

**SUBJECT:      INFORMATION SECURITY**

**Supersedes:**    None; New policy

**Effective:**      February 15, 2005

**Page:**            1 of 3

**1.0      POLICY PURPOSE**

The purpose of this policy is to create an environment within Detroit Public Schools (DPS) that maintains system security and availability, data integrity, and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to, or loss of data. Information is a Detroit Public Schools asset requiring assurance commensurate with its value, criticality, and sensitivity.

This policy is a district level policy, providing high-level direction. The policy will also ensure that Detroit Public Schools is in compliance with regulations set forth in the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). A copy of this Federal law that protects student information can be found at [www.ed.gov/offices/om/fpco/ferpa](http://www.ed.gov/offices/om/fpco/ferpa).

**2.0      SCOPE**

For the purposes of this policy, security is defined as the ability to protect the integrity, confidentiality, and availability of information processed, stored, and transmitted by a department/school and to protect information technology (IT) assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of TIS facilities and off-site data storage; computing, telecommunications, and applications, along with related services purchased from other commercial/private entities; and Internet-related applications and connectivity.

This policy applies to all departments/schools and personnel within as defined by Detroit Public Schools published procedures.

**3.0      POLICY**

Detroit Public Schools is entrusted with their informational assets and owns the accountability for its protection. Measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional, as well as to ensure its authenticity, integrity, and availability. *No matter what tool is used (i.e. application, email, pen & pencil) to create, store, report or destroy care must be taken to appropriately protect information from origin to destination to destruction while both internal and external to Detroit Public Schools information systems and networks.*

Information handling processes, procedures, and practices may contain information (confidential or private) about the district's business, communications, and computing operations or employees. Policy, processes, and procedures for distribution of any

related documentation should consider both the sensitivity of the information and related statutory exemptions for such information, before allowing public disclosure.

*It is essential that DPS employees and business partners understand that informational assets are created and stored in various modes. This policy is not intended to just cover electronically stored information, but information that also resides in hardcopy and in an individual's knowledge base.*

#### **4.0 STATUTORY AUTHORITY**

Detroit Public Schools gives the Division of Technology and Information Systems (DTIS) authorization for "Developing and maintaining security policies and systems to ensure the integrity of the district's information resources and to prevent the disclosure of confidential records". DTIS is also responsible for developing and implementing recommended standards for information technology, including but not limited to system design and systems integration and interoperability, which when implemented shall apply to all departments/schools except as otherwise provided in this document.

#### **5.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES**

The Chief Technology and Information Systems Officer (CTIO) has developed regulations and/or standard operating procedures to implement this policy.

#### **6.0 FAILURE TO COMPLY**

All Detroit Public Schools employees, agents, and contractors of participating departments/schools are responsible for understanding and complying with all Detroit Public Schools enterprise data security policies, standards, processes, and procedures. This includes building, configuring, and maintaining systems in accordance with these policies, standards, processes, and procedures. Non-compliant situations will be brought to the attention of the DTIS, and/or any other applicable department/school for appropriate action. Depending on the severity, employees who violate these policies, standards, processes, and procedures may receive disciplinary action, up to and including loss of network connectivity, immediate dismissal, and/or criminal prosecution. If there is a conflict between this policy and another policy document, the document with the more stringent control takes precedence.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships, and alliances, must be monitored and reviewed to ensure either compliance with enterprise and departmental policies or that a level of control is provided which is equivalent to enterprise policies. This should be accomplished through contractual commitments with provisions to permit auditing and monitoring to ensure compliance.

#### **7.0 EXCEPTIONS**

Any exceptions to this policy must be documented and approved by the DPS Chief Technology and Information Systems Officer.

**8.0 AGREEMENT**

I, \_\_\_\_\_ (print name) have read the Detroit Public Schools Information Security policy, dated \_\_\_\_\_. I understand it and agree to abide by it. I agree to obtain prior approval if I should be required to perform a DPS business function with tools that do not abide with the policy. If I should suspect a security breach in the disclosure, accuracy or availability of DPS informational assets I will contact my manager. I further acknowledge that misuse of informational assets will result in appropriate disciplinary action being taken as outlined in the present DPS disciplinary process.

\_\_\_\_\_  
Signed

**Attachments:** Administrative Regulation 13.03 – Information Security

**See also:** None

**Legal References:** Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

**Labor Contract References:** None

**DETROIT PUBLIC SCHOOLS**  
**ADMINISTRATIVE REGULATION**

**INFORMATION SECURITY**

**This Administrative Regulation implements Detroit Public Schools (DPS) Policy 13.03 – Information Security**

**1.0 Information Categories**

DPS has developed four information categories in to which all informational assets will be classified. Detailed use, storage, protection, and deletion requirements for each category can be found in policy 13.04 - Information Classification.

- Public - Non-sensitive information available for external release.
- Internal - Information that is generally available to employees and approved non-employees.
- Confidential - Information that is sensitive within the district and is intended for use only by specified groups of employees.
- Restricted - Information that is extremely sensitive and is intended for use only by named individuals within the district.

**2.0 Roles and Responsibilities**

Information assurance requires the active support and ongoing participation of all district employees and business partners. It requires support from the executive level and universal compliance. Responsibility for satisfying policy requirements is shared and extends to all personnel involved with the development, implementation, operations, use, and maintenance of district informational assets. Each person shall satisfy the requirements as they relate to the portion of each information system under their control.

The following are specific individual roles and responsibilities for all employees using DPS informational assets.

**2.1 Data Owners/Stewards**

Divisional, department and school leadership (or equivalent) are responsible and accountable for the ultimate use of information processed through DPS' information systems. Through the selection of a designee, department leadership/school principals are also responsible for the implementation of the enterprise security policy in their department/school and the development and implementation of department/school security policies, standards, processes, and procedures. Department directors/school principals will assign data custodians with the responsibility of data protection and authorization on a "need to know" basis. Department leadership/school principals will sponsor awareness and training programs along with furnishing necessary staffing and material resources to ensure compliance with district wide security program

## **2.2 Data Custodians**

Data custodians are designated by the data owner to maintain the designated safeguards. Data custodians are responsible for authorizing access to data. Data custodians approve all accesses to resources under their responsibility, judge the asset's value and label the data as such, and ensure compliance with applicable controls through regular review of data classification and authorized access. Data custodians also assist data owners in assessing the risks to the confidentiality, integrity, and availability of applicable information and information resources.

## **2.3 Data Users**

Each user shall, within their capabilities, protect information and system/network resources against occurrences of sabotage, tampering, denial of service, fraud, misuse, or release of information to unauthorized persons. This includes protecting passwords and other account information; following appropriate policies, standards, processes, and procedures; and notifying appropriate authorities when incidents occur.

## **2.4 District Management**

DPS will comply with reasonable requests from law enforcement and/or federal, state, or local regulatory agencies for business data, personal data created/stored on DPS computing equipment, logs, diaries and archives on an individual's internet or email activity, stored internet, or email information.