School Administrative Unit 39

Data Security and Data Privacy Guidelines

May, 2019

Reviewed by SAU Board May 2021

Contents

Introduction

School Administrative Unit 39 ("SAU 39" and "the SAU" will be used throughout this document to represent the four units of School Administrative Unit 39 – the Amherst School District, the Mont Vernon School District, the Souhegan Cooperative School District and School Administrative Unit 39) is committed to protecting our students' and staffs' privacy through maintaining strong privacy and security protections. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff.

The SAU 39 Data Security and Privacy Guidelines includes information regarding the data governance team, data and information governance, applicable School Board policies, SAU procedures, as well as applicable appendices and referenced supplemental resources.

This document outlines how operational and instructional activity shall be carried out to ensure the SAU 39 data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it. Definitions of terminology can be found in Appendix A: Definitions.

The SAU 39 Data Security and Privacy Guidelines shall be a living document. To make the document flexible, details are outlined in the appendices and referenced supplemental resources. This document and any future modifications to this document will be posted on the SAU 39 website.

Data Governance Team

The SAU 39 Data Governance team consists of the following positions: Superintendent, Assistant Superintendent, Business Administrator, Director of Buildings and Grounds, Director of Human Resources, Director of Student Services and the Director of Technology. Members of the Data Governance Team will act as data stewards for all data under their direction. The Director of Technology will act as the Information Security Officer (ISO), with assistance from members of the full Technology team. The Lead Network Administrator is the SAU's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the SAU administrative team will serve in an advisory capacity as needed.

Purpose

The School Boards recognize the value and importance of a wide range of technologies for a well-rounded education, enhancing the educational opportunities and achievement of students. SAU 39 provides its faculty, staff, and administrative staff access to technology devices, software systems, network and Internet services to support research and education. All components of technology must be used in ways that are legal, respectful of the rights of others, and protective of juveniles and that promote the educational objectives of SAU 39.

To that end, the SAU must collect, create and store confidential information. Accurately maintaining and protecting this data is important for efficient SAU operations, compliance with laws mandating confidentiality, and maintaining the trust of all SAU stakeholders. All persons who have access to SAU data are required to follow state and federal law, SAU policies and procedures, and other rules created to protect the information.

It is the policy of the SAU 39 that data or information in all its forms, written, electronic, or printed, is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. All staff and authorized SAU contractors or agents using confidential information will strictly observe protections put into place by the SAU.

Scope

The data security policy, standards, processes, and procedures apply to all students and staff of SAU 39, contractual third parties and agents of the SAU, and volunteers who have access to SAU data systems or data. This policy applies to all forms of SAU 39 data and information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or any current and future technologies.
- Hard copy data printed or written.
- Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media.
- Data stored and/or processed by any electronic device, including servers, computers, tablets, mobile devices.
- Data stored on any type of internal, external, or removable media or cloud-based services.
- The terms data and information are used separately, together, and interchangeably throughout the document, the intent is the same.
- Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems, assets or resources.
- All involved systems and information are considered assets of SAU 39 and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

SAU 39 will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). SAU 39 will comply with or exceed the https://www.education.nh.gov/data/documents/minimum-standards-privacy.pdf approved in 2019 and standards applicable to data governance are addressed throughout this Data Security and Privacy Guidelines. SAU 39 will be in compliance with all other applicable regulatory acts including but not limited to the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)
- Individuals with Disabilities in Education Act and Section 504 of the Rehabilitation Act (IDEA)
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy
    - NH RSA 189:65 Definitions
    - NH RSA 189:66 Data Inventory and Policies Publication
    - NH RSA 189:67 Limits on Disclosure of Information
    - NH 189:68 Student Privacy
    - NH RSA 189:68-a - Student Online Personal Information
- New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data
- New Hampshire State RSA - Right to Privacy:

    NH RSA 359-C:19 - Notice of Security Breach Definitions

    NH RSA 359-C:20 - Notice of Security Breach Required

    NH RSA 359-C:21 - Notice of Security Breach Violation

Data User Compliance

The Data Security and Data Privacy Guidelines apply to all users of SAU 39 information including: staff, students, volunteers, and authorized SAU contractors or agents. All data users are to maintain compliance

with School Board Policies and SAU administrative procedures, EHAB (Data Governance and Security), EGA (School District Internet Access for Students), EHAA (Computer Security, Email and the Internet) and all policies, procedures, and resources as outlined within this document and School Board Policy.

A consistently high level of personal responsibility is expected of all users granted access to the SAU's technology resources. Any violation of SAU policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the SAU technology resources.

Unless permission has been granted by the ISO or designee, no staff, vendor or other person may remove confidential or critical data from the SAU's premises or the SAU's network, remove a device containing confidential or critical data from the SAU's premises, or modify or copy confidential or critical data for use outside the SAU. If permission is given, the data may be accessed only on a SAU-provided device with appropriate security controls or through a secure virtual private network (VPN). When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied or otherwise used in a manner that would compromise the security and confidentiality of the information.

Staff who fail to follow the law or SAU policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the SAU. The SAU will end business relationships with any contractor who fails to follow the law, SAU policies or procedures, or the confidentiality provisions of any contract. In addition, the SAU reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of a staff member's teaching certificate.

The SAU may suspend all access to data or use of SAU technology resources pending an investigation. Violations may result in temporary, long-term or permanent suspension of user privileges. The SAU will cooperate with law enforcement in investigating any unlawful actions. The Superintendent or designee has the authority to sign any criminal complaint on behalf of the SAU.

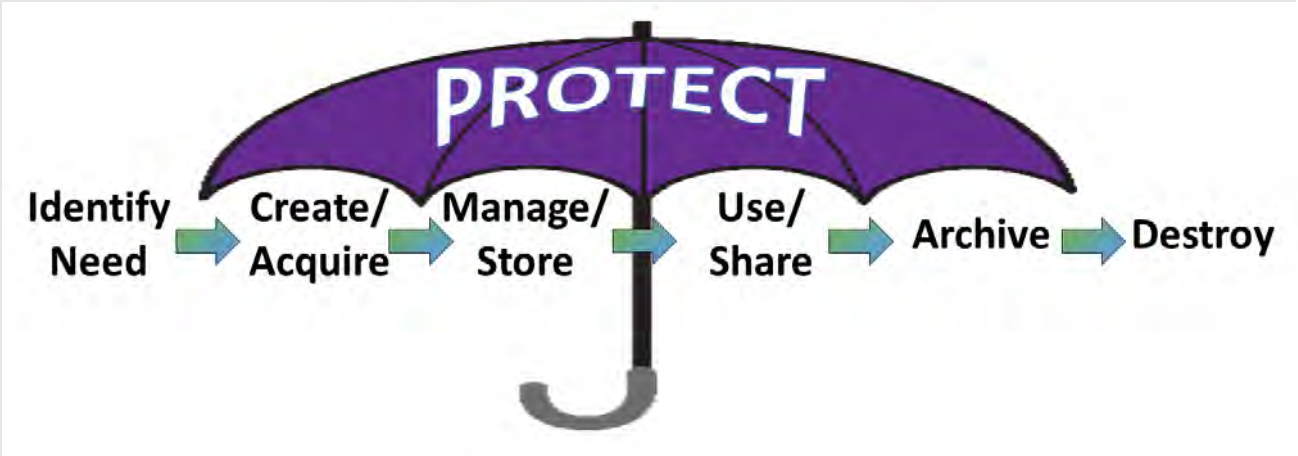
Any attempted violation of SAU policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized technology staff for the purpose of support)
- Applying for a user ID under false pretenses or using another person's ID or password.
- Unauthorized use of an authorized password to invade student or staff privacy by examining records or information for which there has been no request for review.
  The unauthorized copying of system files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for SAU technological systems.
- The intentional unauthorized altering, destruction, or disposal of SAU information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to the following: laptops, internal or external storage, computers, servers, backups or other media, that may contain PII or confidential information.
  The introduction of computer viruses, hacking tools or other disruptive or destructive programs.

Data Lifecycle

Data Governance is necessary at each phase in the data lifecycle. This lifecycle starts at evaluating the need for data collection and ends when the data is destroyed. It is important that appropriate safeguards, policies, procedures and practices are in place for each phase of the data lifecycle.



Identifying Need & Assessing Systems for SAU Requirements

To accomplish the SAU 39 mission and to comply with the law, the SAU may need to maintain confidential information, including information regarding students, parents/guardians, staff, applicants for employment and others. The SAU will collect, create or store confidential information only when the Superintendent or designee determines it is necessary.

New Systems

SAU 39 staff members are encouraged to research and utilize online services or applications to engage students and further the SAU's educational mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or staff, the ISO or designee(s) must approve the use of the service or application and verify that it meets the requirements of the law and School Board policies and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

SAU 39 has an established process for vetting new digital resources. Staff are required to complete steps outlined at the Technology section of the SAU 39 website, to ensure that all new resources meet mission and/or instructional need as well as security requirements.

Memorandums of understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on the technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
  Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
  - SAU 39 continues to own the data shared, and all data must be available to the SAU upon request.
  - SAU 39 vendor's access to and use of SAU data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the SAU. If metadata is collected, it will be protected to the same extent as the SAU's confidential or critical information.
  - SAU data will be maintained in a secure manner by applying appropriate technical, physical

and administrative safeguards to protect the data.
- The provider will comply with SAU guidelines for data transfer or destruction when contractual agreement is terminated.
- No API will be implemented without full consent of the SAU.
- All data will be treated in accordance to federal, state and local regulations
- The provider assumes liability and provides appropriate notification in the event of a data breach.

Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for SAU vetted and approved applications and tools.

A current list of all vetted and approved software systems, tools and applications is available through the links on the Technology section of the SAU 39 Technology website.

Review of Existing Systems

SAU 39 will ensure that data collection is aligned with School Board Policy EHAB. Data systems shall be regularly reviewed to ensure that only necessary data is being transmitted and collected. Individual student level data is submitted to different approved service providers in order to ensure business operations and instructional services. At times, these imports include PII for staff and students. The SAU must ensure that each piece of PII is necessary for operations or instruction and that the providers are abiding by their terms of service.

The SAU will audit data imports annually. These audits should include:

- Review of provider's terms of service to ensure they meet the SAU's data security requirements.
- Verification that software imports are accurate and pulling the correct information.
- Verification that, when applicable, the staff, students and classes included in the imports are still necessary for instructional purposes (only those that need data collected are included in import).
- Determine if the fields included in the imports are still necessary for the intended purpose.

Acquisition and Creation

After reviewing the requirements for adoption of any new systems, staff shall complete an online request form for any new digital app/tool that either has an associated cost or collects staff or student data (see Appendix C: Digital Resource Acquisition and Use). All staff must adhere to the following guidelines regarding a new digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets SAU mission objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted for security/privacy by the Director of Technology, or designee, prior to adoption.

Systems Security

SAU 39 will provide access to confidential information to appropriately trained SAU staff and volunteers only when the SAU determines that such access is necessary for the performance of their duties. The SAU will disclose confidential information only to authorized SAU contractors or agents who need access to the information to provide services to the SAU and who agree not to disclose the information to any other party except as allowed by law and authorized by the SAU (School Board Policy EHAB). Therefore, systems access will only be given on an as-needed basis as determined by the data manager and ISO. Further information regarding Electronic Access Security Controls is contained in the Security/Protection section of this document.

Data Management

The effective education of students and management of SAU personnel often require the SAU to collect information, some of which is considered confidential by law and SAU policy. In addition, the SAU maintain information that is critical to SAU operations and that must be accurately and securely maintained to avoid disruption to SAU operations.

Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. All SAU administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage. Data managers will:

- Ensure that system account creation procedures and data access guidelines appropriately match staff member job function with the data on instructional and operational systems.
- Review all staff with custom data access beyond their typical group's access.
- Review SAU processes to ensure that data will be tracked accurately.
- Review contracts with instructional and operational software providers to ensure that they are current and meet the SAU 39 data security guidelines.
- Ensure that staff are trained in the SAU's proper procedures and practices in order to ensure accuracy and security of data.
- Assist the ISO in enforcing SAU policies and procedures regarding data management.

Data Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is classified according to the most sensitive detail they include. Data recorded in several formats (i.e. source document, electronic record, report) have the same classification regardless of format (see Appendix E: Data Classification Levels).

The ISO or designee will identify all systems containing SAU data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, email systems, instructional software applications and others.

The SAU will create and maintain a data inventory for all information systems containing PII or confidential information. When possible, a data dictionary will be maintained for critical information systems. The data inventory will contain the following elements:

- Data Source
- What data is stored
- Where the data is stored
- Staff or staff categories that have access to the files

- Criticality/Sensitivity Rating

Security/Protection

Risk Management

A thorough risk analysis of all SAU 39 data networks, systems, policies, and procedures shall be conducted on a bi-annual basis by an external third party or as requested by the Superintendent, ISO or designee. An internal audit of SAU network security will be conducted annually by SAU 39 Technology staff. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist (Appendix D). The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Security Logs

The SAU will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data security. These events will include, but are not limited to, access to critical systems and modification of critical data. When applicable, notifications will be established for critical event triggers.

Physical Security Controls

Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Director of Technology, Network Administrator and or Director of Facilities. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see appendix G: Physical Security Controls).

No technological systems shall be disposed of or moved without adhering to the appropriate procedures (see Appendix H: Asset Management).

Inventory Management

The SAU shall maintain a process for inventory control in accordance to federal and state requirements and School Board policy. All SAU 39 technology assets will be maintained in inventory and verified through the regular inventory verification process (see Appendix H: Asset Management).

Virus, Malware, Spyware, Phishing and SPAM Protection

The SAU uses a multi-layered approach to ensure that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. These include, but are not limited to, enterprise virus/malware/ spyware software, group policy, gateways, firewalls, and content filter. Users shall not turn off or disable SAU protection systems or install other systems (see Appendix I: Virus, Malware, Spyware, Phishing and SPAM Protection).

Electronic Access Security Controls

SAU staff will only access personally identifiable and/or confidential information if necessary, to perform their duties. The SAU will only disclose this information to authorized SAU contractors or agents who need access to the information to provide services to the SAU and who agree not to disclose the information to any other party except as allowed by law. All staff are required to read and acknowledge applicable SAU policies annually.

Mechanisms to control access to PII, confidential information, internal information and computing resources

include, but are not limited to, the following methods:

- **Identification/Authentication:** Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, confidential information, and/or internal information. Users will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall not be shared.
- **Authorization:** Access controls are maintained through a partnership between the technology department, human resources (HR) and data managers.

Additionally, only members Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Access security is audited annually or whenever access permission requirements are changed for a particular application/software or when user access to an application/software is no longer necessary.

Staff Users

All new staff accounts are authorized through a Human Resources hiring process (see Appendix J: Account Management). Role-based permissions and security groups are used to establish access to all systems (see Appendix K: Data Access Roles and Permissions). If a staff member requires additional access, a request must be made directly to the ISO with a clear justification for access.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by HR and the ISO. All contractors doing business on SAU premises must also pass a background check unless other security measures are addressed in a vendor contract. Contractor/vendor will be granted access to data as needed and approved by the ISO or designee. Once the approval has been obtained, the technology department will create the account providing or access to the application/information that the contractor/vendor supports.

Password Security

The SAU will enforce secure passwords for all systems within their control (see Appendix L: Password Security). When possible, the SAU will utilize Single Sign On (SSO) or LDAP/Active Directory Integration to maintain optimal account security controls.

Concurrent Sessions

When possible, the SAU will limit the number of concurrent sessions for a user account in a system.

Remote Access

Access into the SAU's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the SAU's network and systems; no other method of remote access shall be granted without explicit authorization from the ISO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protection as information stored and accessed within SAU 39 network.

If a secured connection is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All non-SAU 39 accounts will be reviewed at least annually to determine if remote access is needed.

Securing Data at Rest and Transit

SAU data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. Regular transmission of student data to internal and external services is managed by the technology department using a secure data transfer protocol.

Users must ensure that they are securely storing their data. Guidelines have been established for Cloud Storage and File Sharing, External Storage Devices, and File Transmission Practices. (see Appendix F: Securing Data at Rest and Transit). These guidelines are outlined in the following section.

Usage and Dissemination

A consistently high level of personal responsibility is expected of all users granted access to the SAU technology resources. All SAU staff, volunteers, contractors and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using confidential and critical information will strictly observe protections put into place by the SAU including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

All users are responsible for the security and integrity of the data they create, store or access. Users are expected to act as good stewards of data and treat data security and integrity with a high degree of responsibility and priority. Users must follow all guidelines outlined with Board policies, specifically Employee and Student Technology Usage, Data Governance and Security (EHAB), and Student Records.

SAU staff, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise.

Data Storage and Transmission

All staff and students that log into a SAU owned device will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students may not be able to store data on the local device. It is important to note that this data is not a part of the SAU storage plan, and thus may not be backed up by the SAU backup solution. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document folders to SAU file servers or cloud storage. Access to these files is restricted to the folder's owner (staff or student who is assigned) and SAU enterprise administrator accounts. Staff and students using devices which have limited local storage capabilities are to store data within their Office 365 OneDrive account or their G Suite for Education account.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with an Office 365 OneDrive account and a G Suite for Education account. which provide significant storage. Users are responsible for all digital content on their SAU provided account Drives (see Appendix F: Securing Data at Rest and Transit).

File Transmission Practices

Staff are responsible for securing sensitive data for transmission through email or other channels. Staff should not transmit files that contain PII through email or third-party file transfer services without SAU approval. When possible, staff should de-identify or redact any PII or confidential information prior to transmission. Regular transmission of student data to services such as a single sign on provider is managed by the technology group using a secure data transfer protocol (see Appendix F: Securing Data at Rest and Transit).

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the appropriate level of PCI compliance when handling such

data (see Appendix F: Securing Data at Rest and Transit).

Mass Data Transfers

Downloading, uploading or transferring PII, confidential information, and internal information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be reviewed and approved by the Superintendent or designee. All other mass downloads of information shall be approved by the ISO and include only the minimum amount of information necessary to fulfill the request.

Printing

When possible, staff should de-identify or redact any PII or confidential information prior to printing. PII and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications

Staff shall be aware of their surroundings when discussing PII and confidential information. This includes, but is not limited to, the use of cellular telephones in public areas. Staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or public areas.

Training

The SAU shall create and maintain a data security training program. This program will consist of the following:

- Training for all staff on technology policies and procedures, including confidentiality and data privacy.
- Additional training for new instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for all instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for SAU administration on federal regulations, data privacy and security.
- All training or professional learning that includes the use of data systems shall include data security.

Archival and Destruction

Once data is no longer needed, the ISO or designee will work with the data managers to ensure that it is appropriately destroyed. Special care will be taken to ensure that confidential information is destroyed appropriately and in accordance with law. Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record irretrievable.

SAU 39 Data Destruction Processes

The SAU will regularly review all existing data stored on SAU provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy EHB and EHB-R. SAU data managers will regularly review systems and data to ensure that data that is no longer needed is destroyed. The following exceptions will be made:

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Student Office 365 and G Suite for Education accounts will be maintained for one school year after the student's final date of attendance.

- Staff G Suite for Education and Office 365 accounts will be suspended after the final work day, unless HR or the ISO approves additional access.

Asset Disposal

SAU 39 will maintain a process for physical asset disposal in accordance with School Board Policy. The SAU will ensure that all assets containing PII, confidential, or internal information are disposed of in a manner that ensures that this information is destroyed (see Appendix H: Asset Management).

Critical Incident Response

Controls shall ensure that SAU 39 can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the ISO or designee for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach and natural disaster) that damages/breaches data or systems.

Business Continuity

The SAU administrative procedure EHB-R delineates the timeline for data retention for all SAU data. The SAU will maintain systems that provide near-line and off-site data backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The SAU will test near-line and off-site backups of critical systems quarterly.

Disaster Recovery

The SAU's Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. SAU 39 shall maintain a list of all critical systems and data, including contact information. The Technology Disaster Recovery Plan shall include processes that enable the SAU to continue operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure (see Appendix M: Disaster Recovery Plan).

Data Breach Response

New Hampshire's data breach law (RSA 359-c:19, 20, 21) is triggered when a SAU computer system is breached and personal information is acquired without authorization in a way that compromises the security or confidentiality of the information. The law requires a school district experiencing a breach to conduct a good faith and reasonably prompt investigation to determine the likelihood that personal information was, or will be, misused. The Data Breach Response Plan enables the SAU to respond effectively and efficiently to a data breach involving personally identifiable information (PII) as defined by NH Law, confidential or protected information (i.e.FERPA), SAU identifiable information and other significant cybersecurity incident. The Data Breach Response Plan shall include processes to validate and contain the security breach, analyze the breach to determine scope and composition, minimize impact to the users, and provide notification (see Appendix N: Data Breach Response Plan).

Appendix A - Definitions

Confidentiality: Data or information is not made available or disclosed to unauthorized persons.

Confidential Data/Information: Information that the SAU is prohibited by law, policy or contract from disclosing or that the SAU may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information (PII) regarding students and staff.

Critical Data/Information: Information that is determined to be essential to SAU operations and that must be accurately and securely maintained to avoid disruption to SAU operations. Critical data is not necessarily confidential.

Data: Facts or information. Data can be in any form; oral, written, or electronic.

Data Breach, Breach of Security or Breach: A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information.

Data Integrity: Data is current, accurate and has not been altered or destroyed in an unauthorized manner.

Data Management: The development and execution of policies, practices, and procedures in order to manage the accuracy and security of SAU instructional and operational data in an effective manner.

Data Owner: User responsible for the creation of data. The owner may be the primary user of that information or the person responsible for the accurate collection/recording of data. Ownership does not signify proprietary interest, and ownership may be shared. The owner of information has the responsibility for:

- knowing the information for which she/he is responsible.
- determining a data retention period for the information according to Board policy and state statute.
- ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the data used or created.
- reporting promptly to the ISO the loss or misuse of data.
- initiating and/or implementing corrective actions when problems are identified.
- following existing approval processes for the selection, budgeting, purchase, and implementation of any digital resource.

Information Security Officer: The Information Security Officer (ISO) is responsible for working with the Superintendent, Data Governance Team, data managers, data owners, and users to develop and implement prudent security policies, procedures, and controls. The ISO will oversee all security audits and will act as an advisor to:

- data owners for the purpose of identification and classification of technology and data related resources.
- systems development and application owners in the implementation of security controls for information on systems, from the point of system design through testing and production implementation.

Systems: Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device, whether hosted by the SAU or provider.

Security Incident: An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name,

social security number, State Assigned Student Identification, date and place of birth, mother‘s maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

User: The user is any person who has been authorized to read, enter, print or update information. A user of data is expected to:

- access information only in support of their authorized job responsibilities.
- comply with all data security procedures and guidelines.
- keep personal authentication confidential (user IDs, passwords, secure cards, PINs, access codes).
- report promptly to the ISO the loss or misuse of data.
- follow corrective actions when problems are identified.

Appendix B - Laws, Statutory, and Regulatory Security Requirements

CIPA: The Children's Internet Protection Act was enacted by Congress to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.
https://www.hhs.gov/hipaa/index.html

IDEA: The Individuals with Disabilities in Education Act (IDEA) is a law that makes available a free appropriate public education to eligible children with disabilities throughout the nation and ensures special education and related services to those children.
https://sites.ed.gov/idea/

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.
www.pcisecuritystandards.org

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.
https://www2.ed.gov/policy//gen/guid/fpco/ppra/index.html

New Hampshire State RSA 189:65-189:68: Student and Teacher Information Protection and Privacy as defined by the following sections:

- NH RSA 189:65 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-65.htm) Definitions
- NH RSA 189:66 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-66.htm) Data Inventory and Policies Publication
- NH RSA 189:67 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-67.htm) Limits on Disclosure of Information
- NH 189:68 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68.htm) Student Privacy
- NH RSA 189:68-a (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68-a.htm) Student Online Personal Information

New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data

New Hampshire State RSA Chapter 359-C Right to Privacy:

- NH RSA 359-C:19 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-19.htm) Notice of Security Breach - Definitions
- NH RSA 359-C:20 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-20.htm) Notice of Security Breach Required
- NH RSA 359-C:21 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-21.htm) Notice of Security Breach Violation

Appendix C - Digital Resource Acquisition and Use

The purpose of the Digital Resource Acquisition and Use process is to:

- ensure proper management, legality and security of information systems,
- increase data integration capability and efficiency,
- and minimize malicious code that can be inadvertently downloaded.

New Resource Acquisition

Staff are required to complete steps outlined on the SAU 39 Technology website. An online request form is required for any new digital resources that either has an associated cost or collects staff or student data. All staff must adhere to the following guidelines regarding digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets SAU mission objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted for security/privacy by the Director of Technology, or designee, prior to adoption. All new resources shall be properly evaluated against the following criteria, when applicable:
    - Impact on technology environment including storage and bandwidth
    - Hardware requirements, including any additional hardware
    - License requirements/structure, number of licenses needed, and renewal cost
    - Maintenance agreements including cost
    - Resource update and maintenance schedule
    - Funding for the initial purchase and continued licenses and maintenance
    - Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
        - The SAU continues to own the data shared, and all data must be available to the SAU upon request.
        - The vendor's access to and use of SAU data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the SAU. If metadata is collected, it will be protected to the same extent as the SAU's confidential or critical information.
        - SAU 39 data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
        - The provider will comply with SAU guidelines for data transfer or destruction when contractual agreement is terminated.
        - No API will be implemented without full consent of the SAU.
        - All data will be treated in accordance to federal, state and local regulations
        - The provider assumes liability and provides appropriate notification in the event of a data breach.

    Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for SAU vetted and approved applications and tools.

Approved Digital Resources

In order to ensure that all digital resources used meet security guidelines and to prevent software containing malware, viruses, or other security risk, digital resources that have been vetted are categorized as Approved or Denied.

- A list of vetted software will be maintained and can be accessed from the SAU 39 Technology website.
- It is the responsibility of staff to submit a request to the Digital Resource Workflow Process to use a new digital resource if a resource is not listed.

- Digital resources that are denied or have not yet been vetted will not be allowed on SAU owned devices or used as part of SAU business or instructional practices.

Digital Resource Licensing/Use

All computer software licensed or purchased for SAU use is the property of the SAU and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

All staff must adhere to the following guidelines regarding digital resource licensing/use:

- Only approved SAU resources that create, collect or use personally identifiable information (PII) are to be used.
- SAU software licenses will be:
    - accurate, up to date, and adequate
    - in compliance with all copyright laws and regulations
    - in compliance with SAU, state and federal guidelines for data security
- Software installed on SAU 39 systems and other electronic devices will have a current license or will be removed from the system or device.
- Resources with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly vetted and licensed, if necessary, and is applicable to this procedure.
- Under no circumstances can staff act as a parental agent when creating student accounts for online resources; resources requiring this permission must be approved at the SAU 39 administrative level.

Appendix D - Data Security Checklist

A thorough risk analysis of all SAU 39 data networks, systems, policies, and procedures shall be conducted on a bi-annual basis or as requested by the Superintendent, ISO or designee by an independent third party. The risk analysis will include internal and external vulnerability cybersecurity risk assessments and external penetration testing of the SAU network. An internal audit of SAU network security will be conducted annually by SAU 39 Technology staff.

The Data Security Checklists examine the types of threat that may affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which could potentially expose the information resource to threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Data Security Checklist for SAU 39 Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Physical security of system
- Location within network including network systems protection (firewall, content filter) and if system is externally facing or only allows for SAU network access
- Access controls including password security (can SAU password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, SAU managed account, user managed account)
- Server/system security patch frequency
- Ability to access from mobile devices
- Ability to maintain critical system event logs
- Ability to receive notification for critical system events

Data Security Checklist for Provider Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Contract, terms of service and privacy policy are current and meet SAU data security requirements
- Provider has adequate data security measures including data management and incident response
- Ability to ensure proper access controls including password security (i.e. - can SAU password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, SAU managed account, user managed account)
- Server/system security patch frequency
- Ability to access from mobile devices
- Notification practices in the event of a system compromise or security breach

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

- Any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications.

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. Examples of confidential information may include:

- student records
- personnel information
- key financial information
- proprietary information
- system access passwords
- encryption keys.

Unauthorized disclosure of this information to individuals without a business need for access may violate laws and regulations, or may cause significant consequences for SAU 39, its staff, parents, students or other stakeholders. Decisions about the provision of access to this information shall always be cleared through the

data manager and/or ISO.

Internal Information

Internal Information is intended for unrestricted use within the SAU and in some cases within affiliated stakeholders. This type of information is already widely distributed within the SAU, or it could be distributed within the organization without advance permission from the information owner. Examples of Internal Information include internal policies and procedures and handbooks.

Unauthorized disclosure of this information to outsiders may not be appropriate due to copyright, legal or contractual provisions.

Directory Information

Directory Information is information contained in an education record of a student that generally would not be considered harmful or an invasion of privacy if disclosed without the consent of a parent or eligible student. SAU 39 designates the following items as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended

This information may only be disclosed as permitted in School Board Policy.

Public Information

Public Information has been specifically approved for public release by the Superintendent or appropriate SAU administrator. Examples of public information may include patron mailings and materials posted to the SAU's website.

This information may be disclosed outside of the SAU.

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a SAU owned computer system will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. Certain data stored on local devices may NOT be backed up by the SAU's backup solution. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document folders to SAU file servers (OneDrive and/or G Suite Google Drive may be included or substituted). Access to these files is restricted to the folder's owner (staff or student who is assigned) and SAU enterprise administrator accounts. Staff and students may have limited local storage capabilities.

Confidential and critical information will be saved and maintained in a secure manner using encryption or other password-protected security measures. Likewise, when data is transmitted, the SAU will use encryption or password-protected security measures.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with an Office 365 account and a G Suite for Education account that provides storage. Users are responsible for all digital content on their SAU provided accounts. When using cloud storage, staff must adhere to the following guidelines:

- Staff and students may not access cloud storage through third party applications outside of approved internet browsers and applications on Android & iOS. This will ensure that native operating systems do not replace cloud sharing security.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the SAU and meet SAU student data and data security standards.
- When exiting the SAU, students should responsibly copy their content to their own personal storage solution.
- When exiting the SAU, staff should ensure that they are only copying personal content that they created. Staff are prohibited from copying content that contains confidential information, student records or data.
- Data with personally identifiable information of staff or students may be posted to users' SAU provided accounts with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of SAU administration.
- Staff should never post any documents containing classified, confidential, or restricted information to any cloud storage including SAU 39 provided Office 365 and/or Google Drive accounts without SAU approval.
- All users shall immediately report any cloud storage security problems of the SAU's technology resources to a teacher or administrator.
- Attempting to gain or gaining unauthorized access to cloud storage or the files of another is prohibited.
- As with other forms of SAU technology, staff, students, and other users have no expectation of privacy on data stored on this platform.

The term "File Sharing" is used to define all activities that share access to digital information whether in the cloud or on SAU administered mapped drives. When file sharing, staff must adhere to the following guidelines:

- Users must abide by all policies and procedures regarding professional conduct and communication when sharing, reviewing, updating, commenting and re-sharing.
- When sharing content, users must ensure that other users accessing the information in the files have appropriate access to the information based on job function.
- All users shall immediately report any inappropriate sharing of the SAU's technology resources to

an administrator.

External Storage Devices

The term “External Storage Devices” is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) used by staff and students. While the SAU recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their SAU provided Office 365 and G Suite for Education Drive accounts for all storage needs. When using external storage devices, staff and students must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to SAU technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-SAU approved software, or hacking tools to SAU technology resources.
- Users must ensure that the data will remain secure through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device. Users should only keep the information stored on the external device for the duration of the project, and then promptly remove.
- Staff should never transfer any documents containing PII or confidential information to any external storage device.
- Staff should never transfer or create confidential data or student records on personal storage devices.

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels. When possible, staff should de-identify or redact any PII or confidential information prior to transmission.
- Staff should never include a password in any electronic communication unless directed to do so by Technology Staff.
- Staff should not transmit files labeled classified, confidential, or restricted through email or third-party file transfer services without SAU approval.
- Regular transmission of student data to services including but not limited to the SAU Library Management system, Food Service Management system and Single-Sign-On Provider system is managed by the technology department using a secure data transfer protocol. All such services are approved by a SAU/building administrator and the Director of Technology.

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the following requirements and appropriate level of PCI compliance when handling such data:

- Never store cardholder data on SAU systems or in written form. All cardholder data may only be entered in secured payment systems approved by the SAU. Any cardholder data collected in written form must be shredded immediately after entry into approved system.
- The SAU will never maintain a data system for payment information. All payment information will be stored and processed by a 3rd party accessible through a secure portal.
- Never request cardholder information to be transmitted via email or any other electronic communication system.
- Payment information shall be entered directly into the approved payment system by individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.
- If payment information is collected via a physical form, that form must be shredded, or payment information redacted immediately upon receipt and entry into payment system.

Appendix G - Physical Security Controls

The following physical security controls shall be adhered to:

- Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
- Monitor and maintain data centers' temperature and humidity levels.
- File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
- Monitor and control the delivery and removal of all data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the SAU 39 approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology group.
- Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures (see Appendix H: Asset Management).

Appendix H - Asset Management

Data security must be maintained through the life of an asset, including the destruction of data and disposal of assets. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as a system, asset or device.

All involved systems and information are assets of the SAU and are expected to be protected from misuse, unauthorized manipulation, and destruction.

Inventory

All technology devices or systems considered an asset are inventoried by the technology department. This includes, but is not limited to, network appliances, servers, computers, laptops, mobile devices, and external hard drives. It is the responsibility of the technology department to update the inventory system to reflect any in-school transfers, in-SAU transfers, or other location changes for SAU technology assets.

Disposal Guidelines

Assets shall be considered for disposal in accordance with state/federal regulations and School Board Policy. The following considerations are used when assessing an asset for disposal:

- End of useful life
- Lack of continued need
- Obsolescence
- Wear, damage, or deterioration
- Excessive cost of maintenance or repair
- Salable value

The Director of Technology shall approve disposals of any SAU technology asset.

Methods of Disposal

Once equipment has been designated and approved for disposal (does not have salable value), it shall be handled according to one of the following methods. It is the responsibility of the technology department to update the inventory system to reflect the disposal of the asset.

Discard

All technology assets shall be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. When possible, any re-usable hardware that can be used as parts to repair and/or maintain SAU technology assets shall be removed (motherboards, screens, adapters, memory). In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the SAU.

A SAU-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any technological systems/equipment be placed in the trash.

Donation/Gift

In the event that the SAU determines that an asset shall be donated or gifted, systems shall be wiped clean of Personally Identifiable Information (PII), Confidential, and/or Internal Information prior to leaving the SAU. SAU 39 will not support or repair any equipment that is donated. In addition, software licenses are not transferred outside the SAU. Therefore, systems must be returned to factory installation prior to donation.

Appendix I - Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection

SAU 39 desktops, laptops, and file servers are protected using enterprise virus/malware/spyware software. Definitions are updated daily, and an on-access scan is performed on all "read" files continuously. A full scheduled scan runs weekly. A full scheduled scan is performed on all servers weekly during non-peak hours. All files and systems are scanned.

Internet Filtering

Student learning using online content and social collaboration continues to increase. SAU 39 views Internet filtering as a way to balance safety with learning, letting good content, resources, and connections in while blocking potentially inappropriate content. To balance educational Internet resource and application use with student safety and network security, the Internet traffic from all devices on the SAU network is routed through the SAU firewall and content filter. Filtering levels are based on the role of the user, staff or student and student grade level. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing using Barracuda spam filters and advanced threat protection services.

Security Patches

Server patch management is performed regularly. Security patches are applied on an as needed basis..

Appendix J - Account Management

Access controls are essential for data security and integrity. SAU 39 maintains a strict process for the creation and termination of SAU accounts. All new staff accounts are authorized through an HR hiring process prior to creation. Role-based permissions are used to establish access to all systems. Access security is audited at least annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Staff Accounts

When a staff member is hired by SAU 39, the following process ensures that each staff member has the correct access and permissions to the resources that are required for their position.

- Notification of new staff member is sent from Human Resources to the Technology group. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology group creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix K: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the SAU administrator responsible for the system (data manager) and the Director of Technology.
- When a staff member's employment is ended, either by termination or resignation, account permissions are revoked in one of two ways.
    - In the event of termination, HR will notify the Technology Department via email or phone call requiring the account to be disabled at once, preventing any further access to SAU resources.
    - In the event of resignation, HR will notify the Technology Department via email indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to SAU resources.
    - In the event that a user having elevated permissions to any system separates from the SAU, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

Only members of the SAU Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Remote Access

Access into the SAU's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the SAU's network VPN system; no other method of remote access shall be granted without explicit authorization from the ISO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protection as information stored and accessed within SAU's network.

In the event that external access is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All external accounts will be reviewed at least annually.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by the ISO. All contractors doing business on SAU premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing SAU data will be assigned services based on function. Once the approval has been obtained, the technology department will create the account.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into the SAU 39 student information system. Only staff whose roles require access are provided accounts for the system. The following minimum information is entered for each staff member:

Building/Site location

Status - Active

Staff Type

SAU 39 Email Address

Primary Alert Phone Number and Cell phone number

Access accounts for the SAU's SIS are setup based on staff role/position, building and required access to student data and are assigned by the Director of Technology or designee. Teacher accounts are created for all staff responsible for taking student attendance and entering and maintaining grades. Teacher accounts login to the SIS Teacher Portal. Staff assigned a Teacher account only have access to students they teach or provide services to. Administrative accounts are created based on the staff member's role/position and function and further restrictions to data are controlled through the SIS permissions functionality. Security groups control access permissions to certain data sets such as attendance, demographic data, grades, discipline etc. and whether the staff member can view or maintain data. Additional page level permissions are assigned to the security groups. Administrative accounts log into the SIS Admin Portal.

SIS Security Groups

- Administrators/Principals/Deans
- Admin Read Only
- Athletic
- Counselors
- General User View Only
- Registrar
- School Nurses
- School Admin
- Special Education
- Teacher
- Unassigned - no access

Financial System

All staff members are entered into the SAU's financial system for the purpose of staff payroll and HR tracking. Only staff requiring access are provided accounts for the financial/personnel system.

After basic information and user ID are created, a security role is assigned to the account granting them access to designated areas of the financial system to complete their job responsibilities.

Financial System Security Roles:

- Accounting
- Accounts Payable
- Business Admin
- Directors
- Facilities Managers
- HR
- Office Managers
- Payroll

- Principals
- Prof. Dev.
- Remote Requisitions- (admin assistants, IT, Librarian)
- SAA
- Technology

Within each Connection Group, every user's security can be assigned a "Payroll User Role" and the options we are using for that are:

- None
- Full Access
- HR User
- Payroll User
- View Only Limited

Special Education System

The State of New Hampshire provides the SAU access to the NH Special Education Information System (NHSEIS) that houses all student IEP information. Account access to NHSEIS is maintained by the SAU Director of Special Services office in collaboration with the i4See Coordinator through the MyNHDOE single sign on portal. A user role determines the user's authority and applicable permissions within the NHSEIS system. The established roles are as follows:

- School Administrator
- Provider
- Case Manager
- SAU IT Administrator
- IEP Team Member
- SAU Administrator
- SAU System Administrator
- SAU System Staff
- General Ed Teacher
- SAU Administrator

The following user roles access NHSEIS through the MyNHDOE portal: Case Manager, SAU Administrator, SAU IT Administrator, SAU Administrator, SAU System Administrator, SAU System Staff, and School Administrator. The remaining user roles, Provider, General Ed Teacher and IEP Team Member access NHSEIS through a SAU specific web address.

EDMS (Education Data Management System) houses documentation related to the special education process including student details, evaluation information, meeting minutes and related documents. It is accessible to in-district users as assigned by the SAU Office of Student Services roles: Administrator, Case Manager, Evaluator, Service Provider, Teacher, Team Leader
XLogs supports data management relative to special education service providers in areas billable and reimbursable by Medicaid to schools or Special Education aid.

Health Software System

School Nurses, Nurse Substitutes and Technology Staff are the only staff members granted access to the SAU Health Software system. Technology Staff access is for the purpose of upgrades, and technical support for the use of the system. The medical data that is collected and maintained by the school nurses on the system includes immunizations, conditions, medications, and clinic logs (Time in/out of clinic and action taken).

School nurses are the only accounts that can view and maintain medical information.

Security Roles

- Nurse Administrator
- Nurse
- Health Care Asssistnt

Food Services System

The SAU uses a Food Services software management system to track data and perform functions necessary for the efficient operation of the Food Service Program. Food service staff are granted accounts with access to only the parts of the system that are necessary to complete their job functions. Technology Staff access is for the purpose of upgrades, and technical support for the use of the system and cash registers. Strict security roles and permissions are in place to ensure that confidential information is only viewable by authorized staff. The established roles are as follows:

Security Roles

- Enterprise POS Manager
- Building POS Manager
- Cashier

Appendix L - Password Security

The SAU requires the use of strictly controlled passwords for network access and for access to secure sites and information. All passwords to SAU systems shall meet or exceed the below requirements.

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for SAU network access as outlined below.
- Passwords shall never be saved when prompted by any application with the exception of single sign-on (SSO) systems as approved by the Technology Department.
- Passwords shall not be programmed into a computer or recorded anywhere that someone may find and use them.
- When creating a password for secure information or sites, it is important **not** to use passwords that are easily guessed due to their association with the user (i.e. children's names, pets' names, or birthdays).
- Users and staff who have reason to believe a password is lost or compromised must notify the Director of Technology or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

SAU network access to resources managed through LDAP/SSO:

- Passwords must be "strong," and must be a minimum of 10 characters long
- Passwords will only be changed in the event the user shares their password with another staff member or they believe their account has been compromised.

- Your password must not be too similar to your username.
- Do not use your SAU password for any non-SAU systems.

Where possible, system software should enforce the following password standards:

- Passwords routed over a network shall be encrypted.
- Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- System software shall disable the user password when more than ten consecutive invalid passwords are given. The user account will remain locked until a member of the Department of Technology unlocks the account.

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable SAU 39 to respond effectively and efficiently to a natural disaster or critical failure of the SAU's data center and/or core systems. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to business-critical data.
- Recover and restore the SAU's critical systems and data.
- Maintain essential technology resources critical to the day to day operations of the SAU.
- Minimize the impact to the staff and students during or after a critical failure.

Planning Assumptions

The following planning assumptions were used in the development of SAU 39's TDRP:

- There may be natural disasters that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a disaster.
- There is the possibility of complete loss of the current data center.
- We will have adequate storage to recover systems.
- SAU data is housed at SAU data center and backed up offsite.
- SAU data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, SAU networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

SAU 39 has appointed the following people to the disaster recovery/critical failure team: Director of Technology, Lead Network/System Administrator, Building Network Administrators, Desktop Support Staff, SAU 39 Data Coordinator and SHS Operations Manager.

In the event the TDRP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determining the impact of the natural disaster/critical failure.
- Communication of impact and or loss, and updates of progress to the Superintendent.
- Communication of outages and updates to SAU staff.
- Oversight of the TDRP implementation and restoration of critical systems and data.
- Allocation and management of technology staff during the event.
- Working with manufacturers and/or vendors during the recovery and restoration of critical systems and data.
- Oversight of TDRP implementation debrief.

Activation

The TDRP will be activated in the event of the following:

- A natural disaster has occurred and affects the operation of the SAU's data center. A natural disaster

includes but is not limited to the following: tornado, earthquake, lightning, and floods.

- A fire has impacted the data center.
- Water or flooding has impacted the data center.
- Critical system failure.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the IRT.

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- SAU Staff
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication is available at the time. This could include any one or combination of the following:

- Phone
- Email
- Social Media/Website/Communication services
- Radio or Television

The TDRP team will work with the Superintendent on which information will be conveyed to each above group and what means will be used.

Implementation

The TDRP team has the following in place to bring the SAU back online in the least amount of time possible:

- Maintained spreadsheet listing all server names, physical and virtual, and their function. A hard copy of this document will be secured at the office of the Director of Technology. An electronic version will be housed in the SAU 39 SharePoint site.
- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The SAU data center backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and in an offsite building (future implementation will include cloud backup). The SAU's critical virtual servers can be run directly from the cloud with limited access.

Deactivation

The TDRP team will deactivate the plan once services are fully restored.

Evaluation

An internal evaluation of the SAU 39 TDRP response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after-action report and corrective action plan. The result will be an update to the TDRP and other emergency response plans as appropriate.

Appendix N - Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable SAU 39 to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, SAU identifiable information and other significant cybersecurity incident. The objectives of the TDBP are:

- Convene the Incident Response Team (IRT) as necessary.
- Validate and contain the data security breach.
- Analyze the breach to determine scope and composition.
- Minimize impact to the staff and students after a data breach has occurred.
- Notification of data owners, legal counsel, state/federal agencies and law enforcement as deemed necessary.

Planning Assumptions

The following planning assumptions were used in the development of the SAU 39 TDBP:

- There may be data breaches that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a data breach.
- SAU data is backed up.
- Some SAU data is hosted by 3rd party providers.

Data Breach/Incident Response Team

SAU 39 has appointed the following people to the data breach/incident response team: Director of Technology, Lead Network/System Administrator, Building Network Administrators, and Technology Supports Specialists.

In the event the TDBP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determine the nature of the data compromised and its impact to staff, students and the SAU.
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the Superintendent, Assistant Superintendent and Business Administrator.
- Coordinate with Superintendent to ensure communication with SAU staff and or parents as deemed appropriate.
- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, legal counsel, SAU data breach insurance provider, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of TDBP implementation debrief.

Activation

The TDBP will be activated in the event of the following:

- A data breach has occurred. A data breach includes but is not limited to an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Personal Health Information (PHI) has been compromised.

- Personally Identifiable Information (PII) has been compromised.
- Confidential or sensitive data has been compromised.
- Network hack/intrusion has occurred.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the IRT. The breach response and reporting process will be documented according to state and federal requirements. The Director of Technology will work with the Superintendent to dispense and coordinate the notification and public message of the breach.

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- SAU and District Staff
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication deemed appropriate. This could include any one or combination of the following:

- Email
- Social Media/Website/Communication Subscriptions
- Radio or Television
- Written Notice
- Phone

The TDBP team will work with leadership on which information will be conveyed to each above group, timing of that communication and what means will be used.

Implementation

The TDBP team has the following processes in place to contain the data breach in the least of amount of time possible:

- Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the office of the Director of Technology. An electronic version will be housed on the Technology Group SharePoint site.
- Data dictionary of all SAU hosted information systems. A hard copy of this document will be secured at the office of the Director of Technology. Due to non- disclosure agreements, this data may not be available in other locations/formats. The appropriate vendor(s) can be contacted for this information.
- Maintained spreadsheet listing all server names, physical and virtual, and their function. A hard copy of this document will be secured at the technology office. An electronic version will be housed on the Technology Group SharePoint site.
- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.

- The SAU data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and offsite.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated. The IRT will be comprised of the Director of Technology, Lead Network System Administrator, Building Network Administrators, and Technology Supports Specialists. Additional members of the SAU 39 administrative team and technology group may be designated to assist on the IRT.
- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and ongoing breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.
- The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- The IRM will work with legal counsel and the Superintendent's Leadership Team to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, and local law enforcement.
- Collaboration between the authorities and the IRT will take place with the IRM. The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.
- On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach. When the investigation has concluded, all evidence will be safely stored, recorded or destroyed (where appropriate).
- All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation. Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.
- The IRT will work with the Superintendent's office to outline the notification of the data owners and those affected. Communication will be sent out as directed by legal counsel and advised by the SAU administration. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.
- The IRM, in conjunction with the IRT, legal counsel and the Superintendent's Leadership Team will determine if notification of affected individuals is necessary. Once the determination is made to notify affected individuals, a letter will be written in accordance with all federal and state statutes, and local procedures. If it is determined that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and filed at the Superintendent's office.

Deactivation

The TDBP team will deactivate the plan once the data breach has been fully contained.

Evaluation

Once the breach has been mitigated an internal evaluation of the SAU 39 TDBP response will be conducted. The IRT, in conjunction with the IRM and others that were involved, will review the breach and all mitigation steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities may result in an update to the TDBP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.