SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

SYSTEM SECURITY PLAN

SoftInWay, Inc.

Table of Contents

1. Purpose and Summary 3
2. System Identification 3
2.1 System Name/Title: SP 800-171 Compliant SoftInWay System 3
2.2 Responsible Organization: 3
2.3 General Description/Purpose of System: 4
2.4 General Description of Information 5
3. System Environment 6
3.1 Hardware Inventory 7
3.2 Software Inventory 7
3.3 Hardware and Software Maintenance and Ownership 8
4. Requirements 8
4.1 Access Control 8
4.2 Awareness and Training 15
4.3 Audit and Accountability 17
4.4 Configuration Management 19
4.5 Identification and Authentication 23
4.6 Incident Response 26
4.7 Maintenance 27
4.8 Media Protection 29
4.9 Personnel Security 31
4.10 Physical Protection 32
4.11 Risk Assessment 34
4.12 Security Assessment 35
4.13 System and Communications Protection 37
4.14 System and Information Integrity 41

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

Effective Date: April 14, 2022
Policy Number: P-049
Responsible Unit: Data Protection Group
Phone: 781-328-4310
Email: dpo@softinway.com

RECORD OF CHANGES

Date	Description	Made By:
01/01/2022	Acceptance	LM/MAS
04/14/2022	Change of Address	LM/MAS
02/05/2024	Change of Address/CAO info	TJH

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

1. Purpose and Summary

This document is a System Security Plan (SSP) performed according to NIST SP 800-171 to comply with the DoD Assessment Requirements for Supplier Performance Risk System (SPRS).

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place, or planned, for meeting those requirements. The system security plan also delineates the responsibilities and expected behavior of all individuals who access the system.

This SSP was prepared for the system to be used in the DoD proposal Number A214-033-0932 Topic A214-033.

2. System Identification

2.1 System Name/Title: SP 800-171 Compliant SoftInWay System

2.1.1 System Categorization: Basic Impact for Confidentiality

2.1.2 System Unique Identifier: SIW_SP800_171

2.2 Responsible Organization:

Name:	SoftInWay, Inc.
Address:	20 Burlington Mall Road, Suite 450, Burlington, MA 01921
Phone:	781-328-4310

2.2.1 Information Owner (Government point of contact responsible for providing and/or receiving CUI)**:**

Name:	Vlad Goldenberg
Title:	Principal Investigator
Office Address:	20 Burlington Mall Road, Suite 450, Burlington, MA 01921
Work Phone:	781-328-4310
e-Mail Address:	vlad.goldenberg@softinway.com

2.2.1.1 System Owner (assignment of security responsibility)**:**

Name:	Maksym Burlaka
Title:	Research and Development Manager
Office Address:	20 Burlington Mall Road, Suite 450, Burlington, MA 01921
Work Phone:	781-328-4310
e-Mail Address:	m.burlaka@softinway.com

2.2.1.2 System Security Officer:

Name:	Thomas J. Hogan
Title:	Chief Administrative Officer/General Counsel
Office Address:	20 Burlington Mall Road, Suite 450, Burlington, MA 01921
Work Phone:	617-529-5352
e-Mail Address:	Thomas.hogan@softinway.com

2.3 General Description/Purpose of System:

The system consists of a workstation with specific software packages and a dedicated wired router connected to an internet.

2.3.2 System Purpose

The purpose of the system is to provide to end users the means to perform all required engineering calculations and other activities within the scope of the project, including all steps of CUI life cycle. Engineering calculations might include 1D/2D calculations and 3D calculations using installed inhouse and third-party commercial engineering software packages. The other activities might include exchange emails, preparation of reports or presentations, web meetings, etc.

2.3.3 Number of end users and privileged users

Number of Users	Number of Administrators/ Privileged Users
2	2

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

2.4 General Description of Information

CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

Information	Description	Category Marking	Banner Marking
General Proprietary Business Information	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.	PROPIN	CUI
Controlled Technical Information	Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.	CTI	CUI//SP-CTI
Sensitive Personally Identifiable Information	A subset of PII that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. a. Examples of stand-alone PII include Social Security Numbers (SSN), driver's license or state identification number; Alien Registration Numbers; financial account number; and biometric identifiers such as fingerprint, voiceprint, or iris scan.	SPII	CUI

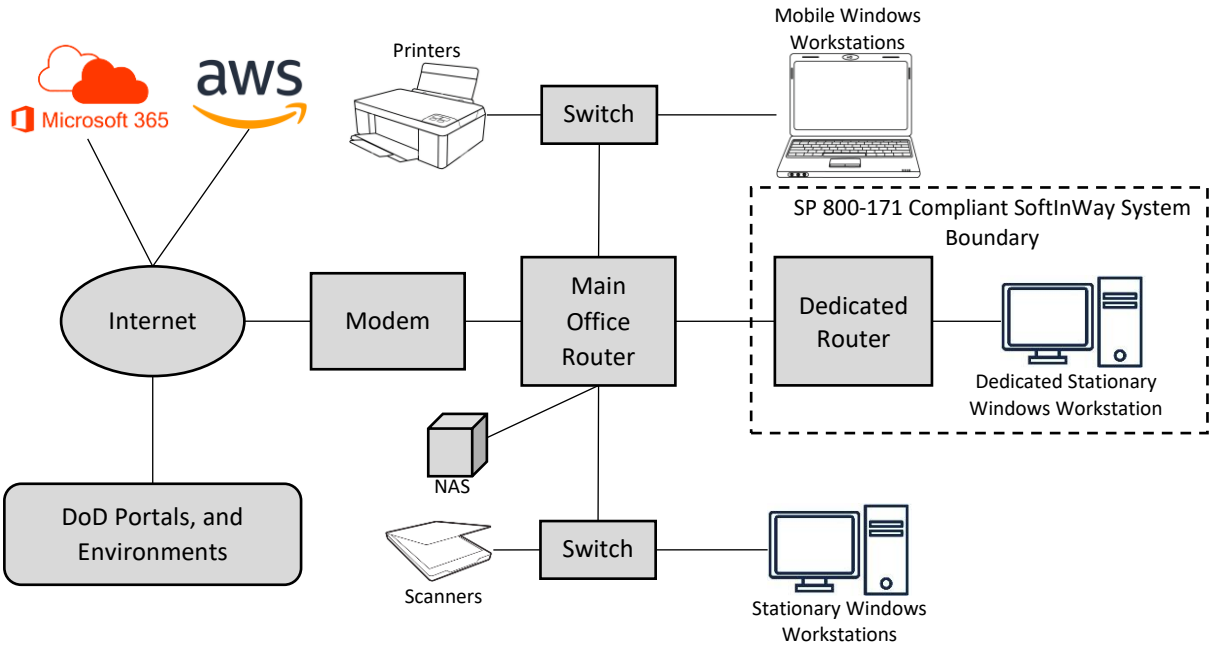
SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

Information	Description	Category Marking	Banner Marking
	b. Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements: • Truncated SSN (such as last four digits) • Date of birth (month, day, and year) • Citizenship or immigration status • Ethnic or religious affiliation • Sexual orientation • Criminal history • Medical information • System authentication information such as mother's maiden name, account passwords, or personal identification numbers c. Other PII may be "sensitive" depending on its context, such in as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.		

3. System Environment

The SP 800-171 Compliant SoftInWay System consists of a Dedicated Router and a Dedicated Stationary Windows Workstation. The boundary of the system is depicted by dashed line in the diagram below. The Dedicated Windows Workstation is connected by ethernet cable to the Dedicated Router. The dedicated router doesn't have other connected devices. The Dedicated Router and the Dedicated Windows Workstation have disabled wi-fi. The dedicated router is configured in the way that does not allow other workstations to access any information behind it, i.e., all CUI information stored on the Dedicated Stationary Windows workstation stays exclusively on the workstation and can be accessed from that workstation by authorized users only. SP 800-171 Compliant SoftInWay System is connected by ethernet cable to the Main Office Router. NAS device is connected by ethernet cable to Main Office Router directly. There are other devices (e.g. workstations, printers, scanners) connected to the Main Office Router by ethernet cable. The Main Office Router is connected by ethernet cable to the Modem which provides access to Microsoft 365, Amazon Web Services via internet. It should be noted that the Dedicated Stationary Windows Workstation and the Dedicated Router are configured in the way that allows access to DoD Portals and Environments only and does not allow connection to the other websites and web services.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310



3.1 Hardware Inventory

The list of hardware inventory for SP 800-171 Compliant SoftInWay System is given in the table below.

#	Component type	Component ID	Make/OEM	Model	Operating System (OS)	OS Build	Responsible Role
1	Stationary Workstation	Brain_CLX	CLX	Custom	Windows 10 Pro	19043.1586	System Owner
2	Router	Nighthawk	NETGEAR	Nighthawk AC1900	NETGEAR Router OS	1.0.11.134	System Owner

3.2 Software Inventory

The list of software installed on SP 800-171 Compliant SoftInWay System is given in the table below.

#	Installed on Component ID	Software type	Make/OEM	Name	Version/Build
1	Brain_CLX	Engineering	ANSYS	ANSYS Fluids and Structures	2022R1
2	Brain_CLX	Engineering	GNU Octave	GNU Octave	6.4.0

#	Installed on Component ID	Software type	Make/OEM	Name	Version/Build
3	Brain_CLX	Engineering	National Institute of Standards and Technology US Dept of Commerice	NIST REFPROP	9.1 & 10.0
4	Brain_CLX	Engineering	SciLab	SciLab	6.1.1
5	Brain_CLX	Engineering	Siemens	STAR-CCM+	2021.3 (16.06.008)
6	Brain_CLX	Engineering	Siemens	NX	2007 series Release 2019
7	Brain_CLX	Engineering	SoftInWay, Inc.	AxSTREAM® Platform Package	3.9 & 3.10
8	Brain_CLX	Engineering	Solidworks	Solidworks	2021 SP2.0
9	Brain_CLX	Office	Microsoft	Microsoft 365 Apps for Business	Version 2203 (15028.20160)

3.3 Hardware and Software Maintenance and Ownership

All Hardware and Software are maintained by SoftInWay, Inc.

4. Requirements

4.1 Access Control

4.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The implementation of the requirement is based on the following means: enforce password policies for accounts; enforce multi-factor authentication; users are required to logon to gain access; authorization of account requests before system access is granted; bookkeeping of the list of authorized users, defining their identity and role and sync with system, application, and data layers.

User access security refers to the set of procedures by which authorized users access the system and unauthorized users are prevented from accessing the system.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

In the system, SoftInWay uses access control lists to limit access to applications and data based on role and/or identity.

The system allows for the separation of access control rights and enforcement of those rights.

Even authorized users are restricted to those parts of the system that they are explicitly permitted to use. This is based on their “need-to-know” and their role within the company.

4.1.3 Control the flow of CUI in accordance with approved authorizations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay controls the flow of CUI physically and electronically.

Physically, SoftInWay has locking doors, key cards, and keys to access our office space and separate offices for accessing sensitive data. Guest and visitors are escorted to conference rooms and are never left alone with company resources. We also assure everyone with access to the data has been cleared via appropriate channels for that access and to what level of access they need.

Electronically, SoftInWay has architectural solutions to control the flow of the system data. The information flow control enforcement is documented by using a protected processing level as a basis for flow control decisions.

The solution includes firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who is allowed to access the information) without explicit regard to subsequent access to that information. The export-controlled information is kept from being transmitted in the clear to the internet. The outside traffic that claims to be from within the organization is blocked. The web requests to the internet that are not from the internal web proxy server are restricted. The information transfers between organizations are limited based on data structures and content. Information transfers between interconnected systems are prohibited. The hardware mechanisms are employed to enforce one-way information flows. The trustworthy regrading mechanisms are implemented to reassign security attributes and security labels.

SoftInWay employs information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, in boundary protection devices (routers, encrypted tunnels, and firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message filtering capability based on message content (e.g., implementing keyword searches or using document characteristics).

4.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay creates separate accounts with appropriate access levels to separate functions for every user that accesses the data and maintains the system in some way.

The responsibilities and duties of individuals are separated to eliminate conflicts of interest. In particular:

- Project objective functions and information support functions are divided among different individuals and/or roles
- The information support functions are conducted by different individuals
- Security personnel administering access control functions do ~~not~~ also administer audit functions
- Audit Logon Events policy defines the auditing of every user attempt to log on to or log off from a computer.

4.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay only grants enough privileges to users to allow them to do their job.

SoftInWay restricts access to privileged functions and security information to authorized employees only.

According to the principle of least privilege in SoftInWay every process, user, or program can only access the information and resources that are needed for its valid purpose. Any process, program, or user account gets only those privileges that are essential for it to perform its intended function.

4.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Users with multiple accounts (privileged and nonprivileged) typically logon with the least privileged account when not performing privileged functions.

Users with privileged access are required to use nonprivileged accounts when accessing other system functions.

Administrators of multi-user systems, systems that allow for concurrent usage of the system by multiple persons, have at least two user credentials. One of these user credentials provides privileged access, with all

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

activities logged; the other one is a normal user credential for performing the day-to-day work of an ordinary user.

Users of information system accounts, or roles, with access to sensitive information, use non-privileged accounts or roles when accessing non-privileged functions. This control enhancement limits exposure when operating from within privileged accounts or roles.

4.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

In the system, all privileged functions are audited.

The execution of privileged functions by non-privileged users is prevented.

The access is controlled by using the access control lists based on the identity or role of the user.

Administrators of multi-user systems, systems that allow for concurrent usage of the system by multiple persons, have at least two user credentials. One of these user credentials provides privileged access, with all activities logged; the other one is a normal user credential for performing the day-to-day work of an ordinary user.

Users of information system accounts, or roles, with access to sensitive information, use non-privileged accounts

4.1.8 Limit unsuccessful logon attempts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system is configured to limit the number of invalid logon attempts.

The system is configured to lock the logon mechanism for a predetermined time (24 hours) after 5 invalid logon attempts.

The system is configured to lock users out after 5 invalid logon attempts.

The system enforces a limit of a defined number of consecutive invalid access attempts during 24 hours.

4.1.9 Provide privacy and security notices consistent with applicable CUI rules.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The logon screen display privacy and security notices upon initial logon.

The system displays the system use information before granting access.

The system ensures that any references to monitoring, recording, or auditing are consistent with the privacy accommodations.

The system includes a description of the authorized uses of the system.

The system use notifications are implemented using warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users.

4.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system is configured to lock sessions after 5 minutes of inactivity.

The pattern hiding display is used when sessions are locked.

The users can lock sessions for temporary absences.

The system session lock mechanism places a publicly viewable pattern onto the screen, hiding what was previously visible on the screen.

It is important to point out that none of the static or dynamic images used with screen savers contains sensitive information.

4.1.11 Terminate (automatically) a user session after a defined condition.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system is configured to automatically end a user session after 72 hours of inactivity. Such a long duration is selected based on the need to run time-consuming calculations, which might take weeks to complete. if the session ends then the calculations stops. However, if the session locks the calculation can continue, and a user

logon again within 72 hours to check the progress of the calculation. This rule enables the opportunity to run week-long calculations.

The user sessions terminated automatically based upon SoftInWay defined conditions.

4.1.12 Monitor and control remote access sessions.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

SoftInWay does not allow remote access to the system because remote access client devices generally have weaker protection than standard client devices. The remote access restriction in the system is enforced by disabling the default Windows Remote Desktop application and by disabling the capability to install any third-party remote desktop application.

4.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

SoftInWay does not allow remote access to the system.

4.1.14 Route remote access via managed access control points.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

SoftInWay does not allow remote access to the system.

4.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

SoftInWay does not allow remote access to the system.

4.1.16 Authorize wireless access prior to allowing such connections.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

The system has wireless devices.

The use of wireless technologies in the system is not approved by the company management and thus they are not used within the system. This is enforced by disabling the wireless broadcasting on the wireless routers and wireless devices without the privilege to enable it by unauthorized personnel.

4.1.17 Protect wireless access using authentication and encryption.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

The use of wireless technologies in the system is not approved by the company management and thus they are not used within the system.

4.1.18 Control connection of mobile devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has established guidelines for the use of mobile devices, including smarphones, tablets, laptops, and alike.

SoftInWay restricts the operation of mobile devices to the guidelines.

The usage of mobile devices is monitored and controlled.

The mobile device connection to the system is not allowed.

The requirements for mobile device connection to the system are enforced.

4.1.19 Encrypt CUI on mobile devices and mobile computing platforms.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

This requirement is not applicable because the mobile device connection to the system is not allowed.

4.1.20 Verify and control/limit connections to and use of external systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

This requirement is not applicable because the connection of external information systems is not permitted.

4.1.21 Limit use of organizational portable storage devices on external systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay restricts the use of SoftInWay controlled portable storage devices by authorized individuals on external information systems per our Data Encryption and Transmission Policy. Limits on the use of SoftInWay -controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

4.1.22 Control CUI posted or processed on publicly accessible systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

SoftInWay does not post or process CUI on publicly accessible systems. All CUI is posted and processed in a restricted area of the network which requires passwords and authentications.

4.2 Awareness and Training

4.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities.

The training provides a basic understanding of the need for information security, applicable policies, standards, and procedures related to the security of the information system, as well as user actions to maintain security and respond to suspected security incidents

SoftInWay employees working in our virtual environment receive NIST SP 800-171 information security training and potential indicators of insider threat.

The basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter training also addresses awareness of the need for operations security.

Employees with security-related responsibilities receive information security training.

Training records are maintained and reviewed per our ISO AS9100 and 9001 certifications policy P-008 Training.

4.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities.

The training addresses required security requirements related to environmental and physical security risks.

The training includes indications of potentially suspicious email or web communications.

The security-related technical training is provided before authorizing access to the system or performing assigned duties when required by system changes and on a periodic basis.

4.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threat, e.g., long-term job dissatisfaction, attempts to gain unauthorized access to information, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies.

The security training includes how to communicate employee and management concerns regarding potential indicators of insider threat.

The practical exercises are included in security awareness training that simulates actual cyber-attacks.

Security-related technical training is provided before authorizing access to the system or performing assigned duties when required by system changes and on a periodic basis.

4.3 Audit and Accountability

4.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system provides alert functions.

The company performs audit analysis and review of the system events.

The company creates, protects, and retains information system audit records for between 30 days and 1 year (depending on the data source and applicable regulations) to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

The appropriate mechanisms are used to integrate audit review, analysis, and reporting to processes for investigation and response to suspicious activity.

4.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Logs for the SoftInWay system uniquely trace each occurrence to a specific user, time, and computer ID used to allow users can be held accountable for their actions. Logs include the date and time of the event, the relevant user or process, the event description, and the SoftInWay equipment or software involved are recorded.

The system protects against an individual denying having performed an action (non-repudiation).

4.3.3 Review and update logged events.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Event logs are reviewed and analyzed weekly. The company has special rules on logging specific details, log retention, and weekly log review procedures. These records are maintained and reviewed per our ISO AS9100 and 9001 certifications.

The reviews ensure that the information system can audit events, coordinate with other company entities requiring audit-related information, and provide a rationale for why auditable events are deemed adequate to support security investigations.

The list of defined auditable events is reviewed by company management and updated on a regular basis.

4.3.4 Alert in the event of an audit logging process failure.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system will alert employees with security responsibilities in the event of an audit processing failure.

The system maintains audit records on local workstation.

There is a real-time alert when any defined event occurs.

4.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The company uses proper mechanisms across different repositories to integrate audit review, analysis, correlation, and reporting processes.

The mechanisms support processes for investigation and response to suspicious activities, as well as gain company-wide situational awareness.

The mechanisms are used to integrate audit review, analysis, and reporting to processes for investigation and response to suspicious activity.

4.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system provides an audit reduction and report generation capability.

The system supports on-demand audit review, analysis, and reporting requirements and after-the-fact security investigations.

The information system alters the original content or time-ordering of audit records if required.

There is the capability to process audit records for events of interest based on selectable event criteria, such as user identity, event type, location, times, dates, system resources, or information object accessed.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Clocks on all computers connected to the SoftInWay system have clocks set to the local time zone automatically via Windows 10. This can not be changed by local users ensuring that the timestamps on documents are accurate.

4.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Audit logs are protected from accidental or unauthorized modification, destruction, or disclosure through policies, limiting access to only authorized users, data is stored in restricted areas only accessible by authorized users, awareness training, software, or hardware that ensure data is accurate, available, and accessed only by those authorized.

4.3.9 Limit management of audit logging functionality to a subset of privileged users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The access to management of audit functionality is authorized only to a limited subset of privileged users.

The audit records of nonlocal accesses to privileged accounts and the execution of privileged functions are protected.

4.4 Configuration Management

4.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The baseline configurations are developed, documented, and maintained for each information system type.

The baseline configurations include software versions and patch level, configuration parameters, network information including topologies, and communications with connected systems.

The baseline configurations are updated as needed to accommodate security risks or software changes.

The baseline configurations are developed and approved in conjunction with the Chief Information Security Officer (CISO) or equivalent and the information system owner.

The deviations from baseline configurations are documented.

The system is managed using a system development life-cycle methodology that includes security considerations.

4.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The security settings are included as part of baseline configurations.

The security settings reflect the most restrictive settings appropriate.

The changes or deviations from baseline configurations are documented.

4.4.3 Track, review, approve or disapprove, and log changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay tracks, reviews, approves, or disapproves, and logs changes to our organizational systems consistent with our ISO AS9100 and 9001 certification requirements.

The configuration-managed changes to the system are audited by company personnel.

Changes to information systems include modifications to hardware, software, or firmware components and configuration settings. SoftInWay ensures that testing does not interfere with information system operations. Individuals/groups conducting tests understand company security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with facilities/processes.

Operational systems are taken off-line or replicated to the extent feasible before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

Changes to information systems are reviewed and approved by company management prior to implementation.

4.4.4 Analyze the security impact of changes prior to implementation.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay analyzes the risks and security impact of changes to our systems consistent with our ISO AS9100 and 9001 certification requirements.

The changes that affect system security requirements are tested prior to implementation.

The testing of the effectiveness of the changes is performed.

Exclusively those changes that continue to meet compliance requirements are approved and implemented.

The configuration changes are tested, validated, and documented before installing them on the operational system.

The testing is ensured to not interfere with system operations.

Employees with information security responsibilities conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/ technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis includes reviewing security plans to understand security control requirements and reviewing system design documentation to understand requirement implementation and how specific changes might affect the requirements. Security impact analyses also include assessments of risk to better understand the impact of the changes and to determine if additional security requirements are required. Security impact analyses are scaled in accordance with the security categories of the information systems.

4.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Only employees who are approved to make physical or logical changes to systems are allowed to do so.

The authorized personnel is approved and documented by the service owner and IT security.

All change documentation includes the name of the authorized employee making the change.

SoftInWay maintains records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The information system is configured to exclude any function not needed in the operational environment. It delivers one function per system, where practical.

The system employs processing components that have minimal functionality and data storage.

4.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Only those ports and protocols are necessary to provide the service of the information system configured for that system.

Only applications and services that are needed for the function of the system are configured and enabled.

The systems services are reviewed to determine what is essential for the function of that system.

SoftInWay disables unused or unnecessary physical and logical ports/ protocols (e.g., Universal Serial Bus, File Transfer Protocol, and HyperText Transfer Protocol) on information systems to prevent unauthorized connection of devices, and unauthorized transfer of information, or unauthorized tunneling. SoftInWay utilizes network scanning tools, intrusion detection, and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

4.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The information system is configured to only allow authorized software to run.

The system is configured to disallow running unauthorized software.

SoftInWay has a defined list of software programs authorized to execute on the system.

The authorization policy is a deny-all, permit by exception for software allowed to execute on the system. It is reviewed annually.

The automated mechanisms are used to prevent program execution in accordance with defined lists.

4.4.9 Control and monitor user-installed software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The user controls are in place to prohibit the installation of unauthorized software.

All software in use on the information systems is approved.

4.5 Identification and Authentication

4.5.1 Identify system users, processes acting on behalf of users, and devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system uses the company-assigned accounts for unique access by individuals.

SoftInWay central identity team when needed creates a service account that is assigned to a member of the service team to perform service duties to separate it from the system users.

SoftInWay user and service accounts are managed centrally and deleted automatically when an individual leaves the company.

4.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The accounts in use are assigned and managed by the company's central identity management system.

The accounts are provisioned as part of the established account creation process.

The accounts are uniquely assigned to new employees, contractors, or subcontractors upon hire.

The initial passwords are randomly generated strings provided via a password reset mechanism to each employee.

The password resets upon first use.

All passwords follow the best practice of at least 12 characters and require a mix of upper and lower case letters, numbers, and special characters.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system uniquely identifies and authenticates users.

Multifactor authentication is used for local access to privileged accounts.

Network access is not permitted in the system.

4.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Network access is not permitted in the system.

4.5.5 Prevent reuse of identifiers for a defined period.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The accounts in use are assigned and managed by the company's central identity management system.

The accounts are provisioned as part of the established account creation process.

The accounts are uniquely assigned to employees, contractors, and subcontractors.

The user account names are different than email user accounts.

4.5.6 Disable identifiers after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The user accounts or identifiers are monitored for inactivity.

The user or device identifiers are disabled after 30 days of inactivity.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The company specifies a degree of complexity, e.g., the account passwords are a minimum of 12 characters and a mix of upper/lower case, numbers, and special characters, including minimum requirements for each type.

The company requires a change of characters when new passwords are created.

4.5.8 Prohibit password reuse for a specified number of generations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The passwords can be re-used after 730 days or after 20 password changes.

The users can re-use the same password when changing their password for at least 50 % of changes.

Password reuse is prohibited for 20 generations.

The passwords are unique to the organization’s systems and not re-used on external information systems.

4.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

New employees receive an account and instructions for creating a password during the hiring process.

New employees receive notification of their account and are required to reset their initial passwords.

Temporary password activation links are sent to validated employees should they require a password reset or change.

The temporary passwords are only good to allow for a password reset.

The system enforces an immediate password change after logon when a temporary password is issued, e.g., a lost or forgotten password.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.5.10 Store and transmit only cryptographically-protected passwords.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The passwords are prevented from being stored in reversible encryption form in any company system.

The passwords are stored as one-way hashes constructed from passwords.

The company follows the best practice of “salting” hashed passwords.

The passwords are encrypted in storage and in transmission.

4.5.11 Obscure feedback of authentication information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The authentication mechanisms obscure feedback of authentication information during the authentication process.

The authentication mechanisms do not return any system-specific information such as “wrong password” or “wrong username”.

4.6 Incident Response

4.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has established the Data Protection Group (DPO). The DPO has created the Data Breach Reporting Policy which lays out our incident-handling capability involving CUI, and how SoftInWay would prepare, detect, analyze, contain and recover any lost data and identify the users responsible for the breach.

4.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has an incident response policy that specifically outlines requirements for tracking and reporting incidents involving CUI to appropriate officials.

The cybersecurity incident information is promptly reported to company management and authorities.

The security incidents related to industrial control systems security incidents are promptly reported to company management and authorities.

The employees are required to report suspected security incidents to the company's incident response authority within 1 hour.

4.6.3 Test the organizational incident response capability

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has an incident response policy, that outlines requirements for regular testing and reviews/improvements to incident response capabilities.

SoftInWay tests its incident response capabilities. Tests include the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises.

4.7 Maintenance

4.7.1 Perform maintenance on organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

IT system maintenance tools (e.g., tools used for diagnostics, scanners, and patching tools) are managed.

SoftInWay has a list of approved tools and their access and location are controlled.

All systems, devices, and supporting systems for the company are maintained per manufacturer recommendations or company-defined schedules.

SoftInWay performs maintenance on the information system.

SoftInWay management approves maintenance activities.

4.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The controls are in place that limit the tools, techniques, mechanisms, and employees used to maintain information systems, devices and supporting systems.

4.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has a media sanitization policy.

The media that are removed from the premises for maintenance, repair, or disposal are sanitized per the company's media sanitization policies.

4.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The media that are provided by authorized maintenance personnel (and not normal systems administrators/owners) for troubleshooting, diagnostics, or other maintenance are run through an anti-virus/anti-malware/anti-spyware program prior to use in the company's information system.

The results of the scans are documented in the maintenance logs. All media provided by authorized maintenance personnel is scanned for malware.

4.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Remote access to a system is prohibited for users. However, when required for maintenance all remote access to a system for maintenance or diagnostics occurs via an approved remote solution using multifactor authentication (Anydesk).

All sessions and remote connections are terminated when remote maintenance is completed.

4.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All activities of maintenance personnel (who do not normally have access to a system) are monitored.

SoftInWay has approved methods for supervision.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.8 Media Protection

4.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The responsible parties for data in these systems are documented and ensured proper authorization controls for data in media and print.

The documented workflow, data access controls, and media policy are enforced to ensure proper access controls.

The system media is securely stored in protected areas.

Only approved individuals have access to media from CUI systems.

An audit log of any media is removed from these systems.

4.8.2 Limit access to CUI on system media to authorized users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All CUI systems are managed under the least access rules.

The company limits CUI media access to authorized users.

4.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All managed data storage is erased, encrypted, or destroyed using mechanisms to ensure that no user data is retrievable.

The system's digital and non-digital media are sanitized before disposal or release for reuse.

All CUI data on media is encrypted or physically locked prior to transport outside of the company’s secure locations.

4.8.4 Mark media with necessary CUI markings and distribution limitations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All CUI systems are identified with an asset control identifier.

The removable system media and system output are marked.

4.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Only approved individuals have access to media from CUI systems. The audit log of any media is removed from these systems.

The accountability for system media is maintained during transport outside controlled areas.

4.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All CUI data on media are encrypted or physically locked prior to transport outside of the company.

The cryptographic mechanisms are used to protect digital media during transport outside of controlled areas.

The utilized removable media support physical encryption.

The key vaulting is utilized to ensure recoverability.

The data backups are encrypted on media before removal from the company's secured facility.

The utilized cryptographic mechanisms comply with FIPS 140-2.

4.8.7 Control the use of removable media on system components.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The use of writable, removable media is restricted on the system.

The removable media are not allowed in the system.

4.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Portable storage devices are prohibited in the system.

4.8.9 Protect the confidentiality of backup CUI at storage locations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The data backups are encrypted on media before removal from a secured facility.

The confidentiality and integrity of backup information are protected at the storage location.

The data backups are encrypted on media before removal from the company's secured facility.

The utilized cryptographic mechanisms comply with FIPS 140-2.

4.9 Personnel Security

4.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay uses E-Verify for all employees hired after 2020. This ensures their identity is verified prior to granting them access to the basic computer system. Additional access is granted after authorized staff is sufficiently trained on how to handle the CUI.

4.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay disables information system access prior to employee termination or transfer.

SoftInWay revokes authenticators/credentials associated with the employee upon termination or transfer within 24 hours.

The company retrieves all company information system-related property from the terminated or transferred employee within 24 hours.

The company retains access to company information and information systems formerly controlled by the terminated or transferred employee within 24 hours.

The company notifies the information security office and data owner of the change in authorization within 24 hours.

The electronic and physical access permissions are reviewed when employees are reassigned or transferred.

4.10 Physical Protection

4.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The facility/building manager designates building areas as "sensitive" and designed physical security protections (including guards, locks, cameras, card readers, etc.) to limit physical access to the area to only authorized employees.

The output devices such as printers are placed in areas where their use does not expose data to unauthorized individuals.

The lists of personnel with authorized access are developed and maintained, and are appropriate authorization credentials issued

4.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The facility/building manager reviewed the location and type of physical security in use (including guards, locks, card readers, etc.) and evaluated its suitability for the company's needs.

The physical access is monitored to detect and respond to physical security incidents.

4.10.3 Escort visitors and monitor visitor activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All visitors to sensitive areas are always escorted by an authorized employee.

The visitors are escorted and monitored as required in security policies and procedures.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.10.4 Maintain audit logs of physical access.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The logs of physical access to sensitive areas are maintained per retention policies.

The visitor access records are retained for as long as required by the approved policy.

4.10.5 Control and manage physical access to devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay maintains an office at the address listed above. This space has locking doors, a separate office for SoftInWay staff, and locking file cabinets. Physical access to SoftInWay property such as electronic devices, computers, network hardware, and data is limited to staff with approved access to specific offices in our space. Offices are locked when no one is working in them to limit access to the devices.

The physical access devices (such as card readers, proximity readers, and locks) are maintained and operated per the manufacturer recommendations. These devices are updated with any changed access control information necessary to prevent unauthorized access.

The facility/building manager reviews the location and type of each physical access device and evaluates its suitability for the company's needs.

The keys, combinations, and other physical access devices are secured.

4.10.6 Enforce safeguarding measures for CUI at alternate work sites.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

SoftInWay does not allow staff to with CUI at alternate work sites.

4.11 Risk Assessment

4.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

As part of SoftInWay's IOS AS9100 and 9001 Certifications, SoftInWay completed internal audits per our Internal Audit Schedule which assessed our organizational operations, assets, staff, risks assessments of business silos, processing of all data, and project execution. Results are discussed at the Management Review and changes are implemented as required.

4.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The vulnerability scanning is performed.

The systems are periodically scanned for common and new vulnerabilities.

The previously undocumented vulnerabilities risks are assessed and documented.

The reports regarding the scans are made available to system owners and company management in a timely manner.

The vulnerability scans are performed on a defined frequency or randomly in accordance with company policy.

The list of scanned system vulnerabilities is updated on a defined frequency or when new vulnerabilities are identified and reported.

4.11.3 Remediate vulnerabilities in accordance with risk assessments.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system owners and company managers upon recognition of any vulnerability provide an action plan for remediation, acceptance, avoidance, or transference of the vulnerability risk. The plan includes a reasonable time frame for implementation.

All high vulnerabilities are prioritized.

The Plan of Action calls out remedial security actions to mitigate risk to company operations, assets, employees, and other organizations.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.12 Security Assessment

4.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

As part of SoftInWay's AS9100 and 9001 Certifications, SoftInWay completed internal audits per our Internal Audit Schedule which assessed our organizational operations, assets, staff, risks assessments of business silos, processing of all data, and project execution. Results are discussed at the Management Review and changes are implemented as required.

The periodic security assessment is conducted to ensure that security controls are implemented correctly and meet the security requirements.

The assessment scope includes all information systems and networks, including all security requirements and procedures necessary to meet the compliance requirements of the environment.

The assessment includes, but is not limited to, vulnerability scanning, penetration testing, security control testing and reviews, configuration testing and reviews, log reviews, and talking with company employees.

The assessment is conducted by company employees.

The final written assessment report and findings are provided to company management after the assessment.

4.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

As part of SoftInWay's AS9100 and 9001 Certifications, SoftInWay completed internal audits per our Internal Audit Schedule which assessed our organizational operations, assets, staff, risks assessments of business silos, processing of all data, and project execution. Results are discussed at the Management Review and changes are implemented as required.

SoftInWay keeps an action plan to remediate identified weaknesses or deficiencies.

The action plan is maintained as remediation is performed.

The action plan designates remediation dates and milestones for each item.

The deficiencies and weaknesses identified in security requirements assessments are added to the action plan within a specified timeframe (e.g., 30 days) of the findings being reported.

4.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

As part of SoftInWay's AS9100 and 9001 Certifications, SoftInWay completed internal audits per our Internal Audit Schedule which assessed our organizational operations, assets, staff, risks assessments of business silos, processing of all data, and project execution. . Results are discussed at the Management Review and changes are implemented as required.

The continuous monitoring tools are deployed for front internet-facing systems (computers with IP addresses that can be reached from the internet) or those used to store or transmit sensitive data. At a minimum, these systems are monitored for privileged access, permission changes, kernel modifications, and binary changes against a control and system baseline.

The continuous monitoring reports and alerts are reviewed frequently daily.

The unauthorized changes or unauthorized access is reported to company management and information system owner within 24 hours of it being discovered.

SoftInWay has an assessor or assessment team to monitor the security requirement in the system on an ongoing basis.

4.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system security plans are consistent with the organization's enterprise architecture.

The system security plan explicitly defines the authorization boundary for the system.

The system security plan describes the operational context of the system in terms of missions and business processes.

The system security plan describes the operational environment for the system.

The system security plan describes relationships with or connections to other systems.

The system security plan provides an overview of the security and privacy requirements for the system.

The system security plan describes the security requirements in place.

The system security plan includes plans for meeting those requirements when they are not in place.

The system security plan is reviewed and approved by company management prior to plan implementation.

The copies of the system security plan are distributed to relevant company employees.

The changes to the system security plan are communicated to relevant company employees.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

SoftInWay annually reviews the system security plan within a certain timeframe.

SoftInWay updates the system security plan to address changes to the system, environment of operation, or problems identified during plan implementation or security assessments.

SoftInWay protects the system security plan from unauthorized disclosure and modification.

SoftInWay plans and coordinates security-related activities affecting the system before conducting any such activities.

The security-related activities are planned to reduce the impact on other company entities.

4.13 System and Communications Protection

4.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has an identified network communications boundaries.

The system monitors and manages communications at the system boundary and key internal boundaries within the system.

SoftInWay has policies for managed interfaces such as gateways, routers, firewalls, VPNs, and company DMZs restrict external web traffic to only designated servers.

4.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay's information security policies (including architectural design, software development, and system engineering principles) are designed to promote information security.

The policies are adequate to meet the needs of the company.

The system security engineering principles are applied in the specification, design, development, and implementation of the system.

The system is managed using a system development life-cycle methodology that includes security considerations.

4.13.3 Separate user functionality from system management functionality.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The physical or logical controls are used to separate user functionality from system management-related functionality.

The user functionality is separated from the system management functionality.

SoftInWay implements separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate.

4.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The requirements are implemented to prevent object reuse and to protect residual information.

The system prevents unauthorized or unintended information transfer via shared system resources, e.g., register, main memory, and secondary storage.

4.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay implements DMZs, that are adequate to meet the needs of the company.

The system monitors and manages communications at the system boundary and at key internal boundaries within the system.

4.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All exceptions to network communications traffic (inbound/outbound) “deny all” policies are documented.

The system denies network traffic by default and allows network traffic by exception.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The controls are in place to prevent split tunneling in remote devices, and to mandate VPN use when necessary for business functions.

The system prevents remote devices that have established connections (e.g., remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks.

4.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The cryptographic mechanisms are used to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

The processes and automated mechanisms are used to provide encryption of CUI during transmission.

All alternative physical safeguards used to provide confidentiality of CUI during transmission are documented.

4.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system terminates a network connection at the end of a session or after a defined timeframe of inactivity.

4.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The processes and automated mechanisms are used to provide key management within the information system.

SoftInWay, Inc.
20 Burlington Mall Road, Suite 450
Burlington, MA 01803
781-328-4310

4.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

FIPS-validated cryptography is used to protect CUI.

4.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The collaborative computing devices (e.g., cameras, microphones, etc.) are configured so they cannot be remotely activated.

The users are notified when collaborative computing devices are in use.

4.13.13 Control and monitor the use of mobile code.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has defined limits of mobile code usage and established usage restrictions, that specifically authorizes the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript, etc.) within the information system.

The use of mobile code is documented, monitored, and managed.

4.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The use of VoIP is controlled.

The use of VoIP is authorized and monitored.

4.13.15 Protect the authenticity of communications sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has controls in place to protect session communications.

The system provides proper mechanisms to protect the authenticity of device-to-device communications sessions.

4.13.16 Protect the confidentiality of CUI at rest.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay has controls used to protect CUI while stored in company information systems.

The system protects the confidentiality of information at rest.

4.14 System and Information Integrity

4.14.1 Identify, report, and correct system flaws in a timely manner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The system flaws are identified, reported, and corrected within company-defined time periods.

SoftInWay performs all security-relevant software updates (patching, service packs, hotfixes, and anti-virus signature additions) in response to identified system flaws and vulnerabilities within the timeframe specified in the policy.

When available, the managers and administrators of the system rely on centralized management of the flaw remediation process, including the use of automated update software, patch management tools, and automated status scanning.

The time between flaw identification and flaw remediation is measured and compared with benchmarks.

4.14.2 Provide protection from malicious code at designated locations within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay employs malicious code protection mechanisms at system entry and exit points to minimize the presence of malicious code.

The system automatically updates malicious code protection mechanisms.

4.14.3 Monitor system security alerts and advisories and take action in response.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay receives security alerts, advisories, and directives from reputable external organizations.

SoftInWay disseminates this information to individuals with need-to-know in the company.

Alerts are responded to promptly.

The internal security alerts, advisories, and directives are generated.

4.14.4 Update malicious code protection mechanisms when new releases are available.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay updates information system protection mechanisms within 5 days of new releases. These updates are completed in accordance with configuration management policy and procedures.

4.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay performs periodic scans of the information system for malware. The scans are performed within the timeframe specified in the policy.

SoftInWay performs real-time scans of files from external sources as the files are downloaded, opened, or executed.

The system disinfects and quarantines infected files.

4.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay monitors the information system to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

SoftInWay strategically deploys monitoring devices within the information system to collect essential information. The information gained from these monitoring tools is protected from unauthorized access, modification, and deletion.

The system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

4.14.7 Identify unauthorized use of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SoftInWay monitors the information system to identify unauthorized access and use.

SoftInWay monitors the information for potential misuse.

The unauthorized use of the system is identified by log monitoring.