

Procedures for Security/IT Awareness Training and Testing

Table of Contents

1. Introduction 2
    a. Objective 2
    b. Scope 2
    c. Audience 2
    d. Document Changes and Feedback 2
    e. Referenced Documents 2
2. Procedure Requirements 3
    a. Information Security Awareness Training 3
    b. Simulated Social Engineering Exercises 4
    c. Remedial Training Exercises 4
3. Compliance with Procedure 4
4. Responsibilities and Accountabilities 5

1. Introduction

Technical security controls are a vital part of our information security framework but are not sufficient in them to secure all information assets. Effective information security also requires awareness and proactive support of all staff, supplementing and making full use of technical security controls. This is obvious in the case of social engineering attacks and other current exploits being used, which specifically target vulnerable humans rather than IT and network systems.

Lacking adequate information security awareness, staff is less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information assets at risk of compromise. To protect information assets, all workers must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

a. Objective

This procedure specifies the Jefferson County School District (JCSD) internal information security awareness and training program to inform and assess all staff regarding their information security obligations.

b. Scope

This procedure applies throughout the organization as part of the corporate governance framework. It applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience. This procedure also applies to third party employees working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

c. Audience

In general, this procedure applies to all JCSD employees and contractors with access to JCSD systems, networks, company information, nonpublic personal information, personally identifiable information, and/or customer data.

d. Document Changes and Feedback

This procedure will be updated and re-issued at least annually to reflect, among other things, changes to applicable law, updates or changes to JCSD requirements, technology, and the results or findings of any audit.

e. Referenced Documents

Documents that are relevant to this procedure include the following:

Procedure	Procedure Owner	Link
HR/Employee Handbook	Human Resources	https://www.jefferson.k12.ga.us/employee/employee-forms

2. Procedure Requirements

All awareness training must fulfill the requirements for the security awareness program as listed below:

- The information security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.
- Security awareness and training activities should commence as soon as practicable after staff join the organization, generally through attending information security induction/orientation as part of the on boarding process. The awareness activities should continue a continuous/rolling basis thereafter to maintain a reasonably consistent level of awareness.
- Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important.
- The company will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

a. JCSD Information Security Awareness Training

The JCSD Technology Department (IT) department requires that each employee upon hire and at least annually thereafter successfully complete these courses on our Global Compliance Network (GCN):

- Digital Security and Protection (which covers Password Security, Email Security and Vulnerabilities, Mobile Device Security, Prevention Strategies and Habits)
- Internet Safety (which covers Definitions of common internet terms; Awareness of Internet dangers; A perspective on students and adults today; Internet resources for school and home; and Recommendations for internet safety for school leaders and parents.)

- Computer Use Policy (users will learn about appropriate vs. inappropriate usage of computerized information resources in the workplace specifically as they relate to educational institutions.)
- Social Media Procedures (Protecting the students, staff and the school district; Raising awareness of acceptable ways to use electronic communication tools when communicating with students; and Raising awareness of the positive and negative outcomes that may result in using these tools with students.)

Phishing campaigns are executed monthly for staff via KnowBe4. We also have a program called Managed Methods that we use to prevent phishing attempts and malware from staff and student emails. Managed Methods also prevents login attempts outside of the United States.

Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Staff will be given a reasonable amount of time to complete each course so as to not disrupt business operations.

b. Simulated Social Engineering Exercises

The JCSD IT department will conduct periodically simulated social engineering exercises including but not limited to: phishing (e-mail), and physical assessments. The JCSD IT department will conduct these tests at random throughout the year with no set schedule or frequency. The JCSD IT department may conduct targeted exercises against specific departments or individuals based on risk determination.

c. Remedial Training Exercises

From time-to-time JCSD staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the JCSD IT department as part of a risk-based assessment.

3. Compliance with Procedure

Compliance with this procedure is mandatory for all staff, including contractors with local accounts and executives. The JCSD IT department will monitor compliance and non-compliance with this procedure and report to the executive team the results of training and social engineering exercises.

4. Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this procedure program.

The Technology/HR Department is responsible for developing and maintaining a comprehensive range of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other corporate functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of staff's responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Directors and Managers are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All Staff are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations always.