

INFORMATION SECURITY For the purposes of this regulation, information security is generally defined as the protection of information and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction as described in CS (LOCAL). To ensure information security, the District must:

INTEGRITY

1. guard against improper information modification or destruction that includes ensuring information non-repudiation and authenticity; and

CONFIDENTIALITY

2. preserve authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

AVAILABILITY

3. ensure timely and reliable access to and use of information.

DEFINITIONS

The following terms, when used in this regulation, shall have the meanings as defined below.

1. **SCHOOL OFFICIALS:** Any employees, Trustees, or agents of the District, as well as attorneys, consultants, and independent contractors who are retained by the District. School officials have a "legitimate educational interest" in a student's record when they are working with the student; considering disciplinary or academic actions or the student's case; compiling statistical data; or investigating or evaluating programs.
2. **IPSP:** Information Privacy and Security Program.
3. **IPSO:** Information Privacy and Security Officer.
4. **PCI:** Payment Card Industry.
5. **GLB:** Gramm-Leach Bliley.
6. **FERPA:** Family Educational Rights and Privacy Act.
7. **HIPAA:** Health Insurance Portability and Accountability Act.
8. **USA PATRIOT Act:** Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

INFORMATION CLASSIFICATIONS

The District, as a public entity, is governed by the Texas Public Information Act, which requires disclosure of information by a public body unless the law specifically protects that information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected by District school officials. The information classification scheme must be reviewed annually by the District Information Privacy and Security Officer.

According to the Texas Administrative Code § 202.71, institutions of higher education are responsible for defining all information classification categories except the confidential information category, which is defined in Subchapter A of § 202.71, and establishing the appropriate controls for each category. These classifications are defined to ensure understanding and consistency in their application. The information classification scheme must be used throughout the District.

The following general categories of information serve to provide guidance for users and recipients in understanding how information is handled and protected by the District.

PUBLIC INFORMATION

This information is public and its disclosure is required by law.

INTERNAL INFORMATION

This information is generally considered only for internal use by District school officials as needed for their job functions and is not disclosable to the public unless required by law.

CONFIDENTIAL INFORMATION

This information is private and requires protection with the highest levels of security, as prescribed by applicable laws, regulations and standards including, but not limited to PCI

| | |
|--|---|
| INFORMATION REQUEST | <p>Data Security Standard, GLB, FERPA, HIPAA, USA PATRIOT Act and Texas Administrative Code, Information Security Standards for Higher Education. This information is available to District school officials on a need-to-know basis (based on applicable laws, regulations and standards).</p> <p>For written requests received for Student Directory Information, notify and send to the Registrar’s Office. For all other written requests, fax to District Legal. Questions regarding whether an employee has a “need-to-know” should be directed to the employee’s supervisor, the location Information Privacy and Security Officer, or the District Legal Counsel.</p> |
| GENERAL RESPONSIBILITIES | |
| EMPLOYEE | <p>Each employee is responsible for understanding and complying with the policies, standards, procedures and requirements relating to information privacy and security and for fully cooperating with the District staff to protect District information and information resources.</p> |
| DISTRICT INFORMATION SECURITY OFFICER | <p>The District Information Privacy and Security Officer, which is comprised of the IPSP Tri-Chairs, is designated to administer the Information Privacy and Security Program for the District.</p> |
| LOCATION INFORMATION SECURITY OFFICER | <p>An Information Privacy and Security Officer at each location is designated to establish and direct a location security program that ensures coordination of all District-wide and location policy functions and implementation of policy requirements.</p> |
| INFORMATION PRIVACY AND SECURITY REGULATIONS | |
| INTENT / DISSEMINATION | <p>It is the intent of the District in these regulations to implement the District's information privacy and security policy, CS(LOCAL), and to provide uniformity in addressing questions that arise in conjunction with the policy. [See CS(LOCAL).] If an employee encounters any problems with interpretation or application of the policy, standards, procedure or these regulations, the employee should notify their Location Information Privacy and Security Officer or District legal counsel.</p> |
| REVIEW / MODIFICATIONS | <p>The District Information Privacy and Security Officer will ensure that the policy procedure and regulations are reviewed periodically. The District Information Privacy and Security Officer shall also ensure that the policy and regulations are effective and are not obsolete by virtue of new technology or information. The District Information Privacy and Security Officer may recommend changes to the existing policy or regulation and present those recommendations to the Chancellor’s Cabinet.</p> |
| COMPLIANCE PROCESSES | |
| AWARENESS, TRAINING AND EDUCATION | <p>The purpose of this compliance process is to raise employee awareness and understanding concerning the policies, procedures and requirements relating to information privacy and security in order to protect District information and information resources.</p> |
| CONSEQUENCES OF VIOLATION | <p>Conduct involving information privacy and security is held to the same standards as any other conduct prescribed in this Manual. Violation of the policy or procedures are grounds for employee disciplinary action, up to and including termination. Employees may consult their location human resources director or District legal counsel with any questions regarding employee violations. The District shall take appropriate action against other school officials who violate this policy or procedures.</p> |

Employees shall comply with any other policies, regulations, and guidelines that impose duties, requirements, or standards attendant to their status as District employees. Violation of any policies, regulations, and guidelines may result in disciplinary action, including termination of employment. [See DM]

COOPERATION WITH
LAW ENFORCEMENT

It is the District's general policy procedure to cooperate with both formal and informal requests from law enforcement authorities when they seek access to information contained in the District's computing resources and facilities, subject to other applicable laws, such as the Family Educational Rights and Privacy Act (FERPA). Any request from law enforcement authorities that involves use or search of District computing resources or facilities shall be referred to District legal counsel.

QUESTIONS

Any questions regarding application of the policy procedure or these regulations should be directed to the location information privacy and security officer or District legal counsel.