (Attachment D) along with the employee's fingerprints (Attachment E) and forward it to the Metropolitan Police Department (MPD) for authorization and signature.

3) **Quality Assurance**

a) Monitor employees' information systems activities to ensure users are able to understand and adhere to the policies and procedures in this directive.

b) Monitor and review automated security tracking log reports at least weekly to ensure current security measures are operating efficiently and identify any attempts to breech security.

c) Maintain a technology performance measurement system that is current with business needs and directions. Key measures/indicators shall be selected and aligned, in coordination with the Warden/Administrators/ Office Chiefs, for tracking daily operations and overall performance. The results shall be used as a basis for projections and for performance improvement.

d) Conduct system compliance reviews on DOC IT systems to ensure that the information security policies and procedures in this directive are strictly adhered.

4) **Incident Management**

a) Report significant incidents or unusual occurrences.

b) Manage the resolution of any reported security incidents and maintain a record of the problem report.

c) Review all retained reports twice annually for purposes of improving operations, policies, and procedures.

d) Prepare a report of findings and recommendations for quality assurance purposes when applicable.

5) **Computer Rooms**

a) Maintain an inventory of computer rooms and their contents.

b) Maintain Entry Authorization Lists (EALs) and Visitor Access Control Logs (Attachment F) for computer rooms in accordance with this directive.

c) Maintain and enforce procedures to ensure cleanliness and minimal accumulation of paper, dust, and flammables in and around computer rooms.

d) Assess each computer room's equipment to determine the requirements related to environmental controls (temperature, humidity, fire suppression, fail safe mechanisms, and alarms). Acquire, install and maintain automated tools for each computer room to:

(1) Provide a record of environmental data;

(2) Monitor environmental conditions (temperature, humidity, power, fire safety, intrusion detection, and emergency lighting); and

(3) Provide notification (electronic and audible) to designated key personnel and/or designated workstations when conditions approach or have exceeded pre-established limits (upper or lower).

e) **Computer Room Security.** The Information Technology Administrator shall conduct an annual site analysis/survey of each computer room and document all findings and recommendations. The survey, at a minimum, shall address the following areas:

(1) Power and electrical backup;

(2) Fail safe mechanisms;

(3) Fire protection and detection;

(4) Physical security;

(5) Information security; and

(6) Structural conditions: heating, ventilation, air conditioning, and environmental monitoring systems.

6) **Software Security**

a) **System Access Control.** These controls shall include, at a minimum, the use of user identifications and passwords, as well as their implementation procedures.

b) **Logging.** Automated logging shall be used to track sensitive system operations and use of critical functions, as well as the activities of key users.

1) Logging shall also be used to monitor all detected or suspected cases of computer crime or abuse;

2) Access to logs shall be restricted; and

3) Retention and disposition of logs shall be strictly controlled in accordance with guidance outlined in PS 2000.2, Retention and Disposal of Department Records (2/26/01).

c) **Computer Viruses and Worms.** Active preventive measures against computer viruses, worms, and other forms of hostile code shall be used throughout the DOC.

d) **Development and Change Control Process.** Formal development and change processes for software, including risk assessment, shall be used to ensure compliance with security policies and avoidance of negative effects on DOC operations.

7) **Electronic Data Disposal.** Dispose and destroy electronic information by:

a) Ensuring information on a hard disk is concealed or destroyed prior to being traded-in, serviced or otherwise disposed;

b) Degaussing or Zeroizing; and

c) Destroying CD's and diskettes in accordance with the Records Retention and Disposal policy.

8) **Backup and Recovery.** Acquire, install and maintain automated tools to ensure DOC's readiness to implement backup and recoverability procedures in the event of an emergency or disaster, in accordance with PS 2420.8, "Recoverability Disaster Plan" (12/15/03).

12. **TRAINING**

a. The DOC Training Office, in conjunction with OMITS, shall:

1) Provide basic orientation about information security policies and procedures before employees, consultants, volunteers or contractors are granted access to a system;

2) Provide annual In-Service Training on DOC's Information Security Program; and

3) Provide training, as appropriate, when new systems are implemented.

b. NCIC Clearance. The OMITS chief shall ensure that employees, whose duties require access to NCIC, complete NCIC training and certification via MPD prior to authorization.

Odie Washington
Director

ATTACHMENTS:

Attachment – A “Application Access Request Form”

Attachment – B “Data Access Review Committee Data Request Detail”

Attachment – C “Data Access Review Committee Data Access Decision Log”

Attachment – D “Metropolitan Police Department WALES/NCIC Computer Request Form”

Attachment – E “Fingerprint ”

Attachment – F “Grimke Computer Room Visitor Access Control Log”