Broward County Public Schools
Information Security Guidelines

Contents

1.0 - Introduction

The School Board of Broward County (SBBC) Policy 5306, *School and District Technology Usage* and the Broward County Public Schools (BCPS) *Acceptable Use of Information Resources Guidelines* provide overarching governance of district technology resources and provide the foundation for other Information Technology and internally scoped Information Technology standards, guidelines, and procedures, to include this guideline.

Under the authority of the Chief Information Officer (CIO), Information Technology Security leads a comprehensive information security program to effectively manage risk and ensure the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

The Information Security Guideline, aligns with SBBC Policy 5306, *School and District Technology Usage* and the BCPS *Acceptable Use of Information Resources Guidelines*, is the cornerstone of the district's information security program and provides the foundation for ensuring the confidentiality, integrity, and availability of information assets. This guideline outlines the principles, practices, and expectations that govern BCPS' approach to information security. Remember, security is a shared responsibility, and as such, this guideline is applicable to faculty, staff, students, volunteers, vendors, and any other individual utilizing district-provided technology resources.

2.0 - Security Principles and Practices

Security principles are overarching concepts that should be followed when developing or acquiring technology. Principles address information systems security from a high-level viewpoint and cover areas such as accountability, cost-effectiveness, and integration.
The principles contained in this section are based on the National Institute of Standards and Technology (NIST) Special Publication 800-series, a broadly reviewed and accepted set of security frameworks.

- **Information security supports the mission of the district.** Information security's role is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, information security helps the district protect its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.
- **Information security is an integral element of sound management.** Information systems are critical assets supporting the mission of the district. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or people.
- **Information security should be cost-effective.** The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure the cost of controls does not exceed expected benefits. Security should be appropriate and

proportionate to the value of and degree of reliance on the IT (Information Technology) systems and to the severity, probability, and extent of potential harm.

- **Information security responsibilities and accountability should be made explicitly.** The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be clearly defined.
- **Information security requires a comprehensive and integrated approach.** Providing effective information security requires a comprehensive approach that considers a variety of areas both within and outside of IT. This comprehensive approach extends throughout the entire information life cycle. To work effectively, security controls often depend upon the proper functioning of other controls.
- **Information security should be assessed periodically.** Information systems and the environments in which they operate are dynamic, and changes in the system or the environment can create new vulnerabilities so the information security program should be regularly reviewed to ensure it continues to function as intended.

While security principles are broad, security practices are specific in nature and serve as a reference guide. They establish a common baseline of requirements to be followed by district personnel. The remainder of this document focuses primarily on security practices.

3.0 - Risk Assessment

Risk assessment in cybersecurity involves identifying, analyzing, and evaluating potential risks and vulnerabilities to the district's information systems, networks, and data. The goal is to understand the potential impact of threats and the likelihood of these threats occurring so the district can make informed decisions about how to manage and mitigate those risks effectively. By assessing risks, the district can prioritize security efforts and allocate resources effectively to address the most critical threats first.

Different situations require different methods of risk assessment; however, the following guidelines and standards should be consulted when performing a risk assessment.

- NIST Cybersecurity Framework: The National Institute of Standards and Technology Cybersecurity Framework provides a comprehensive approach to managing cybersecurity risk.
- ISO/IEC 27001 Standard: Outlines best practices for establishing, implementing, maintaining, and continually improving an information security management system.
- PCI DSS: The Payment Card Industry Data Security Standard provides requirements for securing payment card transactions and protecting cardholder data.
- COBIT: Control Objectives for Information and Related Technologies is a framework for governance and management of enterprise IT that includes guidance on risk management.

3.1 - Responsibilities:

To be effective, risk assessment requires input from a variety of people. In general, risk assessment will involve the IT security team and may include system administrators, network engineers, and other IT personnel to help provide technical expertise and insights. Additionally, the risk assessment will include the system/process/business owners; they are responsible for understanding and accepting the risks identified during the assessment and making decisions about risk mitigation strategies.

Each of the following items are important to the overall success of the risk assessment process.

- The district must maintain an accurate inventory of information and technology resources and associated owners.
- Identified vulnerabilities in and threats to the district's information and technology assets and the potential harm to the district's reputation, finances, and operations if a vulnerability is exploited must be documented.
- Acceptable risk levels and risk mitigation strategies for each information and technology resource must be documented. **Note:** Acceptance of risk is a joint decision made by the Information and Technology Resource Owner, in consultation with The Director of Information Security or designee, for resources that have a Low or Moderate risk. For resources that have a High risk, the Chief Information Officer, or designee, decides what is acceptable and will consult with the Information and Technology Resource Owner and The Director of Information Security.

3.2 - Information Technology Projects:

Project Managers must perform annual security assessments, in collaboration with the Director of Information Security, of the implementation of required security controls for projects under their authority.

3.3 Risk Assessment of Third-party Service Providers:

A risk assessment of a third-party service provider is required in the following situations:

- when purchasing services that result in exchange of or access to sensitive district data or
- when purchasing systems or software, whether it is to be hosted on premises or at a vendor facility, sensitive district data will be stored within or processed by the system or software.

4.0 - User Account Management

The district has standardized processes for requesting, creating, assigning, tracking, and closing user accounts. The processes follow two essential principles:

- **Separation of Duties:** Roles and responsibilities are divided so no single person can undermine critical processes. Separation of duties helps prevent potential abuse of power.
- **Least Privilege:** Users are granted access only to the functions necessary for them to carry out their official duties. This minimizes the risk of unauthorized actions.

The district regularly reviews user accounts to ensure the integrity of user account management. These reviews examine access levels, adherence to the principle of least privilege, account activity, updated authorizations, and completion of required training.

Additionally, the district employs various mechanisms, including auditing and analysis of audit trails, to detect any unauthorized or malicious activities.

5.0 - Data Protection

Protecting SBBC data from unauthorized access, use, modification, or destruction must be given top priority. Towards that end, the following must be followed by anyone using district information and technology resources.

5.1 - Third-Party Service Providers Storing District Data

District data may not be stored on personally procured third-party storage services. Any third-party service storing district data must have a district approved agreement in place.

5.2 - Password and Encryption Protection for Sensitive District Data

Passwords and encryption are key parts of the district's data protection processes.

Users must enter a district approved password before being granted access to a district computer system. When possible, multi-factor authentication must also be employed. Additionally, USB thumb drives and similar removable storage devices owned, leased, or controlled by the district must be encrypted, using methods approved by the Director of Information Security before storage of any sensitive district data on the device.

Best practice is to not store sensitive district data on personally owned devices; however, the CIO may, after consulting with the business owner and the Director of Information Security, determine there is a valid business need and an acceptable risk level that warrants storing sensitive district data on personally owned devices.

5.3 - Protecting Data in Transit

Data Owners shall implement appropriate administrative, physical, and technical safeguards necessary to adequately protect the security of sensitive data during transport and electronic transmissions. At a minimum, data owners must do each of the following:

- ensure sensitive data is properly labeled as such and that its transmission is necessary to achieve the intended business objective.

- encrypt sensitive information before it is transmitted over the Internet.
- properly dispose of sensitive information in accordance with district policies, standards, guidelines, and practices.

5.4 - Media Protection

Any media containing district data must be discarded in a manner that adequately protects the confidentiality of the data and renders it unrecoverable, such as overwriting or modifying the media to make it unreadable, indecipherable, or otherwise physically destroying the electronic media.

6.0 - Contingency Planning

Owners of systems and data considered mission critical must have a disaster recovery plan commensurate with the risk and value of the systems and data. The disaster recovery plan must incorporate procedures for:

- recovering data and restoring the system to operational status following any event that denies access to the data and our system for an extended period (e.g., natural disasters, terrorism).
- assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions.
- testing the disaster recovery plan and procedures every two years at minimum (the results of the test should be documented and maintained).
- presenting the disaster recovery plan and testing results for review to the Director of Information Security and other stakeholders.

7.0 - Incident Response

A cybersecurity incident refers to any event or occurrence that jeopardizes the confidentiality, integrity, or availability of information systems, networks, or data. These incidents can take various forms and may include unauthorized access to systems, data breaches, malware infections, denial-of-service attacks, insider threats, and other malicious activities. In simpler terms, a cybersecurity incident is any event that poses a threat to the security of the district's information and technology resources. The severity and impact of a cybersecurity incident can vary depending on factors such as the nature of the attack, the vulnerabilities exploited, and how effective the district's security measures are.

Handling cybersecurity incidents requires swift and effective response to mitigate damages, contain the threat, and restore normal operations. This often involves activities such as incident detection, analysis, containment, eradication of threats, recovery of affected systems and data, and post-incident evaluation to learn from the experience and improve security measures for the future.

While some aspects of incident response are covered by the district's contingency plan there are also specific cybersecurity incident response procedures. The response details will vary according to the specifics of the incident; however, the goal of incident response remain the same regardless of the type of incident:

- Promptly respond to the incident to help minimize disruption to district operations.
- Contain any damage resulting from incidents, preventing further harm to district systems, data, and operations.
- Prevent future damage by applying lessons learned from each incident.

7.1 - Reporting Incidents:

All district staff members are required to promptly report any suspected or actual unauthorized or inappropriate disclosure of sensitive district data to their immediate supervisor; the supervisor will report this information to their director/principal who will then notify the Director of Information Security.

The Director of Information Security will report the unauthorized disclosure of sensitive district data to the CIO prior to informing external agencies or organizations, unless mandated by State or Federal law.

7.2 - Monitoring for Incidents:

The district has monitoring controls and procedures to detect, report, and investigate incidents.

8.0 - Security Awareness and Training

Security awareness, training, and education are central to the success of the district's cybersecurity program. The greatest asset the district has is the people working throughout it and

this is especially true when it comes to what it takes to help keep the district secure. Without a trained technical staff and user base all the policies, guidelines, and tools in the world will not help protect the district; this is where the security awareness, training, and education programs come into play.

The district provides appropriate training to all personnel and non-employee contractors who interact with district systems and data.

All users of district information and technology resources must agree and adhere to the BCPS *Acceptable Use of Information Resources Guidelines*.

9.0 - IT Support and Operations Security

IT systems administration and tasks external to IT systems (such as maintaining documentation) are critical to protecting District information. Systems administration functions, maintenance accounts and other special modes of IT systems operation can inflict great harm on the confidentiality, integrity or availability of a system or systems infrastructure. Because of this, the district places special security considerations around these elevated functions:

9.1 - User Support:

IT support is provided through the district help desk and support personnel must be trained to be able to identify security problems, respond appropriately, and inform appropriate individuals.

9.2 - Software Support:

Controls are placed on system software commensurate with the risk. Specifically, there are policies and controls related to the following:

- Loading and executing new software on a system
    - Executing new software can lead to viruses, unexpected software interactions, or software that may subvert or bypass security controls.
- Using system utilities
    - System utilities have a high potential for misuse that could lead to compromise the integrity of operating systems and logical access controls.
- System changes.
- License management
    - All district software must be properly licensed, and all district-owned systems are subject to periodic audit to ensure no illegal software is being used.
- Windows servers should be upgraded, at a minimum, to the latest version receiving vendor support.
    - If mission requirements do not allow this, the exception must be approved in writing by the Director of Information Security.

- Apple servers should be upgraded, at a minimum, to the latest version receiving vendor support.
    - If mission requirements do not allow this, the exception must be approved in writing by the Director of Information Security.
- Patches must be applied in accordance with the district's patch management guidelines.
- Games, chat sessions, peer-to-peer (P2P), and instant messenger applications are prohibited on district networks unless needed to support a district business need and then, prior, written approval is needed before the application can be installed and used.
- Streaming audio and video are also prohibited unless it is needed to support a district business need.
- Installing or using remote access services or applications are prohibited unless authorized by the Information Technology department.
- Installing "hacking software," including network scanning tools, is prohibited unless authorized by the Information Technology department.

9.3 - Change Management:

The district's technology infrastructure is constantly changing and evolving to support the mission of the district. Additionally, networks, systems, and applications frequently require upgrades, maintenance, and fine-tuning. All system owners must follow approved district change management guidelines and processes to ensure secure, reliable, and stable operations.

9.4 - Software Updates:

All district systems should be updated as needed to eliminate known security vulnerabilities. The Information and Technology Department has the right to disable and restrict the use of any application or device that cannot be upgraded, updated, or patched to eliminate known security vulnerabilities.

9.5 - Malware Protection:

The district's technology must be continuously protected from threats posed by malware.

- All computing devices owned, leased, or under the control of the district must, to the extent technology permits, use, and keep up to date all required protection software and adhere to any other protective measures as required by applicable district policies and guidelines.
- Any personally owned device that contains sensitive district data must be configured to comply with required district security controls while storing such data.
- Any system identified as a security risk due to a lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place.

- Exceptions should be acknowledged in writing and documented in accordance with the district's risk guidelines.

9.6 - Backups:

All district data must be backed up in accordance with risk management decisions implemented by the data owner. Each backup plan must incorporate procedures for:

- recovering data.
- assigning operational responsibility for backing up of all servers.
- scheduling data backups and establishing requirements for off-site storage.
- securing on-site/off-site storage and media in transit, as necessary.
- testing backup and recovery procedures.

System and data backups for district information and technology resources shall comply with the district data backup guidelines.

9.7 - Maintenance:

Only authorized personnel should be permitted to perform maintenance on a district system.

9.8 - Standardized Log-on Banner:

Prior to user authentication, district systems should display a banner warning that use of the system is restricted to authorized people.

10.0 - Physical and Environmental Protection

Physical and environmental security controls are implemented to protect district facilities housing system resources, the system resources themselves, and the facilities used to support their operation. These controls are designed to prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

The Special Investigative Unit (SIU) is responsible for investigating incidents that occur in a district facility.

11.0 - Identification and Authentication

Identification and authentication refer to the technical measures used to prevent unauthorized people or processes from accessing an IT system. All information and technology systems should be able to identify and differentiate among users. Additionally, the systems should ensure all activities occurring on the system can be attributed to the specific individual that performed the activities. To enable this, district information and technology systems must require users to uniquely identify themselves before being allowed to perform any actions on a district system. Users must also be required to authenticate their claimed identities on district systems by using

district approved passwords, multi-factor authentication, and or other district approved authentication methods. Additionally, authentication data must:

- be protected with access controls and one-way encryption to prevent unauthorized individuals, including system administrators, or threat actors from obtaining the data.
- use encryption when transmitted over public or shared data networks.
- not allow unlimited log-on attempts; automatic lockouts should be applied after a set number of failed log-on attempts to prevent guessing of authentication data.
- be masked as it is entered into any District system to help prevent inadvertent disclosure as it is entered.
- be carefully administered using procedures to disable lost or stolen passwords or tokens and monitoring systems to look for stolen or shared accounts.

12.0 - Access Management Requirements

Proper management and use of computer accounts are components of the district's information security program. All offices that create access accounts for applications, networks, or systems are required to manage the accounts in accordance with the district's access management processes. Access to an information and technology resource may not be granted without the permission of the owner or the owner's delegated custodian of that resource. All accounts are to be created and managed using the following required account management practices:

- All accounts must include documentation on who the account belongs to, why the account was created, and who approved the creation of the account.
- Each account must adhere to the district's password requirements for length, complexity, history, and age.
- All accounts must be associated with an identifiable individual or group of individuals authorized to use that account.
- Accounts of individuals on extended leave (more than 120 days) or accounts that have not been accessed in more than 120 days must be disabled.
- Accounts of individuals who have had their status, roles, or affiliations with district change must be updated to reflect their status.
- Accounts must be reviewed at least annually to ensure their current state is correct.

12.1 - Remote and Wireless Access:

Remote and wireless Access to district resources must be managed to preserve the integrity, availability, and confidentiality of district data. Remote and wireless access policies, standards, guidelines, and procedures must:

- establish and communicate to users the roles and conditions remote or wireless access is permitted.
- require the use of secure and encrypted connections.

- require monitoring for identifying and disabling unauthorized wireless access points.

12.2 - Data Access Control Requirement:

Data owners and custodians must:

- use appropriate administrative, physical, and technical safeguards to control and monitor access to data within their scope of responsibility.
- limit access to data to those who need access for the performance of the employees' job responsibilities.
- monitor access to records containing sensitive district data.
- establish log capture and review processes that, a minimum, define the:
    - Data elements to be captured in logs.
    - time interval for custodial review of the logs.
    - appropriate retention period for logs.
- not disclose, or allow to be disclosed, sensitive district data to unauthorized persons or Districts except:
    - as required or permitted by law.
    - as approved by the district's Office of General Counsel.
    - where the third-party is allowed access to the data due to established agreements.

12.3 - Access for Third Parties:

If the district intends to provide sensitive district data to a third-party, a written agreement with the third-party is required. Such third-party agreements must specify:

- data authorized to be provided.
- the purpose of providing the data.
- all data must be returned to the district, or destroyed, in a manner specified by district upon end of the third-party engagement.

If the district determines providing data to a third-party will result in unacceptable risk to the confidentiality, integrity, and/or availability of the data, the agreement must specify terms and conditions, including appropriate administrative, physical, and technical safeguards for protecting the data.

12.4 - Administrative/Special Access Accounts:

Those with administrative or special access accounts must be made aware of the privileges granted to their accounts and any misuse of the privileges will not be tolerated. Anyone using accounts with elevated access privileges must:

- use these accounts only for their intended administrative purposes.
- understand usage will be logged and audited.
- not perform investigations of individuals except under the direction of the CIO (or designed) or the Office of General Counsel.
- acknowledge their responsibilities by annually signing the Acceptable Use Acknowledgement form.

13.0 - Audit and Accountability

Audit trails maintain a record of system activity by system or application processes and by user activity. Audit trails can help with establishing individual accountability, reconstructing events, performing intrusion detection, and troubleshooting problems.

System audit trails must include sufficient information to establish what events occurred and who (or what) caused them. Audit trails should be protected from unauthorized access or tampering. Access to online audit logs should be strictly controlled, and the confidentiality of audit trail information should be protected. Audit trail information should be reviewed periodically.

14.0 - Artificial Intelligence (AI)

AI refers to the simulation of human intelligence in machines programmed to *think, learn*, and perform tasks autonomously. Unlike traditional computer programs that follow predefined instructions, AI systems can analyze data, recognize patterns, and make decisions based on the information they gather.

AI has the potential to revolutionize how the district carries out its mission by streamlining processes, automating repetitive tasks, and providing valuable insights.

While AI offers numerous benefits, it also presents security challenges for safeguarding sensitive information and protecting against potential threats. Some key security concerns associated with AI include:

- Data Privacy: AI systems rely on vast amounts of data to learn and make decisions, raising concerns about the privacy and confidentiality of sensitive information. Robust data protection measures must be implemented to ensure personal and proprietary data is not compromised or misused.
- Cybersecurity Risks: AI systems can be vulnerable to cyberattacks, including manipulation of input data to deceive AI algorithms or exploit vulnerabilities in AI

models. Strong cybersecurity measures are crucial to defend against threats such as malware, phishing, and data breaches.

- Bias and Fairness: AI algorithms may inadvertently perpetuate bias and discrimination if they are trained on biased datasets or programmed with biased rules. It is imperative any AI output is carefully evaluated to ensure fairness and equity in decision-making processes.
- Trust and Transparency: AI systems often operate as "black boxes," making it difficult to understand how they reach decisions or interpret results. This lack of transparency can erode trust so the district must prioritize transparency and accountability to build confidence in AI technologies.
- Regulatory Compliance: AI applications may be subject to regulatory requirements related to data privacy, cybersecurity, and fairness so district must ensure any use of AI complies with relevant laws and regulations to avoid legal and financial consequences.

15.0 - Document Revision

Document revision is a critical aspect of maintaining robust information security guidelines, as such this document will undergo an annual review with periodic changes as deemed necessary by current security requirements. The review of the District Information Security Guidelines will include aligning security documentation with the latest industry standards, compliance requirements, and technological advancements. The document will be reviewed by the Assistant Director and the Director of Information Technology Security.