A. Information Technology Access Control Standards

The purpose of these standards is to ensure that Somerset County Public Schools' information, information systems, computing platforms and networks are accessed by the appropriate persons for authorized use only.

1. Authentication

1.1. All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as functional ids. Functional ids are user accounts associated with a group, role or task(s) that may be used by multiple individuals. They must be approved by the Director of Planning and Technology.

1.2. All systems will have an authentication process for verifying the identity of users prior to initiating sessions or transactions

2. Password Construction Rules and Change Requirements

Passwords must meet the following usage, construction and change requirements:

2.1. Passwords must meet the following requirements

- The password must not be the same as the user id
- Passwords must never be displayed on the screen
- Initial passwords issued to users must force the user to change the password upon initial logon
- Passwords must be a minimum of eight (8) characters and consist of three of the following: Uppercase alphabetic characters, lower case alphabetic characters, numeric characters and special characters
- Passwords must not contain leading or trailing blanks
- Password reuse must be prohibited by not allowing the last 5 passwords to be reused with a minimum password age of at least 2 days
- Automated controls must ensure that passwords are changed at least every sixty (60) days
- Passwords older than its expiration date must be changed before any other system activity is performed
- User ids associated with a password must be disabled after not more than four (4) consecutive failed login attempts while allowing a minimum of a ten (10) minute automatic reset of the account

3. Authorization

The following controls will be implemented:

3.1. A documented process which specifically grants access to information ensuring that access is strictly controlled and will be reviewed annually
3.2. An automated process to ensure that individual user sessions either time out or initiate a password protected screen saver after a period of 30 minutes of inactivity
3.3. A documented process to ensure that access rights, physical access and logical access are immediately disabled upon a change in employment status and that it's done within 24 hours of the change
3.4. A documented process to establish, manage and document user id administration

4. Audit Trail

All systems should have the ability to log and report specific security incidents and all attempted violations of system security.

4.1. The following minimum set of events/actions will be logged for domain controllers:
- Success and failure of account logon events
- Success and failure of account management
- Success and failure of logon events
- Failure of object access
- Success and failure of policy changes
- Success and failure of privilege use
- Success and failure of system events
- The audit trails must include at least the following information:
    - Date and time of event
    - User id of person performing the action
    - Type of event
    - Asset or resource name and type of access
    - Success or failure of event
    - Source (terminal, port, location, etc.) where technically feasible

4.2. Auditing for proxy/firewall traffic must include the following information:
- Date and time of event
- Username where applicable
- Protocol Used
- Source IP Address
- Source Port
- Destination IP Address or URL
- Destination Port

B. Information Technology Network Security Standards

The purpose of these standards is to ensure that Somerset County Public Schools' information networks are protected from unauthorized access at all entry points.

1. Dial-In Access

The following services are prohibited except where they are specifically approved by the Director of Planning and Technology. Any system with a modem connected to the public phone network cannot be connected to the Somerset County Public Schools data network. Use of any of the below must be documented in the External Connections Review.

- Dial-in desktop modems
- Use of any type of "remote control" product (e.g., PCAnywhere, GoToMyPC);
- Use of any network-monitoring tool

2. Banner Text

The following banner text must be displayed at all system entry points and at all access points to servers, subsystems, etc. where initial user logon occurs. An automatic pause, slow roll rate, or user acknowledgement is required to ensure that the banner can be read.

"Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of Somerset County Public Schools and may be used by Somerset County Public Schools for any purpose. Logging on with someone else's account is a violation of Somerset County Public Schools Policy 500-14."

The banner is:

- Required for all servers, workstations, routers and networked systems
- Must be used in addition to, and is not a substitute for, any default banners or copyright/proprietary notices
- The first banner that is displayed, except for citizen interfaces where use will negatively impact the citizen

3. Firewall & Network Devices

3.1.1. Somerset County Public Schools networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. The Somerset County Public Schools firewall will be configured to:

- block all services not required
- disable unused ports
- hide and prevent direct access to Somerset County Public Schools trusted network addresses from untrusted networks
- prevent access by unauthorized source IP addresses or subnets

- maintain comprehensive audit trails
- fail in a closed state

3.1.2. All traffic flowing into and out of Somerset County Public Schools' firewalls and proxy servers must be logged. These logs will be archived to CD and kept in the office of the Director of Planning and Technology.

3.1.3. All network devices (e.g. servers, routers) shall have all non-needed services disabled and the security for those devices hardened.

3.1.4. Publicly managed email and chat services will be prohibited inside the Somerset County Public Schools network unless approved by the Director of Planning and Technology.

3.1.5. All devices shall have updates and patches installed on a timely basis to correct significant security flaws.

3.1.6. Default or initial passwords shall be changed upon installation of all firewall and network equipment.

4. Wireless Security Standards

4.1. General Controls

4.1.1. The Somerset County Public Schools wireless networks may only be accessed by SCPS owned equipment

4.1.2. The Somerset County Public Schools wireless networks may only be accessed by SCPS staff, students and accounts approved by the Network Administrator or Director of Planning and Technology

4.1.3. Installation of access points and other wireless equipment will be restricted to the Network Administrator and contractors approved by the Director of Planning and Technology

4.1.4. A current, documented diagram of the topology of the wireless networks will be kept with the network documentation

4.1.5. All wireless devices will be labeled and inventoried where physically possible

4.1.6. Access points will not be installed where they can be physically reached by students

4.1.7. Access points should not be installed where they are easily physically reached

4.1.8. Access Point Configuration:

4.1.9. All wireless access points must be managed

4.1.10. All default passwords must be changed to comply with Somerset County Public Schools password policies before production implementation

4.1.11. The Secure Set Identifier (SSID) must be changed from the factory default before production implementation

4.2. Authentication and Encryption Standards

4.2.1. The WLAN must verify the identity of the wireless device using 802.1x with authentication to a RADIUS (Remote Authentication Dial In User Service) server

4.2.2. Wireless clients must have a certificate provided by the Somerset County Public Schools Certificate Authority before being allowed physical access to the WLAN

4.2.3. The strongest 128 bit TKIP (Temporal Key Integrity Protocol) encryption must be used

4.2.4. Authentication must use PEAP (Protected Extensible Authentication Protocol) with MSCHAP v2 (Microsoft's Challenge Handshake Authentication Protocol)

C. Information Technology Incident Response Process

The purpose of this process is to ensure that information technology related security incidents are handled properly, necessary steps are documented and that escalation and notification procedures are outlined.

1. Opening an Incident

- Only the Director of Planning and Technology and the Network Administrator can open an incident report.
- Requests for information that would require the opening of an incident report must be made to the Director of Planning and Technology or the Network Administrator. Based on the incident details, they will decide the appropriate parties to report the incident to.
- Requests for Internet audits for students and staff must be made by the building Principal to the Director of Planning and Technology.

2. Incident Reports

- Security Incidents details will be recorded in a SCPS Incident Response Form.
- Incident Reports will be saved in a single location with access being restricted to the Director of Planning and Technology and the Network Administrator.
- The Director of Planning and Technology will be responsible for reporting incidents or sharing reports with the Superintendent, Principal or Law Enforcement.
- The Network Administrator will be responsible for reporting incidents to the Maryland Computer Incident Response Capability.

3. Incident Reporting

- The Director of Planning and Technology and the Network Administrator will decide the appropriate parties to report the incident to based on the incident details.

D. PC and Laptop Security Standards

The purpose of these standards is to ensure that all workstations, desktop computers, laptops and PDAs are secured against unauthorized access or use.

4. General Controls

1.1. Virus Protection will be installed on all systems and kept up to date

1.2. Local Administrator passwords will follow the Somerset County Public Schools' password requirements, kept from end users and documented with other system passwords

1.3. Inventory of all IT equipment will be kept
1.4. All devices shall have updates and patches installed on a timely basis to correct significant security flaws.

2. Software Licenses and Use

Unless specifically approved by the Director of Planning and Technology, personal or corporate IT equipment shall not have Somerset County Public Schools licensed software installed. Only Somerset County Public Schools owned and authorized software is to be used on standalone, networked computer workstations. Only software that has been legally purchased or legally acquired is to be used on Somerset County Public Schools laptops.

3. Personally Owned Data Processing Equipment

Personal or contractor owned data processing and data storage equipment are prohibited from accessing the Somerset County Public Schools systems unless approved by the Somerset County Public Schools Network Administrator or the Director of Planning and Technology. Approvals will be documented in the External Connections Review.

E. Information Technology Disaster Recovery Plan

The purpose of this document is to provide an outline of procedures aimed at reducing the impact of disaster events on critical information technology in the Somerset County Public School District. It will also provide references to materials for emergency support personnel to bring critical systems back online in a disaster situation.

The scope will be limited to emergencies which involve site damage which in turn would cause sustained downtime for critical systems. It will cover who to contact in an emergency and who to contact if the primary contact is unavailable.

The Disaster Recovery Plan contains non public information. It is contained in the Network Documentation.

F. Security Awareness Training and Education

The purpose of the Security Awareness Training and Education plan is to ensure that all employees and students are aware of this Security Policy, its accompanying guidelines, the Somerset County Public School Acceptable Use Policy (AUP) and their responsibilities associated with each document.

1. Initial Training

All employees with access to the SCPS Information System will receive Awareness training on the IT Security Policy, the associated guidelines and the Acceptable Use Policy through

required staff meetings to be held in the fall. Topics covered are listed in section 3 below. All employees will sign off that they have received the initial training. The documentation will be kept on file by the Director of Planning and Technology.

2. Annual Awareness Training

New Employees: All new employees with access to the SCPS Information System will receive Awareness training on the IT Security Policy, the associated guidelines and the Acceptable Use Policy through required staff meetings to be held in the fall. Topics covered are listed in section 3 below. All employees will sign off that they have received the initial training. The documentation will be kept on file by the Director of Planning and Technology.

All Employees: All employees with access to SCPS Information System will receive the following Awareness Training at the beginning of each school year.

- Information will be provided on any revisions made to the IT Security Policy or the associated guidelines over the past 12 months.
- A copy of the SCPS Acceptable Use Policy will be presented and each staff member will be required to sign the sign off sheet.

3. Awareness Training Content

A. IT Security Policy and Guidelines
   a. Password Construction and Change Requirements
   b. Review of SCPS Banner Text message
   c. PC, Laptop and Software Security Standards
   d. Security Roles and Responsibilities

B. Acceptable Use Policy
   a. A Review of the entire policy

G. Security Roles and Responsibilities

Every member of Somerset County Public Schools is responsible for the protection of the electronic data, applications, computer systems, networks and accounts under their control. Users are expected to exercise the level of care appropriate to the sensitivity of the data stored on the SCPS systems and networks.

1. Roles and Responsibilities

All members of the SCPS community play a role in the protection of the district's data and Information Technology resources. In particular:

1.1. The Director of Planning and Technology is responsible for the development and maintenance of information security standards.

1.2. The Network Administrator is responsible for the development and maintenance of information security standards. He or she is also responsible for implementing measures to minimize the probability of a security incident involving systems under his or her control and ensuring adherence to the information security standards. He or she is responsible for investigating incidents and reporting them to the Director of Planning and Technology.

1.3. The Student Information Specialist is responsible for implementing measures to minimize the probability of a security incident involving the PowerSchool systems.

1.4. The Computer Technicians are responsible for implementing measures to minimize the probability of a security incident involving systems and software under their control. Such measures include the installation of virus protection, disabling unnecessary services, keeping accurate inventories and adherence to SCPS security standards. They area also responsible for reporting incidents to the Network Administrator.

1.5. The Principals are responsible for reporting Information Technology security incidents involving staff and students to the Director of Planning and Technology. They are also responsible for helping to minimize security incidents involving students through discipline and restrictions on physical access to computer equipment.

1.6. The Teachers are responsible for minimizing security incidents involving students by constantly monitoring students' activities while the students are using Information Technology equipment. They are also responsible for reporting incidents to the Principal.

1.7. The Individual Users of the SCPS network are responsible for protecting their workstations, laptops, accounts and passwords from unauthorized use and shall comply with the SCPS Acceptable Use Policy.

H. External Connections Review

The purpose of the External Connection Review is to document external connection points to information technology assets in Somerset County Public Schools. Documentation will include an annual review documenting approval from the Director of Planning and Technology or Network Administrator.

The External Connection Review contains non public information. It is contained in the Network Documentation.

I. Information Technology Risk Management Guidelines

This guide provides a framework for Somerset County Public Schools Information Technology risk management program, containing the practical guidance necessary for assessing and mitigating risks identified within IT systems. These guidelines provide information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information. The ultimate goal is for Somerset County Public Schools to better manage IT-related mission risks.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The risk management process includes identification and evaluation of risks and risk impacts. Risk mitigation involves recommendations of risk-reducing measures, risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures. Evaluation and assessment involves the continual evaluation process and keys for implementing a successful risk management program.

1. Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

1.1. Identification

Describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment.

1.2. System Characterization

Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users.

1.3. Threat Statement

Compile and list the potential threat-sources and associated threat actions applicable to the system assessed. List the Security Area and Security Criteria. Those categories are as follows:

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

1.4. Risk Assessment Results

Add the following elements to the Threat Statement table for each vulnerability.

- Likelihood Level (High, Medium, or Low likelihood)
- Magnitude of Impact (High, Medium, or Low impact)
- Risk Rating based on the risk-level matrix (High, Medium, or Low risk level)

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability

	from being exercised.

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability may result in the highly costly loss of major tangible assets or resources; may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	Exercise of the vulnerability may result in the costly loss of tangible assets or resources; may violate, harm, or impede an organization's mission, reputation, or interest
Low	Exercise of the vulnerability may result in the loss of some tangible assets or resources or may noticeably affect an organization's mission, reputation, or interest.

Risk Level Matrix			
	Impact		
Threat Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	Risk Rating Low 10 X 1.0 = 10	Risk Rating Medium 50 X 1.0 = 50	Risk Rating High 100 X 1.0 = 100
Medium (0.5)	Risk Rating Low 10 X 0.5 = 5	Risk Rating Medium 50 X 0.5 = 25	Risk Rating Medium 100 X 0.5 = 50
Low (0.1)	Risk Rating Low 10 X 0.1 = 1	Risk Rating Low 50 X 0.1 = 5	Risk Rating Low 100 X 0.1 = 10

1.5. Recommendations or Comments

Summarize the recommendations and add any comments into the Threat Statement to facilitate the implementation of recommended controls during the risk mitigation process.

Threat Statement

Identification	
System Characterization	

Vulnerability	Threat-Source	Security Area	Security Criteria	Likelihood Level	Magnitude Of Impact	Risk Rating	Comments/ Recommendations

2. Risk Mitigation Guidelines

Risk mitigation, the second process of risk management, involves recommending appropriate risk-reducing controls, prioritizing risks, and implementing the controls.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

2.1. Prioritize Actions

List the risk and risk level in the Risk Mitigation Plan. Based on the risk levels presented in the risk assessment report, assign each vulnerability a priority. In allocating resources, top priority should be given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect an organization's interest and mission.

2.2. Recommended Controls

In implementing recommended controls to mitigate risk, considerations include technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for the IT systems and for Somerset County Public Schools as an organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to Somerset County Public Schools' mission.

Determine controls that could mitigate or eliminate the identified risks, as appropriate to Somerset County Public Schools operations. List them in the Risk Mitigation Plan. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

- Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

- Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising vulnerability (e.g., use of supporting, preventive, detective controls)
- Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance

The goals and mission of Somerset County Public Schools should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the vulnerabilities that have the potential to cause significant mission impact or harm.

2.3. Selected Planned Controls

The controls recommended in the risk assessment process may not be the most appropriate and feasible options for Somerset County Public Schools or the specific IT system. During this step, the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option for minimizing risk.

Management determines the most cost-effective control(s) for reducing risk to the organization's mission. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the IT system and the organization.

2.4. List Required Resources

List the required resources for implementing the selected planned controls.

2.5. Assign Responsibility

Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

2.6. Timeline

List the start date and target completion date for implementation.

2.7. List Review/Documentation Requirements or Comments
Add review or documentation requirements and add the item to the Somerset County Public Schools Risk Evaluation and Assessment so that continuous review and evaluation takes place. Add any additional comments that are necessary.

Risk Mitigation Plan

Vulnerability	Risk Level	Recommended Controls	Action Priority	Selected Planned Controls	Required Resources	Responsible Team/Persons	Maintenance Requirements/ Comments

3. Risk Evaluation and Assessment

The third part of the Somerset County Public Schools risk management plan involves the monitoring of progress of the risk management controls. The different risk levels should be periodically reviewed on a progressive time scale. Higher risks should be monitored more often than lower risks. Somerset County Public Schools information technology risks will be monitored as follows:

Risk	Timeline
High	1 Day
Medium	6 Months
Low	1 Year

High Risk Evaluation & Assessment				
Vulnerability	**Date Reviewed**	**Auditor**	**Selected Planned Controls**	**Progress**

Medium Risk Evaluation & Assessment				
Vulnerability	Date Reviewed	Auditor	Selected Planned Controls	Progress

Low Risk Evaluation & Assessment				
Vulnerability	**Date Reviewed**	**Auditor**	**Selected Planned Controls**	**Progress**

J. Standards for Electronic Media Disposal

The purpose of these procedures is to ensure that any Somerset County Public School's sensitive information is removed by an industry approved method from electronic media before it is disposed of or repurposed.

1. Disposal versus Repurposing

When equipment becomes obsolete or damaged, there are two courses of action that can be taken by the technical staff at SCPS.

- Collect the equipment and keep it for sale at a surplus auction or use other means of disposal.
- Reassign the equipment for some other purpose.

Whether the equipment is collected for surplus or repurposed, it is important to take steps to protect any sensitive information that may have been stored on the hard drive or other media.

2. Repurposing of Electronic Storage Media

All electronic storage media, specifically including hard drives installed in computers, must be formatted or erased prior to being transferred from its current owner to a new owner for a different use. Hard drives must be formatted or have its partition removed prior to transfer. Other media should undergo a format or media erase. Insofar as special recovery tools would have to be used by an individual to access the data erased by this method, any attempt by an individual to access unauthorized data would be viewed as a violation of the Somerset County Schools IT Security Policy.

3. Disposal of Electronic Media

Overwriting is an approved method for sanitization of electronic storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable.

4. Disposal of Damaged or Inoperable Electronic Media

Some media cannot be sanitized. Final disposal of these electronic storage media shall be to destroy the media physically so that it is not usable by any device normally used to read such electronic information such as a computer, tape reader, video or audio player.

5. "Accidental Disposal" – Loss or Theft

If a computer/laptop – or a device such as a CD or thumb drive – is lost or stolen, any information on the device can fall into the hands of someone who could misuse the information. Confidential or Personally Identifiable Information should therefore never be stored on any local hard drive or portable devices.