TITLE: Information Security Training and Awareness

NUMBER: BUL-079114

ISSUER: Soheil Katal
Chief Information Officer

James Thurmond
Director, IT Security

DATE: June 30, 2020

ROUTING
All Employees
All Locations

POLICY: All employees (full or part time), contractors and volunteers are required to complete annual Information Security Training and Awareness instruction provided by the Information Technology Division.

MAJOR CHANGES: This is a new Policy Bulletin.

GUIDELINES:

I. BACKGROUND

Many District employees have regular access to sensitive information, which is protected with multiple layers of security. Employees are the first of these layers to protect District data but they are also the most vulnerable. Most data breaches start with an attacker exploiting the human nature of employees in various social contexts to gain access to sensitive information.

Currently, security controls designed to prevent the exploitation of District employees are limited. Most employees do not realize they are a target and are unsure how to prevent, identify, or report cybersecurity threats.

II. PURPOSE

The District has implemented an Information Security Training and Awareness (ISTA) program with the purpose of achieving the following strategic goals**:**

1. Improve the District's resilience to cybersecurity threats.
2. Establish a strong security-minded culture and integrate it into day-to-day District operations and decision-making.
3. Improve compliance with external regulatory and contractual requirements that require mandatory training and awareness (e.g. HIPAA).
4. Minimize the frequency and impact of security incidents.

III. REQUIREMENTS

A. SCOPE

Personnel with a Single Sign-On (SSO) account or access to protected District data are required to comply with this policy including but not limited to:

1. Classified Employees (full or part time)
2. Certificated Employees (full or part time)
3. Contractors
4. Volunteers

B. TRAINING PROGRAM

The cybersecurity training program must help new and ongoing employees and non-employees protect District information, understand risks to computer security, and successfully mitigate common cybersecurity threats. Annual basic cybersecurity training is mandatory and must be completed by the end of the calendar year. Additional security training may be assigned at the discretion of the department head.

1. ROLE-BASED TRAINING

The Information Technology Division has developed a series of educational videos highlighting tips for information security including showing users how to secure District data and accounts. The following table provides the mandatory training schedule for all applicable persons:

Table 1: Annual Training Schedule by Role

Role	Cybersecurity Topic			
	Basic Training	FERPA[1]	HIPAA[2]	IT Administration
Users with an SSO Account	✓			
Users with access to student records	✓	✓		
Users with access to protected health information	✓		✓	
IT Administrators	✓			✓

1. FERPA – Family Educational Rights and Privacy Act
2. HIPAA – Health Insurance Portability and Accountability Act

All required training must be based on a person's job duties and responsibilities as described in his/her job classification. For example, each year, School Nurses are required to complete the Basic cybersecurity training because they have SSO accounts and the HIPAA training because their job responsibilities require access to student Personal Health Information (PHI).

Training content is made available through the District's centralized learning management system, MyPLN. The ISTA program must track the progress of all trainees, evaluate their understanding of the content, and make them aware of their responsibility to protect District data.

2. COMPROMISED ACCOUNT TRAINING

SSO account owners are responsible for securing their passwords. However, if their passwords are believed to be compromised, their SSO account may be suspended in order to prevent unauthorized parties from accessing protected District data or performing illicit actions against District systems.

Owners of compromised SSO accounts are required to take a separate remedial cybersecurity training as a condition to restoring their SSO account privileges. Remedial training is limited in scope, which only addresses occasional gaps in employees' basic cybersecurity awareness when demonstrated by a verifiable information security risk. Remedial training cannot be substituted for or performed in lieu of the required annual training.

3. NEW EMPLOYEE TRAINING

All new employees are required to complete the basic cybersecurity training as part of their on-boarding process. In order to avoid suspension of the new employee's account, supervisors must ensure that all new hires complete their training before the completion of their probationary period.

4. EMPLOYEE TRAINING CERTIFICATION AND MONITORING

Certificates of Completion may be printed once they have passed an assessment test with a score of 100% and provide a copy to their immediate supervisor, who will keep them on file. Principals and supervisors are to ensure that their direct reports have completed their mandatory training.

C. AWARENESS PROGRAM

1. **EMPLOYEES**
   Due to rapidly changing cybersecurity threats, one (1) annual training alone will unlikely prevent employees from reverting back to unsecure cyber behaviors. Because human errors regarding computer security can lead to embarrassing and expensive consequences for the entire District, ITD must regularly maintain an awareness campaign to ensure that all employees remain aware of trends and threats in security.

   ITD will deliver monthly role-based security awareness materials such as tips and best practices, through a variety of communication methods. Awareness materials will reflect emerging threats and the needs of the District, which will make the awareness program effective and interesting.

2. **PARENTS**
   The ISTA program may include cybersecurity awareness content intended to inform parents on how to better protect their children and their personal data privacy while using the Internet. ITD is responsible for distributing and updating all parent awareness content provided through the ISTA program. Schools may elect to utilize the awareness content and integrate it into their parent engagement activities without restriction.

D. ADMINISTRATION AND GOVERNANCE

Computer security changes rapidly, and it's important that the District's ISTA program is regularly updated to reflect new risks and developments. The Director of IT Security will oversee the program. The Director of IT Security or his/her designee will conduct annual program reviews and deliver program performance metrics to the Chief Information Officer for the purpose of managing and improving the program.

Though this program is administered by ITD, it is the job of each individual District employee to complete the training by the due date. Any delay in work tasks or limited email access due to a disabled account is the responsibility of the employee. Supervisors should ensure that employees in their respective department are completing the required trainings on time to avoid any loss in productivity.

The owner of this document is the Director of IT Security, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Data collected from anti-phishing simulations, anonymous surveys, and periodic reviews
- Number of compromised accounts

IV. POLICY VIOLATION:

Failure to comply with this policy may result in suspension of the employee's SSO account. Violations may also result in discipline up to and including dismissal.

AUTHORITY: *California Education Code Sections 49060 et seq., 49073 et seq.*

ISO/IEC 27001 standard, clauses: *A.7.2.1, A.7.2.2, A.7.2.3*

RELATED RESOURCES: BUL-999.13 *"Responsible Use Policy (RUP) for District Computer and Network Systems"* dated March 5, 2019

BUL-1077.2 *"Information Protection Policy"* dated July 18, 2017

REF-3757 *"Description of Security Standards for Networked Computer Systems Housing Confidential Information"* dated June 13, 2007

Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g

Health Care Insurance Portability and Accountability Act ("HIPAA") Pub. L.104 – 191

ASSISTANCE: For further information, please contact IT Security at 213-241-5200 or information.security@lausd.net.