Broward County Public Schools

Information Security Guidelines

1.0 Introduction

This document provides the foundation and strategic framework for the protection of Broward County Public Schools (District) information and information systems. District management, users, system developers and security practitioners should use these guidelines to gain an understanding of the basic security requirements District information systems should contain.

These information security guidelines are composed of generally accepted security principles as well as common security practices:

- **Security principles** address information systems security from a high-level viewpoint. These principles must be considered when developing new computer applications and when establishing or updating information security policies. Principles are expressed broadly, encompassing areas such as accountability, cost effectiveness and integration.
- **Security practices** guide the organization in establishing the specific control objectives and security procedures that comprise an effective security program. These security practices are common to all District systems.

This document has two distinct uses. The chapter covering principles is to be used by all levels of District management and by those individuals responsible for information security at the system level and organization level. The principles are intended as a guide when creating program policy or reviewing existing policy. The common practices are intended as a reference guide. The goal of this document is to provide a common baseline of requirements that shall be used within District by managers, users and information security personnel.

2.0 Definitions

The following definitions are used within the context of this document and all District standards and procedures related to information security:

Authentication – a process used to verify one's identity.

Backup – copy of files or applications made to avoid loss of data and facilitate recovery in the event of a system failure or other data loss event.

Centralized IT – the District's institutional information technology services and support organization, reporting to the District Chief Information Officer (CIO), that supports institutional legacy administrative systems or enterprise resource planning (ERP) systems such as student administration, financial information systems, procurement systems, human resource systems, payroll, Network Infrastructure, institutional electronic communications, video, library systems, etc.

Change – any addition or removal of, and any modification or update to an Information Resource.

Change Management – process of controlling the communication, approval, implementation, and documentation of modifications to hardware, software, and Procedures to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Cloud Computing (Cloud Services) – the practice of utilizing services that provide network access to a shared pool of configurable computing resources on demand, including networks, servers, storage,

applications, or related technology services, which may be rapidly provisioned and released by the service provider with minimal effort and interaction.

Commodity Server – a system providing commodity services to District affiliates (e.g., web servers, e-mail servers, file servers, database servers, directory servers).

Common Use Infrastructure – an IT facility, network, system, or other Information Resource managed, owned or controlled by the District or any part thereof (such as an individual school or department) that provides services to multiple schools, divisions, departments or locations under the auspices of the District. Examples: shared data centers, the SBBC Network, the District's Identity Management Federation, SAP, TERMS, FOCUS, etc.

Computing Device – any device capable of sending, receiving, or storing Digital Data, including but not limited to: computer servers, workstations, desktop computers, laptop computers, tablet computers, cellular/smart phones, personal digital assistants, USB drives, embedded devices, smart watches and other wearable electronic devices, etc.

Confidential Data – one of three data classifications defined within SBBC Data Classification Standard. The "Confidential" classification applies to data/information that is exempt from unauthorized disclosure under applicable State law, including the Florida Public Records Act, and Federal laws.

Controlled Data – one of three data classifications defined within SBBC Data Classification Standard. The "Controlled" classification applies to information/data that is not generally created for or made available for public consumption, but that is subject to release to the public through request via the Florida Public Records Act or similar State or Federal law.

Data – elemental units, regardless of form or media, which are combined to create information used to support District business processes. Data may include but are not limited to: physical media, digital, video, and audio records, photographs, negatives, etc.

Data Center – a facility used to house computer systems and associated components, such as telecommunications and storage systems.

Decentralized IT – information technology service and support organizations reporting to the heads of business units, departments, or schools that manage or support their own information systems.

Digital Data – the subset of Data (as defined above) that is transmitted by, maintained, or made available in electronic form.

District – The School Board of Broward County, Florida, inclusive of all of its public schools and other facilities, along with all services and activities directly related to education in that district which are under the direction of the district school officials, including but not limited to alternative site schools and any other entities as from time to time may be assigned by specific legislative act to the governance, control, jurisdiction, or management of SBBC.

Emergency Change – a change to an Information Resource made in response to unexpected events or circumstances that pose a threat to the environment, and thereby justify use of expedited change procedures.

Electronic Communication – method used to convey a message or exchange information via Electronic Media instead of paper media. It includes the use of Electronic Mail, instant messaging, Short Message Service (SMS), facsimile transmission, Social Media, and other paperless means of communication.

Electronic Mail (Email) – any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Electronic Media – any of the following:

- electronic storage media including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, intranet, and the physical movement of removable/transportable electronic storage media.

Guideline – recommended, non-mandatory controls that help support Standards or serve as a reference when no applicable Standard is in place.

High Impact Information Resources – Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- result in major damage to organizational assets;
- result in major financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

High Risk Computing Device – a computing device meeting any of the following criteria:

- is in a public or high-traffic area and is used by a person who has access to Confidential Data;
- is used to create, store, or process Confidential Data or is used within a functional area that handles such data;
- is used by any executive officers or their support staff; or
- contains data that if accessed, changed, or deleted by an unauthorized party could have highly adverse impact on the District.

Based on these criteria, designation of a computing device as being "High Risk" is made by the Information Resource Owner in consultation with The Director of Information Security. In event of disagreement regarding the designation of a computing device as being "High Risk," the Information Resource Manager will work to mediate the disagreement with all parties.

Inappropriate Communications – Any communication which is:

a) harmful to minors;
b) inconsistent with the School Board Policies, federal or state laws, or the Code of Ethics for the Education Profession in Florida; or
c) involving a minor student, through the use of District Information Resources or personally-owned devices and/or telecommunication services, that is not related to school connected activities/assignments and that is made without parental permission to do so.

Information – Data organized, formatted and presented in a way that facilitates meaning and decision making. All information is comprised of data.

Information Resources – any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise

capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, hand-held computers, pagers, distributed processing systems, network attached and computer controlled equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Custodian (Custodian) – an individual, department, District, or third-party service provider responsible for supporting and implementing Information Resources Owner defined controls to Information Resources. Custodians include Information Security Administrators, institutional information technology/systems departments, faculty or staff, vendors, and any third-party acting as an agent of or otherwise on behalf of a District.

Information Resources Owner (Owner) – the manager or agent responsible for the business function that is supported by the Information Resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The Owner is responsible for establishing the controls that provide the security, as well as authorizing access to the Information Resource. The Owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared. Note: In the context of this Policy and associated Standards, Owner is a role that has security responsibilities assigned to it and does not imply legal ownership of an Information Resource. All District Information Resources are legally owned by SBBC.

Information Security Administrator – a departmental employee, designated by management, who assists with information security tasks as described by District policy.

Information Security Program – the Policies, Standards, Procedures, Guidelines, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services adopted for securing District Information Resources.

Information System – an interconnected set of Information Resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, Network Infrastructure, information, data, applications, communications, and people.

Information Technology (IT) – the hardware, software, services, supplies, personnel, facilities, maintenance, and training used for the processing of Data and telecommunications.

Inherent Impact – the degree of Impact (High, Moderate, or Low) that could result if Information Resources were subjected to unauthorized access, use, disclosure, disruption, modification, or destruction.

Integrity – the accuracy and completeness of information and assets, and the authenticity of transactions.

Internet – a global system interconnecting computers and public computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and institutions.

Local Area Network (LAN) – a data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Low Impact Information Resources – Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to organizational assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Malware – a computer program that is inserted into an Information System, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of data, applications, or operating system, or of otherwise annoying or disrupting the User or Information System. Malware (malicious software) may attach itself to a file or application; deliver a payload without the knowledge or permission of the User; insert itself as a service or process to intercept sensitive information and/or keystrokes and deliver it to a third-party; or compromise the User's computer and use it to launch compromises against other computers, among other capabilities. Viruses, worms, Trojan horses, spyware, adware, ransomware, and any code-based entity that infects a host are examples of malicious software.

Mission Critical Information Resources – Information Resources defined to be essential to SBBC's ability to meet its instructional, business or public service missions. The loss of these resources or inability to restore them in a timely fashion would result in the failure of SBBC's operations, inability to comply with regulations or legal obligations, negative legal or financial impact, or endanger the health and safety of faculty, students and staff. Mission Critical Information Resources include but are not limited to:

- Information Systems managing Confidential Data;
- Common Use Infrastructures;
- School Network and Data Center Infrastructure;
- Identity and Access Management Systems, such as single-sign-on or other applications required to enable access to other critical systems;
- Administrative systems (e.g., HR, Finance, Payroll, etc.);
- Student information systems;

Moderate Impact Information Resources – Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

Network Infrastructure – the distributed hardware and software (i.e., cabling, routers, switches, wireless access points, access methods, and protocols), information, and integrating components that allow devices to communicate with one another and enable the administrative, learning, and business missions of the District.

Non-District Owned Computing Device – any device that can receive, transmit, and/or store electronic data, and that is not owned, leased, or under the management of SBBC, including personally owned devices.

Owner – See Information Resources Owner.

Password – a string of characters used to verify or "authenticate" a person's identity. Passphrases and personal identification numbers (PIN) serve the same purpose as a Password.

Personally Identifiable Information (PII) – information that alone or in conjunction with other information identifies an individual. PII includes but is not limited to: an individual's name; a Social Security number; a date of birth; a government-issued identification number; a mother's maiden name; unique biometric data (including an individual's fingerprint, voice print, and retina or iris image); a unique electronic identification number, address, or routing code; or a telecommunication access device.

Policy – high level statements of intent relating to the protection of Information Resources across an organization (e.g., SBBC). Compliance with a Policy is mandatory.

Portable Computing Device – any easily movable device capable of receiving, transmitting, and/or storing data. These include, but are not limited to: notebook computers, handheld computers, tablets (e.g., iPads, etc.), PDAs (personal digital assistants), pagers, smartphones (e.g., iPhones, etc.), Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, and similar storage devices.

Practice – customary actions, which may or may not be documented, taken to accomplish information security tasks.

Procedure – step by step instructions to assist information security and technology staff, Custodians, and Users in implementing various policies, standards, and guidelines.

Published Data – one of three data classifications within SBBC Data Classification Standard. This classification includes data/information made available to the public through posting to public websites or distribution through email, social media, print publications, or other media.

Remote Access – access to District Information Resources that originates from a Remote Location.

Remote Location – a location outside the physical boundary of the District (inclusive of District leased/rented properties and locations within the District's compliance environment).

Residual Risk – the risk (Low, Moderate, or High) that remains after security controls have been applied.

Risk – a function of the likelihood that a threat will exploit a vulnerability and the resulting impact to District missions, functions, image, reputation, assets, or constituencies if such an exploit were to occur.

SBBC Information Security Program – SBBC policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services that establish requirements to provide for program oversight.

Scheduled Change – a change to an Information Resource made under normal working conditions following formally defined change control processes as defined in the District's Change Management Policy.

Security Incident – an event that results in unauthorized access, loss, disclosure, modification, disruption, or destruction of Information Resources whether accidental or deliberate.

Server – a program that provides services to (programs on) other devices. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Social Media – a forum or media for social interaction, using highly accessible and scalable communication techniques. Examples include but are not limited to wikis (e.g., Wikipedia); blogs and microblogs (e.g., Blogger, Twitter); content communities (e.g. Flickr, YouTube); social networking sites (e.g., Facebook, LinkedIn); virtual game worlds; and virtual communities.

Standards – specific mandatory controls that are components of this Policy or the SBBC Information Security Program.

Strong Password – a Password constructed so that another User cannot easily guess it and so that a "hacker" program cannot break it within a reasonable amount of time. It typically consists of a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters.

Two-factor Authentication – a process for verifying a person's identity that requires use of two of the following three elements:

- something the person knows, such as a password;
- something the person has, such as a token or smart card; or
- a unique characteristic of the person, such as a fingerprint.

User – an individual, automated application, or process that is authorized by the Owner to access the resource, in accordance with Federal and State law, District policy, and the Owner's procedures and rules. The User has the responsibility to (1) use the resource only for the purpose specified by the Owner, (2) comply with controls established by the Owner, and (3) prevent the unauthorized disclosure of Confidential Data. A user is any person who has been authorized by the Owner of the information to read, enter, or update that information.

Vendor – any third-party that contracts with SBBC to provide goods and/or services to SBBC.

3.0 Security Principles

The principles contained in this section provide an anchor on which District should base its IT security program. These principles are intended to guide District personnel when creating new systems, practices, or policies. They 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 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 that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees.
- **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 that 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 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 explicit.
- **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.

4.0 Information Security Practices

The following information security guidelines, in conjunction with appropriate state and federal statutes, serve as a foundation and strategic framework for the protection of Broward County Public Schools (District) information systems.

4.1 Information Security Program Management

SBBC Policy 5306, *School and District Technology Usage*, grants the Superintendent of Schools (or designee) sole responsibility for "establishing and maintaining procedures for disabling or otherwise modifying any technology protection measures." All individuals who use District-owned or leased technology, applications, networks or telecommunications infrastructure and systems agree to abide by the terms and tenets of SBBC Policy 5306.

This document, *Information Security Guidelines*, is incorporated by reference to SBBC Policy 5306, requiring all users to follow and abide by the security practices contained in this document. This includes all District staff, temporary help, volunteers, students, auditors, consultants and vendors seeking access to District computer resources. The Policy also requires that all District Information Resources comply with the guidelines set forth in this document. As defined by Policy, the term "Information Resources" includes any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, hand-held computers, smartphones, tablets, distributed processing systems, network attached and computer controlled equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. The term "Information Resources" also includes the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

In addition to SBBC Policy 5306, other supplemental guidance, practice standards and procedures are implemented and incorporated by reference to these guidelines. Supplemental guidance, practice standards and procedures are referenced throughout this document and indexed in Appendix A – Related Guidelines, Process Standards.

4.2 Risk Assessment

Risk assessment is an ongoing process of identifying, assessing and responding to the possibility of something adverse happening. District employs a structured information security risk management process based on NIST Special Publication 800-39, *Managing Information Security Risk*.[1] As it relates to the protection of District information and systems infrastructure, any District data (regardless of where or how it is stored or managed) should be considered in-scope for purposes of risk assessment and risk mitigation.

4.2.1 Information Asset Inventory

The Information Security Office must maintain an accurate inventory of Information Resources and associated Owners.

[1] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

4.2.2 Information Resources Owners

For Information Resources under the Owners' authority, Owners must, in consultation with The Director of Information Security:

- define, approve, and document acceptable Risk levels and Risk mitigation strategies; and
- conduct and document Risk assessments to determine Risk and the Inherent Impact that could result from their unauthorized access, use, disclosure, disruption, modification, or destruction. Timing of assessments shall be annually for all Information Resources and Information Resources.

4.2.3 Information Resources Custodians

Custodians of Mission Critical Information Resources must implement approved Risk mitigation strategies and adhere to Information Security Policies and Procedures to manage Risk levels for Information Resources under their care.

4.2.4 Annual Information Security Risk Assessments

The Director of Information Security must ensure that annual Information Security Risk assessments are performed and documented by each Owner of Information Resources.

4.2.5 Information Technology Projects

Project Managers must perform security assessments, in collaboration with the Office of Technology Planning and Policy and The Director of Information Security, of the implementation of required security controls (i.e. control objectives, controls, Policies, processes, and Procedures for Information security) for sponsored projects under their authority. Security assessments for sponsored projects must be performed annually based on Risk.

4.2.6 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 Confidential District Data or hosting of Confidential District Information Resources with a Vendor or other organization; or
- when purchasing systems or software, whether it is to be hosted on premises or at a Vendor facility, if Confidential District Data will be stored within or processed by the system or software.

4.2.7 Risk Acceptance

Decisions relating to acceptance of Risk must be documented and are to be made by:

- the Information Resource Owner, in consultation with The Director of Information Security or designee, for resources having a residual Risk of Low or Moderate.
- the Chief Information Officer, or designee, considering recommendations of the Owner and The Director of Information Security for resources having a residual Risk of High.

4.3 System and Services Acquisition

Security, like any other aspect of an information system, is best managed if planned for throughout the development life cycle. During the development of new systems for District, security activities must be integrated during each of the development phases. Regardless of the methodology employed in building the system, a security plan for the development effort must be utilized to ensure that security is considered during all phases of the effort.

4.4 Personnel / User Issues

A broad range of security issues relate to how District personnel and non-employee users interact with District information systems. Determining the appropriate level of systems access and the authorities required for individuals to do their job is critical to securing the systems environment.

4.4.1 Staffing

Early in the process of defining a new position, security issues should be identified and addressed. Once a position has been broadly defined, the responsible supervisor should determine the type of systems access needed for the position. Two general security rules should be applied when granting access:

- **Separation of duties.** Roles and responsibilities should be divided so that a single individual cannot subvert a critical process.
- **Least privilege.** Users should only be granted access to functions they need to perform their official duties.

4.4.2 User Administration

District ensures effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access by requiring the following for all District applications and systems:

- **User Account Management.** The District has a standard process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
- **Audit and Management Reviews.** It is necessary to periodically review user account management on a system. Reviews should examine the levels of access everyone has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews should be conducted on an application-by-application basis and a system wide basis.
- **Detecting Unauthorized/Malicious Activities.** All District systems should have mechanisms besides auditing and analysis of audit trails to detect unauthorized and/or malicious acts.

4.5 System and Communications Protection

SBBC’s Policies, Standards, and/or Procedures must describe and require steps to protect District Data using appropriate administrative, physical, and technical controls in accordance with SBBC Information Security Program and Data Classification Standard.

- The Minimum Security Standards for Systems describe and require appropriate steps to protect Confidential Data stored, processed, or transmitted on the District's computing devices.
- The Minimum Security Standards for Application Development and Administration describe and require appropriate steps to protect Confidential Data stored, processed, or transmitted on the District's applications.

4.6 Third-Party Service Providers Storing District Data

District Data must not be stored on personally procured third-party (e.g. Cloud) storage services. All third-party services storing District data must have a valid contract in place that has been approved by the Office of General Counsel.

4.7 Password and Encryption Protection for Computing Devices and Data

4.7.1 Desktop Computers

- All High-Risk Desktop Computers owned, leased, or controlled by the District must be Password protected and encrypted, regardless of data classification, using methods approved by The Director of Information Security.
- All desktop computers must meet the Minimum Security Baseline for desktop computers, regardless of data classification, before their deployment.

4.7.2 Laptop Computers and Other Mobile Devices

- All laptop computers and other mobile devices, including but not limited to mobile and smart phones, and tablet computers, which are owned, leased, or controlled by the District, must be encrypted, regardless of data classification, using methods approved by The Director of Information Security.
- 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 Confidential District Data on the device.

4.7.3 Personally Owned Devices

- Specific permission must be obtained from the department head before a user may store Confidential District Data on any personally owned computers, mobile devices, USB thumb drives, or similar devices. Such permission should be granted only upon demonstration of a business need and an assessment of the risk introduced by the possibility of unauthorized access or loss of the data.
- All personally owned computers, mobile devices, USB thumb drives, or similar devices must be Password protected and encrypted using methods approved by The Director of Information Security if they contain any of the following types of District Data:
    a) Information made confidential by Federal or State law, regulation, or other legally binding order or agreement;
    b) Federal, State, District, or privately sponsored Research that requires confidentiality or is deemed sensitive by the funding entity; or
    c) any other Information that has been deemed by SBBC District as essential to the mission or operations of SBBC to the extent that its Integrity and security should be maintained at all times.

4.8 Protecting Data in Transit

Data Owners shall implement appropriate administrative, physical, and technical safeguards necessary to adequately protect the security of Data during transport and electronic transmissions. Each of the following shall be addressed:

- identification and transmission of the least amount of Confidential Data required to achieve the intended business objective;
- encryption of all Confidential Data transmitted over the Internet;
- deletion of transmitted and received Confidential Data upon completion of the intended business objective.

4.9 Media Protection

Electronic Devices and 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 Electronic Media to make it unreadable, indecipherable, or otherwise physically destroying the Electronic Media; and
- in accordance with the applicable institutional records retention schedule.

4.10 Contingency Planning

Owners of Mission Critical Information Resources and of Information Resources containing Confidential Data must adopt a disaster recovery plan commensurate with the Risk and value of the Information Resource and a completed Business Impact Analysis. The disaster recovery plan must incorporate Procedures for:

- recovering Data and applications in the case of events that deny access to Information Resources 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 (example: tabletop or scenario testing, leveraging major scheduled upgrades, activating actual service outages in a controlled scenario; and
- making the disaster recovery plan available to The Director of Information Security and other stakeholders.

4.11 Incident Response

An IT security incident can result from a computer virus, other malicious code, unauthorized access to systems or a data breach. Although some elements of security incident handling can be addressed by the District contingency plan, the organization also maintains specific Security Incident Handling Procedures, posted on Broward County Public Schools Intranet under Information Technology's homepage, as well as a Cyber Security Incident Response Team (CSIRT). The objectives of these guidelines and the CSIRT are to provide the ability to respond quickly and effectively to incidents, contain damage from incidents and prevent future damage.

4.11.1 Reporting Requirements

All employees must promptly report unauthorized or inappropriate disclosure of Confidential Data, in digital, paper, or any other format, to their immediate supervisor.

The Director of Information Security must report significant Security Incidents, as defined by the SBBC Security Incident Reporting Requirements, to the Chief Information Officer. Security Incidents resulting in unauthorized disclosure of District Data must be reported immediately. The Director of Information Security must report Security Incidents to the Chief Information Officer prior to reporting to non-SBBC agencies or organizations except as required by State or Federal law.

4.11.2 Monitoring Techniques and Procedures

Data Custodians must implement monitoring controls and Procedures for detecting, reporting, and investigating incidents.

4.12 Security Awareness and Training

Effective computer security awareness and training requires proper planning, implementation, maintenance, and periodic evaluation. District provides appropriate training to all personnel and non-employee contractors who interact with District systems and data.

All Users of District Systems must agree and adhere to the Acceptable Use of Information Resources Guidelines.

The District evaluates elements of its security awareness and training periodically and endeavors to ascertain how much information is retained by personnel, to what extent information security procedures are being followed, and general attitudes toward information security.

4.13 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. To that end, District places special security considerations around these elevated functions:

4.13.1 User Support

Systems support and operations staff must provide assistance to users through the help desk. Support personnel must be trained to be able to identify security problems, respond appropriately, and inform appropriate individuals.

4.13.2 Software support

Controls are placed on system software commensurate with the risk. The controls include:

- **Policies for 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.
- **Use of powerful system utilities.** System utilities can compromise the integrity of operating systems and logical access controls.
- **Authorization of system changes.** This involves the protection of software and backup copies and can be done with a combination of logical and physical access controls.
- **License management.** All District software should be properly licensed, and all District-owned systems including end-user systems such as desktops and mobile devices are subject to periodic audit to ensure that no illegal software is being used.

4.13.3 Change Management

The District's Information Resources infrastructure is constantly changing and evolving to support the mission of the District. Computer networks, systems, and applications require planned outages for upgrades, maintenance, and fine-tuning. The Change Management Guidelines, posted on Broward County Public Schools Intranet under Information Technology, provide expanded detail for the following change management procedures that are required, as warranted by the Data Classification Standard and commensurate with the risk and value of the system and/or data:

- All changes to environmental controls affecting computing facility machine rooms (for example, air-conditioning, water, heat, plumbing, electricity, and alarms) must be logged and reported to the appropriate school or business unit managing the systems in that facility.
- Schools or business units responsible for Information Resources will ensure that the change management procedures and processes they have approved are being performed.
- Schools or business units may object to a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out contingencies, inopportune timing in terms of impact on service to users or in relation to key business process such as year-end accounting, or lack of resources to address potential problems that may be caused by the change. The responsible party

will review all objections. A security exception request may be submitted to the Information Security Office if there are objections to a planned change that is triggered by security requirements.

- Whenever possible, customers will be notified of changes following the steps contained in the change management procedures.
- Consistent with change management procedures, a change management log is maintained for all significant changes including emergency changes. Change management log entries must contain at least the following information:
    a) Date of submission and date of change;
    b) Owner and custodian contact information; and
    c) The nature of the change.
- All Custodians must implement and adhere to approved SBBC Change Management guidelines to ensure secure, reliable, and stable operations.

4.13.4 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. Machines maintained by the Information and Technology Department to provide any kind of specialized services are not exempt from this practice.

4.13.5 Malware Protection

SBBC's Network Infrastructure and other Information Resources must be continuously protected from threats posed by Malware.

- All computing devices owned, leased, or under the control of SBBC must, to the extent technology permits, execute and keep up to date all required protection software and adhere to any other protective measures as required by applicable Policies and Procedures.
- Any personally owned Computing Device that contains Confidential District Data must be configured to comply with required District security controls while holding 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 District's risk guidelines.

4.13.6 Backups

All SBBC 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 and applications in case of events such as natural disasters, system disk drive failures, malicious tampering, Data entry errors, human error, or system operations errors;
- 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; and
- testing Backup and recovery Procedures.

System and data backups for District Information Resources shall comply with the SBBC Data Backup Guidelines posted on Broward County Public Schools Intranet under Information Technology's homepage.

4.13.7 Documentation

All aspects of computer support and operations should be documented to ensure continuity and consistency. Security documentation should be designed to fulfill the needs of the different types of people who use it. The security of a system also needs to be documented, including security plans, contingency plans, and security policies and procedures.

4.13.8 Maintenance

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

4.13.9 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.

4.14 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect District IT 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 School Board of Broward County has directed the Special Investigative Unit (SIU) to be responsible for the investigation of all incidents that occur in District facilities.[2]

4.15 Identification and Authentication

Identification and Authentication refers to the technical measures that prevent unauthorized people or processes from accessing an IT system. Generally, access control principles require that the system can identify and differentiate among users. Similarly, user accountability principles require that all activities on an IT system be attributable to specific individuals. Therefore, all District systems must have the ability to identify users.

4.15.1 Identification

Identification is how a user provides a claimed identity to the system. The most common form of this identification is the user ID. The following should be considered when using user IDs:

- **Unique Identification.** Users should be required to identify themselves uniquely before being allowed to perform any actions on a District system.
- **Correlate Actions to Users.** District systems should internally maintain the identity of all active users and be able to link actions to specific users.
- **Maintenance of User IDs.** Identification data must be kept current by adding new users and deleting former users.

4.15.2 Authentication

Authentication is the means of establishing the validity of this claim. Generally, account passwords are used for this purpose, though other means (e.g. SSL certificates, tokens, biometrics) can also be used. The following should be considered:

- **Require Users to Authenticate.** Users should be required to authenticate their claimed identities on District systems.

[2] http://www.broward.k12.fl.us/sbbcpolicies/docs/P2302.000.pdf

- **Restrict Access to Authentication Data.** Authentication data should be protected with access controls and one-way encryption to prevent unauthorized individuals, including system administrators, or hackers from obtaining the data.
- **Secure Transmission of Authentication Data.** Authentication data should be protected when transmitted over public or shared data networks.
- **Limit Log-on Attempts.** The number of log-on attempts should be limited with automatic lockouts after a set number of failed log-on attempts to prevent guessing of authentication data.
- **Secure Authentication Data as it is Entered.** Authentication data should be protected as it is entered into any District system, including suppressing the display of the password as it is entered.
- **Administer Data Properly.** Authentication data and tokens should be carefully administered including procedures to disable lost or stolen passwords or tokens and monitoring systems to look for stolen or shared accounts.

4.15.3 Passwords

All District systems utilizing passwords for authentication should follow the established password policy guidance.

4.16 Access Control

Proper management and use of computer accounts are basic requirements for protecting the District's Information Resources. 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 Resource may not be granted by another User without the permission of the Owner or the Owner's delegated custodian of that Information Resource. All accounts are to be created and managed using the following required account management practices:

4.16.1 Access Management Requirements

- All accounts that access non-public District Information Resources must follow an account creation process. This process shall document who is associated with the account, the purpose for which the account was created, and who approved the creation of the account at the earliest possible point of contact between the account holder and the District. All accounts wishing to access the District's non-public Information Resources must have the approval of the Owner of those resources. These measures also apply to accounts created by/for use of outside vendors or contractors.
- Each account having special privileges must adhere to the District's password requirements.
- All accounts must be able to be associated with an identifiable individual or group of individuals that are 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.
- Account passwords shall be expired based on Risk.
- Accounts of individuals who have had their status, roles, or affiliations with District change must be updated to reflect their current status.
- Accounts must be reviewed at least annually to ensure their current state is correct.
- Password aging and expiration dates must be enabled on all accounts created for outside vendors, external contractors, or those with contractually limited access to the District's Information Resources.

4.16.2 Remote and Wireless Access

Remote and wireless Access to SBBC Network Infrastructure must be managed to preserve the Integrity, availability, and confidentiality of SBBC Information. Remote and Wireless Access Policies and Procedures must:

- establish and communicate to Users the roles and conditions under which Remote or wireless Access to Information Resources containing Confidential Data is permitted;
- require the use of secure and encrypted connections when accessing Information Resources containing Confidential Data across the Internet, or across unsecured or public networks (e.g., use of VPN for access, SFTP for transfers, encrypted wireless); and
- require monitoring for identifying and disabling of unauthorized (i.e., rogue) wireless access points.

4.16.3 Access to SBBC Networks

Through appropriate use of administrative, physical, and technical controls, SBBC office or offices charged with maintaining the Network Infrastructure are required to establish processes for approval of all network hardware connected to SBBC network and the methods and requirements for attachment, including any Non-SBBC Owned Computer Systems or Devices, to ensure that such access does not compromise the operations and reliability of the network, or compromise the Integrity or use of Information contained within the network.

4.16.4 Data Access Control Requirement

All Owners and Custodians must control and monitor access to Data within their scope of responsibility based on Data sensitivity and Risk, and through use of appropriate administrative, physical, and technical safeguards including the following:

- Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees' job responsibilities. An employee may not access Confidential Data if it is not necessary and relevant to the employee’s job function.
- Owners and Custodians must monitor access to records containing Confidential Data using appropriate measures as determined by applicable Policies, Standards, Procedures, and regulatory requirements.
- Owners and Custodians must establish log capture and review processes based on Risk and applicable Policies, Standards, Procedures, and regulatory requirements. Such processes must define:
    a) the Data elements to be captured in logs;
    b) the time interval for custodial review of the logs; and
    c) the appropriate retention period for logs.
- Employees may not disclose Confidential Data to unauthorized persons or Districts except:
    a) as required or permitted by law, and, if required, with the consent of the Data Owner;
    b) where the third-party is the agent or contractor for SBBC and the safeguards described in this Policy are in place;
    c) as approved by SBBC Office of General Counsel or the SBBC Office of General Counsel.

4.16.5 Access for Third Parties

If SBBC intends to provide District Data to a third party acting as an agent of or otherwise on behalf of SBBC (example: an application service provider) a written agreement with the third-party is required. Such third-party agreements must specify:

- the Data authorized to be accessed;
- the circumstances under and purposes for which the Data may be used; and

- that all Data must be returned to SBBC, or destroyed, in a manner specified by SBBC upon end of the third-party engagement.

If SBBC determines that its provision of Data to a third-party will result in significant Risk to the confidentiality, Integrity, or availability of such Data, the agreement must specify terms and conditions, including appropriate administrative, physical, and technical safeguards for protecting the Data.

4.16.6 Two-factor Authentication Requirements

Two-factor Authentication is required in the following situations:

- when an employee or other individual providing services on behalf of the District (such as a student employee, contractor, or volunteer) logs on to a District network using an enterprise Remote Access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;
- when an individual described in (a) who is working from a Remote Location uses an online function such as a web page to modify or view employee banking, tax, or financial Information; or
- when a Computing Device administrator or other individual working from a Remote Location uses administrator credentials to access another Computing Device that contains or has access to Confidential District Data.

Additional implementation details are available in SBBC Information Security Office's Approved Two-Factor Authentication Methods

4.16.7 Administrative/Special Access Accounts

Users must be made aware of the privileges granted to their administrative accounts, especially those that impact access to Information Resources or that allow them to circumvent controls in order to administer the information resource. Abuse of such privileges will not be tolerated. Anyone using accounts with elevated access privileges of this type must adhere to the following access requirements:

- All IT System Custodians will be granted administrative access to the District-owned IT devices (e.g., laptops, desktops, tablets, servers) deployed in their school, department or business unit. Individuals who use accounts with special privileges (for example, System Administrators) must only use these accounts for their intended administrative purposes.
- All access via administrative accounts must be logged to system management services in place centrally or within the respective school, department or business unit to ensure proper accountability and transparency. These logs should be retained, according to SBBC retention schedules, and routinely audited.
- Individuals who use administrative accounts may not perform investigations relating to the potential misuse of Information Resources by an individual user except under the direction of the Information Security Office or the Office of General Counsel.
- All schools, departments and business units of the District must maintain an updated list of IT Support Staff.
- All SBBC employees must complete a Background Check for staff/faculty and must acknowledge their responsibilities by annually completing the Acceptable Use Acknowledgement form.
- The password for a shared administrative account must change when any individual knowing the password leaves the department or District or changes role; or upon a change in the vendor personnel assigned to District contracts having password access.
- For all systems serving out Information Resources there must be a password escrow procedure in place to enable someone other than the administrator to gain access to the system in an emergency.

- When access to a District-owned IT device's administrative account is required by someone other than an IT Support Staff member, the following exception criteria must apply:
    a) Individuals must annually complete the Acceptable Use Acknowledgement form;
    b) Individuals must only use the administrative account for special administrative functions and default to a lower privileged user account for other day-to-day use;
    c) Individuals must review training to inform them how they can limit use of their administrative access and still accomplish their primary day-to-day functions (example: How not to Login as Administrator (and still get your job done);
    d) IT System Custodians are required to periodically review the use of administrative account exceptions.

4.17 Audit and Accountability

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

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 trails should be reviewed periodically.

5.0 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.

Appendix A – Related Guidelines, Process Standards and Procedures

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and all regulations adopted to implement FERPA.

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and all regulations adopted to implement HIPAA.

Health Information Technology for Economic and Clinical Health Act, (HITECH) Act of 2009, and all regulations adopted to implement HITECH.

Federal Privacy Act of 1974 (Section 7 of Pub. L. 93-579 in Historical Note), 5th U.S.C. § 552a

Social Security Act, 42 U.S.C. §§ 408(a)(8) and 405(c)(2)(C)(viii)(I)