Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure defines the functional areas of the Office of Information Technology (IT) Cybersecurity Program in the Washoe County School District (District) to ensure adherence to the District's cybersecurity doctrine, processes, and standards. The IT Cybersecurity Program safeguards District information resources and technology assets in support of business systems and educational technology.

DEFINITIONS

1. "Chain of Custody" refers to a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle.

2. "Computer Forensics" refers to the application of investigation and analysis techniques to gather and preserve evidence from computing devices.

3. "Cybersecurity Incident" refers to an occurrence that results in the loss of confidentiality, integrity, or availability of District Information Resources.

4. "Defense in Depth" refers to a type of security architecture where several independent layers of security controls are used to complement and reinforce each other.

5. "Incident Response" refers to the people, processes, and technologies that support the District's ability to detect and respond to cybersecurity threats, breaches, and cyberattacks.

6. "Information Resources" refers to data, information bearing materials, and systems that support the District including networks, computers, software, and data.

7. "Personal Information" refers to information that could be used to identify a person, including their name, address, phone number, or numerical identifiers.

8. "Security Architecture" refers to a set of principles, methods, and models designed to align your objectives and help keep your organization safe from cyber threats.

9. "System Administrators" refers to the party or person responsible for installing, managing, and maintaining IT systems.

10. "System Owners" refers to the party or person responsible for business processes that IT assets support.

11. "Unencrypted" refers to information that is viewable in a clear-text, human or machine-readable form.

PROCEDURE

1. The District has established an IT Cybersecurity Program that takes a proactive approach to improving information security throughout all District operations to provide a safe and secure learning and computing environment.

2. The IT Cybersecurity Program is a holistic program to manage IT-related security risks. The program must be integrated into all aspects of District operations to be effective. District personnel must follow District policies, regulations, and procedures designed to protect Information Resources.

3. All District Staff, Students, and Contractors are responsible for the security and protection of Information Resources over which they have control including networks, computers, software, and data.

4. System Owners and Administrators must evaluate and secure District systems by performing holistic assessments of their processes and allocating resources to support safeguarding the physical and logical integrity of resources that they oversee. Information Resources must be protected against threats, such as unauthorized intrusion, misuse, or inadvertent compromise.

5. At all levels, the District must:

    a. Incorporate cyber risk management principles and best practices into District-wide strategic planning considerations, operations, business processes, and supporting District IT systems;

    b. Integrate cybersecurity requirements into IT planning processes at the District, departmental, and school levels;

    c. Ensure that District personnel identify and understand their role in protecting sensitive information under their direct management and control. Information systems must be protected with controls commensurate with the sensitivity of data stored or processed;

d. Implement processes and supportive technologies that bolster the IT Cybersecurity Program mission and capabilities by implementing the CIS Controls or equivalent standards where practicable; and

e. Meet regulatory, compliance, and Cybersecurity reporting requirements.

6. The IT Cybersecurity Program is divided into six key functional areas including:

    a. Governance;

    b. Cybersecurity Incident Response;

    c. Security Architecture and Engineering;

    d. IT Risk Management;

    e. Security Awareness and Training; and

    f. Cyber Threat Intelligence.

7. Cybersecurity Governance:

    a. The District maintains an IT Cybersecurity Governance Working Group that serves in an advisory capacity to coordinate the implementation, support, and management of the District IT Cybersecurity Program.

    b. The Cybersecurity Working Group provides oversight, strategy, and expert counsel to ensure that the IT Security Program can best respond to emergent cyber threats while meeting the District's regulatory and operational requirements.

    c. The IT Security Department maintains and documents the Cybersecurity Program implementation by maintaining an IT Cybersecurity plan based on the Center for Internet Security (CIS) controls or equivalent National Institute for Standards and Technology (NIST) standards.

8. Cybersecurity Incident Response:

    a. The District maintains Cybersecurity Incident Response capabilities including resources and personnel designated to respond to cybersecurity incidents using documented plans and procedures that support direct response, investigation, and recovery.

    b. The Office of Information Technology establishes and maintains a process for reporting IT Cybersecurity incidents from the workforce to the IT Security department. Reporting processes will be provided to District employees through the Emergency Operations Plan (EOP).

c. Incident Responders coordinate with internal and external support agencies, including law enforcement, insurance providers, and threat intelligence or information sharing networks.

d. Internal and third-party data breach disclosures must meet or exceed statutory and regulatory reporting requirements by notifying affected parties that their unencrypted Personal Information (PI) has been, or is reasonably believed to have been, accessed or acquired by an unauthorized party following discovery or notification of breach provided by a third-party or Service Provider.

9. Security Architecture and Engineering:

i. The District implements protective, detective, and response technologies to safeguard District Information Resources.

ii. Security technologies are implemented in a "data-focused" security architecture which protects systems with safeguards commensurate with the sensitivity of the data or resources being protected.

iii. IT Security Architecture must be implemented as a complementary suite of host, network, and enterprise protections that safeguard information systems using a "Defense in Depth" strategy.

iv. Information Systems must be:

a. Implemented to provide the least privilege by only assigning necessary rights and functions to support legitimate District business and restrict capabilities that are redundant or unnecessary;

b. Securely configured or "hardened" according to vendor guidance, industry best practices, CIS benchmarks, or equivalent security standards;

c. Monitored to identify anomalous system behavior, unauthorized use, and data ingress/egress through centralized log collection; and,

d. Centrally managed using Enterprise IT Tools.

v. Technologies and activities outsourced to third-party Service Providers must comply with appropriate security measures equivalent security measures as internal capabilities.

10. IT Risk Management:

    a. The District identifies risks, vulnerabilities, and the probability that these factors will result in an exposure resulting in a financial or operational loss to the District impacting resources supporting business objectives or student learning.

    b. Risks must be addressed appropriately through risk treatment strategies, including mitigations or countermeasures. District leaders must provide adequate resources to ensure that the activities of their respective departments and schools may be performed safely and securely.

11. Security Awareness and Training:

    a. IT Cybersecurity Program addresses human vulnerability by ensuring that employees at every level of the District are provided with current and relevant IT Cybersecurity Awareness training.

    b. Example training topics include:

        i. Secure Authentication best practices;

        ii. Social Engineering;

        iii. Secure data handling;

        iv. Causes of unintentional data exposure;

        v. Cybersecurity Incident reporting;

        vi. Ensuring systems have installed all available patches and updates;

        vii. Risks of connecting to unsecure networks.

    c. Training should be role specific, when practicable.

    d. Simulations and exercises (simulated or live) may be performed to assess and improve readiness.

12. Cyber Threat Intelligence:

    a. The IT Security Department performs internal data collection and monitors third-party Cyber Threat Intelligence feeds to identify actionable insights that may be used to bolster IT Cybersecurity capabilities.

    b. System Administrators must leverage intelligence insights and configure IT systems to address newly emerging adversary tools, tactics, and procedures identified through the Cyber Threat Intelligence mechanisms.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:
    a. Board Policy 7205, Information Technology – Data Access; and
    b. Board Policy 7210, Information Technology Services and Operations.
2. This Administrative Procedure aligns and complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC), to include:
    a. NRS Chapter 603A, Security and Privacy of Personal Information.

REVISION HISTORY

Date	Revision	Modification
09/06/2024	v1	Adopted