Softdocs

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Softdocs SC, LLC **("Vendor")** are parties to a contract dated 3.13.25 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Document Management Software ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means Softdocs SC, LLC .

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For (Vendor Name)
[signature]	Abe Gruber
Date 3/17/25	**Date** 3.13.25

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
	Abe Gruber
Date	**Date**
3/17/25	3.13.25

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

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

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attach)

Softdocs

SECURITY COMPLIANCE POLICY AND PROCEDURES

PII and PHI

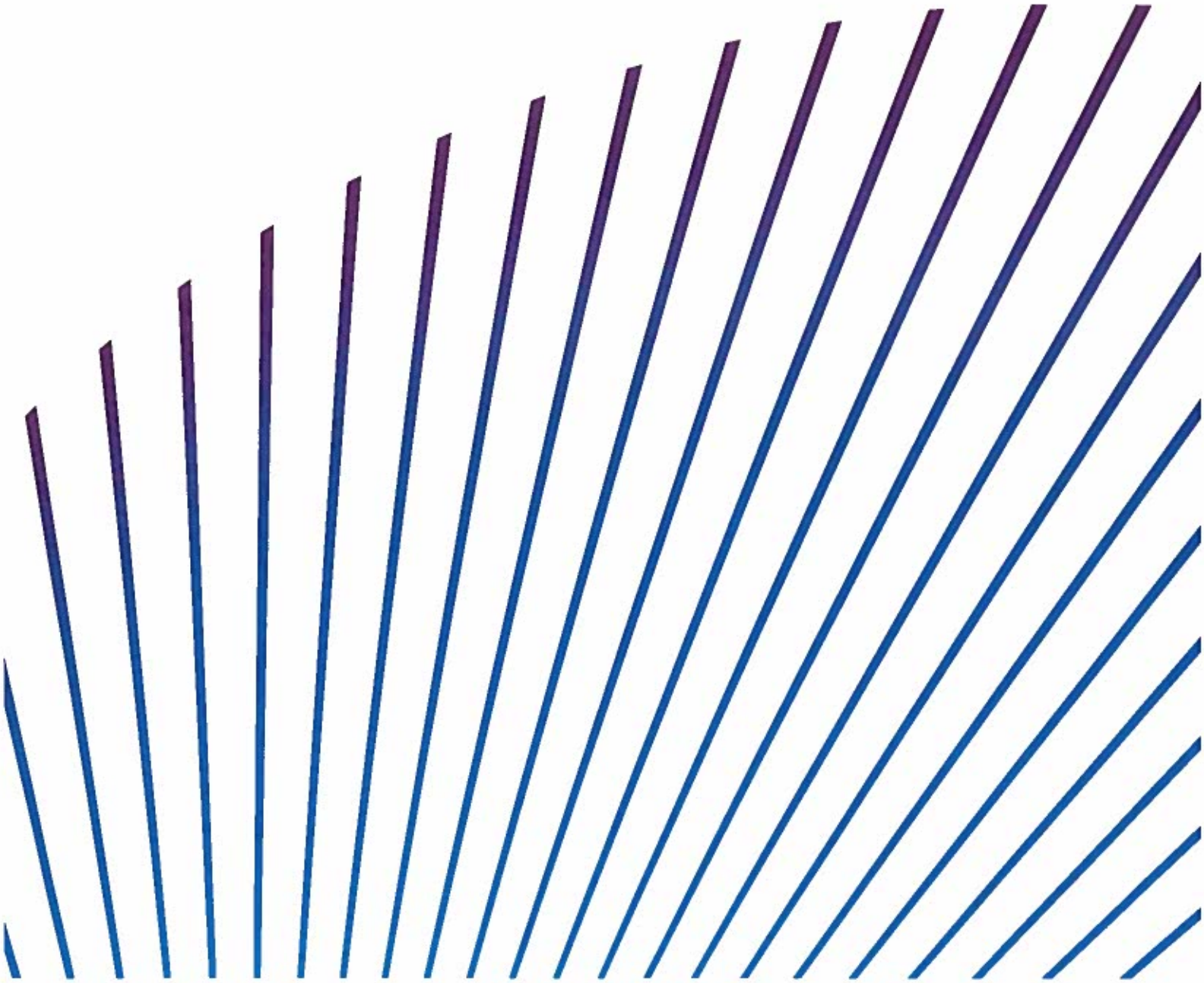

TABLE OF CONTENTS

Softdocs PII & PHI Data

1.0 Overview

Softdocs employees handle and process information that is considered PII (*Personally Identifiable Information*) and/or PHI (*Personal Health Information*) daily.

This document serves as a guide to ensuring compliance with the company policies. This is not an all-encompassing document. If you have questions about specific scenarios, please see the Compliance Officer.

All employees agree to a data protection and confidentiality agreement at the time of employment and every year thereafter as a condition of employment.

2.0 Scope

The provisions of these policies pertain to all Softdocs employees, contractors, third parties, and others who have access to company and customer confidential information within Softdocs systems and facilities.

3.0 Management Commitment

Softdocs and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Softdocs system by implementing adequate security controls.

4.0 Compliance

Compliance with these policies is mandatory. It is Softdocs policy that production systems meet or exceed the requirements outlined in this document. The Compliance Officer will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team's recommendations.

5.0 Examples of PII and PHI

PII (Personally Identifiable Information): Any information that can be used to identify an individual, such as name, address, phone number, email address, Social Security number, and biometric data.
PHI (Protected Health Information): Any information in a medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed while providing healthcare services, such as medical history, test results, insurance information, and other health-related data.
Examples of data considered to be PII.

PII Identifier	Examples of PII
Name	Full names (first, middle, last name) maiden name, mother's maiden name, alias
Addresses	Street address, email address, IP or MAC addresses
Phone Numbers	Mobile, business, personal
Personal Identification Numbers	Social security number (SSN), passport number, driver's license, state identification number, taxpayer identification number, patient identification number, financial account or credit/debit
Personal Biometric Features	Photographic images (that have distinguishing features e.g. show the face), x-rays, fingerprints, retina scan, voice signature
Information Identifying Personally Owned Property	Vehicle registration number

Examples of data considered to be PHI.

PHI Identifier	Examples of PHI
Medical History	Diagnoses, treatment plans, medications, immunization records, allergies
Test Results	Lab results, imaging results (e.g., X-rays, MRIs), genetic test results
Insurance Information	Insurance provider, policy number, coverage details
Health-related Data	Appointment dates, medical bills, health insurance claims, referral information
Personal Identification	Patient ID number, medical record number, health plan beneficiary number
Biometric Data	Fingerprints, retinal scans, voice prints, facial recognition data

6.0 Employee and Company Responsibilities

As an employee of Softdocs, you are required to always protect customer data. Below is a list of responsibilities that must be always maintained.

- PII data should be stored in the customer's environment and not transferred to Softdocs.
- At no time should any customer PII/PHI data be stored locally on your devices for longer than the data is being processed.
- If you are accessing a customer environment or processing PII/PHI data, at no time should your computer be left unattended. If you need to leave your machine, you are required to lock the Operating System.
- Softdocs requires that customer's data be stored on their servers or sent to us via a secure method (SFTP or Encrypted Drives). Egnyte is Softdocs organizational end-user cloud-based solution for sharing files outside our organization.

  When Sharing via Egnyte:
  - Use folders to share groups of files with others online and never share customers' data with others.
  - From Egnyte, share files with specific individuals (default sharing option), never with "everyone." Share settings, by default, require a password before the invitation is sent.
  - An expiration date on all shares is applied by default, but if more time-sensitive expiration is needed shortening the expiration date is recommended.
- Under no circumstances should employees accept and/or send unencrypted PII/PHI over email.
- If PII/PHI must be printed, it must not be left unattended and should be shredded after use.
- No PII is to be stored unencrypted on SharePoint, Network Drives, CRM, Computers, Mobile Devices, etc.
- **If you encounter unencrypted PII/PHI data on a Softdocs system, you should immediately report the issue to the Compliance Officer.**
  - If such data is mistakenly saved unencrypted in a shared location, the employee should remove the data immediately.
  - If found on a hard drive, please also reference the Media Destruction Policy and turn it in to the IT Department immediately.
- Once processing of data has been completed, (Taxes, Serve Jobs, Migrations, Contracts Process, etc.) all PII/PHI data must be permanently purged.
- On-Premises customers are responsible for maintaining backups of their processed data. It is not the responsibility of Softdocs to keep this data unless specifically contracted.
  - Please see the Softdocs Recommend Backup Procedures via www.community.softdocs.com to assist customers with Backup Best Practices.

7.0 Audit Procedures

All network drives will be reviewed annually for any sensitive or confidential information. Any information that is found will be immediately deleted and removed. All results will be housed on the Softdocs Operations SharePoint Site. The logs will include the results of the audits.

Quarterly and weekly reviews of connected peripherals are also performed on devices to include any hard drives attached to workstation machines. This may apply to personal hard drives that are visible and in use while on company property. These results will reside in the documented quarterly endpoint review audit logs.

8.0 Revision History

Revision #:	Purpose / Changes	Author	Date
1.0	Initial Draft.	Steve Johnston	04/20/2018
2.0	Addition of Section 3.0 & 4.0 and format to Policy Template.	Lexi Pearson	11/14/2018
2.5	Policy Approved.	Steve Johnston	11/14/2018
3.0	Minor adjustments.	Brady Morris	12/07/2018
4.0	Changed process after initial cleanup of drives to annual vs. quarterly.	Audit Team	04/04/2019
5.0	Policy reviewed and approved.	Terri McKinney	05/10/2019
6.0	Policy reviewed and approved.	Terri McKinney	05/18/2020
7.0	Policy reviewed and approved.	Terri McKinney	06/16/2021
8.0	Policy reviewed and approved.	Terri McKinney	06/16/2022
9.0	Added Egnyte details.	Alan Atkins	01/23/2023
10.0	Added approval history.	Terri McKinney	01/23/2023
11.0	Added table for PII examples. Updated to include the following: Scope, roles and responsibilities, management commitment and compliance.	Terri McKinney	11/22/2023
12.0	Added definitions of PII and PHI.	Terri McKinney	06/10/2024
12.0	Policy review. Addition to section 8.0 Audit Procedures to include weekly review of peripherals.	Alan Atkins	06/18/2024
13.0	Added examples of PHI.	Terri McKinney	02/10/2025

9.0 Approval History

Revision #:	Approval Notes	Approval By:	Date
10.0	Policy reviewed and approved.	Terri McKinney	01/23/2023
10.0	Policy reviewed and approved.	Terri McKinney	03/22/2023
11.0	Policy reviewed and approved.	Terri McKinney	11/22/2023
12.0	Policy reviewed and approved.	Terri McKinney	07/17/2024
13.0	Policy reviewed and approved.	Terri McKinney	02/10/2025

TABLE OF CONTENTS

Information Security Policy

1.0 Purpose

Softdocs understands that the business and its employees handle sensitive information during standard business operations. To protect against and mitigate potential security failures, Softdocs has established this policy to define the security controls and measures used to protect Softdocs' information. As security threats are continually evolving, the Softdocs Information Security Policy is intended to be periodically reviewed and, at a minimum this policy will be reviewed annually.

.

2.0 Scope

The provisions of these policies pertain to all Softdocs employees, contractors, third parties, and others who have access to company and customer confidential information within Softdocs systems and facilities.

3.0 Roles and Responsibilities

These policies apply to all Softdocs employees, contractors, business partners, third parties, and others who need or have access to Softdocs systems and our customer's confidential information.

Individual or Group	Role	Responsibility
Adam Park	CEO	Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives.
Steve Johnston	COO	Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program.
Terri McKinney	Director of Operations and Compliance Officer	Has statutory, management, or operational authority for Softdocs information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. Responsible for operating information system at an acceptable level of risk to organizational operations and assets.
Alan Atkins, Cameron Armistead and Steven Lowder	Director of IT, Cloud Engineering Manager and Security Architect	Acts on behalf of Compliance Officer to coordinate and conduct day-to-day activities associated with security authorization process.

Individual or Group	Role	Responsibility
		Responsible for conducting information system security engineering activities. Responsible for providing appropriate security, to include management, operational, and technical controls.
Alan Atkins, Cameron Armistead, Steven Lowder, Ben Spann	Director of IT, Cloud Engineering Manager, Security Architect, System Administrator	Responsible for conducting information system security engineering activities. Responsible for providing appropriate security, including management, operational, and technical controls. Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.
Terri McKinney, Alan Atkins, Cameron Armistead, Steven Lowder, and Ben Spann	Director of Operations and Compliance Officer, Director of IT, Cloud Engineering Manager, Security Architect, System Administrator	Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures.
Ben Spann	System Administrator	Responsible for conducting information system security Administration activities.
Leadership, Management	Managers	Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures
All end users	Users	Responsible for understanding and complying with Policies and Procedures.

4.0 Management Commitment

Softdocs and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Softdocs system by implementing adequate security controls.

5.0 Compliance

Compliance with these policies is mandatory. It is Softdocs policy that production systems meet or exceed the requirements outlined in this document. The Compliance Officer will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team's recommendations.

6.0 Policy Overview

Information security is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. It ensures the confidentiality, integrity, and availability of data.

- **Security** means system resources are protected against all types of unauthorized access, including network and application firewalls, two-factor authentication, and intrusion detection.
- **Availability** looks at how accessible a company's services, products, and systems are based on the contracts and service level agreements (SLA). It includes performance monitoring, disaster recovery and security incident handling.
- **Confidentiality** relates to data that has access and disclosure limited to specific groups. It involves encryption, access controls, and network and application firewalls.[1]

The following policies are outlined in this document and should be referenced for detailed documentation of the procedures.

Security Authorization and IT Infrastructure Access and Support

- Disaster Recovery Policy
- Business Continuity Policy
- Security Incident or Data Breach Policy
- Data Encryption Policy
- Enterprise Monitoring Tools
- Antivirus and Anti-Malware Policy
- Audit and Accountability Policy
- Password Policy

Privacy and Confidentiality

- Access Control Policy
- Password Policy
- Change Management Policy
- PII and PHI Data Policy
- Two-factor Authentication
- Media Destruction Policy
- Microsoft 365 Data Policy

Availability

- Etrieve Cloud Service Level Agreement

7.0 Security Authorization and IT Infrastructure

7.1 Disaster Recovery Policy Overview

Softdocs developed a strategy for mitigating any events resulting in extended delays of service, and this also ensures that we have a well-tested contingency plan to minimize the potential impact of these events. Disasters are not limited to adverse weather or power outages. The policy is directed to any staff

[1] https://www.clearskydata.com/blog/what-soc-2-compliance-means-for-you-and-your-data

that is accountable for ensuring the continuation of vital business processes in the event of a disaster. Softdocs Disaster Recovery Plan and Disaster Recovery procedure policy are part of an on-going process of planning, developing, testing, and implementing these procedures. The Disaster Recovery Strategy was developed and is maintained by the Softdocs Executive Team, Operations Team, and Cloud Operations Team. The initial discovery was performed to determine which systems were at risk of being impacted by a potential disaster. Once these systems were listed, the effort was focused on how each system would impact the Company and our ability to assist our customers in the event that the system failed or was interrupted. This analysis allowed the team to determine the best solution to remedy any potential loss of access or loss of data. Each flow was mapped out via team agreement on how Softdocs would proceed in the event of a disaster. Testing of the procedures is performed bi-annually to test the plan and update policy and procedures documentation with necessary updates discovered during the test.

7.2 Business Continuity Policy Overview

Business Continuity Planning is developed in conjunction with the Disaster Recovery Plan to assess all existing risks of an organization and determine a plan for preparedness. The approach that is created serves to ensure that all critical business operations can function during and after an interruption. This plan is executed should customer systems become inaccessible.

The Business Continuity Plan was created via multiple brainstorming sessions that included IT, Operations, Cloud Operations, and the Executive Team. During these sessions, risks were determined and identified. Once the risk was isolated, a determined disaster recovery plan was developed for each risk. After all systems had a tested recovery plan in place, the next step was to determine and assess how to maintain the business's overall operations.

All necessary contact information was retrieved and put in one shared document that is accessible via SharePoint. This assists in calling internal key resources and external key resources should this plan need to be invoked. The plan itself was then re-examined to create an effective and efficient procedure that limits the loss of business operations internally and externally.

7.3 Security Incident or Data Breach Policy Overview

Our Security Incident and Data Breach Policy illustrates the processes to be followed by Softdocs' employees in the event that our company experiences a security incident or data breach or suspects that a data breach has occurred. A data breach involves the loss of unauthorized access to, or unauthorized disclosure of, personal information. Our procedure documents all steps involved if a breach or security incident occurs. It also includes the workflow for assistance for employees to follow.

7.4 Data Encryption Policy Overview

Our Data Encryption Policy provides standards for protecting sensitive customer data and related credentials. Invoking a Data Encryption Policy preserves the confidentiality and integrity of where confidential information is stored, processed or transmitted. When properly implemented, encryption provides an enhanced level of assurance that the encrypted data cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss, or interception. This policy applies to all staff that create, deploy, transmit, or support applications and system software containing PII (Personal Identifiable Information) or customer data. It addresses encryption controls for data that is at rest, data that is in motion, and key standards and management.

7.5 Enterprise Monitoring Tools Overview

Softdocs currently uses a variety of monitoring tools that are supplied by vendors and reside in the Admin Portals. These tools include Microsoft 365 Security Center, Azure Dashboards, Azure Application Insights, Datadog SIEM, CrowdStrike MDR, Uptime, and Cloudflare Firewall Monitoring Tools.

7.6 Antivirus and Anti-Malware Policy Overview

Softdocs' antivirus, anti-malware is based on a secure layered policy. Malicious incidents can cause severe damage, affecting the security of business and leading to business interruption, privacy breaches, and compliance failures. Softdocs policy and procedures that are in place proactively protect our systems, including cloud-deployed systems, from potential threats. These threats could include viruses, Trojans, rootkits, exploits, spyware and other types of malicious software. This document also addresses the steps that will be taken to address computer, network, or cloud-employed instances in the event of such an attack. It is the responsibility of Softdocs and all employees to protect our customers' business data and associated networks on a consistent and regular basis.

7.7 Audit and Accountability Policy Overview

The Audit and Accountability policy specifies auditable events such as logon attempts, account management, and data access, requiring detailed audit records for each event, including the event type, date, source, outcome, and user identity. Softdocs must ensure sufficient audit storage, alert staff to audit failures, and conduct weekly reviews of audit logs for unusual activity. The policy includes automated audit analysis, reduction, and reporting tools to facilitate investigations, timestamp synchronization, and protection of audit information. Audit records are retained for 90 days online and longer offline. The system must generate audit records for defined events and allow designated employees to select specific audit events.

The procedural requirements for Softdocs' audit and accountability involve configuring audit logging mechanisms using Azure Log Analytics, Datadog, and PagerDuty. The Cloud Engineering Manager defines auditable events for various systems, such as Azure, IIS, CrowdStrike, and Cloudflare, and ensures they are configured to generate comprehensive audit records. Datadog is used for audit reduction, dashboard generation, and on-demand reporting without altering original logs. Audit storage is managed within Azure, with a retention timeline of 365 days, and alerts are set up for log processing failures. Weekly reviews of audit logs are conducted, and unusual findings are reported and tracked. Time synchronization for Azure VMs is maintained with Microsoft-owned Stratum 1-time servers. Audit logs are protected via role-based access control, and access is reviewed quarterly. Audit logs are stored for 30 days online and 365 days offline.

8.0 Privacy and Confidentiality

8.1 Access Control Policy Overview

The purpose of this policy is to describe how Softdocs works to keep customer environments secure using access control. Cloud customers have access to their data through the Softdocs applications, and the Softdocs Cloud Operations team has access to the cloud servers and data that is contained within.

The Professional Services Team needs access to a client's server to assist in the successful implementation of our solutions. This access is requested and granted on a project-by-project basis. Once the Technical and Implementation Teams have completed their work, access is revoked, and the customer is transitioned to our Support Team. The Support Team needs access to the cloud environments and data from time to time to work on issues reported by the clients or to make modifications to the data and/or applications.

The Support team on occasion may need access to the cloud environments and data to work on issues reported by the clients or to make modifications to the data and/or applications. The client's reports inform of application issues and/or data issues to the Support team for resolution. There will also be times

when a client wishes to make modifications to the applications and/or data. These requests are reported to the Support team. During normal operations, the Support Team does not have direct access to the client's servers or the data that resides on them unless access is requested and granted.
A request is made to the Cloud Operations Team to gain access to the client's servers and/or data. This request includes which client system needs access and how long access is necessary. The Cloud Ops Engineer logs the request and grants access for the period specified. When the work is complete or the period has ended, whichever occurs first, access is removed, and the audit log for the request is updated and closed. All-access support requests are submitted, tracked, and worked via our Internal Support Change Management system (powered by Salesforce).

8.2 Change Management Policy Overview

Our Change Management policy describes the responsibilities, policies, and procedures to be followed when any changes to internal infrastructure, cloud infrastructure, access control (including new employee onboarding). The Change Control policy is designed to provide a managed and auditable method in which changes to the information technology environment are requested, tested, and approved prior to installation or implementation. The purpose is not to question the rationale of a change, but to ensure that all elements are in place, there is no negative impact on the infrastructure, all the necessary parties are notified in advance, and the schedule for implementation is coordinated with all other activities

The Internal Change Management Process is used to document all changes and requests made by employees for infrastructure and internal solutions. This includes but is not limited to the Onboarding Process, Internal IT requests, and computer-related/access problems, Access Requests, Credential Requests and System Configuration changes. Below are the assignees used within the Change Management Process and their use cases:

Access Request | This is used whenever an employee needs to access a customer or internal cloud instance of Etrieve. The process allows us to track the start date and the expiration of the cloud access request.
Operations | Any request for solution credentials to internal solutions, such as but not limited to Salesforce, HubSpot, or MavenLink, must be requested through this procedure to ensure the correct employees receive the credentials and security needed to perform their jobs. All internal infrastructure changes to the systems mentioned above are also requested and recorded.
Internal IT | All Softdocs IT requests must be made through the Salesforce Service Cloud ticketing system. Requests may include but are not limited to email support, hardware, and software needs, building access or badge ID request, and phone issues.
Employee Onboarding | HR submits a request to IT to initiate the new employee onboarding process. IT submits a ticket to start the onboarding process internally. This documents whom we are hiring and provides a tracking mechanism of credentials to network, hardware/software, and email and phone extension.
Employee Offboarding | HR submits a request to IT to initiate the offboarding process. IT submits a ticket to start the offboarding process internally.
Cloud Operations | This group is used whenever an upgrade or scheduled maintenance is required or requested for a customer. All security and penetration testing for our cloud environments are requested here.

8.3 PII and PHI Policy Overview

Softdocs employees handle and process information that is considered PII (*Personally Identifiable Information*) and/or PHI (*Personal Health Information*) daily. It is important to understand your role in the collection, storage, and disposal of PII.

All employees agree to a data protection and confidentiality agreement at the time of employment and every year thereafter as a condition of employment.

PII (Personally Identifiable Information): Any information that can be used to identify an individual, such as name, address, phone number, email address, Social Security number, and biometric data.
PHI (Protected Health Information): Any information in a medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing healthcare services, such as medical history, test results, insurance information, and other health-related data.

Examples of data considered to be PII.

PII Identifier	Examples of PII
Name	Full names (first, middle, last name) maiden name, mother's maiden name, alias
Addresses	Street address, email address, IP or MAC addresses
Phone Numbers	Mobile, business, personal
Personal Identification Numbers	Social security number (SSN), passport number, driver's license, state identification number, taxpayer identification number, patient identification number, financial account or credit/debit
Personal Biometric Features	Photographic images (that have distinguishing features e.g. show the face), x-rays, fingerprints, retina scan, voice signature
Information Identifying Personally Owned Property	Vehicle registration number

Examples of data considered to be PHI.

PHI Identifier	Examples of PHI
Medical History	Diagnoses, treatment plans, medications, immunization records, allergies
Test Results	Lab results, imaging results (e.g., X-rays, MRIs), genetic test results
Insurance Information	Insurance provider, policy number, coverage details
Health-related Data	Appointment dates, medical bills, health insurance claims, referral information

Personal Identification	Patient ID number, medical record number, health plan beneficiary number
Biometric Data	Fingerprints, retinal scans, voice prints, facial recognition data

8.4 Multi-factor Authentication Policy Overview

The purpose of the Multi-Factor Authentication (MFA) Policy is to enable positive and secure authentication methods for the entire Softdocs internal employee base. This authentication method is a security enhancement that requires the individual to present two different methods of verification before accessing Softdocs internal infrastructure. MFA assists in protecting the access to sensitive information, internal resources, and customer system support.

8.5 Media Destruction Policy Overview

Softdocs Media Destruction Policy outlines the proper disposal and destruction of media (physical or electronic) at Softdocs.
Softdocs utilizes RAID drives to increase server storage and backup safety via redundancy. They are operating functionally in the server RAID array. Once a drive failure occurs, these are removed and stored in a locked closet until destruction. The closet is only accessible by the IT Team and the Executive Team. When these hard drives are no longer useful, it is the responsibility of the IT Department to properly dispose of them. Softdocs does not utilize any workstation desktop media devices to store any customer information. Softdocs does not allow the storage of any classified or sensitive customer information on any devices. Please review in detail Softdocs PII & PHI Policy to review how internal employees, contractors, and temporary staff are instructed to handle sensitive customer data.

8.6 Microsoft 365 Data Policy Overview

Microsoft 365 (M365) is Softdocs organizational end-user cloud-based solution for workflow (email, team chats/channels, team share sites, and end-user document storage). The M365 solution includes the applications OneDrive for Business (OneDrive), Teams, SharePoint, Microsoft Outlook and Office Application Suite products, and Azure DevOps.

Although M365 is the organizational workflow solution for Softdocs users, there are security practices that still must be followed to ensure the service is being used properly.

For Workstations:

- Ensure virus/malware detection software is installed with the latest definitions.
- Do not log into your workstation or device as an administrator (unless necessary).
- Keep your operating system and software up to date.
- Password-protect your workstation or device and use idle-time screen-saver passwords where possible.
- Do not synchronize files to a machine or device that is not secured by Softdocs.
- Do not store personal files in OneDrive, Team channels, or SharePoint Team sites.

When Sharing:

- Use folders to share groups of files with others online and never share customers data with others.
- From OneDrive, SharePoint Sites, and Teams channels share files with specific individuals (default sharing option), never with "everyone" or the "public." Always review "Other settings"

options for allowing editing of shared files, viewing mode, and blocking of download before sending links to others ("i" icon to the right explains the setting options).

- For the best practice on collaboration training video visit Best practices for collaboration (microsoft.com)
- Be careful sending links to shared folders because they can often be forwarded to others whom you did not provide access to.

9.0 Availability

9.1 Etrieve Cloud Service Level Policy

The Etrieve Cloud Service Level policy provides information about the management of the production Etrieve Cloud environment, including data backup and retention, restoration, disaster recovery, business continuity and availability, traditional and emergency change management, compliance, security, and notifications.

10.0 Revision History

Revision #:	Purpose / Changes	Author	Date
1.0	Initial draft.	Terri McKinney	03/29/2019
2.0	Minor revisions.	Brady Morris	04/10/2019
3.0	Incorporated multi-factor authentication. Policy review and approved	Terri McKinney	05/09/2019
4.0	Changes made to reflect Salesforce vs Zendesk as external and internal support ticketing solution. Policy reviewed and approved.	Terri McKinney	06/01/2020
5.0	Changes made to Change Management and Access Control. Access Control now includes all customer environments including on-premises environments	Terri McKinney	06/01/2021
6.0	Policy reviewed and approved.	Terri McKinney	06/18/2021
7.0	Removed Human Resources from Change Management Policy as Paycor is now the system of record for all new employee documentation. Added Microsoft 365 Data Policy. Policy reviewed and approved.	Terri McKinney	02/10/2022
8.0	Security team reviewed and approved.	Terri McKinney	04/06/2022
9.0	Policy reviewed and approved	Terri McKinney	06/16/2022
10.0	Added policy to be reviewed at a minimum annually based on KP recommendation. Minor revisions to Employee Onboarding. Added Employee Offboarding to Change Management section. Added approval history.	Terri McKinney	01/23/2023
11.0	Updated to include the following: Purpose, scope, roles and responsibilities, management commitment and compliance. Included updated examples of PII and PHI.	Terri McKinney	11/29/2023
12.0	Policy review. Update to enterprise monitoring tools.	Alan Atkins	06/13/2024
13.0	Added audit and accountability summary. Included definitions of PII and PHI.	Terri McKinney	06/13/2024
14.0	Updated definition of Information Security.	Terri McKinney	10/02/2024
15.0	Made minor grammar changes, included UpTime as a new Enterprise Monitoring tool. Additionally, removed references to office network as it is no longer in play as all resources are now in the Cloud.	Terri McKinney	02/10/2025

11.0 Approval History

Revision #:	Approval Notes	Approval By:	Date
10.0	Policy reviewed and approved.	Terri McKinney	01/23/2023
10.0	Policy reviewed and approved.	Terri McKinney	03/22/2023
11.0	Policy reviewed and approved.	Terri McKinney	11/29/2023
13.0	Policy reviewed and approved.	Terri McKinney	06/13/2024
14.0	Policy reviewed, updated and approved.	Terri McKinney	02/10/2025