Information Security and Privacy Program

INTRODUCTION

The District shall create and implement an Information Security and Privacy Program that provides clear and comprehensive information and administrative procedures on the prescribed measures to be used to establish and enforce the cybersecurity program in the District.

The District is committed to protecting its students, employees, partners, clients and District information technology infrastructure from damaging acts that are intentional or unintentional. Effective information security and privacy protection is a team effort involving the participation and support of District employees and every vendor, community partner, or external entity that interacts with District data and/or systems. Therefore, the District will provide District cybersecurity requirements to every vendor, community partner, or external entity. The cybersecurity requirements shall be incorporated into any contract, data sharing agreement, or memorandum of agreement between the District and a vendor, community partner, or external entity.

Protecting District data and the systems that collect, process, and maintain data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset potential threats, as well as controls to ensure the confidentiality, availability, and integrity of District data.

Commensurate with risk, cybersecurity and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of District data and systems. This also includes protection against accidental loss or destruction. The security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure Confidentiality, Integrity, Availability, and Safety (CIAS).

PURPOSE

The purpose of the Information Security and Privacy Program is to prescribe a comprehensive framework through a set of administrative procedures for:

- Creating a leading practice-based Information Security Management System (ISMS) that is structured on the NIST Cybersecurity Framework (CSF);
- Protecting the Confidentiality, Integrity, Availability, and Safety (CIAS) of District data and systems;
- Protecting the District, its employees, and its clients from illicit use of District systems and data;
- Ensuring the effectiveness of security controls over data and systems that support the District's operations;
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review, and maintenance of minimum security controls required to protect support the District's data and systems.

Information Security and Privacy Program

PURPOSE (CONTINUED)

The formation of the cybersecurity policy and administrative procedures is driven by many factors, with the key factor being a risk. The policy and related administrative procedures set the ground rules under which the District operates and safeguards District data and systems to both reduce risk and minimize the effect of potential incidents.

The administrative procedures, including control objectives, standards, processes, and guidelines, are necessary to support the management of information risks in daily operations. The development of administrative procedures provides clarity to ensure District users understand their day-to-day security responsibilities and the threats that could impact the District.

Implementing consistent security controls across the District will help the District comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of District data.

SCOPE & APPLICABILITY

The Information Security and Privacy Program established in this policy and related administrative procedures shall apply to all District data, systems, activities, and assets owned, leased, controlled, or used by the District, its agents, contractors, or other business partners on behalf of the District. The administrative procedures apply to all District employees, contractors, sub-contractors, and their respective facilities supporting District business operations, wherever District data is stored or processed, including any third-party contracted by the District to handle, process, transmit, store, or dispose of District data.

Some documents apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting District business functions shall comply with the administrative procedures.

The administrative procedures do not supersede any other applicable law or Board Policy or existing labor management agreement approved by the Board.

The District may revoke, change, or supplement the administrative procedures, including control objectives, standards, processes, and guidelines at any time without prior notice. Such changes shall be effective immediately unless otherwise stated.

POLICY OVERVIEW

To ensure an acceptable level of cybersecurity risk, the District shall design, implement and maintain a coherent set of administrative procedures, including control objectives, standards, processes and guidelines to manage risks to its data and systems.

District users are required to protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of data and systems, regardless of how its data is created, distributed or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

Information Security and Privacy Program

ADMINISTRATIVE PROCEDURES OVERVIEW

The administrative procedures for the District Information Security and Privacy Program may include, but not be limited to, the following:

Security & Privacy Governance (GOV)
Management Intent: The purpose of the Security & Privacy Governance (GOV) administrative procedure is to specify the development, proactive management and ongoing review of the District's security and privacy program.
Summary: The District shall protect the confidentiality, integrity, availability and safety of its data and systems, regardless of how its data is created, distributed or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all statutory, regulatory and contractual obligations.

Asset Management (AST)
Management Intent: The purpose of the Asset Management (AST) administrative procedure is to ensure that technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal.
Summary: The District shall protect its assets and data by implementing and maintaining appropriate IT Asset Management (ITAM) business practices across the enterprise.

Business Continuity & Disaster Recovery (BCD)
Management Intent: The purpose of the Business Continuity & Disaster Recovery (BCD) administrative procedure is to establish processes that will help the District recover from adverse situations with the minimal impact to operations.
Summary: The District shall establish and manage the capability for maintaining the Continuity of Operations (COOP) to ensure the availability of critical technology resources during adverse conditions.

Capacity & Performance Planning (CAP)
Management Intent: The purpose of the Capacity & Performance Planning (CAP) administrative procedure is to prevent avoidable business interruptions caused by capacity and performance limitations through requiring both technology and business leadership to maintain situational awareness of current and future performance.
Summary: The District shall protect against avoidable impacts to operations by proactively managing the capacity and performance of its critical technology and supporting infrastructure.

Change Management (CHG)
Management Intent: The purpose of the Change Management (CHG) administrative procedure is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

Information Security and Privacy Program

ADMINISTRATIVE PROCEDURES OVERVIEW (CONTINUED)

Summary: All technology changes to production environments must follow a standard process to reduce the risk associated with change. The District requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change on a production network.

Compliance (CPL)
Management Intent: The purpose of the Compliance (CPL) administrative procedure is to ensure safeguards are in place to be aware of and comply with applicable statutory, regulatory and contractual compliance obligations.
Summary: In accordance with all applicable legal requirements, the District shall ensure appropriate safeguards are in place to protect sensitive business data against loss, unauthorized access or disclosure.

Configuration Management (CFG)
Management Intent: The purpose of the Configuration Management (CFG) administrative procedure is to establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced.
Summary: All technology platforms must adhere to configuration management requirements. The District shall maintain accurate inventories of its technology platforms and enforce security configuration settings those technology platforms used in support of the District's business operations.

Continuous Monitoring (MON)
Management Intent: The purpose of the Continuous Monitoring (MON) administrative procedure is to establish and maintain situational awareness across the enterprise through the centralized collection and review of security-related event logs. Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the District will have "blind spots" in its situational awareness that could lead to system compromise and / or data exfiltration.
Summary: Only through the ongoing and continuous monitoring of the District's technology assets can situation awareness of cybersecurity events be maintained. Therefore, technology assets must adhere to configuration management requirements to log security events and forward those events to allow for the centralized monitoring and review of logs to identify anomalous behavior so that appropriate steps can be taken to remediate potential cybersecurity incidents.

Cryptographic Protections (CRY)
Management Intent: The purpose of the Cryptographic Protections (CRY) administrative procedure is to ensure the confidentiality of the District's data through implementing appropriate cryptographic technologies to protect systems and data.
Summary: Appropriate cryptographic safeguards must be used to protect sensitive business data against loss, unauthorized access or disclosure. This applies to data, regardless if it is at rest or in transit.

Information Security and Privacy Program

ADMINISTRATIVE PROCEDURES OVERVIEW (CONTINUED)

Data Classification & Handling (DCH)
Management Intent: The purpose of the Data Classification & Handling (DCH) administrative procedure is to ensure that technology assets are properly classified and measures are implemented to protect the District's data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity and availability of data.
Summary: In accordance with all applicable legal requirements, the District shall protect data in both hardcopy and digital form by limiting access to authorized users and utilize methods of sanitizing or destroying media so that data recovery is technically infeasible.

Endpoint Security (END)
Management Intent: The purpose of the Endpoint Security (END) administrative procedure is to ensure that endpoint devices are appropriately protected from reasonable threats to the confidentiality, integrity, availability and safety of the device and its data. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity, availability and safety considerations.
Summary: The District shall implement the concept of "least functionality" for its technology endpoints and proactively govern security mechanisms to keep its technology assets secure from evolving threats.

Human Resources Security (HRS)
Management Intent: The purpose of the Human Resources Security (HRS) administrative procedure is to create a security-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.
Summary: The District shall ensure industry-recognized leading practices for cybersecurity are incorporated into Human Resources (HR) personnel management practices

Identification & Authentication (IAC)
Management Intent: The purpose of the Identification & Authentication (IAC)) administrative procedure is to implement the concept of "least privilege" through limiting access to District systems and data to authorized users only.
Summary: The District shall implement the principle of "least privilege" within logical access control mechanisms so that only authorized users can gain access to District systems and data.

Incident Response (IRO)
Management Intent: The purpose of the Incident Response (IRO) administrative procedure is to establish and maintain a capability to guide the District's response when security-related incidents occur.
Summary: The District shall maintain a cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery and reporting activities.

Information Security and Privacy Program

ADMINISTRATIVE PROCEDURES OVERVIEW (CONTINUED)

Maintenance (MNT)
Management Intent: The purpose of the Maintenance (MNT) administrative procedure is to ensure that due diligence is performed by properly maintaining District technology assets across the enterprise.
Summary: In order to minimize risk from evolving threats, the periodic and ongoing maintenance and upgrades of District assets shall be performed and governed accordingly, including technology assets owned or maintained by trusted third-parties.

Network Security (NET)
Management Intent: The purpose of the Network Security (NET)) administrative procedure is to ensure sufficient security controls are in place to protect the confidentiality and integrity of the Districts communications, as well as to provide situational awareness of activity on the District's networks.
Summary: The District shall implement the concept of "least functionality" for its network infrastructure and proactively govern security mechanisms to keep its networks secure from evolving threats, while providing situational awareness of network activities so that proactive measures can be implemented to address evolving threats.

Physical & Environmental Security (PES)
Management Intent: The purpose of the Physical & Environmental Security (PES) administrative procedure is to minimize risk to District systems and data by addressing applicable physical security and environmental concerns.
Summary: The District shall implement appropriate physical access controls to limit access to systems, equipment and the respective operating environments to authorized individuals. The District shall provide appropriate environmental controls in facilities containing systems to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions.

Project & Resource Management (PPM)
Management Intent: The purpose of the Project & Resource Management (PRM) administrative procedure is to ensure resource management addresses cybersecurity requirements across project and program management enterprise-wide, regardless of the type of the project.
Summary: Risk must be managed throughout the System Development Life Cycle (SDLC). Therefore, all technology projects and programs shall address resource requirements to implement and maintain appropriate security controls through the life cycle of the asset(s) or service(s).

Risk Management (RSK)
Management Intent: The purpose of the Risk Management (RSK) administrative procedure is to ensure that cybersecurity-related risk is visible to and understood by the business unit(s) that own the assets and/or processes involved. Since the cybersecurity team merely facilitates and educates the management of risk, business units and other key stakeholders are expected to be active participants in J the District's risk discussions.
Summary: The management of risk at the appropriate level of corporate management is of critical importance to the District's long-term success. Therefore, the District shall periodically assess the

Information Security and Privacy Program

ADMINISTRATIVE PROCEDURES OVERVIEW (CONTINUED)

risk to operations, assets and data that are associated the processing, storage or transmission of information to support the District's business processes and take appropriate action to remediate unacceptable risks.

Secure Engineering & Architecture (SEA)
Management Intent: The purpose of the Secure Engineering & Architecture (SEA) administrative procedure is to align cybersecurity decisions with the corporate architectural strategy and industry-recognized leading practices for secure engineering.
Summary: The District relies on its technology strategy and architecture to ensure its success in the long-term. This requires its cybersecurity architecture to support both its technology architectural direction and business strategy. Furthermore, the District's secure engineering principles must address applicable statutory, regulatory and contractual obligations to implement and manage reasonable security measures, as defined by industry-recognized leading practices.

Security Awareness & Training (SAT)
Management Intent: The purpose of the Security Awareness & Training (SAT) administrative procedure is to develop a security and privacy-minded workforce.
Summary: The District shall ensure that users are made aware of the security and privacy risks associated with their roles and that users understand the applicable statutory, regulatory and contractual compliance requirements related to the security and privacy of systems and data within their sphere of influence.

Technology Development & Acquisition (TDA)
Management Intent: The purpose of the Technology Development & Acquisition (TDA) administrative procedure is to ensure secure technologies are developed and / or acquired.
Summary: The District shall implement the principles of "least privilege" and "least functionality in the development and implementation of technology, regardless if it is internally-developed or acquired from a third party. Technology development and acquisition must employ adequate security measures during all phases of the System Development Life Cycle (SDLC) to ensure security and privacy-related risks are identified and appropriately remediated.

Third-Party Management (TPM)
Management Intent: The purpose of the Third-Party Management (TPM) administrative procedure is to ensure that security and privacy risks associated with third-parties are minimized or avoided.
Summary: The District must assess the cybersecurity and privacy risks posed by both its current and potential third-party providers. It is imperative that the District's third-parties implement mechanisms to identify and remediate deficiencies and / or vulnerabilities on an ongoing basis, in order to ensure the continued effectiveness of security and privacy controls. As third-party providers' technology and processes evolve over time, the District must ensure the appropriate levels of due care and due diligence are applied to validate that appropriate security and privacy controls are effective.

Information Security and Privacy Program

ADMINISTRATIVE PROCEDURES OVERVIEW (CONTINUED)

Threat Management (THR)

Management Intent: The purpose of the Threat Management (THR) administrative procedure is to establish a capability to proactively govern technology-related threats to the security and privacy of the District's systems, data and business processes.

Summary: The District shall implement the capability to proactively govern threats that include the identification, assessment and remediation of threats to District systems, data and business processes.

Vulnerability & Patch Management (VPM)

Management Intent: The purpose of the Vulnerability & Patch Management (VPM) administrative procedure is to proactively manage the risks associated with technical vulnerability management.

Summary: Vulnerability management is a never-ending process that requires the District to proactively manage vulnerabilities both in how its assets are configured and the level of currency in software patching. Therefore, the District shall apply a risk-based approach minimize its attack surface area through aggressive vulnerability management and patching operations.

VIOLATIONS OF THIS POLICY AND RELATED ADMINISTRATIVE PROCEDURES

In accordance with KRS 160.290 and Board Policy 01.5, all policies of the Board are binding on employees of the District, schools, students, and on the Board itself. Employees and students who fail to comply with Board policies and related administrative procedures may be subject to disciplinary action.

UPDATES TO THIS POLICY AND RELATED ADMINISTRATIVE PROCEDURES

Updates to the Information Security and Privacy Program policy and related administrative procedures will be announced to employees via management updates or email announcements. Changes will be noted in an Information Security and Privacy Program Record of Changes to highlight the pertinent changes from the previous administrative procedures.

District administrative procedures for the Information Security and Privacy Program, are maintained by the District and available on the webpage for the Information Technology Division at https://www.jefferson.kyschools.us/department/information-technology.

RELATED POLICIES:

01.5; 01.61

REFERENCES:

Information Security and Privacy Program Procedures Incorporated by Reference