INFORMATION SECURITY POLICY & PROCEDURES

THIS DOCUMENT IS CLASSIFIED AS:

PUBLIC

Table of Contents

Table of Contents 2
0.0 BOARD POLICY 3
1.0 INFORMATION SECURITY 4
2.0 ROLES AND RESPONSIBILITIES 6
3.0 INFORMATION HANDLING 10
4.0 DATA CLASSIFICATION 13
5.0 DATA DESTRUCTION 16
6.0 DATA PROTECTION 18
7.0 ASSET MANAGEMENT 19
8.0 RISK MANAGEMENT 20
9.0 ACCESS CONTROL 21
10.0 INFORMATION SECURITY TRAINING 23
11.0 SYSTEM PROTECTIONS 24
12.0 CHANGE CONTROL 25
13.0 OPERATING ENVIRONMENT 26
14.0 NETWORK PROTECTIONS 27
15.0 INCIDENT RESPONSE 28
16.0 INTERNAL EVALUATION 32
17.0 OPERATIONAL IMPACT 33

0.0 BOARD POLICY

Network and Internet Acceptable Use

It is the belief of the Forsyth County Board of Education that the use of technology for the purpose of instruction and operation is an important part of preparing children to thrive in the 21st century and in providing a modern and efficient workplace for staff. The Board further believes that a technology-rich environment can significantly enhance both the teaching and learning process. This technology includes – but is not limited to – computer hardware, software, wired and wireless network connectivity, and access to the Internet. Due to the complex nature of these systems and the magnitude of information available via the Internet, the Forsyth County Board of Education believes guidelines regarding responsible use are warranted in order to serve the educational needs of students and workplace needs of staff.

It shall be the policy of the Forsyth County Board of Education that the school system shall have in continuous operation, with respect to any devices using district-provided network resources have:

1. A qualifying "technology protection measure," as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000; and
2. Procedures or guidelines developed by the superintendent, administrators and/or other appropriate personnel which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children's Internet Protection Act of 2000. Additionally, those measures will also include staff behavior on districted-provided devices and services. Such procedures or guidelines shall be designed to:
    a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet;
    b. Educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response as required by the Children's Internet Protection Act.
    c. Prevent unauthorized access, including hacking, denial-of-service, credential theft, and other unauthorized activities by minors and staff;
    d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors and staff; and
    e. Restrict minors' access to materials "harmful to minors," as that term is defined in Section 1703(b)(2) of the Children's Internet Protection Act of 2000; and
    f. The Forsyth County Board of Education will adopt and maintain a procedure manual that outlines and mandates the operation of a reliable, safe, and secure network for all students, teachers, and staff.

The district's technology resources are provided for educational and instructional purposes that promote and are consistent with the instructional goals of the Forsyth County School System or are for the business operations/use by FCS staff. Use of computers and network resources outside the scope of these purposes is strictly prohibited. Students and employees accessing network services, or any device utilizing those services, shall comply with the district's responsible use guidelines. The district reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications without the consent of the user.

It must also be understood that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable tool for instructional and operational uses, there are sections that are not commensurate with community, school, or family standards. It is the belief of the Board that the Internet's advantages far outweigh its disadvantages. The Forsyth County Board of Education will, through its administrative staff, provide an Internet screening system which blocks access to a large percentage of inappropriate sites. It should not be assumed, however, that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, access to the Internet and computer resources is a privilege, not a right. Therefore, users violating the Forsyth County Board of Education's responsible use policy shall be subject to revocation of these privileges and potential disciplinary action.

1.0 INFORMATION SECURITY

1.1 Purpose

The mission of Forsyth County Schools (FCS) is to prepare and inspire all learners to lead and succeed. The vision of FCS is to provide quality learning and superior performance for all. The primary customer of FCS is the individual student, this is the core of everything that we do. FCS understands its place in the infrastructure of the United States to educate students.

The FCS mission is heavily reliant on Information System Assets to accomplish the mission and vision. Because of this dependency, critical risks to information assets cannot be tolerated. These procedures serve to establish the minimum information security practices for computer resources and associated communication networks. Furthermore, these procedures are intended to give direction on security practices that are designed to ensure confidentiality, integrity, and availability of data, and to ensure compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

1.2 Scope

All employees, contractors, and agents or other individuals utilizing computer resources, data communication networks, or other information technology infrastructure resources owned or leased by FCS - including any other corporation or agency having connectivity to the network - are subject to these Information Security policies.

Additionally, any remote access mechanisms such as dial up connections, Internet Service Provider (ISP) access, Virtual Private Network (VPN) connection onto the enterprise network or associated domains are subject to all same security Procedures, just as if they were components of direct access infrastructure via FCS provided equipment or facilities.

1.3 Information Security Elements

Information Security is defined as the protection of information and its critical elements, including people, systems and hardware that store, use or process, and transmit that information. FCS uses a layered security model consisting of technical controls, education and awareness, and procedures designed to ensure data confidentiality, integrity, and availability. These procedures are intended to give direction on accepted security practices.

1.4 Security Program

Information security is a business issue. The objective is to identify, assess, and take steps to avoid or mitigate risk to FCS information assets. Governance is an essential component for the long-term strategy and direction of an organization with respect to the security procedures and risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that provides an appropriate venue to inform and advise executive, operational and information technology management on security issues and acceptable risk levels.

In order to implement and properly maintain a robust information security function, FCS recognizes the importance of:

- Understanding FCS's information security requirements and the need to establish procedure and objectives for information security;
- Implementing and operating controls to manage FCS information security risks in the context of overall business risks;
- Ensuring all users of FCS information assets are made aware of their responsibilities in protecting those assets;
- Monitoring, reviewing the performance and effectiveness of information security procedures and controls; and
- Continual improvement based on assessment, measurement, and changes that affect risk.

1.5 Security Policy

The objective of information security policy is to provide management direction and support for information security in accordance with business requirements and governing laws and regulations. Information security procedures will be approved by management, published, and communicated to all employees and in relevant external parties. These procedures will set out FCS's approach to managing information security.

Each procedure will have an owner who has approved management responsibility for the development, review, and evaluation of the procedure. Information security policies will be reviewed at least annually or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Reviews will include assessing opportunities for improvement of FCS's information security procedures and approach to managing information security in response to changes to FCS's environment, new threats and risks, business circumstances, legal and procedure implications, and technical environment.

1.6 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

2.0 ROLES AND RESPONSIBILITIES

2.1 Purpose

The purpose of this policy is to establish the roles and responsibilities for the safeguarding of sensitive information.

2.2 Responsibilities

2.2.1 Director of Technology Services (DOT)

The DOT is responsible for overseeing all aspects of information security, including, but not limited to:

- The creation and distribution of security policies and procedures;
- Distributing procedural information and directives to appropriate information security and management personnel;
- The production and administration of security incident response and escalation procedures that include the following components:
- Defining roles, responsibilities, and communication;
- Ensuring coverage and responses for all critical system components;
- An analysis of legal requirements for reporting compromises;
- The designation of personnel to monitor for intrusion detection, intrusion prevention, and respond to integrity monitoring alerts on a 24/7 basis;
- Developing periodic training schedules to be completed and discharged;
- Maintaining a formal security awareness program for all employees via multiple methods of communicating awareness and education;
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement;
- Maintain a program to verify compliance with the NIST CSF;
- Communicate technology risk profile to the Board of Education (BOE);
- Communicating BOE risk tolerance to IT leaders;
- Determine strategic technology plan for supporting the mission of FCS;
- Report any network security incidents to the Chief Technology & Information Officer (CTIO).

2.2.2 Network Operations Coordinator (NOC)

The Network Operations Coordinator is responsible for:

- Planning and supervising hardware and software conversions, migrations, and upgrades for information systems;
- Maintaining an up-to-date inventory of information systems equipment including routers, hubs, servers, firewalls, and monitors;
- Supervising the change control process for centralized computer equipment, computer facilities, and software;
- Supervising the work of information system vendor personnel;
- Serving as custodian of information in accordance with FCS's policies, applicable laws and regulations;
- Maintaining business applications, underlying systems and technologies per security procedures and standards;
- Ensuring applications are developed and maintained in a manner that complies with all applicable regulations;
- Reporting known or suspected violations of this policy to the Chief Information Officer;

2.2.3 Technology Services Department

The Technology Services Department shall maintain daily administrative and technical operational security procedures that are consistent with the NIST CSF (for example, user account maintenance procedures, and log review procedures). Develop, maintain, and test Business Continuity and Disaster Recovery Plans for Technology Department (TD) controlled assets.

2.2.4 Network Operations

System and Application Administrators shall:

- Monitor and analyze security alerts and information and distribute to appropriate personnel;
- Implementing technical security configurations;
- Administer user accounts and manage authentication;
- Monitor and control all access to data;
- Maintain a list of service providers;
- Retain audit logs for at least one year;

- Report network security incidents to the DOT & NOC immediately upon discovery;

2.2.5 Network Administrators

The Network Administrators shall:

- Follow all change control policies and procedures;
- Assure that changes to firewall security rules are approved by the NOC and document all firewall security rules and changes.
- Apply hardware and software updates from the firewall vendor(s) after change management acceptance and approval by the NOC.
- Enable appropriate logging of firewall performance and events and perform active monitoring of the logs;
- Report network security incidents to the DOT & NOC immediately upon discovery;
- Coordinate an appropriate response with the NOC to mitigate security events related to traffic flowing through the firewall;
- Monitor the up/down status of the interfaces;
- Notify the appropriate parties in the event of a firewall failure or security event;
- Implementing technical security configurations;

2.2.6 Human Resources Office

The Human Resources Office (HR) is responsible for tracking employee participation in the security awareness program, including:

- Facilitating participation upon hire during the Intake process;
- Oversee employees' written acknowledgement that they have read and understand the District's responsible use policy;
- Thoroughly screen potential employees prior to hereto minimize the risk of attacks from internal sources;
- Executing enforcement of this policy through corrective action.

2.2.7 Student Information Office (SIS)

The Student Information Office (SIS) will be responsible for operating and maintaining all student information systems, including data and records, in the District's approved information system(s). The responsibilities will include:

- Maintaining the approved student information system, such as Infinite Campus, and all corresponding linked databases contained therein or associated with;
- Communicating risk to NOC & DOT;
- Implementing technical protection of SIS assets and corresponding linked databases contained therein or associated with;
- Establish, test, and maintain Disaster Recovery Plan and Process for information system (IS) assets on an annual schedule;
- Publishing and maintaining results of compliance audit(s) in a controlled-access repository.

2.2.8 Director of Instructional Technology (DIT)

As defined in Section 10.0, the DIT is responsible for overseeing all aspects of information security training, including, but not limited to:

- The creation and distribution of information security training for all FCS staff;
- Maintaining and conducting a current and comprehensive training program for all FCS staff;
- Conducting basic security training for all new staff at Intake;
- Defining training roles and responsibilities for Instructional Technology staff;
- Reporting training outcomes to the Chief Information Officer and Director of Technology Services;

2.2.9 Transportation

The Transportation Office (TRANS) will be responsible for operating and maintaining all relevant logistics and transportation data in an approved application and/or database. Associated responsibilities include:

- Maintaining the approved transportation and logistics systems, such as those for coordinating bus routes and those for fueling services, and all corresponding linked databases contained therein or associated with;

- Communicating risk to NOC & DOT;
- Implementing technical protection of TRANS assets and corresponding linked databases contained therein or associated with;
- Establish, test, and maintain Disaster Recovery Plan and Process for TRANS assets on an annual schedule;
- Publishing and maintaining results of compliance audit(s) in a controlled-access repository.

2.2.10 Finance Office

The Finance Office (FIN) will be responsible for operating and maintaining all financial and benefits-related information in an approved – and regulatorily-compliant – application and/or database. Associated responsibilities include:

- Maintaining the approved financial and benefits systems and all corresponding linked databases contained therein or associated with;
- Communicating risk to NOC & DOT;
- Implementing technical protection of FIN assets and corresponding linked databases contained therein or associated with, including mobile assets that may contain or access confidential FIN data;
- Establish, test, and maintain Disaster Recovery Plan and Process for FIN assets on an annual schedule;
- Publishing and maintaining results of compliance audit(s) in a controlled-access repository.

2.2.11 Facilities Office

The Facilities Office (FAC) will be responsible for operating and maintaining all relevant departmental information in approved applications and/or databases. Associated responsibilities include:

- Maintaining the approved GIS, Maintenance, HVAC, Refrigeration, Generator systems and all corresponding linked databases contained therein or associated with;
- Communicating risk to NOC & DOT;
- Implementing technical protection of FAC assets and corresponding linked databases contained therein or associated with, including mobile assets that may contain or access confidential FAC data;
- Establish, test, and maintain Disaster Recovery Plan and Process for FAC assets on an annual schedule;
- Publishing and maintaining results of compliance audit(s) in a controlled-access repository.

2.2.12 School Safety Office

The School Safety Office (SAF) will be responsible for operating and maintaining all systems and/or databases in approved and vetted applications. Associated responsibilities include:

- Maintaining the approved Camera, Access Control, Badging systems and all corresponding linked databases contained therein or associated with;
- Communicating risk to NOC & DOT;
- Implementing technical protection of SAF assets and corresponding linked databases contained therein or associated with, including mobile assets that may contain or access confidential SAF data;
- Establish and follow a logical and repeatable process to provide/revoke access to all SAF systems;
- Establish, test, and maintain Disaster Recovery Plan and Process for SAF assets on an annual schedule;
- Publishing and maintaining results of compliance audit(s) in a controlled-access repository.

2.2.13 School/Department Leadership (LDR)

School and department leadership (LDR) will be responsible for ensuring staff are provided adequate opportunities to participate in information security training programs. Associated responsibilities include:

- Supporting District initiatives to train staff in information security;
- Following all prescribed security and privacy mandates for maintaining and using third-party services, such as (but not limited to) school social media accounts, school-purchased instructional programs, and engagement of outside entities related to technology/network use at the school;
- Communicate risk to the NOC and DOT.

2.2.14 District Administrators (DADM)

The DADM is ultimately responsible for the operation of FCS. The DADM responsibilities regarding this policy include:

- Approving the policies and procedures
- Setting the risk tolerance of FCS
- Providing budgetary support to above positions to support risk treatment
- Reviewing and approving risk profile at least annually

2.2.15 Third-Party Service Providers

All third-party service providers that provide any service that involves FCS information systems or classified information should be required by operational agreement to:

- Maintain assets that create, store, transmit, or maintain FCS information
- Demonstrate risk and vulnerability management for information systems
- Agree to all applicable policies and procedures
- Maintains training program for all users that access FCS information or systems

2.2.16 Physical Security Personnel

All personnel responsible for the physical security of all sites that create, store, process, or transmit FCS classified data or information systems must:

- Control access to sensitive areas through approved access control lists
- Maintain structures capable of protecting information assets from physical risks

2.2.17 Director of Communications and Community Engagement (DCOM)

The Director of Communications and Community Engagement (DCOM) will be responsible for communicating pertinent information with public authorities in the event of a security/privacy compromise. Additional responsibilities also include:

- Create and maintain a list of standards to be used for “official” FCS/school social media accounts;
- Communicate risk to the NOC and DOT.

3.0 INFORMATION HANDLING

3.1 Purpose

The purpose of this policy is to ensure that all FCS digital information is properly handled, whether being transmitted within the organization or to a trusted external third party. This document provides guidance on how to handle sensitive district information, including the physical security requirements and the distribution of sensitive information internally and externally.

3.2 Policy

Users are responsible for safeguarding and monitoring FCS information against unauthorized disclosure, modification, and destruction. FCS information must be used only for FCS related business in accordance with its procedures and standards.

Many students, parents, and district employees have entrusted their information to FCS for official purposes, and all employees must do their best to safeguard the privacy and security of this information. Personally Identifiable Information (PII) is **CONFIDENTIAL,** and access must be strictly limited based on operational need for such access. Access will be granted only when a legitimate business need has been demonstrated and access has been approved in advance based on their role and supervisor consent. Access to special hardware and software must be restricted based on business needs.

Employees with access to sensitive information such as PII, FCS internal documents, and documents classified as confidential must not store such data on any removable media, mobile or portable device, unsanctioned cloud storage, or otherwise unencrypted location without approval and should never be stored or shared or transmitted through personal accounts and/or personal devices. This also includes the printing of sensitive information on paper or electronic documents without an approved security process as outlined below.

3.2.1 Safeguards for Documents

All documents containing sensitive information must be stored appropriately to reduce the potential for disclosure. Documents must not be easily accessible to unauthorized individuals and any documents containing sensitive information should be placed with identifying information face down on counters and desks. These documents should not be left out on printers, desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, or other secure areas. When discarding documents containing sensitive information, use a shredder or place the document in a secure bin specifically designated as a shredding bin where the documents will be retrieved for shredding.

3.2.2 Printers, Copiers, and Fax Machines

Printers, copiers, and fax machines that are used to process sensitive information must be placed in secure locations and areas not easily accessible to unauthorized persons. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment.

All documents containing sensitive information must be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location. Any documents containing sensitive information that must be disposed of due to an error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed.

If a printer, copier, or fax machine jams or malfunctions when printing Confidential or Restricted information, the involved users must not leave the machine until all copies of the sensitive information are removed or are no longer legible. All paper copies of sensitive information must be disposed of by shredding or other methods approved by management.

3.2.3 Faxing Precautions

Sensitive materials should be transmitted through the district secure file transfer system as practicable. Sensitive materials must not be faxed unless an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site, the fax is sent to a locked room to which only authorized employees have access, or a password-protected fax mailbox, after verbal confirmation that the receiving party is on hand to

restrict release to an authorized recipient, or recipient is ready. Sensitive information must not be faxed through untrusted intermediaries.

The receipt of sensitive information by fax must be confirmed promptly. All faxes must employ a standard cover page that includes language approved by the district.

3.2.4 Printer Precautions

When printing sensitive information, the user must be present at the printer at the time of printing or use a secure print queue (follow me printing) to prevent the information from being revealed to unauthorized parties or direct the output to a printer inside an area where only authorized employees are permitted to go.

3.2.5 Copy Machine Precautions

Unless permission from the copyright Owner is obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary business appropriate.

3.2.6 Electronic Safeguards

3.2.6.1 Computer Access

Only employees who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals. The posting, sharing and any other disclosure of passwords and/or access codes is prohibited. Access to computer-based sensitive information shall be limited to staff members who need the information to perform their work-related duties. Computer displays must be positioned such that the information cannot be readily viewed by unauthorized persons.

3.2.6.2 Sensitive Data Transmission and Storage

All sensitive data must be encrypted while at rest and during transit across public networks to protect it from internal and external threats and provides a second line of defense in high threat areas. The requirements for data encryption are based on its classification, sensitivity, location, and media where it is stored. Sensitive data shall not be stored on any media other than secure services provided by FCS (such as district provided Microsoft OneDrive).

If sensitive information is transmitted over public computer networks such as the Internet, this transmission must take place with encryption facilities. All portable and remote systems storing sensitive information must also employ hard disk encryption systems. In all but a few rare instances, if information is to be protected, then the user must take specific action to enable encryption facilities. Users must be careful about the inclusion of sensitive information in electronic mail messages that are not protected by encryption. See Data Classification for applicable requirements. FCS Technology department will maintain a list of all district provided services that support encryption. Any district provided services that do not support encryption shall not be used for storage of sensitive data.

3.2.6.3 Electronic Mail

Sensitive data, such as confidential documents or PII, shall not be sent via e-mail in an unencrypted format. If an electronic mail message contains sensitive information, users must not forward it to another recipient unless the other recipient is known to be authorized to view the information, or the originator approves the forwarding. Electronic correspondence that contains sensitive data must be clearly labeled as such See Data Classification for applicable requirements.

3.2.6.4 Data Backup

Formal data back-procedures are required for all multi-user systems that support critical business functions. This shall include, but not be limited to, database servers, mainframes, network file shares and other integral systems. At minimum, all backups must follow the following standards:

- Backups must be made of all essential operational data.
- All physical backups must have externally visible labels identifying the classification of the data.
- All backups containing confidential data must be encrypted.
- Backup media must be stored in a secure location.

- Backup media inventories stored offsite must be reviewed on a periodic basis to any detect any inventory losses.
- Backups must be stored in a location approved by Technology Services.

3.2.7 Media Distribution

All media containing sensitive information must be distributed in a secure manner both internally and externally. External distribution of such media from FCS must be logged and authorized by the data owner. If it is necessary to remove computer-readable sensitive information from FCS facilities, this information must be protected with encryption.

3.2.8 Data Auditing

The retention requirements will be driven by applicable legal, regulatory, or business reasons. If such data is found stored beyond the duration of its storage requirements duration, then it will be securely purged.

3.2.9 Destruction of Sensitive Information

3.2.9.1 Written

Documentation that contains sensitive information must be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

3.2.9.2 Electronic

Prior to the disposal of any computer equipment, including donation, sale or destruction, the IT Department must determine if sensitive information has been stored on the equipment and delete all sensitive information prior to the disposal of the equipment or obtain a certificate of destruction by a certified 3rd party. See Data Destruction for applicable requirements.

4.0 DATA CLASSIFICATION

4.1 Purpose

The FCS data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the procedures defined in this document, will protect FCS information from unauthorized disclosure, use, modification, and deletion.

4.2 Policy

4.2.1 Classification Labels

4.2.1.1 Data Custodians and Production Information

All information types possessed by FCS must have a designated Owner. Production information is information routinely used to accomplish business objectives. Information Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the FCS administrative team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

4.2.1.2 Data Custodians and Access Decisions

Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

4.2.2 Data Classifications

4.2.2.1 RESTRICTED

This classification label applies to the most sensitive information that is intended for use strictly within FCS. Its unauthorized disclosure could seriously adversely impact FCS, students, employees, and the FCS mission.

Examples could be security audit results, school safety audit results and school safety plans.

4.2.2.2 CONFIDENTIAL

This classification label applies to less-sensitive operational information that is intended for use within FCS. Its unauthorized disclosure could adversely impact FCS, students, employees, and the FCS mission. Information that some people would consider to be private is included in this classification.

Examples include employee performance evaluations, student performance and statistical information, PII, computer passwords, identity token personal identification numbers, and internal audit reports.

Personal Information (PI) is defined in Ga. Code § 10-1-910 et seq. as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security Number;
- Driver license or state identification card number;
- Account number or credit card number or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the above items when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

4.2.2.3 FOR INTERNAL USE ONLY

This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact FCS or its employees, suppliers, business partners, or its customers.

Examples include the FCS telephone directory, new employee training materials, and internal policy manuals.

4.2.2.4 PUBLIC

This classification applies to information that has been approved by management for rele ase to the public. There is no such thing as unauthorized disclosure of this information, and it may be disseminated without potential harm.

Examples include product and service brochures, advertisements, job opening announcements, and press releases.

4.2.2.5 Other Labels

Department or division-specific data classification labels are permissible but must be consistent with and supplemental to the data classification system. These supplementary labels might for example include the use of words like “Personnel” or “Financial.”

4.3.3 Labeling

4.3.3.1 Consistent Classification Labeling

Most of the FCS information falls into the **Internal Use Only** category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label is by default classified as **Internal Use Only**.

If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate data classification designation. Such markings must appear on all manifestations of the information, such as hard copies, removable media and CDs/DVDs. Personnel must not remove or change data classification system labels for sensitive information unless the permission of the Owner has been obtained.

4.3.3.2 Incorrect Labeling

If the recipient of FCS internal information believes that the data classification label accompanying this information is incorrect, the recipient must protect the information in a manner consistent with the more stringent classification labels. Before using this information or distributing it to any other party, such a recipient must check with the Information Owner to ensure that the label currently applied to the information is correct.

4.3.3.3 Information Collections

Personnel who create or update a collection of information are responsible for choosing an appropriate data classification label for the new collection. This label must be consistent with the decisions made by the relevant Owners and generally should be the most restricted classification level found in the collection.

4.3.3.4 Hardcopy

All printed, handwritten, or other paper manifestations of **RESTRICTED** or higher level must have a highly visible sensitivity label on the upper right-hand corner of each page. If bound, all paper manifestations of sensitive information must have an appropriate sensitivity label on the front cover, the title page, and the rear cover. The cover sheet for faxes containing sensitive information must contain the appropriate classification label.

4.3.3.5 Computer Storage Media

All removable media, and other computer storage media containing sensitive information must be externally labeled with the appropriate sensitivity classification. Unless it would adversely affect the operation of an application program, computer files containing sensitive information must also clearly indicate the relevant classification label in the first two data lines.

If information recorded on computer storage media with a higher sensitivity classification is moved to media with a lower sensitivity classification, then the media with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification.

4.3.3.6 Additional Public Information Labels

Unless it is unquestionably already public information, all FCS information with a **Public** label must also be labeled "Approved for Public Release" along with the date when the Owner declared the information Public.

4.3.3.6 Voice Recordings

To reduce the chance of unauthorized disclosure, in general, employees must not record sensitive information. If the use of recording devices is an operational necessity, the proper sensitivity classification must be specified at the beginning and end of each segment of sensitive information. In this case, the recording media must also be marked with the most stringent data classification found on the media. In addition, the media must be protected in accordance with the most stringent classification found on the media and erased as soon as practicable. Any recording generated through official FCS duties will receive a classification of no less than **'FOR INTERNAL USE ONLY'** unless formally approved by appropriate personnel.

4.3.4 Declassification and Downgrading

4.3.4.1 Schedule for Review

To determine whether sensitive information may be declassified or downgraded, at least once annually, Information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical.

4.3.4.2 No Unauthorized Downgrading

Personnel must not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of the declassification or downgrading process approved by the Owner.

5.0 DATA DESTRUCTION

5.1 Purpose

The storage of sensitive information must be maintained to the shortest period to satisfy legal, regulatory, and business requirements. The purpose of this policy is to establish a standard for the storage and subsequent destruction of stored, sensitive information.

5.2 Policy

All sensitive information must be destroyed or disposed of when no longer needed for business purposes. To support this policy, FCS personnel must review the continued value and usefulness of sensitive information on a periodic basis. The data retention schedule must be reviewed to determine the minimum legal periods that information must be retained. See Data Retention Schedule for applicable requirements.

5.2.1 Destruction and Locked Boxes

All sensitive information no longer being used or no longer needed must be placed in designated locked boxes until such time as authorized FCS personnel or a bonded destruction service picks it up. If no locked disposal boxes are in the immediate vicinity, sensitive information in hardcopy form must be either shredded, while sensitive information in all other forms must be delivered to management for secure destruction. The shredders used for this purpose must create confetti or other similar small particles. Strip-cut shredders must not be used for this purpose. If unable to immediately dispose of information by the recommended method, it may be locked in a secure location.

Erasing or reformatting magnetic media such as removable media is not an acceptable data destruction method. The use of overwriting programs approved by the CTIO is permissible to destroy sensitive information stored on servers or hard drivers. Only after these programs have been used can storage media containing sensitive information be reused, trashed, recycled, or donated to charity.

5.2.2 Destruction Approval

Personnel must not destroy or dispose of potentially important records or information that is not “owned” by them without specific advance management approval. Unauthorized destruction or disposal of FCS records or information will subject the personnel to disciplinary action up to and including termination and prosecution.

Records and information must be retained if they are likely to be needed in the future, regulation or statute requires their retention, or they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts. Any questions about data destruction must be referred to the CTIO.

5.2.3 Permissible Destruction

Personnel may destroy FCS records when approval has been granted by documented instructions from the Owner or the Owner’s delegate, or CTIO. The documented instructions must include the type of records that may be destroyed and when, or the records retention and disposition schedule. Destruction is defined as any action that prevents the recovery of information from the storage medium on which it is recorded.

5.2.4 Removable Storage Media

All materials used in the handling of sensitive information, which could be analyzed to deduce the sensitive information, must be destroyed according to methods approved by the CTIO. Examples of removable storage media include, but are not limited to:

- Thumb drives
- External Hard drives
- CD
- DVD
- Backup Tapes

5.2.5 Photocopies

All waste copies of sensitive information that are generated in the course of copying, printing, or other sensitive information handling must be destroyed according to the instructions found in this policy. If a copy machine jams

or malfunctions when personnel are making copies of sensitive information, the involved personnel must not leave the machine until all copies of the information are removed from the machine or destroyed beyond recognition.

5.2.6 Equipment Disposal or Servicing

Before computer or communications equipment is sent to a vendor for trade, servicing, or disposal, all sensitive information must be destroyed or concealed according to methods approved by the CTIO. Internal hard drives and other computer storage media may not be donated to charity, disposed of in the trash, or otherwise recycled unless they have been subjected to overwriting processes approved by the CTIO.

6.0 DATA PROTECTION

6.1 Purpose

Encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is readable only by authorized individuals. This policy establishes that encryption for electronic information shall be consistent with FCS need for continued availability of the information. The purpose of this policy is to define the minimal requirements for the use of encryption.

6.2 Policy

All FCS information and systems must meet the data protections listed in this policy to protect the information assets for FCS.

6.2.1 Data-at-Rest

All data that is classified at or above **FOR INTERNAL USE ONLY** must be encrypted at rest in all locations that it resides. The encryption must utilize a non-deprecated standard of encryption cipher. Currently acceptable encryption protocol is Advanced Encryption Standard (AES) 256 bit.

6.2.2 Data-in-Transit

All data that is classified at or above **FOR INTERNAL USE ONLY** must be encrypted in transit on any public network or wireless network. Encryption must utilize a non-deprecated standard of encryption protocol. Currently, the only approved transit protocols are Transport Layer Security (TLS) 1.2 and 1.3.

6.2.3 Data Loss Prevention

Data Loss Prevention (DLP) techniques should be used to prevent and alert Data Custodians to the misuse of all data that is classified at or above **FOR INTERNAL USE ONLY**. Methods of DLP can include:

- Access control restrictions
- Access notifications
- DLP Products
- DLP Capabilities in host solutions

6.2.4 Integrity Checking

Mechanisms will be in place for checking software, firmware, and hardware before they are installed in the environment. Software, firmware, and hardware that is introduced to the network will only be implemented if they are from known sources.

7.0 ASSET MANAGEMENT

7.1 Purpose

Assets allow FCS to accomplish its mission. The purpose of this policy is to establish the standards for managing assets throughout the asset lifecycle.

7.2 Policy

All assets will have designated owners that are responsible for maintaining the assets throughout its life cycle.

7.2.1 Hardware Asset Management

Hardware includes physical devices and systems. All hardware assets will be maintained in an asset inventory. All hardware items must be identified via a serial or other number or unique identifier.

7.2.2 Software Asset Management

Software includes all computer programs that are used by systems and applications to perform designed functions. All software on all systems will be inventoried at least annually. Software installed on systems will only remain on systems if the software is required for the proper operation of the system. Software can be inventoried via software management platform or manual documentation. All critical systems will be reviewed at least annually for removal of unnecessary software. All non-critical systems will be reviewed every 3 years for required software.

7.2.3 Network Mapping

The FCS Networking team will maintain an accurate map of the network. Network mapping will include Layers 1-4 of the Open Systems Interconnection (OSI) model. Network maps can be maintained in software programs or via manual methods. The network maps must be reviewed and updated at least annually.

7.2.4 External Information Systems

The FCS IT Team will maintain an inventory of all external information systems that create, transport, store, or manage classified information. External systems include all systems that require the Internet to access. Systems may be managed by third-party service providers, but agreements must include requirements for asset and data security. External assets may be managed through software or manual documentation. Assets must be reviewed at least annually. (Fortify Data is used to meet this procedure.)

7.2.5 Asset Value

Asset managers will conduct annual value asset assessments. Value of the assets will be calculated via the formula of:

Single Loss Expectancy (SLE) x Annual Rate of Occurrence (ARO) = Annual Loss Expectancy (ALE)

The SLE is calculated by Asset Value (AV) x Exposure Factor (EF). AV is the actual cost of the asset, and EF is calculated by the sum of the production loss of asset being down and the cost of the effort to restore the asset to operational capacity. ARO is calculated by utilizing historical records to determine the number of times per year that the asset will go down. ALE is the amount of capital that should be spent to keep the asset in place. All assets must be included in total value.

8.0 RISK MANAGEMENT

8.1 Purpose

Risk is the nature of adverse events that can impact FCS ability to accomplish its' mission. The FCS BOE has dictated that critical risks are unacceptable to the organization. The BOE has charged asset managers with assessing, planning, reducing, reporting, and eliminating risk. Asset managers should maintain a risk management program for the assets in their charge and be able to brief the BOE on their risk profile at least annually.

8.2 Policy

All asset managers will maintain a risk management program that includes qualitative and quantitative risk assessments

8.2.1 Risk Assessment

All Asset Managers will maintain a Risk Assessment that includes all assets they are responsible for. Asset Managers may use any platform that meets these requirements:

- The platform lists all assets (internal and external) under the Asset Manager's charge;
- The platform has an analysis of threats and vulnerabilities against the assets;
- The platform allows for quantitative risk analysis that stems from the US Dollar value of the asset;
- The platform allows for qualitative risk analysis that stems from value that assets provide from a non-USD value; (examples would be loss of trust or reputation)
- The platform allows the calculation of risk to be the likelihood of an occurrence and the severity or impact of the threat event;
- The platform assigns responsibility for risk treatment;
- The platform allows risks to be prioritized based on criticality;
- The platform allows the Asset Managers to inform the Stakeholders of risk levels;
- The platform is updated at least quarterly;
- The platform allows the assigning of controls for risks;
- The platform allows Asset Managers to utilize threat intelligence sources for updates to vulnerabilities to assets.

8.2.2 Risk Treatment

Risk Treatment is the process of addressing risks to meet the Stakeholder's risk tolerance for the assets. There are several options available to Asset Managers for addressing risks including:

- Risk Mitigation - this is the process of selecting and implementing a control to reduce the likelihood or severity of an event. An Example of this would be purchasing a firewall to place at the network perimeter.
- Risk Transference - this is the process of transferring the risk to another party. An example of this would be insurance.
- Risk Avoidance - this is the process of avoiding the risks associated with an asset altogether. An example of this would be deciding not to do something because the risks are too great.
- Risk Acceptance - this is the process of accepting risks to an asset because they are within the guidance of the Stakeholders for risk tolerance. An example of this would be accepting Low criticality vulnerabilities because they do not allow an attacker to exploit any system or information.

8.2.3 Supply Chain Risk Management

All external service providers that provide operational support critical to the mission of FCS will be included in the risk assessment process. Applicable asset managers will monitor and assess risks to critical services provided by external parties. Operational agreements made with third parties will include requirements to meet all policies and procedures of FCS including system and information protection requirements. Incident response, disaster recovery, and operational continuity will be understood between the applicable Asset Manager and the external party. Annually, critical external parties will be audited to ensure they meet the requirements of this policy. It is also acceptable to maintain documentation from the third-party demonstrating compliance through other assessment methods (ex- SOC II, ISO 27001, or other report). Testing for incident response and disaster recovery should be conducted annually.

9.0 ACCESS CONTROL

9.1 Purpose

Controlling access to information assets is critical to the security of FCS. Access for all users, devices, and processes will be granted, verified, revoked and audited depending on operational need for continued access. Logical and Physical access will be granted and revoked based on the Principle of Least Privilege. The Principle of Least Privilege states that access is only allowed based on requirement to perform necessary functions and no more. Where possible, duties should be separated to prevent fraud and suspicion.

9.2 Policy

Access to all FCS information should be controlled by information owners and custodians.

9.2.1 Role Based Access Control

Where possible, logical and physical access should be based on a role or job function. Users that are granted access should be assigned to roles based on position and need. All roles should be audited annually for their permissions. All members of all roles should be audited at least annually for required access. Users, devices, and processes should have unique identifiers to prevent non-repudiation. The continuation to generic accounts will be decided by the Technology Services Department on an annual basis.

9.2.2 Physical Access

Physical access to all areas that contain FCS information and systems that create, store, process, or transmit FCS information that is classified at or above must be marked **FOR INTERNAL USE ONLY**. Physical access lists must be maintained by the manager of the area via electronic or hard-copy lists. All possible access methods should be documented in a risk assessment for the assets. Physical access can be limited via many methods including any method to restrict physical access to the area and information assets.

9.2.3 Remote Access

Remote access to internal information systems will follow the principle of least privilege. Only (Technology Department) approved methods of remote access will be used.

Only approved users and processes will be allowed access to the above methods of remote access. Approved user accounts will be managed via the Remote Users Group in Active Directory (AD). No other method of remote access to internal systems is allowed. All unnecessary ports and services should be closed at the perimeter.

9.2.4 External Asset Access

All assets that reside outside the network perimeter must managed access control carefully. External assets include (but are not limited to):

- Websites that maintain student and FCS data
- Cloud-based resources
- Third-party management tools hosted outside the FCS network
- Document and file sharing services

Access to external resources must be managed by an Asset Manager that is responsible for granting, verifying, revoking, and auditing access. Access to external resources should be federated wherever possible.

9.2.5 Privileged Access

Any elevated privileges to any system or information asset must be carefully controlled by the information owner or custodian. All elevated privileges must be reviewed at least quarterly for necessity. All elevated user passwords should be changed at least annually. Where possible Multi-Factor Authentication should be used for user accounts with elevated privileges. Elevated user accounts should be separated by a naming convention from standard user accounts. Users with elevated access should not perform standard activity (answering email, surfing web, etc.) while utilizing their elevated account. All users that have elevated access will have clear roles and responsibilities established and sign an agreement stating their understanding.

9.2.6 Authentication Architecture

Where possible, all authentication architecture should be designed with a single Source of Truth (SoT). Utilizing a single SoT will allow a unified place for permissions and roles to be assigned without having many places to alter or audit. The approved SoT for FCS is Active Directory (AD). The AD SoT will be managed through on-premise AD Domain Controllers (DC)s that are federated to an Azure AD instance for cloud-based authentication. If at all possible, applications, services, users, processes, devices, and systems should be authenticated through federation with AD. Any system classified as operationally critical shall have, at least, multi-factor authentication (MFA) assigned to all staff user accounts. Though not required, that MFA should be tied to the SoT. All connections and authentication assertions should be made through an acceptable level of encryption. Where possible, authentication data should be encrypted at rest and in transit.

9.2.7 Authentication Classification

Data that is capable of authenticating a user (a password, ticket, session, etc.) is classified as **CONFIDENTIAL**. Users should never share their passwords with anyone, including IT. Users are not permitted to write down their passwords and keep them in an unsecure place. If a user suspects their authentication information may have been lost, it is imperative that the user change their password and notify the Technology Department immediately.

9.2.8 Event Detection

All users, employees, contractors, students, visitors, volunteers, and anyone else who utilizes any FCS information system, network component, or classified data should expect that all actions are monitored and logged for security applicability. Users should not expect privacy of personal information while using the FCS network.

9.2.9 Type 1 Authentication Policy

Type 1 authentication is something that a user knows. Examples of Type 1 authentication are passwords, passphrases, pin numbers, secret codes, etc. Type 1 authentication is the least secure method of authentication because it can easily be stolen or guessed and used to authenticate a malicious actor in the user's place. Type 1 authentication is also the most common form of authentication. Users will be required to create strong passphrases consisting of 16 or more characters, upper- and lower-case letters, and numbers or symbols. Users will be required to change their passphrases at least annually. Users should never use their FCS credentials in any other online service such as social media or another website.

10.0 INFORMATION SECURITY TRAINING

10.1 Purpose

The purpose for this policy is to establish the method for which the organization will accomplish awareness and training for information security.

10.2 Policy

Training shall be the responsibility of the Instructional Technology department. All users should attend some form of information security training at least annually. Users that are granted an account in AD are all required to have annual information security training. New users must be given information security training no later than 30 days after being granted access.

10.2.1 Training Requirements

The training program must include the following:

- Awareness of all information security policies and procedures
- Updated training on attack vectors that are common for users
- Social engineering
- Acceptable use of information systems
- Data handling and classification
- Applicable standards and regulations
- Incident response and recovery
- Reporting security incidents
- Enforcement measures

10.2.2 Elevated Access Training

Users that have any form of administrative, system, root, or other form of network, application, or local elevated privilege must be given additional training to understand the additional risks of elevated permissions. Designated cybersecurity personnel should be given a training program that includes certifications for industry expertise.

10.2.3 Training Records

The Instructional Technology department, under the supervision of the Director of Instructional Technology, will oversee the storage and completion of all training records.

10.2.4 Program Effectiveness

The CTIO will be responsible for assessing the information security awareness and training program and assessing its effectiveness. The program content should be updated at least annually.

11.0 SYSTEM PROTECTIONS

11.1 Purpose

The purpose of this policy is to specify the system protections for FCS Information Systems. Information Systems are the endpoint devices that allow users, programs, and applications to fulfill their purpose. Due to the level of criticality that information systems provide to FCS, significant protections need to be in place to ensure availability.

11.2 Policy

11.2.1 Baseline Configurations

The Technology Department will maintain a baseline configured virtual image of all regularly used operating systems that is created with the Principle of Least Functionality in mind. This means applications, services, and ports that are unnecessary are unused.

- System configuration standards must be based upon industry recognized best practices such as those provided by SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), or Center for Internet Security (CIS).
- System configuration standards must be reviewed at least annually and updated to reflect current industry best practices and newly discovered vulnerabilities. A vulnerability scanning and management program will be managed by the Technology Services Department.

11.2.2 Minimal System Configuration Standards

The following are the minimum standards for system configuration:

- All systems that are used to process FCS information must employ an access control mechanism which is activated at the time the device is powered on, and when it is reactivated after a period of inactivity.
- All vendor-supplied defaults must be changed or removed before any system is used for FCS operations. Vendor defaults include but are not limited to items such as login credentials
- Where possible, systems must be configured to perform only one primary function to prevent functions that require different security levels from co-existing on the same server.
- Systems must be configured to re-authenticate access if there has been no activity for a defined interval. The system must automatically blank the screen, suspend the session, and require a password for the re-establishment of the session.
- All staff will be expected to enroll in password self-service (PSS). High school students shall have the ability to enroll in PSS by the end of the 2022 calendar year.

Before deployment, operating systems, database management systems, firewalls, and applications must be updated to the most recent stable release level. For systems actively in production, patches with a risk level of:

- CRITICAL must be applied within 30 days
- HIGH must be applied within 90 days
- MEDIUM (MODERATE) or lower will be evaluated for effect before

Vulnerability scans of all FCS information systems classified as CRITICAL will be scanned with a vulnerability scanner at least weekly. All other FCS information systems will be scanned at least quarterly.

11.2.4 Security Software

Where possible, all endpoints will have an endpoint protection software that utilizes both process evaluation (exploit-based) and file evaluation (signature-based) to detect the operation or use of malicious code or mobile code. Where possible, all endpoints should have a host-based firewalls enabled to only allow the necessary ports and services to remain open.

11.2.5 Backups

All systems and applications that are required to accomplish the mission of FCS must be backed up at regular intervals. The interval of backups must be set for each asset based on the risk assessment and criticality of the CIA. Backup recovery should be tested at least annually to ensure recovery capabilities.

11.2.6 Review and Improvement

All system protections must be evaluated by the Asset Manager at least annually for effectiveness and applicability. System protections should be tested by internal or external parties to evaluate the technical capabilities. Effectiveness of critical controls should be shared in a report at least annually.

12.0 CHANGE CONTROL

12.1 Purpose

Change control is a vital process to protect the necessary network and systems that allow FCS to accomplish its mission. This process must be followed for all significant changes to the environment. A significant change is any asset alteration that could impact the confidentiality, integrity, or availability of that are required to meet the mission of FCS. Assets required to accomplish the mission of FCS are identified in the Business Continuity Plan.

12.2 Policy

12.2.1 Change Requests

Any user that needs a change to be made to a required asset will submit the request via email to the appropriate system administrator or Asset Manager. System administrators and Asset Managers must evaluate the change for potential effect to the CIA of the asset. Plans to implement the change must be developed and approved by the Asset Manager.

12.2.2 Monitoring and Evaluation

All changes to required assets must be monitored for a period of 30 days to determine actual effect to the CIA of the asset. Changes must be evaluated to determine efficacy and applicability to the policies and procedures of FCS. All changes to critical assets will be logged. Remote maintenance should only be performed in required cases with approved tools.

13.0 OPERATING ENVIRONMENT

13.1 Purpose

The purpose of this policy is to set the standards for the physical operating environment for systems and data .

13.1 Policy

13.1.1 Minimum Physical Security Requirements

All areas that allow access to FCS data classified at or above **FOR INTERNAL USE ONLY** must be controlled. Minimum security requirements are:

- Keep a safe computing environment for all computing equipment by keeping them from being exposed to liquids, excessive moisture, excessive dust, and excessive heat;
- Maintain a secure environment for all system control units, file servers, or master units that control or serve shared units and allow physical access to these units only to authorized employees;
- Ensure that computing resources are secured from unauthorized access or theft whenever left unattended;
- Keep equipment out of plain sight when it is left in a vehicle or hotel room;
- Backup data and program code regularly and store the backups in a secure, off-site location;
- Store approved removable media containing classified corporate information or programs in a secure storage container when not in use.
- Physical environments that contain access to critical assets will be monitored for unauthorized access.

13.1.2 Visitors

Visitors to any building or site containing FCS information processing facilities must be granted access for specific, authorized purposes. All visitors will be provided with a sticker that clearly identifies them as a visitor. These stickers must always be worn and easily visible. All visitor stickers must be set to expire no longer than the end of the current day. Visitors must surrender their sticker or badge to the issuing party or their employee escort before leaving any FCS facility.

Visitors who have not been granted special access privileges must always be escorted and monitored in access-controlled areas. Visitors shall be required to wear identification that is always clearly visible and will not be permitted uncontrolled freedom of movement around the premises.

14.0 NETWORK PROTECTIONS

14.1 Purpose

The purpose of this policy is to specify the protection mechanisms for the FCS network. The network provides vital services to FCS to accomplish its mission.

14.2 Policy

14.2.1 Network Diagram

A current network diagram must be established and maintained by the Technology Department to show all connections, including connections to any/all wireless networks. This diagram must be reviewed and updated at least every year, or immediately after any major configuration change.

14.2.2 Logging and Event Detection

Security event logs must be gathered from all critical assets. Security event logs should be gathered on all other systems that are capable of being monitored. Network security events should also be gathered and correlated to system events for security management. Event logs should be available for immediate access for 3 months and for 12 months in cold storage. Security events must be ranked in criticality and monitored by a security professional. Alerting thresholds will be set to alert administrators for events that need to be addressed immediately. User activities on any critical information systems, the FCS network, and any application that stores, creates, processes, or transmits FCS classified data will be monitored and logged by security tools. All network and system security event logs that are required by applicable regulations and standards will be gathered and maintained for the required period.

14.2.3 Intrusion Detection and Prevention

The network should include Intrusion-detection systems (IDS), and/or intrusion-prevention systems (IPS) which must be deployed with the purpose of monitoring all traffic at the perimeter as well as at critical points inside the FCS network and cloud environments. These intrusion detection systems must detect unauthorized modifications to firewall system files and detect denial of service attacks in progress. Such intrusion detection systems must also immediately notify the technical staff that is able to take corrective action. All intrusion-detection and prevention engines, baselines, and signatures must be kept up to date.

14.2.4 Network Segmentation

The network should be segmented to prevent unnecessary communication between network objects and endpoints that do not need to communicate. Assets categorized in the Business Continuity Plan as CRITICAL must be protected from the rest of the network. Data classified at or above **CONFIDENTIAL** must be segmented from the rest of the network. Logs of security events related to segmentation controls must be forwarded to the security alerting system. Only necessary devices and users will be allowed to join the network and segmented sections of the network will be allowed to gain access to the network.

15.0 INCIDENT RESPONSE

15.1 Purpose

The purpose of this policy is to set the standards and procedures for security incident determination and response.

15.2 Policy

15.2.1 Incident and Breach Definitions

A “Breach” is defined in Ga. Code § 10-1-910 et seq. as an unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality, or integrity of Personal Information (PI) of such individual maintained by an Entity. Good-faith acquisition or use of PI by an employee or agent of an Entity for the purposes of such Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

An “Incident” is any security event (or collection of them) that activates the alert process in this policy; they are any information system related event involving a violation of the law, or a violation of security policy. Such an incident may alternatively involve any significant disruption of operational operations or any event that seriously jeopardizes the security or privacy of classified FCS data or assets. Incidents will be determined by the Alert Process Tree listed below. Incidents must be logged and documented in a Computer Security Incident Response (CSIR) Report.

A “Security Event” is any occurrence of a user, application, system, or network function that could be relevant to the security posture of FCS. The vast majority of these will not be relevant to cybersecurity but must be logged and correlated by security tools for correlation to potential incidents.

15.2.2 Reporting

All users of FCS information systems and assets must be trained and prepared to report any violation of this policy or suspected security incidents to the Technology Department by:

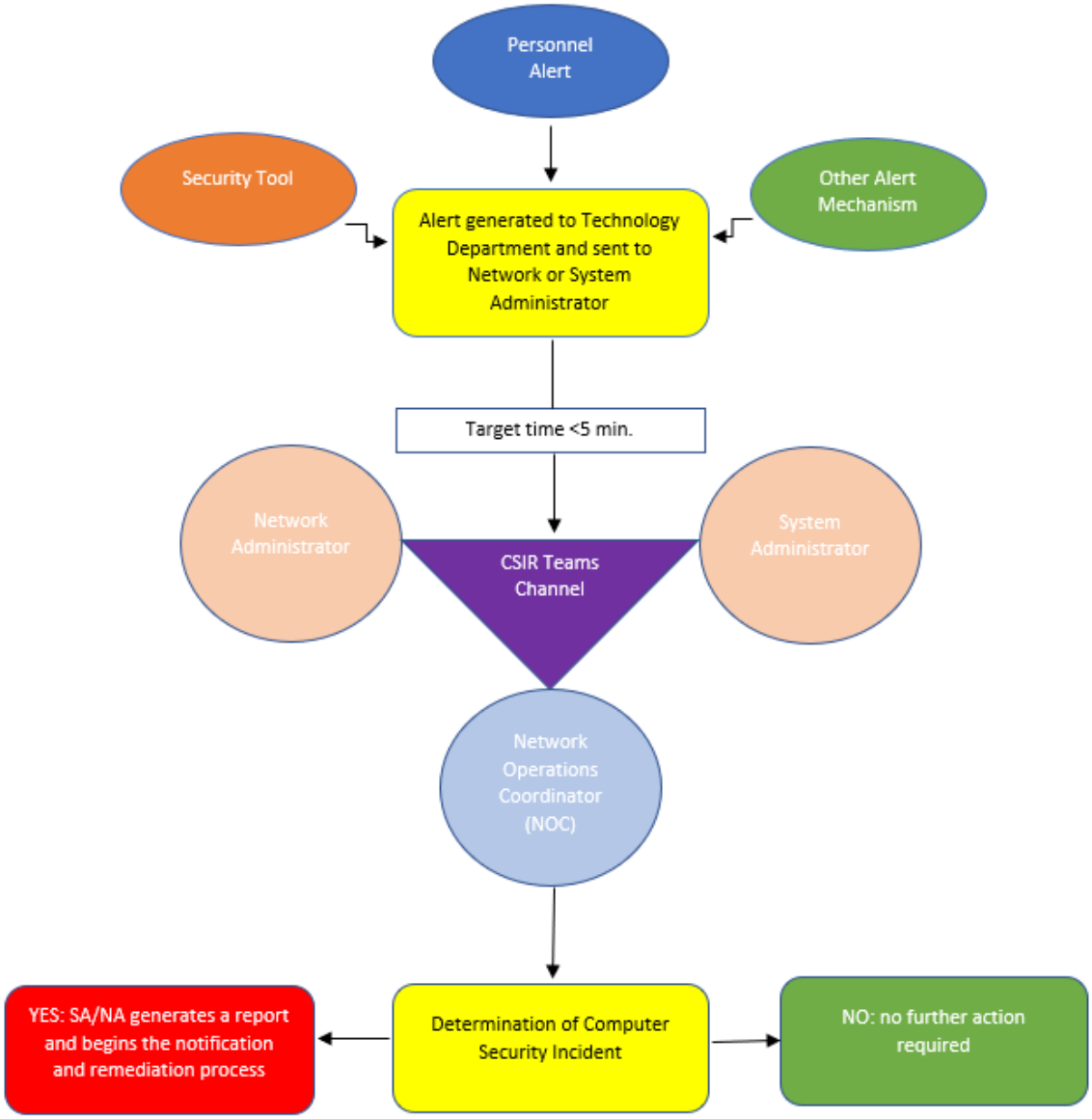
Alerting their immediate supervisor or ITS

All users are responsible for the cybersecurity of FCS and must be trained and prepared to report security events.

15.2.3 Alert Process

The following is how Security Events will be categorized into one of the definitions above. Security Events will be delivered to the Technology Department through security tool alerts, personnel reporting, technical discovery, or many other forms. The Network and Systems Engineers (NE and SE) as well as the Network Operations Coordinator (NOC) will serve on the Computer Security Incident Response (CSIR) Team. The NOC will maintain a Microsoft Teams channel that will serve as the primary means of communication and coordination for security incidents and determination. When an event enters the TD, one of the parties above will investigate the event to determine if the CSIR need to determine if an impact to FCS data or critical assets has possibly occurred. The CSIR will meet on a Microsoft Teams meeting at the soonest possible time to determine if FCS classified data or a critical asset may have been affected. In the event a definitive Breach, Incident or Security Event is identified, the NOC or Director of Technology Services will notify the CTIO, who will then notify the Superintendent and Public Relations Director. The process to define the event as an Incident or Breach is shown below:

Computer Security Incident Report Generation:



Alerts from security tools for Events that meet a threshold of Critical will be reviewed by the Network Operations Team and will generate an alert to the CSIR via email. The Event will be reviewed by the responsible administrator and either elevated to the CSIR Teams channel or dismissed as a false positive. If the administrator believes the Event may be accurate, the administrator will raise the issue in the Teams CSIR channel, and the NOC will determine if an Incident or Breach has occurred.

15.2.4 Incident Documentation

All Security Events that are determined to be an Incident or Breach will be documented in a Computer Security Incident Response form. The form will be saved in the CSIR Teams Channel in documentation. The applicable administrator will be responsible for creating and maintaining the document for the duration of the incident. The CSIR form will be based on the requirements of NIST SP 800-61r2 and will have the following sections:

- Executive Summary
- Impact Assessment
- Timeline
- Technical Data
- Comments
- Figures (as applicable)

Once a CSIR has been started, the document will be classified as **RESTRICTED** and will only be used by personnel involved that have a need to access the document.

15.2.5 Incident Closure

All Security Incidents and Breaches will remain open or in progress until the CSIR Team has sufficient evidence to determine that the adverse condition to FCS classified data or critical assets has been halted. Once the Incident or Breach has been closed, the responsible administrator will fill out the remaining sections of the document and the DOT will schedule a briefing for the CTIO to review:

- Incident or Breach Summary
- Impact to Assets and Data
- Actions Taken to Close the Incident or Breach
- Lessons Learned
- Next Steps

The CTIO will be responsible for briefing the Superintendent and/or BOE if the incident does cause serious affect to FCS classified data or critical assets.

15.2.5 Incident Response Procedures

15.2.5.1 Classified Data Exposure

All Data Custodians of classified FCS data will implement (where possible) Data Loss Prevention (DLP) mechanisms to alert the custodian of any form of misuse of the data. Misuse of the data could include but is not limited to:

- Unauthorized Access
- Unauthorized Destruction
- Unauthorized Alteration
- Unauthorized Exfiltration
- Unauthorized Storage
- Personnel Errors

Any alert to the possible misuse of FCS data classified at or above **CONFIDENTIAL** must be reported to the CSIR Team immediately for a determination of a Breach or Incident.

Upon discovery of an alert to the misuse of FCS classified data the Data Custodian must investigate the Event to determine if the alert is valid or not. If the alert is valid, the Data Custodian must take immediate action to stop the misuse of the data or ask for help from the CSIR or Physical Security personnel. Once the Data Custodian has sufficient evidence to verify that the misuse of the data has ceased, the Data Custodian will assist the CSIR in documenting the incident in a CSIR Report. Data Custodians immediate supervisors are responsible for briefing the Superintendent and notification requirements.

15.2.5.2 Information System and Network Incidents or Breaches

The Network Operations team is responsible for determining if Security Events are worth elevating to the CSIR Team for determination of an Incident or Breach. The applicable administrator will be responsible for

taking action to halt any Breach or Incident to a critical information system asset. Once a Security Event has been investigated, the SA or NA will take action to reduce the effect of the event. If the asset is critical, the Director of Technology Services or NOC will make the decision to act on the critical asset. To gather information on the incident, the responsible administrator should:

- Gather initial evidence, including logs and alerts.
- Determine the current and potential technical effect of the incident.
- Determine the criticality of the affected resources.
- Determine the general state of the network overall.
- Determine if malicious or non-malicious in origin (worm vs. configuration error or hardware failure.)
- Determine if internal or external in origin.
- Determine if attempting to propagate.

If possible, affected systems and network objects should be preserved for evidence and investigation, but this should not take priority over stopping the Breach or Incident.

15.2.5.3 Recovery

Each asset classified as CRITICAL in the Business Continuity Plan (BCP) will have a procedure for recovery in the Disaster Recovery Plan. Disaster Recovery Plans must be tested for operational capability. All disaster recovery procedures must have a primary and secondary employee that are prepared to implement the disaster recovery procedure.

15.2.6 Notification

If a Security Event has been determined to be a Breach (In Accordance With [IAW] Ga. Code § 10-1-910 et seq.) the CSIR Team will include legal counsel to determine legal breach notification requirements. All external Breach notifications or Incident communications will be conducted through the Communication and Community Engagement Office. All internal Incident and Breach communication and notification will be conducted through the Technology Department. Data surrounding security Events, Incidents, and Breaches should only be shared with the necessary parties and should be limited to the data that is relevant to their position. All data should be shared with necessary parties to include the lessons learned and next steps for prevention in the future. Public announcements and relations will be managed by the Communications Office.

16.0 INTERNAL EVALUATION

16.1 Purpose

The purpose of this policy is to set the standards for internal evaluation of FCS procedures and controls.

16.2 Policy

16.2.1 Security Assessments

At least every other year, the FCS Technology Services Department will conduct a security assessment or penetration test to verify the efficacy security controls in place. The test should include an assessment of the FCS network and information systems. All assets and applications classified in the BCP as CRITICAL will be included in some form of security assessment. In cases where a third party manages an asset, the third-party will be required, unless given a variance by FCS, to demonstrate proof that a security assessment or penetration test was conducted. Applications that process data classified at or above **CONFIDENTIAL** must undergo application security assessments as well as infrastructure. All security controls should be tested at least annually to ensure they are operating properly. An adversarial exercise should be conducted at least every other year to test detection, incident response, and recovery capabilities.

16.2.2 Evidence

All Asset Managers responsible for FCS assets or data must maintain evidence that they meet the requirements of the NIST CSF. For assets and applications that are managed by a third-party, the applicable asset manager must maintain evidence that the third-party conducts and remediates annual security assessments. Annually, each of the requirements of the NIST CSF will be assessed for continued compliance.

16.2.3 Improvement

All assessments, tests, Incidents, and Breaches will be used to improve the detection, alerting, and response functions of FCS. The NOC will be responsible for coming up with the plan to alter the processes of FCS.

16.2.4 Policy and Procedures Review

Annually, the Director of Technology Services or NOC will review all policies, procedures, and plans for accuracy and needed updates. The personnel responsible for the review and update must log the changes in the Version and Revision section of the document including a summary of the changes made.

17.0 OPERATIONAL IMPACT

17.1 Purpose

The purpose of this policy is to outline the operational financial impacts of following the tenets of this document.

17.2 Policy

17.2.1 Financial Impacts

The workflows mandated by this policy have a direct financial impact to short and long-term financial obligations of FCS. As such, bond-issuing companies, cybersecurity insurers, and other financial third parties should be made aware of the District's adherence to the policies outlined in this document.

Completion Timeline

Weekly

Patching (11.0) - Before deployment, operating systems, database management systems, firewalls, and applications must be updated to the most recent stable release level. Vulnerability scans of all FCS information systems classified as CRITICAL will be scanned with a vulnerability scanner at least weekly.

Monthly

Patching (11.0) - Before deployment, operating systems, database management systems, firewalls, and applications must be updated to the most recent stable release level. For systems actively in production, patches with a risk level of: CRITICAL must be applied within 30 days

3 Months

Patching (11.0) - Before deployment, operating systems, database management systems, firewalls, and applications must be updated to the most recent stable release level. For systems actively in production, patches with a risk level of: HIGH must be applied within 90 days

Quarterly

Risk Management (8.0) - All Asset Managers will maintain a Risk Assessment that includes all assets they are responsible for. Asset Managers may use any platform that meets these requirements: The platform is updated at least quarterly.

Access Control (9.0) - Any elevated privileges to any system or information asset must be carefully controlled by the information owner or custodian. All elevated privileges must be reviewed at least quarterly for necessity.

Patching (11.0) - Before deployment, operating systems, database management systems, firewalls, and applications must be updated to the most recent stable release level. For systems actively in production, patches with a risk level of:

- CRITICAL must be applied within 30 days
- HIGH must be applied within 90 days
- MEDIUM (MODERATE) or lower will be evaluated for effect before

Vulnerability scans of all FCS information systems classified as CRITICAL will be scanned with a vulnerability scanner at least weekly. All other FCS information systems will be scanned at least quarterly.

Annually/Yearly

Student Information Office (2.0) - Establish, test, and maintain Disaster Recovery Plan and Process for IC assets on an annual schedule.

Transportation (2.0) - Establish, test, and maintain Disaster Recovery Plan and Process for TRANS assets on an annual schedule.

Finance (2.0) - Establish, test, and maintain Disaster Recovery Plan and Process for FIN assets on an annual schedule.

Facilities (2.0) - Establish, test, and maintain Disaster Recovery Plan and Process for FAC assets on an annual schedule.

School Safety (2.0) - Establish, test, and maintain Disaster Recovery Plan and Process for SAF assets on an annual schedule.

District Administration (DADM) (2.0) - Reviewing and approving risk profile at least annually.

Software Asset Management (7.0) - All software on all systems will be inventoried at least annually. All critical systems will be reviewed at least annually for removal of unnecessary software.

Network Mapping (7.0) - The FCS Networking team will maintain an accurate map of the network. Network mapping will include Layers 1-4 of the Open Systems Interconnection (OSI) model. Network maps can be maintained in software programs or via manual methods. The network maps must be reviewed and updated at least annually.

Risk Management (8.0)- Risk is the nature of adverse events that can impact FCS ability to accomplish its' mission. The FCS BOE has dictated that critical risks are unacceptable to the organization. The BOE has charged asset managers with assessing, planning, reducing, reporting, and eliminating risk. Asset managers should maintain a risk management program for the assets in their charge and be able to brief the BOE on their risk profile at least annually.

Access Control (9.0) - Where possible, logical and physical access should be based on a role or job function. Users that are granted access should be assigned to roles based on position and need. All roles should be audited annually for their permissions. All members of all roles should be audited at least annually for required access. Users, devices, and processes should have unique identifiers to prevent non-repudiation. The continuation to generic accounts will be decided by the Technology Services Department on an annual basis.

Privileges Access (9.0) - Any elevated privileges to any system or information asset must be carefully controlled by the information owner or custodian. All elevated privileges must be reviewed at least quarterly for necessity. All elevated user passwords should be changed at least annually.

Information Security Training (10.0) - All users should attend some form of information security training at least annually. Users that are granted an account in AD are all required to have annual information security training.

The CTIO will be responsible for assessing the information security awareness and training program and assessing its effectiveness. The program content should be updated at least annually.

System Protections (11.0) - System configuration standards must be reviewed at least annually and updated to reflect current industry best practices and newly discovered vulnerabilities. A vulnerability scanning and management program will be managed by the Technology Services Department.

All system protections must be evaluated by the Asset Manager at least annually for effectiveness and applicability. System protections should be tested by internal or external parties to evaluate the technical capabilities. Effectiveness of critical controls should be shared in a report at least annually.

Backups (11.0) - All systems and applications that are required to accomplish the mission of FCS must be backed up at regular intervals. The interval of backups must be set for each asset based on the risk assessment and criticality of the CIA. Backup recovery should be tested at least annually to ensure recovery capabilities.

Network Protections (14.0) - The Network diagram must be reviewed and updated at least every year, or immediately after any major configuration change.

Internal Evaluations (16.0) - All security controls should be tested at least annually to ensure they are operating properly. Annually, the Director of Technology Services or NOC will review all policies, procedures, and plans for accuracy and needed updates.

Every Other Year

Internal Evaluations (16.0) - At least every other year, the FCS Technology Services Department will conduct a security assessment or penetration test to verify the efficacy security controls in place. The test should include an assessment of the FCS network and information systems. All assets and applications classified in the BCP as CRITICAL will be included in some form of security assessment. In cases where a third party manages an asset, the third-party will be required, unless given a variance by FCS, to demonstrate proof that a security assessment or penetration test was conducted. Applications that process data classified at or above **CONFIDENTIAL** must undergo application security assessments as well as infrastructure. All security controls should be tested at least annually to ensure they are operating properly. An adversarial exercise should be conducted at least every other year to test detection, incident response, and recovery capabilities.

Every 3 Years

Asset Management (7.0) - All software on all systems will be inventoried at least annually. Software installed on systems will only remain on systems if the software is required for the proper operation of the system. Software can be inventoried via software management platform or manual documentation. All critical systems will be reviewed at least annually for removal of unnecessary software. All non-critical systems will be reviewed every 3 years for required software.