Book	Administrative Regulations
Section	3000 BUSINESS & INSTRUCTION SUPPORT OPERATIONS
Title	District Information Security Program
Code	AR 3522
Status	First Reading
Cross References	BP 1700 - Relations Between Private Industry and the Schools BP 3580 - District Records BP 4112.6 - Personnel Records BP 4119.23 - Unauthorized Release of Confidential Information BP 4119.25 - Political Activities of Employees BP 5125 - Student Records AR 1340 - Access to District Records AR 4119.25 - Political Activities of Employees

Introduction

The Kenai Peninsula Borough School District Information Services department has a responsibility to protect sensitive District data to include financial, employee, and student data, while allowing for a positive learning environment. The objective is to employ technology resources that create equitable and accessible learning systems that make learning possible everywhere and all the time.

Program elements described are informed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Utilizing the NIST CSF framework allows KPBSD to tailor associated security controls based on risk tolerance. The following sections describe the framework and provide an outline of implementation.

Section 1. Framework

The District recognizes an effective information security program (ISP) is essential to protecting sensitive data and ensuring information technology enables a rich learning environment. The Director of Information Services is responsible for ensuring recommendations made by Information Service staff are implemented in a manner designed to protect District information and resources. The information security framework will employ a layered defense strategy with protocols to prevent, detect, and respond to potential threats. The core framework shall be implemented through a combination of people, processes, and technologies capable of meeting the requirements and standards. In addition, the Information Services department will develop and maintain a knowledge base that will act as a document and information repository for all information security related information. The following sections outline the core governance framework for the ISP.

- Information Security
- Governance Network Security
- Endpoint Security
- Application Security
- Data Security and
- Protection Identity & Access Management

Section 2. Information Security Governance

The Information Services department shall establish a governance structure to ensure the confidentiality, integrity, and availability of District systems and data. The Information Services department shall maintain an electronic document repository with all required procedures, guidelines, and checklists including the following elements:

- **Information Security Plan** – Develop and implement an ISP that provides an overview of District information security requirements and describes the controls, responsibilities, and expected behavior of
- individuals who access various systems. **Incident Response Plan** – Develop and establish an incident response plan that provides a set of instructions to help staff detect, respond to, and recover from network security incidents and document the approved recovery process. The Data Protection Leader shall update the incident response plan annually.
- **Configuration / Change Management Plan** – Develop and establish a formal process for change and configuration management where appropriate
- **Risk Management Plan** – Develop and establish a formal risk management plan related to Information Technology operations.
- **Business Continuity / Disaster Recovery (BC/DR) Plan** – Develop, implement, manage, and train a
- BC/DR plan. **Security Awareness Training** – Develop and establish a district information security awareness training program. This program shall include, at minimum, annual information security exercises.

Section 3. Network Security

The Director of Information Services shall implement adequate policies, procedures, and technical controls to protect the security of the network to include the following elements at a minimum:

- **Perimeter Security** - Develop and deploy network security devices and tools in such a manner as to ensure District data is appropriately protected from unauthorized use or access.
- **Network Design Documentation** - Develop and update network diagrams as needed and should include the following information at a minimum:

    - All entry points from the Internet
    - All firewalls, switches, routers, and wireless access
    - points Type, size, and bandwidth of all connections
    - External IP address and Internal virtual local area networks
    - (VLANs) Externally connected systems

- **Firewall Security** - Ensure the firewall configuration is documented and configured in accordance with District requirements. Policies for firewall rule changes, audit logging, and monitoring and managing perimeter and internal firewalls must be established and maintained at all times.
- **Remote Access** – Establish a secure process and deploy effective controls for remote access to District resources and. monitor remote access through approved monitoring tools to prevent unauthorized access.
- **Router and Switch Security -** Develop standards and configure routers and switches in accordance with best practices. Switch and router configurations shall be backed up as needed and routine audits should be conducted to ensure configurations are correct.
- **Wireless Security –** Enable and secure District wireless access points and networks in accordance with industry and manufacturer best practices.
- **Internet Use** - Will be monitored and manage in accordance with a District Internet Use policy and at a minimum filtered in accordance with legal requirements such as CIPA, FERPA, etc.
- **Network Monitoring -** The District must maintain an appropriate network monitoring capability to detect, identify, respond, and recover from network security events.
- **Vulnerability & Patch Management –** The District must develop and maintain an effective vulnerability and patch management process. This process shall include capabilities to scan the network for vulnerabilities and ensure appropriate system/software patches have been implemented.
- **Ports & Protocols –** The must develop and maintain a ports and protocols list to include permissible and blocked ports and protocols.

Section 4. Endpoint Security

The Director of Information Services shall implement adequate policies, procedures, and technical controls that require endpoint device compliance before they are granted access to network resources. At a minimum the program will include:

- **Mobile Device Management** – Deploy network security devices and tools in such a manner to ensure District data is appropriately protected from unauthorized use or access and can be remotely managed.
- **Anti-Virus Protection** – Deploy effective anti-virus protection throughout the District. Update and monitor this program routinely.
- **Vulnerability & Patch Management –** Develop and maintain an effective vulnerability and patch management process. Include capabilities to scan endpoints for vulnerabilities and implement appropriate system/software patches.
- **Endpoint Monitoring** - Assess and deploy an endpoint solution that addresses malware exploits by observing attack techniques and behaviors. Coordinate enforcement with network and cloud security to prevent successful attacks.

Section 5. Application Security

The Director of Information Services shall implement adequate policies, procedures, and technical controls that enable application security. At a minimum the program will include:

- **Software Inventory** - The Information Services department shall develop and maintain a software inventory of applications, systems, and databases for the District.
- **Application Access Management** – The Information Services department shall work with system owners to ensure appropriate application access controls are in place to protect information.
- **Data at Rest** – The Information Services department shall implement data at rest controls as deemed appropriate in support of the District's risk appetite.

Section 6. Data Security

The Director of Information Services shall implement appropriate policies and technical and physical controls to protect sensitive data. The Information Services department shall work with data owners to identify sensitive data and implement controls to allow for the timely detection, response, and recovery of unauthorized access or handling of sensitive data. At a minimum the program:

- **Cloud Security** - Shall develop and maintain a process for managing all cloud applications and identifying the types of data being stored.
- **Data Backup** – Shall develop, implement, and maintain data backup support based on coordinated Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and outline off-site and off-line backup requirements.
- **Data in Transit** – Shall consider data in transit controls as deemed appropriate.
- Account for and maintain the specific controls for externally managed systems accessed by the district in the normal course of business. Examples of this may include the Criminal Justice Information Services (CJIS) which requires the Information Services department to work with a Local Agency Security Officer (LASO) to implement compliant security measures and procedures.

Section 7. Identity & Access Management

The Director of Information Services shall implement adequate policies, procedures, and technical controls that comply with an established framework, such as NIST, and/or best practices. At a minimum the program will:

- **User Management** - Develop and maintain a directory service to manage user access to various IT resources such as systems, devices, applications, storage systems, and networks. The directory service and associated automation should enable admins to control user access and on-board and off-board users to and from IT resources. The directory service must authenticate, authorize, and audit user access to IT resources.

- **Privileged Account Management** – Ensure appropriate application/system access controls for various applications, systems, and network administrators.
- **Least Privilege** – Implement the principle of least privilege across the enterprise.
- **Access Controls** – Implement district-wide role-based access controls.
- **Multi-Factor Authentication** – Assess and deploy multi-factor authentication as deemed appropriate.

Legal References:
47 U.S.C. 201 et seq., Communications Decency Act of 1995, as amended.
20 U.S.C. 1232g., Federal Family Educational Rights and Privacy Act of 1974, as amended.
47 U.S.C. 231 et seq., Children's Online Privacy Protection Act of 2000, as amended.