
**Iseehear Inc. Life Sciences**

Turning Data into Scientific Insight

# Written Information Security Program

## Document History

| Revision Number | Date | Reviewed By | Comments |
|---|---|---|---|
| 1.0 | 11/2/2021 | John Conroy, vCISO | Conversion of Individual Policies in a single document (WISP) |
| 2.0 | 1/28/2022 | John Conroy, vCISO | Updated Backup locations |
| | | | |

Approved by: _____ Signature _____

Jimmy Ayers, Chairman

# Table of Contents

# Written Information Security Policy

## INTRODUCTION

Like all companies that handle Confidential information such as Personally Identifiable Information (PII) and Personal Health Information (PHI), Iseehear Inc. Life Sciences (ISH) is exposed to a variety of organizational risks to include but not limited to: operational, legal/regulatory, Physical, technical, financial, and risks involving fraud. Additionally, because of the nature and amount of information gathered regarding ISH's customer's data and the extensive use of technology to process this information, ISH is exposed to specific information and technology risks.

ISH works to comply with Information Security frameworks such as HIPAA, NIST, ISO 27001, and many state and federal requirements have come up with a set of standards surrounding best practices for information security. These standards recommend (and in some cases for state laws require) that each company implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the organization and the nature and scope of its activities. This allows a uniform set of information security expectations to be followed throughout the different areas of the organization, and provide a consistent, repeatable set of documentation to create procedures and processes with.

## PURPOSE

The primary purposes of ISH's Information Security Program are to ensure that the organization, the Executive Management Team and Staff:

- Understand the risks and threats to which information systems are exposed,
- Evaluate the potential exposures to such risks / threats
- Implement appropriate information security systems and administrative, technical, and physical security controls to mitigate such risks, threats, and exposures, and test the efficacy of information security systems and controls
- Ensure the accuracy, integrity, security, and confidentiality of customer information received, processed, and maintained by ISH.
- Ensure that such information, and proprietary Company information, is adequately protected against anticipated threats or hazards to its security or integrity.
- Protect against unauthorized access to or use of customer and proprietary information that might result in substantial harm or inconvenience to any customer or present a safety and soundness risk to the Company.
- Provide for the timely and comprehensive identification and assessment of vulnerabilities and risks that may threaten the security or integrity customer and proprietary information.
- Document Policy standards for managing and controlling identified risks.
- Provide standards for testing the Policy and adjust on a continuing basis to account for changes in technology, sensitivity of customer information, and internal or external threats to information security.
- Specify the various categories of Information Systems data, equipment, and processes subject to comprehensive Information Security Procedures.
- Ensure the Company complies with all relevant regulations, common law, explicit agreements, or conventions that mandate the security and confidentiality of customer information.

• Ensure protection of the hardware and software components that comprise ISH's Information Systems.
• Protect against the use of ISH's assets in a manner contrary to the purpose for which they were intended, including the misallocation of valuable organizational resources, threats to the Company's reputation or a violation of the law.

## SCOPE

The ISH Information Security Policy applies to all the users in the Organization, including contractors, temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency. The policies in this document, unless otherwise indicated, apply to all electronic systems and applications in place and in use at ISH

## RESPONSIBILITIES

| Role | Responsibility |
|---|---|
| Staff | Use information resources with good judgment and in compliance with information security policies and report any inappropriate use of information resources to the Information Security Program Officer. |
| Management | Ensure that personnel understand and agree to the policies in the Information Security Program. |
| Business Owners | Implement measures to protect their resources and monitor them against inappropriate use. |
| TechOps/IT Staff | Help to implement security solutions in compliance with this policy and assist business owners implementing measures to protect their resources against inappropriate use. |
| Chief Information Security Officer | Maintain the information security program and monitor compliance with the Information Security Policies within the program. |

## ENFORCEMENT

Personnel using ISH's information resources in opposition to these policies may be subject to limitations on the use of these resources, suspension of privileges (including internet access), as well as disciplinary and/or legal action, including termination of employment.

Employees, contractors, consultants, temporaries, and all personnel affiliated via third parties shall sign an agreement to comply and be governed by this policy and the ISH Information Security Policies upon hire and again annually.

## GENERAL POLICY DEFINITIONS

To comply with regulatory guidelines, a company's information security program should be designed to:

- Ensure the security and confidentiality of customer information

- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Information Security Committee is required to be involved in the development and implementation of the Information Security Program. The Leadership Committee must oversee the development, implementation, and maintenance of the ISH's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

The Information Security Program will be reviewed, updated, and approved by the Executive Vice President and the CISO with input from the IT Steering Committee on an annual basis.

In connection with this general Information Security Policy presented above, ISH has also adopted the following specific policies. The policies are presented below to provide a comprehensive program.

*POL-01 – IT Acceptable Use Policy*
*POL-02 – Problem Management Policy*
*POL-03 – Segregation of Duties Policy*
*POL-04 – Vendor/Third Party Management Policy*
*POL-05 – Endpoint Protection Policy*
*POL-06 – Encryption Policy*
*POL-07 – Information Protection Policy*
*POL-08 – Internet Security Policy*
*POL- 09 – Mobile Devices Policy*
*POL- 10 – Password Management Policy*
*POL- 11 – Security Training and Awareness Policy*
*POL- 12 – Incident Response Policy*
*POL- 13 – Information Classification Policy*
*POL- 14 – Information Disposal Policy*
*POL- 15 – Information Retention Policy*
*POL- 16 – Access Control Policy*
*POL- 17 – Remote Access Policy*
*POL- 18 – Physical and Environmental Security Policy*
*POL- 19 – Audit, Logging, and Monitoring Policy*
*POL- 20 – Risk Assessment Policy*
*POL- 21 – Network Device Configuration Policy*
*POL- 22 – Server and System Configuration Policy*
*POL- 23 – Systems Acquisitions and Development Policy*
*POL- 24 – Change Management Policy*
*POL- 25 – Patch Management Policy*
*POL- 26 – Backup and Recovery Policy*
*POL- 27 – Business Resiliency Policy*
*POL- 28 – Asset Management Policy*

*POL- 29 – Vulnerability and Penetration Testing Policy*
*POL- 30 – Data Breach Policy*
*POL-31 – Personal Device Policy*
*POL-32 - Third Party Access Policy*
*POL-33 – Social Media Policy*

# POL-01 – IT Acceptable Use Policy

**PURPOSE**

This policy outlines the acceptable use of information resources at ISH and applies to employees, contractors, consultants, temporaries, and other staff at ISH, including all personnel and affiliated via third party contractors. This policy applies to all data and equipment that is owned or leased by ISH.

The purpose of this policy is to protect employees, partners and the company against internal and/or external exposure of confidential information, malicious activity, including the compromise of systems and services, legal issues, financial loss, and damage to reputation by individuals, either knowingly or unknowingly.

**SCOPE**

Personnel using data and information resources (including but not limited to Internet/Intranet/Extranet-related and core systems, computer equipment, software, operating systems, storage media, and network accounts providing electronic messaging), must use them for business purposes in accordance with their job functions and responsibilities, serving the interests of the company and the customers in a legal, ethical, responsible, and secure manner, with respect for the rights of others.

**POLICY**

It is the responsibility of every user of information resources to know the Information Security Policies and the acceptable use of information resources, and to conduct their activities accordingly.

**General Use**

- Safeguard user accounts and passwords, and use them only as authorized
- Respect all pertinent licenses, copyrights, contracts, as well as other restricted and proprietary resources
- To accommodate employees, ISH understands employees will access the Internet for personal needs periodically
- It is expected that employees will exercise good judgment regarding the reasonableness of personal use and any question regarding appropriate use will be decided by management.
- Notify the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents.
- Secure all unattended workstations from unauthorized viewing or use.

- All workstations must be configured to automatically lock after 15 minutes of inactivity and users should log off or lock their machines during extended periods of inactivity.

**Unacceptable Use**

The following unacceptable activities are by no means exhaustive, but attempt to provide a framework for activities that are strictly prohibited:

- Damaging computer systems
- Preventing another user from authorized resources
- Accessing unauthorized systems or data resources, or utilizing functions that are not necessary for the performance of the employee's duties
- Revealing account passwords to others. Employees who receive usernames and passwords must keep their usernames and passwords confidential and must not share that information with others.
- Using another person's computer account, with or without their permission
- Providing information about employees to parties outside the company
- Providing protected customer or vendor information to any unauthorized person
- Intentionally corrupting, misusing, or stealing software or any other computing resource
- Sending unsolicited (spam) electronic messaging (e.g. email) and chain letters
- Forging electronic messaging header information
- Using electronic messaging, telephone or other communication method, to actively engage in procuring, viewing, or transmitting material that is in violation of sexual harassment or hostile workplace laws
- Accessing, editing, deleting, copying, or forwarding files or communications of another user in any media (e.g., paper, electronic, video, etc.), unless assigned as a job requirement or with prior consent from the file owner
- Deleting, editing, or copying files in another person's computer or electronic messaging account
- Illegal use, including duplication or distribution of copyrighted or company proprietary material, including electronic, hardcopy, audio, and video in any medium
- Employees are forbidden to install software on their computers without the prior approval of their supervisor
- Procurement of or use of any Software as a Service (SaaS) providers without the approval of Information Technology
- Implementation of any information technology component, product or service without the approval of and involvement from IT
- Removing software from systems, unless assigned as a job requirement or prior consent from Information Technology is obtained
- Circumventing any of the information security measures of any host, network or account without officer approval for emergency business purposes
- Using resources for personal benefit
- Introducing malicious programs into the information systems

- Unauthorized modification of configuration files
- Knowingly executing a program that may hamper normal activities, without prior authorization
- Operating a wireless network or allowing other computers to connect to your computer wirelessly
- Employees must not reveal any information about the company's clients or employees which is not already publicly available without expressed permission from their manager
- Unauthorized disclosure of confidential information to individuals outside the company and to individuals within the company without a business need, legal or regulatory requirement
- Disclosure of Personally Identifiable Information (PII) such as social security numbers, bank/credit card numbers, driver's license/id numbers, etc. and any other information classified as confidential, personal or sensitive to any unauthorized individual within the company without a business need
- Disclosure of PII to any individual outside of the company unless there is a legal or regulatory requirement
- Unencrypted transmission of PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information and financial account numbers such as in the body of or an attachment to an electronic message, via FTP, via instant messenger or via fax
- Storing confidential information including PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information or financial account numbers on laptop computers and mobile computing devices unless no alternative exists and then it must be encrypted
- Downloads from the internet are strictly forbidden. If downloads are required for business use, contact IT and arrangements may be made
- Under no circumstance is an employee authorized to engage in any activity deemed illegal by international, federal, state, or other local laws while utilizing company assets
- Under no circumstances may an employee disable anti-virus software or alter anti-virus software settings
- Under no circumstances may an employee disable firewall software or alter firewall software settings
- Employees should not open any electronic messaging attachments that are not expected, or are from unknown addresses, or appear in any way suspicious
- Employees must not use company accounts to post publicly accessible messages or posts.
- Employees may not perform vulnerability scans, monitor network traffic, attempt to elevate rights or privileges, or gain access to information not expressly intended for them
- Employees must be extremely cautious about the use of instant message applications, as these applications are insecure. Sensitive information must not be shared through this mechanism

To ensure compliance with this policy, ISH may perform periodic monitoring of systems, networks, and associated equipment at any time. Personnel using any ISH's information resources consent to disclose the contents of any files or information stored or passed-through ISH's equipment. All data contained on or passing through the company's assets is subject to monitoring and remains the property of the company at all times.

**Other provisions:**

- Explicit management approval must be provided for use of IT resources by employees or third parties
- Explicit management approval is required in order to add a new device to the network
- Authentication is required in order to use any technology
- Accessing unauthorized systems or data resources, or utilizing functions that are not necessary for the performance of the employee's duties
- A list of all devices and personnel with access shall be maintained
- Devices will be labeled with owner, contact information and purpose
- A list of acceptable uses of technology and acceptable network locations shall be maintained
- A list of company approved products shall be maintained

**References**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-8 System Use Notification<br>IR-6 Incident Reporting<br>PL-4 Rules of Behavior<br>PS-6 Access Agreements<br>PS-8 Personnel Sanctions</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(6)(i): Security Incident Procedures<br>§ 164.310(a)(1): Facility Access Controls<br>§ 164.310(a)(2)(ii): Facility Security Plan<br>§ 164.310(b): Workstation Use</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL-02 – Problem Management Policy

**PURPOSE**

The purpose of this policy is to minimize adverse business impacts of incidents or problems at ISH caused by errors in the IT infrastructure, applications, and processes, as well as initiating actions to prevent recurrence of incidences related to those errors.

**SCOPE**

This policy applies to all incidents and problems whether they were explicitly reported by a user or detected using a logging or monitoring tool such as Intrusion Detection/Prevention (IDS/IPS), File Integrity Monitoring (FIM) or a Web Application Firewall (WAF).

This policy requires that problem management is performed in accordance with established Problem Management procedures to ensure that controlled and stable baselines are established for managing problems and restoring or improving IT services.

**POLICY**

The overall objective of problem management is to ensure that all service requests concerning ISH supported systems, resources and services are handled in the most expeditious manner with an acceptable balance of risk, resource/service effectiveness, and minimal disruption to the client community. Problem management supports the mission of the business by providing the highest possible levels of IT service availability through minimization of the impact of incidents and problems within the environment by:

- Proactive prevention of incidents and problems
- Elimination of recurring incidents

The objectives of problem management are to:

- Identify and take ownership of problems affecting infrastructure and service
- Take steps to reduce the impact of incidents and problems
- Identify the root cause of problems and initiate activity aimed at establishing workarounds or permanent solutions to these identified problems
- Use recorded problem and incident data, perform trend analysis to predict future problems and enable prioritization and implementation of problem management activity

The problem management process has both reactive and proactive aspects. The reactive elements provide direct support to the day-to-day operational activities of other service management functions,

such as incident management, and are concerned with initiating activity aimed at resolving problems in response to one or more incidents currently causing issues. Proactive problem management is concerned with identifying and mitigating problems and known errors before incidents occur.

All problems will be recorded in the problem management tool used for the logging and tracking of problems and known errors. A problem becomes a known error once a root cause and workaround have been identified. When logged each problem is assigned an initial severity. Severity may be later adjusted by the Help Desk/IT after further investigation of the problem and assessment of the impact. All actions taken as a result of the problem will be recorded in the problem management tool.

- User calls or emails the Help Desk to report the problem
- Problem is logged into problem management system by the Help Desk; the Help Desk follows-up with the problem reporter for additional information if necessary
- If the problem is resolved by Help Desk, then the problem record is updated and closed
- If the problem is not resolved at the Help Desk, then it is assigned to the appropriate party for further investigation and resolution
- Problem may be reassigned or escalated during problem resolution
- If the resolution of a reported incident or problem initiates a change to the IT infrastructure Change Management Policies and Procedures must be followed
- After resolution, all problems are closed

## REFERENCES

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>SA-10 Developer Configuration Management<br>SA-11 Developer Security Testing<br>SI-2 Flaw Remediation</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(6)(i): Security Incident Procedures<br>§ 164.310(a)(2)(iv) Maintenance Records</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL-03 – Segregation of Duties Policy

**PURPOSE**

The purpose of this policy is to define segregation of duties at ISH and the assignment of access privileges in a way which minimizes or prevents fraud and errors. When duties are segregated, there has to be collusion between two or more employees or multiple mistakes for irregularities to occur.

**SCOPE**

This policy applies to applications, systems and network infrastructure operated by ISH to areas such as change management, system administration, and software development including testing and migration.

**POLICY**

It is company policy that an appropriate segregation of duties shall be maintained in accordance with the principles set forth in this document. The company shall identify, remediate, and maintain a separation of incompatible functions. In permissible instances where functions cannot be fully and appropriately segregated due to specific circumstances, management shall implement mitigating controls to compensate for such situations. As changes occur in the organizational, functional, and technological environments, assessments shall be performed to address the impact on the segregation of duties resulting from such changes.

Segregation of duties is critical because it ensures separation of different functions and defines authority and responsibility over transactions. Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing for separate processing by different individuals at various stages of a transaction and for independent reviews of the work performed. The segregation of duties provides four primary benefits:

- The risk of a deliberate fraud is mitigated as the collusion of two or more persons would be required in order to circumvent controls
- The risk of legitimate errors is mitigated as the likelihood of detection is increased
- The cost of corrective actions is mitigated as errors are generally detected relatively earlier in their lifecycle
- The organization’s reputation for integrity and quality is enhanced through a system of checks and balances

The fundamental premise of segregated duties is that an individual should not be in a position to initiate, review and approve the same action. Job functions will be reviewed annually to ensure functions incompatible for security reasons will be separated.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-1 Access Control Policy and Procedures<br>AC-2 Account Management<br>AC-3 Access Enforcement<br>AC-8 System Use Notification<br>AC-14 Permitted Actions Without Identification or Authentication<br>AC-16 Security Attributes<br>AC-19 Access Control for Mobile Devices<br>AC-21 Information Sharing<br>AU-9 Protection of Audit Information<br>CM-5 Access Restrictions for Change<br>IA-1 Identification and Authentication Policy and Procedures<br>IA-2 Identification and Authentication (Organizational Users)<br>IA-4 Identifier Management<br>IA-5 Authenticator Management<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PS-1 Personnel Security Policy and Procedures<br>PS-4 Personnel Termination<br>PS-5 Personnel Transfer</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(3)(ii)(B) Workforce Clearance Procedure</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL-04 – Vendor/Third Party Management Policy

**PURPOSE**

The purpose of this policy is to describe the information security requirements to be followed in the selection and management of third-party service providers at ISH. This policy also defines the information security requirements for contracts with third parties.

**SCOPE**

All engagements with service providers shall be in accordance with the policy. Arrangements involving third party access to company information processing facilities or assets shall be based on a formal contract. The contract will contain, or reference, all security requirements and the assigned responsibilities to ensure that there is no misunderstanding between the company and the third party.

**POLICY**

Sponsors and owners of outsourced business functions shall exercise appropriate due diligence in the selection of the service provider, including the following consideration:

- Service provider references and experience
- Security expertise of service provider personnel
- Background checks on service provider personnel
- Non-disclosure agreements covering the company's systems and data
- How legal requirements are to be met, as data protection legislation or regulations
- The right to audit, and review of any recent audit reports
- Availability of services to be maintained in the event of disasters
- Service provider physical and logical controls used to restrict and limit the access to the organization's sensitive business information of unauthorized users
- Service provider levels of security to be provided for outsourced equipment
- Clear understanding of the service provider security and incident response policy and assurance that the provider shall communicate incidents promptly

The company shall contractually require that the service provider implements appropriate security controls in accordance with company policies. Services provided by the service provider shall be monitored to confirm that they are in accordance to these policies.

If the service provider provides confidential information, it is the sponsor's responsibility to ensure that any obligations of confidentiality are satisfied.

In higher-risk relationships, the company shall require the right to require changes to standards and obtain access to the service provider for evaluations of its performance. In lower risk relationships, the company shall require the use of standardized reports, such as trust services reports or an SSAE 16 - SOC 2 report (Statement on Standards for Attestation Engagements No. 16 - Service Organization Control).

Service providers that do not meet these requirements shall not be used for projects.

The following terms shall be included in all third party contracts:

- The general policy on information security
- Asset protection, including:

    - Procedures to protect company assets, including information and software
    - Procedures to determine whether there has been any compromise of assets, e.g., whether loss or modification of data, has occurred
    - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract
    - Provisions regarding integrity and availability
    - Restrictions on copying and disclosing information
- A description of each service to be made available
- The target level of service and unacceptable level of service
- Provisions for the transfer of staff where appropriate
- The respective liabilities of the parties to the Agreement
- Responsibilities with respect to legal matters, e.g., the service provider will comply with US legislation including commerce and export control laws in securing the data
- Intellectual Property Rights (IPRs) and copyright assignment and protection of any collaborative work
- Access control agreements covering:
    - Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords
    - An authorization process for user access and privileges
    - A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use
- The right to monitor, and revoke, user activity
- The right to audit contractual responsibilities, or to have those audits carried out by a mutually agreed upon third party
- A requirement that all subcontractors be approved, and that the third party remain responsible for the acts of any approved subcontractors
- A description of the third party provider's contingency plans to ensure that services are maintained in the event of a disaster
- Any required physical protection controls and mechanisms to ensure that the controls are followed
- Any proprietary software and documents be kept in escrow to provide the company access to these resources in the event the third party is no longer a viable entity
- An acknowledgement that the service provider is responsible for the security company information including cardholder data the service provider processes, transmits or stores
-

Accounts used by vendors for remote maintenance (including remote access accounts) shall be enabled only during the time period needed where appropriate.

**REFERENCES**

| | | |
|---|---|---|
| **Frameworks** | **Name** | **Reference** |
| | **NIST** | AC-1 Access Control Policy and Procedures<br>AC-2 Account Management<br>AC-3 Access Enforcement<br>AC-8 System Use Notification<br>AC-14 Permitted Actions Without Identification or Authentication |

| | | |
|---|---|---|
| | | AC-16 Security Attributes<br>AC-19 Access Control for Mobile Devices<br>AC-21 Information Sharing<br>AU-9 Protection of Audit Information<br>CM-5 Access Restrictions for Change<br>IA-1 Identification and Authentication Policy and Procedures<br>IA-2 Identification and Authentication (Organizational Users)<br>IA-4 Identifier Management<br>IA-5 Authenticator Management<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PS-1 Personnel Security Policy and Procedures<br>PS-4 Personnel Termination<br>PS-5 Personnel Transfer |
| **Regulations and Requirements** | **Name** | **Reference** |
| | **HIPAA** | § 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(8): Evaluation<br>§ 164.308(b)(1): Business Associate Contracts and Other Arrangements<br>§ 164.308(b)(3): Written Contract or Other Arrangement |
| **Supporting Standards and Procedures** | | |

# POL-05 – Endpoint Protection Policy

**PURPOSE**

The purpose of this policy is to define guidelines to minimize the impact of malicious software at ISH. This policy applies to all company servers and workstations, as well as any computers used for remote access to the company network.

## SCOPE

Use of endpoint protection software is essential for protecting company resources from the danger posed by computer viruses and other malicious programs.

## POLICY

The following processes are mandatory to prevent virus problems:

- Every server, workstation and all other systems commonly affected by malicious software must run the endpoint protection software supported by the organization.
- All devices running endpoint protection software will have scans run on a periodic basis
- Any computer used for remote access to the ISH network must have approved endpoint protection software loaded and updated on a regular basis
- endpoint protection software must be kept up-to-date and capable of generating audit logs

If infected devices are detected, they shall be repaired, quarantined or deleted. Any devices that cannot be cleaned by the endpoint protection software must be removed from the network until they can be verified as malware-free.

## REFERENCES

**Frameworks**

| Name | Reference |
|---|---|
| **NIST** | AU-2 Audit Events<br>CA-1 Security Assessment and Authorization Policy and Procedures<br>CA-2 Security Assessments<br>CA-5 Plan of Action and Milestones<br>CA-6 Security Authorization<br>CA-7 Continuous Monitoring<br>RA-1 Risk Assessment Policy and Procedures<br>RA-3 Risk Assessment<br>RA-5 Vulnerability Scanning<br>SA-12 Supply Chain Protection<br>PM-9 Risk Management Strategy<br>PM-10 Security Authorization Process<br>PM-11 Mission/Business Process Definition |

| | |
|---|---|
| **Regulations and Requirements** | <table><tr><th>Name</th><th>Reference</th></tr><tr><td>**HIPAA**</td><td>§ 164.308(a)(5)(ii)(B) Protection from Malicious Software</td></tr></table> |
| **Supporting Standards and Procedures** | |

# POL-06 – Encryption Policy

**PURPOSE**

The purpose of this policy is to provide information security requirements at ISH for the use of encryption algorithms that have received substantial public review and have been proven to work effectively. The company shall adopt procedures to support use of cryptographic techniques, including secret key and public key techniques.

**SCOPE**

All sensitive data at ISH that is stored or transmitted.

**POLICY**

The company shall use encryption to protect sensitive data, both in storage and in transmission – this policy covers the circumstances under which encryption must be used. This policy also responds to all applicable provincial regulations, or applicable industry requirements pertaining to protection of sensitive and confidential information that require encryption.

General encryption requirements:

- Sensitive data that is encrypted in storage or during transmission will use strong cryptographic techniques and protocols based on current best practices that meet or exceed the federal, state, or provincial regulation, or applicable industry requirement
- The password or key must not be transmitted together with the information
- Wireless networks transmitting sensitive data or connected to data environments containing sensitive data shall use current practices that meet or exceed the federal, state, or provincial regulation, or applicable industry requirement

Use of proprietary encryption algorithms is not allowed for any purpose unless authorized by appropriate company management.

The content of service level agreements or contracts with external suppliers of cryptographic services shall cover issues of liability, reliability of services, and response times for the provision of the services.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-3 Access Enforcement<br>AU-9 Protection of Audit Information<br>AU-10 Non-Repudiation<br>CP-9 Information System Backup<br>IA-3 Device Identification and Authentication<br>IA-5 Authenticator Management<br>MP-4 Media Storage<br>MP-5 Media Transport<br>SC-8 Transmission Integrity<br>SC-9 Transmission Confidentiality<br>SC-12 Cryptographic Key Establishment and Management<br>SC-13 Use of Cryptography</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL-07 – Information Protection Policy

**PURPOSE**

The purpose of this policy is to define how information stored, processed or transmitted electronically, or on hardcopy must be protected at ISH from unauthorized access or disclosure. Controls must be in place to ensure confidentiality, integrity and availability of information.

**SCOPE**

This policy applies to all electronic and hardcopy information. This encompasses non-public information which should not be disclosed outside ISH as well as information with limited disclosure within the company.

This coverage includes all such non-public information physically located at ISH or located off-site including cloud computing, cloud storage, third-party service providers and offsite storage.

**POLICY**

Information systems storing, processing, or serving non-public information, as defined by the Information Classification Policy, will be secured with logical and physical access controls. Physical access controls will be used to restrict access to hardcopy non-public information.

Logical access to electronic information will be granted only with written approval by the employee's manager granting them the minimum level of access required for job responsibilities.

Physical access controls must be used to restrict physical access to information systems storing non-public information, to areas storing non-public hardcopy information, and offices where the public is not allowed without an escort and a log of their visit.

Non-public hardcopy information must be protected be stored in locked cabinets when not in use especially outside of office hours. Locked offices may not provide sufficient protection as cleaning and/or facilities maintenance staff may have access. To secure non-public information in a locked office, it must be verified that there is no access by any unauthorized employees or service staff.

ISH requires all employees to properly secure all hard copy sensitive or confidential information (especially including any data related to a person) at the end of the day and at any other time they expect to be away from their desk for more than a few minutes.

Non-public hardcopy information should not be copied or faxed from equipment not owned and/or operated by the company.

The rules for handling non-public information are outlined below:

Employees that will have access to confidential or sensitive information must have a background investigation check

- Third parties that have access to confidential or sensitive information must be contractually obligated to comply with the appropriate privacy and security laws, regulations and standards for the information including, Health Insurance Portability and Accountability Act (HIPAA), NIST, and ISO 27001

- Non-public information should only be printed or faxed when required for business, legal or regulatory purposes
- Care should be taken when printing non-public information to printers configured for general office use
- Printouts and fax receipt of non-public information should be retrieved immediately
- Fax transmissions of non-public information should be made only if the recipient is confirmed to be physically present at the receiving fax machine
- Unencrypted confidential and sensitive information must never be sent by end-user messaging technologies such as e-mail, instant messaging and chat
- If transmission of any confidential or sensitive information is necessary via e-mail, strong encryption must be used and passwords and/or keys must not be transmitted together with the information
- Non-public information must be securely disposed if when no longer needed
- Any confidential or sensitive information required for testing purposes must be sanitized before using in a development or test environment including personally identifiable information, health care information and payment card information
- Confidential and sensitive information stored on laptops, USB devices, CD-ROMs, smart phones and other portable devices must be stored only if there is a legitimate business need and no alternative exists and it must be protected by strong encryption
- All backups of non-public information must be encrypted using industry standard strong encryption techniques
- Distribution of any media off-site containing non-public information must be approved by management
- Distribution of any media off-site containing confidential or sensitive information must be approved by management and encrypted using industry standard strong cryptography
- Information that is accessible on the internet for staff, customers, vendors, partners, agencies, etc.… will be protected by a firewall and a DMZ (demilitarized zone)
- Hardcopy non-public information should only be taken off the premises if there is a legitimate business need, management approval, and the user maintains possession of such documents at all times
- All users are responsible for adherence to this policy and violations may be subject to disciplinary measures up to and including termination

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>CSC 13: Data Protection<br>CSC 14: Controlled Access Based on the Need to Know</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(5)(i): Security Awareness and Training</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL-08 – Internet Security Policy

**PURPOSE**

The purpose of this policy is to define how to protect the confidentiality, integrity and availability of information, systems and infrastructure at ISH while permitting access to the internet.

**SCOPE**

This policy applies to all internet connectivity, all systems connected to the internet, and all internet users. In addition, this policy applies to protection of internal logical or physical segments of the network defined as containing confidential information where applicable.

**POLICY**

- All access to/from the internet from the ISH network will be via a firewall(s) which is/are maintained according to the Network Device Configuration Policy
- Two firewall administrators (one primary and secondary) shall be designated and shall be responsible for the upkeep of the firewall
- The primary administrator shall make changes to the firewall and the secondary shall only do so in the absence of the former so that there is no simultaneous or contradictory access to the firewall
- There shall be a firewall at each internet connection and between any DMZ and the internal trusted network
- An Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) will be used and configured to generate alerts to IT security personnel and staff when suspicious activity occurs
- A File Integrity Monitoring (FIM) system will be used to identify changes to critical files for networks, systems and applications and generate alerts to IT security personnel and staff upon changes to these files. They include but are not limited to firewall rule sets, router configuration files, application executables, and network component configuration files
- Laptop and tablet computers that connect to the company IT systems will have personal firewall protection installed per the Mobile Devices Policy
- Users are prohibited from making any changes to the firewall settings on company owned equipment
- ISH reserves the right to block access to any internet site for any reason
- Users with a legitimate business need to access a site that is blocked from access should open a Help Desk ticket to obtain approval
- ISH reserves the right to lock the web browser security settings for users

- All internet use may be logged and monitored, users should have no expectation of privacy or confidentiality with respect to their browsing/internet usage history

## REFERENCES

**Frameworks**

| Name | Reference |
|---|---|
| **NIST** | AC-1 Access Control Policy and Procedures<br>AC-2 Account Management<br>AC-3 Access Enforcement<br>AC-8 System Use Notification<br>AC-14 Permitted Actions Without Identification or Authentication<br>AC-16 Security Attributes<br>AC-19 Access Control for Mobile Devices<br>AC-21 Information Sharing<br>AU-9 Protection of Audit Information<br>CM-5 Access Restrictions for Change<br>IA-1 Identification and Authentication Policy and Procedures<br>IA-2 Identification and Authentication (Organizational Users)<br>IA-4 Identifier Management<br>IA-5 Authenticator Management<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PS-1 Personnel Security Policy and Procedures<br>PS-4 Personnel Termination<br>PS-5 Personnel Transfer |

**Regulations and Requirements**

| Name | Reference |
|---|---|
| **HIPAA** | § 164.316 (a)) Policies and Procedures |

**Supporting Standards and Procedures**

# POL- 09 – Mobile Devices Policy

**PURPOSE**

The purpose of this policy is to establish the rules for the use of mobile computing devices at ISH. These rules are necessary to preserve the integrity, availability and confidentiality of the company's information.

**SCOPE**

This policy applies to all individuals who own or operate a mobile device that communicates with ISH's equipment and networks, or stores ISH data in any way. Mobile devices include but are not limited to smart phones, tablets, laptop computers, zip drives, flash drives etc.…

**POLICY**

Every employee, temporary worker, or contractor who utilizes a laptop computer or mobile electronic data device is responsible for the company information stored, processed and/or transmitted via that computer or device and for following the security requirements set forth in this policy.

ISH seeks to protect company mobile devices from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal. Mobile devices must be appropriately secured to prevent confidential data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the computing and information infrastructure.

- Confidential and sensitive information should not be stored on portable computing devices such as trade secrets, proprietary financial information and financial account numbers, Personally Identifiable Information (PII) or Personal Health Information (PHI) such as social security numbers, bank/credit card account numbers, driver's license/id numbers and all other confidential information as defined in the Information Classification Policy
- In the event that there is a business need and no alternative to local storage all confidential and sensitive information on a mobile device must be protected using a password and approved, industry standard strong encryption
- Confidential or sensitive information must not be transmitted via wireless communication to or from a portable computing device unless approved, industry standard strong encryption is utilized
- All remote access to information resources via mobile devices must follow the Remote Access Policy
- Mobile devices not owned or controlled by ISH that require ISH network connectivity require management approval and must conform to this mobile device policy

- Laptop and tablet computers must have endpoint protection software and personal firewall protection and users are prohibited from adjusting any settings on the virus and firewall protection
- The physical security of these devices is the responsibility of the employee to whom the device has been assigned
- Devices shall be kept in the employees' physical presence whenever possible
- Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight
- Unattended portable computing devices must be physically secured
- Loss or theft of such devices must be reported to IT immediately
- Enable password protection for access to mobile devices, passwords must comply with the Password Management Policy
- Do not store passwords on the mobile device or configure the mobile device for automatic login
- Anytime a user must leave a mobile device unattended for any reason, it must be locked in such a way that a password is required to access the device
- Whenever possible all mobile devices must enable screen locking and screen timeout functions requiring a password to unlock the screen
- Applications and services that will not be used must be disabled to reduce security risk such as Bluetooth and Wi-Fi
- In case of employee termination or resignation a company owned mobile device must be returned to the employee's supervisor immediately upon termination or resignation
- Terminated employees must not be given time to retrieve information from a mobile device without supervision to ensure that no confidential data is copied and removed, or any work product is destroyed

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-1 Access Control Policy and Procedures<br>AC-2 Account Management<br>AC-3 Access Enforcement<br>AC-8 System Use Notification<br>AC-14 Permitted Actions Without Identification or Authentication<br>AC-16 Security Attributes<br>AC-19 Access Control for Mobile Devices<br>AC-21 Information Sharing<br>AU-9 Protection of Audit Information<br>CM-5 Access Restrictions for Change<br>IA-1 Identification and Authentication Policy and Procedures<br>IA-2 Identification and Authentication (Organizational Users)<br>IA-4 Identifier Management<br>IA-5 Authenticator Management<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PS-1 Personnel Security Policy and Procedures<br>PS-4 Personnel Termination<br>PS-5 Personnel Transfer</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(4)(ii)(B): Access Authorization<br>§ 164.308(a)(4)(ii)(C): Access Establishment and Modification<br>§ 164.310(b): Workstation Use § 164.312(a)(1): Access Control</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 10 – Password Management Policy

**PURPOSE**

The purpose of this policy is to establish a standard for passphrase/password control management at ISH including the creation of strong passphrases/passwords, protection of passwords and the frequency of renewing passwords.

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of ISH's resources. All users, including contractors and vendors with access to ISH systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

**SCOPE**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ISH facility, has access to the network, or stores any non-public information.

This policy applies to all devices and software that require authentication to access including network devices such as firewalls, routers and switches, servers, computers including workstations and laptops, and software such as operating systems, and applications that process, transmit or store company information that must be protected such as the personally identifiable information of customers and employees, financial information such as bank accounts and payment card data, and business information critical to the company.

In the event a device or software cannot support the policy compensating controls will be documented and used to mitigate the risk of a breach by a compromised passphrase/password.

**POLICY**

Passwords must have the following characteristics:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least ten characters in length
- Must be changed every 120 days
- Contain at least one occurrence of characters from 3 of the following 4 categories:
    1) English uppercase characters (A through Z)
    2) English lowercase characters (a through z)
    3) Base 10 digits (0 through 9)
    4) Non-alphabetic characters (for example, !, $, #, %)
- Are not a word in any language, slang, dialect, jargon, etc.…
- Are not based on personal information, names of family, etc.…
- Passwords must be unique from previous 24 passwords, unique from passwords used on other sites, and difficult to crack with some personal or company information. Do not use anything someone might guess (birthday, children's names, 12345, etc.).
- Minimum Time Between Password Changes: 1 day

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-4 Information Flow Enforcement<br>AC-11 Session Lock<br>AC-18 Wireless Access<br>AC-19 Access Control for Mobile Devices<br>AU-8 Time Stamps<br>CM-1 Configuration Management Policy and Procedures<br>CM-2 Baseline Configuration<br>CM-6 Configuration Settings<br>CM-7 Least Functionality<br>CM-9 Configuration Management Plan<br>SA-10 Developer Configuration Management<br>SC-10 Network Disconnect<br>SC-15 Collaborative Computing Devices</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.310 (d)(1) Device and Media controls<br>§ 164.308(a)(5)(ii)(D) Password Management</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 11 – Security Training and Awareness Policy

**PURPOSE**

The Purpose of this policy is to define the program to be implemented to maintain an effective knowledge transfer of company information security policies at ISH and provide security awareness training. Employees, temporaries and contractors who have access to the company information systems must understand how to protect the confidentiality, integrity, and availability of information systems. ISH understands that people, not technology, are often the largest threat to sensitive information.

## SCOPE

It is the responsibility and policy of ISH to conduct an on-going information security awareness and training program for all employees, temporaries, and contractors. The company shall develop and maintain an Information Security Training and Awareness Program to communicate and educate employees about information security policies and procedures, and make them aware of their roles and responsibilities in safeguarding information resources. All employees, temporaries and contractors are responsible for participating in the program, for being knowledgeable about information security policies and practices, and for complying with the procedures and instructions provided in the training.

This policy refers to all company information resources whether individually controlled or shared, stand-alone or networked. This includes networking devices, personal computers, workstations and any associated peripherals and software as well as any hardcopy information.

## POLICY

The security and stability of the information systems are vital to daily operations. An awareness and training program for staff is critical to achieving and maintaining an effective information security capability. Information security awareness, training, and education will improve employee behavior and accountability, and reduce the risk of unauthorized activity.

All users shall complete security awareness training and training on information security policies upon hire and subsequently at least annually. The employee's manager is responsible for notifying the Information Security Officer of a new hire immediately so that the workforce member can be trained in a timely manner. Employees shall sign an agreement that they understand the company information security policies and that they shall abide by them. After the training has been conducted ISH will maintain such records as it deems appropriate that confirm that an employee, temporary or contractor received training.

Training may be delivered in person or online.

The TechOps and HR department is responsible for managing the IT security training and awareness program. The Chief Information Security Officer will inform users and supervisors of their requirements, monitor compliance with the training requirement and update supervisors regarding compliance of their employees.

Business owners responsible for managing information resources must have adequate training on the proper implementation of security controls for the systems and data under their control.

Information technology personnel responsible for administering security controls must have adequate training on procedures related to security administration.

## REFERENCES

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><td>Name</td><td>Reference</td></tr>
<tr><td>NIST</td><td>AT-1 Security Awareness and Training Policy and Procedures<br>AT-2 Security Awareness Training<br>AT-3 Role-Based Security Training<br>AT-4 Security Training Records<br>CP-3 Contingency Training<br>IR-2 Incident Response Training</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><td>Name</td><td>Reference</td></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(5)(i): Security Awareness and Training</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 12 – Incident Response Policy

**PURPOSE**

The Purpose of this policy is to define the steps to be followed to respond to information security-related incidents at ISH.

**SCOPE**

Users shall report any suspected information security incidents immediately to the Information Security Officer, including:

- Suspected violations of any information security policies
- Loss or theft of laptops, mobile devices (such as mobile phones and PDAs), security tokens, or other items that may provide access to company resources
- Attempts by unauthorized external personnel to gain access to company systems and data
- Accidental disclosure, modification, or destruction of information

Security incidents may be explicitly reported or detected as a result of system monitoring. Monitoring systems such as IDS/IPS and file integrity monitoring systems will be configured to generate alerts.

An incident response team will be appointed by the Executive VP and the Chief Information Security Officer, and will be ready for deployment in case of a security incident.

**POLICY**

All reported security incidents shall be responded to in a timely manner.

If a compromise is suspected:

- Alert the Information Security Officer who will perform an initial investigation and notify the Incident Response Team if necessary and will follow the within the ISH Incident Response Program.

An incident report form must be completed and submitted for each incident.

In response to a security incident, the Information Technology Department in conjunction with the Incident Response Team shall address the following:

- Detection - Corroborate and define the incident.
- Assessment - The incident should be classified based on available information to determine whether Network communications require closure or Business Continuity Plans require implementation.
- Forensics - Data related to the incident shall be gathered and analyzed
- Containment - Measures shall be taken to separate impacted systems from the rest of the company environment.
- Recovery - Systems shall be restored to normal operation as soon as possible and follow policy and procedures for applicable Backup and Recovery, and BCP and DR.

In the event a compromise has been confirmed the ISH legal department will be consulted to determine the legal requirements for reporting the breach.

A log must be kept of all the actions taken, including triage steps and other regular or routine work performed on the affected systems. This log should be separate from normal system logs, since it may be used as evidence.

Any system that has been compromised by malware will be removed from the network until the system can be verified as malware-free. Accounts where the password has been compromised will be disabled until the password can be reset and communicated to the account owner. Connections between information systems components may be interrupted in response to an incident as part of the containment process.

An incident post-mortem must be conducted to determine if changes are needed to security policies and/or procedures and/or configuration settings and documentation. Additionally the Incident Response Plan will be tested annually. Alerts from US-CERT or some other security monitoring organization will be monitored for potential changes to the Incident Response Plan based on industry developments.

## REFERENCES

**Frameworks**

| Name | Reference |
|---|---|
| **NIST** | AU-6 Audit Review, Analysis and Reporting<br>CP-4 Contingency Plan Testing<br>IR-1 Incident Response Policy and Procedures<br>IR-2 Incident Response Training<br>IR-3 Incident Response Testing<br>IR-4 Incident Handling<br>IR-5 Incident Monitoring<br>IR-6 Incident Reporting<br>IR-7 Incident Response Assistance<br>IR-8 Incident Response Plan<br>PE-10 Emergency Shutoff |

**Regulations and Requirements**

| Name | Reference |
|---|---|
| **HIPAA** | § 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(6)(i): Security Incident Procedures<br>§ 164.308(a)(6)(ii) Response and Reporting |

**Supporting Standards and Procedures**

# POL- 13 – Information Classification Policy

**PURPOSE**

The purpose of this policy is to define information classification at ISH to allow management and staff to appropriately handle information and ensure that it is protected from unauthorized access, modification, disclosure or deletion, and to mitigate the risk of loss of customers or public confidence, and the direct monetary loss due to fines and penalties imposed by regulatory bodies.

**SCOPE**

All information resources (including data and systems) shall be consistently protected, from their origination to their destruction, according to their level of sensitivity, criticality, and business "need to know".

**POLICY**

Data owned, used, created, or maintained by the company shall be classified into the following four (4) categories:

**Public**:

This classification shall apply to all data, information, materials, and other assets that are intended for public circulation. This information may be freely disseminated without potential harm. Information includes:

- Company's marketing website
- Service brochures
- Advertisements
- Job opening announcements
- Press releases.

**Internal**:

This refers to all data, information, materials, and other assets that support the company's business and therefore must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This information is not intended for public use and its unauthorized disclosure could adversely impact the company, customers, or employees.

This classification applies to information including:

- Procedures
- Operational work routines
- Project plans
- Designs and specifications that define the way in which the company operates

Such information is normally for the proprietary use of authorized personnel only.

**Confidential**:

This classification applies to all data, information, materials, and other assets that are confidential to the company, whether by regulation, by law, by contract, or deemed Confidential by management. Information that, if made public or even shared around the organization, could seriously damage company employees and the organization. Information includes but is not limited to:

- Customer and employee names, usernames, addresses, phone numbers
- Technical information, including source code, data center infrastructure and security information
- Pending mergers or acquisitions
- Investment strategies
- Plans or designs
- Accounting information
- Business plans
- Electronic and paper communications and files, and all other information that is labeled as "Confidential"

- Third Party Confidential Information, which is confidential information pertaining to another corporation which has been entrusted to the company by a third party under non-disclosure agreements or other confidentiality obligations

Information classified as Confidential has very limited distribution and should not be copied or removed from the company without specific authority. Confidential information:

- Has access granted on a “Need to Know” basis to authorized employees only
- Must not be disclosed to parties without explicit management authorization
- When stored in an electronic format, must be protected with strong passwords in order to protect against loss, theft, unauthorized access and unauthorized disclosure
- Must be stored only in a place with sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without authorization from management
- Must not be posted on any public website
- Must be destroyed when no longer required according to a records retention schedule based on legal requirements, regulatory compliance requirements and business need.

**Sensitive:**

This classification applies to all data, information, materials, and other assets that are required to be protected by regulation, by law, by contract, or deemed Sensitive by management. Information that, if made public or even shared around the organization, could seriously damage the any individuals or organizations it pertains to, and to the organization. Information includes but is not limited to:

- Customer and employee, social security numbers, driver’s license numbers, bank account or credit card numbers, and all related financial and transaction information including tax information, financial advisement, and payment information, and employee evaluation
- Customer and employee health care and health insurance information
- Account passwords and other identification information such as secret questions, fingerprints, etc…
- Electronic and paper communications and files, and all other information that is labeled as “Sensitive”

Information classified as Sensitive has very limited distribution and should not be copied or removed from the company without specific authority. Sensitive information:

- Has access granted on a “Need-To-Know” basis to authorized employees only
- Must not be disclosed to parties without explicit management authorization
- When stored in an electronic format, access must be protected with strong passwords and the data must be encrypted in order to protect against loss, theft, unauthorized access and unauthorized disclosure
- Must be stored only in a place with sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without authorization from management
- Must be transmitted using only industry standard strong encryption methodology
- Must not be posted on any public website
- Must be destroyed when no longer required according to a records retention schedule based on legal requirements, regulatory compliance requirements and business need.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>CSC 13: Data Protection<br>CSC 14: Controlled Access Based on the Need to Know</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(4)(ii)(B): Access Authorization<br>§ 164.312(a)(1): Access Control</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 14 – Information Disposal Policy

**PURPOSE**

The purpose of this policy is to define what ISH will do to properly dispose of media in electronic or hardcopy format that is used to store information. Unauthorized disclosure of sensitive information may subject the company to legal liability, negative publicity, and monetary penalties.

**SCOPE**

The scope of this document includes the disposal of both electronic and hardcopy media that stores company information classified as Public, Internal, Confidential and Sensitive. See the Information Classification Policy.

For electronic media, this policy addresses the secure removal of information from storage media before the sale, donation or disposal of the associated electronic media and equipment it is used on. This policy also applies to sanitizing electronic media and equipment for reuse within the company.

For hardcopy information, this policy addresses the requirement to destroy documents so the information on them cannot be recovered.

**POLICY**

Information shall be reviewed to verify that the retention period for the information in question has been properly reached. All known audits and audit discrepancies regarding information scheduled for destruction must be settled before the records can be destroyed; all known investigations or court cases involving said information must be resolved before the records can be destroyed.

All electronic media holding company information that is intended for reuse within the company, intended to be sold or donated, be sent out for destruction must be first sanitized. Data sanitization is the process of deliberately, permanently, irreversibly erasing the information stored on an electronic storage device using a software utility intended for that purpose. A device that has been sanitized has no usable residual information and even advanced forensic tools should not be able to recover erased information.

The use of standard disk formatting programs, simple file overwriting or deletion is not sanitization and does not meet the requirement of erasing information from electronic media.

Electronic media that will not be reused can also be physically destroyed so that any information on the device cannot be recovered.

Media shall be turned over to the Information Technology Manager for disposal. All electronic media shall be secured by the IT manager to prevent any unauthorized access prior to sanitization.

Hardcopy media must be cross-cut shred prior to recycling or disposal or be incinerated prior to disposal. Only secured recycle bins are to be used for hardcopy documents.

IT shall inspect company equipment that is deemed obsolete and tagged for disposal to ensure that sensitive information has been properly deleted. Once verification is received that all information has been erased, the equipment shall be properly discarded, traded, resold or donated in accordance with applicable laws.

A log of all destroyed media including electronic and hardcopy containing company information shall be maintained, identifying the information that was on the destroyed media and when it was destroyed.

The following items are examples of electronic media that may contain information requiring the proper disposal of information:

- Backup tapes
- Removable disks
- Optical storage media
- Copiers
- Fax machines
- Hard disks
- Flash drives

- Voice or other recordings
- Smart phones

If a third-party service provider is used to dispose of electronic or hardcopy information, ISH must ensure this policy is followed regarding the disposal of information supported by contract terms and appropriate bonding. See the Third-Party Management Policy.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>MP-6 Media Sanitization<br>AU-11 Audit Record Retention<br>SI-12 Information Handling and Retention</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.310(d)(1): Device and Media Controls<br>§ 164.310(d)(2)(i): Disposal<br>§ 164.310(d)(2)(ii) Media Re-Use<br>§ 164.12(a)(1): Access Control<br>§ 164.312(c)(1): Integrity</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 15 – Information Retention Policy

**PURPOSE**

The purpose of this policy is to define ISH's requirements for records retention.

**SCOPE**

All company records, in electronic or hardcopy format, governed by laws, regulatory requirements, industry requirements, or specific business need. In addition, filing systems, storage arrangements, access procedures, retention schedules and destruction procedures must conform to sound business practices, provide safe and secure methods of handling records and prevent the inadvertent or malicious disclosure of confidential information.

**POLICY**

ISH requires that company records, regardless of format, must be retained for specific periods of time and then disposed of in accordance with laws, regulatory requirements, industry requirements, or specific business need.

Records retention schedules are an established timetable for maintaining company records and provide an established retention period as to the length of time a record must be maintained to satisfy the purposes for which it was created, and to fulfill the legal, fiscal, historical, and administrative requirements of the company and interested agencies.

ISH requires that its records be maintained in a consistent and logical manner and be managed so that the company:

- Meets legal standards for protection, storage and retrieval
- Protects the privacy of employees, customers, and partners
- Optimizes the use of space
- Minimizes the cost of record retention

Each Business Owner in conjunction with the legal department is responsible for outlining a records retention schedule for records maintained by their department.

On at least an annual basis media inventories shall be conducted. Media inventories must produce logs and shall include both electronic and hardcopy media.

ISH expects all employees to fully comply with any published records retention or destruction policies and schedules, provided that all employees should note the following general exception to any stated destruction schedule: If you believe, or the company informs you, that company records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until the Legal Department determines the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that exception may apply, or have any question regarding the possible applicability of that exception, please contact the Legal Department.

# POL- 16 – Access Control Policy

**PURPOSE**

The purpose of this policy is to control logical access at ISH to applications, systems, and hardware and the execution of automated functions.

**SCOPE**

Access to specific applications shall be granted to personnel with a legitimate need. Privileges assigned shall be limited to the minimum required to perform assigned duties and in accordance with the Information Classification Policy. Business Owners may further limit access (i.e., transaction dollar and frequency limits, pre-approval of critical function assignments, etc.). All access not explicitly authorized is forbidden.

**POLICY**

When assigning access rights, access should be limited to only those individuals and functions that require them to perform their assigned duties (the principle of least privilege).

A segregation of duties will exist between individual with authority to determine who has access to systems and data and the individual assigning the access rights. This is to minimize the risk of fraudulent activity.

Logical access to confidential information will require Multi Factor Authentication

Administrative access to ISH systems is limited to members of the TechOps team.

Access to confidential hardcopy information will be protected by physical controls including but not limited to Key or combination locks, keypad, or swipe card.

All users and services will have unique IDs for system access. No users will share IDs or use any generic IDs such as admin, teller, etc.

ISH will provide “Break the glass” accounts for access to critical systems. These will be admin level accounts with a unique ID and password. The credentials will be secured in a vault at two locations. Access codes will be obtained from the vault when it becomes necessary to log on to particular system as administrator only when the designated administrator is unavailable, and the situation is considered serious by Management. A new password will be generated and stored in the vault as soon as possible but within 24 hours of the termination of the emergency situation. All access from this account will be monitored and logged.

Business Owners / System Administrators shall:

- Update access rights based on personnel, business or system changes
- Review user access rights and changes as follows:
    - Business Owners shall Conduct a review of all admin level account rights on a monthly basis for critical systems
    - Business Owners shall Conduct a review of all user level account rights on a quarterly basis for critical systems.
    - Business Owners shall Conduct a review of all account rights on an annual basis for non-critical systems.
- Maintain a list of users who have access to the system and what rights and privileges each user has
- Create and administer accounts for specific individuals and not allow any shared, group or generic accounts for access to confidential data. If such accounts are built-in to applications they will be disabled if possible and not used.

Human Resources shall:

- Notify Information Technology when a termination or transfer occurs so that access rights can be revoked as appropriate in a timely manner

Users shall:

- Be authorized by their manager on an authorization form or system prior to being assigned access to a particular application
- Not circumvent the access granted to their accounts in order to gain access to unauthorized information resources
- Only access applications to which they have been authorized, regardless of actual system permissions
- Not allow anyone else to use their accounts, or use their computers while logged in under their account, except as required for system administration. Users are responsible for any activity initiated by their own user ID.

**REFERENCES**

**Frameworks**

| Name | Reference |
|---|---|
| **NIST** | AC-1 Access Control Policy and Procedures<br>AC-2 Account Management<br>AC-3 Access Enforcement<br>AC-8 System Use Notification<br>AC-14 Permitted Actions Without Identification or Authentication<br>AC-16 Security Attributes<br>AC-19 Access Control for Mobile Devices<br>AC-21 Information Sharing<br>AU-9 Protection of Audit Information<br>CM-5 Access Restrictions for Change<br>IA-1 Identification and Authentication Policy and Procedures<br>IA-2 Identification and Authentication (Organizational Users)<br>IA-4 Identifier Management<br>IA-5 Authenticator Management<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PS-1 Personnel Security Policy and Procedures<br>PS-4 Personnel Termination<br>PS-5 Personnel Transfer |

| | |
|---|---|
| **Regulations and Requirements** | **Name** / **Reference**<br>**HIPAA**: § 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(4)(i) Information Access Management<br>§ 164.308(a)(4)(ii)(B): Access Authorization<br>§ 164.308(a)(4)(ii)(C): Access Establishment and Modification<br>§ 164.312(a)(1): Access Control |
| **Supporting Standards and Procedures** | |

# POL- 17 – Remote Access Policy

**PURPOSE**

The purpose of this policy is to define standards for connecting to the ISH network from any remote host. These standards are designed to minimize the potential exposure to damages which may result from unauthorized use of company resources. Damages include the breach of sensitive or confidential information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system availability, or the corruption of information integrity.

**SCOPE**

Remote Access is term used to describe connectivity to the network from devices not directly connected to the network, such as those located in a private residence or other offsite location. All remote access to systems with the exception of accessing email via a web browser or handheld device, is to occur via encrypted remote desktop or VPN connections.

This policy applies all company employees, contractors, consultants, temporaries, agents, workers, affiliates, and other third parties utilizing the Virtual Private Network (VPN) connections to access the company's network. All such connections must be via the approved VPN client -- no other VPN or Virtual Desktop connectivity or remote access is approved, supported or permitted.

**POLICY**

Employees and third parties authorized to utilize remote access connections shall ensure that unauthorized users are not allowed access to the ISH internal network. All individuals and machines, while accessing the network, including company-owned and personal equipment, are a de facto extension of ISH's network and therefore their machines are subject to the same rules and regulations stated in the Information Technology Security Program. Users of computers that are not company property shall configure the equipment to comply with security practices dictated by the ISH TechOps Department.

Remote access connections shall:

- Use the approved ISH Remote Access technology
- Be automatically disconnected from company's network after 30 minutes of inactivity
- Use multi-factor authentication for remote access
- Require strong passwords for authentication. Password criteria can be located in the Information Technology Security Program
- Not be connected to any other external network at the same time

No devices or software may be installed that allows remote access to the network such as modems, wireless access points, or VPN servers. All remote access will be provided centrally by IT.

Any remote access to the internal network must be reviewed and approved by the appropriate manager and executive officer. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

If users are accessing the network through ISH equipment, the TechOps department will configure and secure systems according to ISH standards. If the user is accessing systems using a personal device, the following steps should be taken prior to access:

- Anti-virus software must be installed and current.
- Security patches for installed operating systems (windows) should be current.
- A personal firewall (Windows has one by default) must be installed and enabled on each host.

Remote access services may be used only for the conduct of business related to work. Personal, family, private or commercial use of any service available remotely is not permitted.

Users agree to apply safeguards to protect ISH's information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remote access to data or services, prevention of inadvertent or intentional viewing of displayed information.

Remote access to data or services may not be used to copy private or personal information such as that residing on a privately-owned computer, to company file shares or other company-owned information systems.

ISH retains the right to amend the terms of the remote access policy at any time, and to alter, change, suspend or terminate remote access service as may be required at any time in its sole discretion.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-17 Remote Access<br>AC-18 Wireless Access<br>AC-19 Access Control for Mobile Devices<br>AC-20 Use of External Information Systems<br>IA-2 Identification and Authentication (Organizational Users)<br>CM-1 Configuration Management Policy and Procedures<br>CM-2 Baseline Configuration<br>CM-6 Configuration Settings<br>MP-2 Media Access<br>SC-7 Boundary Protection</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(4)(ii)(B): Access Authorization<br>§ 164.308(a)(4)(ii)(C): Access Establishment and Modification<br>§ 164.310(b): Workstation Use<br>§ 164.312(a)(1): Access Control</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 18 – Physical and Environmental Security Policy

**PURPOSE**

The purpose of this policy is to define information security requirements at ISH to prevent unauthorized physical access, damage and interference to company premises, information and sensitive assets.

This policy defines the requirements for protecting company information and technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference with ISH operations.

**SCOPE**

All company premises including the corporate office and branch locations shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

**POLICY**

Company equipment shall be installed in suitably protected areas with minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities. The following controls shall be implemented:

- All doors and entrance locations of the company shall be locked when unattended and protected during non-business hours by electronic alarms
- Physical access controls such as locks and keys, cameras, and alarms are necessary to ensure protection and safety of company staff, resources, and property, and to comply with health and safety regulations

- Private office doors, desk drawers, personal computers, peripherals, and related equipment shall be locked when not in use
- Sensitive computer areas like network closets and server rooms will be restricted to only authorized personnel and kept locked at all times.
- Workstation areas frequented by customers or visitors shall be arranged so that monitor screens do not face customers, and that there is no access to the systems by unauthorized personnel.
- Access to server areas by authorized 3rd parties shall be limited to those with a clear business need. ISH personnel are required to remain present when authorized 3rd parties are in or near the server areas, unless specifically vetted and authorized prior.
- A visitor log shall be maintained for all non-public areas of the ISH facility. This log shall indicate the name of the visitor, firm or organization represented, arrival time, reason for visit, and departure time.

Specific requirements for the datacenter:

- Comply with all requirements listed above
- Install fire suppression equipment
- Provide emergency power shutdown controls
- Equipment is to be located on racks raised above floor level
- Provide an uninterruptible power supply
- Annual testing will be performed on all fire and protective systems
- A video camera will be pointed at the door with recordings retained for three months
- Environmental controls will be implemented to ensure that temperature and humidity are maintained within limits for the equipment contained therein
- Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Each UPS should have sufficient capacity to provide at least 30 minutes of uptime to the systems connected to it. Systems hosting confidential data should also be protected with a standby power generator where feasible.
- All network information technology resources must be fitted with effective Surge Protectors to prevent power spikes and subsequent damage to data and Hardware.
- Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or loaned to others by authorized users.

**Visitors**

Third party support services personnel are granted access to secure areas only when required, authorized, and supervised. The employee hosting the visitor must come to the reception area, have the visitor sign in to the Visitor Log Book, documenting their name, and purpose of visit, and escort them to the appropriate office. Visitors are to be issued a badge identifying the individual as a visitor.

Upon the completion of the visit, the visitor must be escorted to the reception area and sign out in the Visitor Log Book and return their badge.

Visitors to the datacenter must be escorted at all times and sign in and out on the datacenter access log book.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>CM-5 Access Restrictions for Change<br>IA-4 Identifier Management<br>MP-2 Media Access<br>MP-4 Media Storage<br>MP-5 Media Transport<br>PE-1 Physical and Environmental Protection Policy and Procedures<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PE-4 Access Control for Transmission Medium<br>PE-5 Access Control for Output Devices<br>PE-6 Monitoring Physical Access<br>PE-8 Visitor Access Records<br>PE-9 Power Equipment and Cabling<br>PE-10 Emergency Shutoff<br>PE-11 Emergency Power<br>PE-12 Emergency Lighting<br>PE-13 Fire Protection<br>PE-14 Temperature and Humidity Controls<br>PE-15 Water Damage Protection<br>PE-16 Delivery and Removal<br>PE-18 Location of Information System Components</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.310(a)(1): Facility Access Controls<br>§ 164.310(a)(2)(ii): Facility Security Plan<br>§ 164.310(a)(2)(iv): Maintenance Records</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 19 – Audit, Logging, and Monitoring Policy

**PURPOSE**

The purpose of this policy is to ensure that the information security controls in place at ISH are effective and are not being bypassed or abused.

One of the benefits of security monitoring is the early identification of abnormal activity indicating wrongdoing or new security vulnerabilities. This early identification can help block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact.

In addition to security the other purpose of this policy is to provide information for service level monitoring, performance measurement, and capacity planning.

**SCOPE**

This policy applies to all network components in the ISH's environment and to all individuals who are responsible for the installation of new information resources, the operation of existing information resources and individuals charged with information resource security.

**POLICY**

Automated tools will be used to provide real-time notification of suspected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed, and the tools will report exceptions.. These tools will be deployed to monitor areas including but not limited to:

- Internet traffic
- Electronic messaging traffic
- LAN traffic, protocols, and device inventory
- Operating system security parameters
- Potential security breaches via an intrusion detection system or intrusion prevention system (IDS/IPS) which is kept up-to-date
- Firewall and Router Rule Sets via File Integrity Monitoring (FIM)
- Executable Code via FIM
- Configuration files on critical network devices and servers via FIM

The following files will be checked for signs of wrongdoing and vulnerability exploitation at least daily:

- Automated intrusion detection/prevention system (IDS/IPS) logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs

- Anti-Virus logs
- Application logs
- Data backup and recovery logs

Automated audit trails will be configured for all system components and include the following:

- All individual accesses to confidential data including any cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects (files, directories, etc.)

For each event the following information will be recorded:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Audit trails will be secured by the following measures so they cannot be altered:

- Limit viewing of audit trails to those with a job-related need
- Protect audit trail files from unauthorized modifications
- Promptly back up audit trail files to a centralized log server or media that is difficult to alter
- Write logs for external-facing technologies onto a log server on the internal LAN
- Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)
- Audit trails will be retained for at least one year with at least three months readily available (e.g., from backup tape)

Users are advised that any systems usage activity undertaken may be logged and these logs may be retained and activity monitored or audited. If such logs indicate a violation of the IT Acceptable Use Policy or any IT policy disciplinary action may be taken up to and including termination.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-1 Access Control Policy and Procedures<br>AC-2 Account Management<br>AC-3 Access Enforcement<br>AC-8 System Use Notification<br>AC-14 Permitted Actions Without Identification or Authentication<br>AC-16 Security Attributes<br>AC-19 Access Control for Mobile Devices<br>AC-21 Information Sharing<br>AU-9 Protection of Audit Information<br>CM-5 Access Restrictions for Change<br>IA-1 Identification and Authentication Policy and Procedures<br>IA-2 Identification and Authentication (Organizational Users)<br>IA-4 Identifier Management<br>IA-5 Authenticator Management<br>PE-2 Physical Access Authorizations<br>PE-3 Physical Access Control<br>PS-1 Personnel Security Policy and Procedures<br>PS-4 Personnel Termination<br>PS-5 Personnel Transfer</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(5)(ii)(C) Log-in Monitoring<br>§ 164.312(b) Audit Controls</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 20 – Risk Management and Assessment Policy

**PURPOSE**

The purpose of this policy is to define inclusion of information security within the scope of ISH's auditable universe to assure information security risks are considered for appropriate evaluation.

**SCOPE**

An IT Risk Assessment will be conducted on an annual basis. IT auditors have the ability to review any information security records, policies, procedures, contracts, processes and any other information required to verify the effectiveness of the information security policy.

**POLICY**

On an annual basis, a formal, written IT Risk Assessment will be conducted considering factors that could affect the confidentiality, availability, and integrity of ISH's information assets and systems. Both internal and external threats will be considered. The IT Risk Assessment will be conducted by personnel independent of implementing the security controls either with internal staff or contracted to a third party. In cases where risk has been accepted, risk acceptance will be documented along with justification for risk acceptance and any compensating controls. Employees are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable.

At a minimum and as appropriate, the following areas will be addressed for risk:

1. Operational risk - The risks and effects due to operational failure or disruption.
2. Security risk - The risks and effects due to lost, exposed, corrupted or otherwise misused data/information.
3. Fraud risk - The risks and effects due to either internal or external fraud.
4. Third-party risk - The risks and effects due to third-parties' failures.

Periodic IT audits may be scheduled to evaluate the effectiveness of the IT controls.

The Leadership Committee will evaluate risk through various methods, including but not limited to:

- Interviews with employees, and vendors
- Consultation with subject matter experts
- Diagramming of potential risk
- Simulation of potential risks
- Testing of controls

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AU-2 Audit Events<br>CA-1 Security Assessment and Authorization Policy and Procedures<br>CA-2 Security Assessments<br>CA-5 Plan of Action and Milestones<br>CA-6 Security Authorization<br>CA-7 Continuous Monitoring<br>RA-1 Risk Assessment Policy and Procedures<br>RA-3 Risk Assessment<br>RA-5 Vulnerability Scanning<br>SA-12 Supply Chain Protection<br>PM-9 Risk Management Strategy<br>PM-10 Security Authorization Process<br>PM-11 Mission/Business Process Definition</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(A) Risk Analysis<br>§ 164.308(a)(1)(ii)(B) Risk Management<br>§ 164.308(a)(1)(ii)(C): Sanction Policy</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 21 – Network Device Configuration Policy

**PURPOSE**

The purpose of this policy is to define what ISH will do to manage network device configurations to protect the security of the network (availability, integrity and confidentiality).

**SCOPE**

This policy applies to all network devices including but not limited to firewalls, routers, switches, intrusion detection/prevention devices, and network monitoring devices.

**POLICY**

IT owns and is responsible for the internal network infrastructure, including developments and enhancements to this infrastructure. Designated IT staff are the only individuals authorized to connect or disconnect network devices to the network. Users must not extend or re-transmit network services in any way. This means users must not install a router, switch, hub, or wireless access point to the network without IT approval.

To be able to diagnose network problems, avoid duplicate addresses, etc. it is critical that IT is responsible and administers all the devices on the network. This means registering not only workstations but also any laptops, printers, hubs, or instruments that are connected to the network even occasionally. IT must know when networked devices are removed from service so their registration can be cancelled.

- All network devices must be inventoried
- Documented configuration baselines will be maintained for all network devices
- Configuration baselines will conform to industry best practices with exceptions documented along with any compensating controls
- Twice a year baseline configurations will be reviewed to identify any needed changes to enhance the security posture of the organization
- Security monitoring and reporting organizations will be used to stay up-to-date on new and emerging threats which may necessitate changes in network device configuration
- Vendor-supplied defaults will be changed before installing a system on the network including passwords, SNMP (simple network management protocol) community strings, and the elimination of unnecessary accounts
- All unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function) will be disabled
- All non-console administrative access (such as web based management) will be encrypted
- Firewall and router rule-sets will be reviewed every six months
- Firewalls will have stateful inspection implemented, also known as dynamic packet filtering.
- Router configuration files will be secured and synchronized
- Change Management Policy and Procedures will be followed for the installation of new network devices and for configuration changes to existing network devices
- Network devices will be patched with latest available patches in a timely manner according to Patch Management Policy and Procedures

- Trust relationships between systems constitute a security risk, and should be avoided where possible. Do not use a trust relationship when another method of communication is possible
- Always adhere to a standard security principle of “minimum required access” to perform a function
- Do not use root access for functions that can be accomplished through a non-privileged account
- Production equipment must be physically located in an access-controlled environment

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-4 Information Flow Enforcement<br>AC-11 Session Lock<br>AC-18 Wireless Access<br>AC-19 Access Control for Mobile Devices<br>AU-8 Time Stamps<br>CM-1 Configuration Management Policy and Procedures<br>CM-2 Baseline Configuration<br>CM-6 Configuration Settings<br>CM-7 Least Functionality<br>CM-9 Configuration Management Plan<br>SA-10 Developer Configuration Management<br>SC-10 Network Disconnect<br>SC-15 Collaborative Computing Devices</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.310(a)(2)(iv) Maintenance Records</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 22 – Server and System Configuration Policy

**PURPOSE**

The purpose of this policy is to define proper server and computer configuration to enable the protection of confidentiality, integrity and availability of ISH's information systems.

Since data that is created, manipulated and stored on these systems may be proprietary, sensitive or legally protected, it is essential that the computer systems and computer network, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is also critical that these systems and machines be protected from misuse and unauthorized access.

The overriding goal of this policy is to reduce operating risk. This server and computer configuration policy intended to:

- Minimize configuration errors and reduce server and computer outages
- Reduce undocumented configuration changes that tend to open up security vulnerabilities
- Facilitate compliance with the regulations and requirements applicable to the company
- Protect corporate data from unauthorized use and/or malicious attack

**SCOPE**

This policy applies to all ISH owned and operated servers and computers, including laptop computers. Servers include file and print servers, application servers, and database servers, and all associated operating systems. Any cloud devices (servers, applications) under the control of ISH also is in scope for this policy.

**POLICY**

All server and computer configurations will have restrictions that are designed to protect the equipment and information, maximize system performance and to reduce maintenance costs. Different standard configurations may exist depending on the final installation location and purpose.

- All servers and computers must be inventoried
- Documented configuration baselines will be maintained for all servers and computers
- Configuration baselines will conform to industry best practices with exceptions documented with compensating controls
- All unnecessary ports, protocols and services will be disabled
- Services and applications that will not be used must be disabled where possible.
- All unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function) will be disabled
- All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers will be removed
- Security monitoring and reporting organization will be used to stay up-to-date on new and emerging threats which may necessitate changes in server or computer configuration
- No server or computer will be placed on the network without appropriate security configurations.
- Default usernames and passwords will be changed/disabled at server and computer configuration prior to connection to the network

- Default usernames and passwords will not be used for server and computer access and administration
- All non-console administrative access will be encrypted using SSH, VPN, or SSL/TLS
- Change Management Policy and Procedures will be followed for the installation of new servers and computers and for configuration changes to existing servers and computers
- Computers and servers will be patched with latest available patches in a timely manner according to Vulnerability Management Policy and Procedures
- All servers and computers will be protected with endpoint protection measures per the Endpoint Protection Policy and Procedures
- Additionally, all servers must be located in secure areas and protected by firewall(s)
- Servers and computers will be configured so that data is logged according to the Audit Logging and Monitoring Policy
- Inactivity timeouts will be implemented requiring a user to re-authenticate after a period of inactivity on their computer
- All critical system clocks and times shall be synchronized
- All software installed on computers must be approved by Information Technology
- Information Technology will maintain a list of approved software
- Laptop and tablet computers will be equipped with personal firewalls
- Laptop computers storing confidential data will have full disk encryption installed

**REFERENCES**

**Frameworks**

| Name | Reference |
|---|---|
| **NIST** | AC-4 Information Flow Enforcement<br>AC-11 Session Lock<br>AC-18 Wireless Access<br>AC-19 Access Control for Mobile Devices<br>AU-8 Time Stamps<br>CM-1 Configuration Management Policy and Procedures<br>CM-2 Baseline Configuration<br>CM-6 Configuration Settings<br>CM-7 Least Functionality<br>CM-9 Configuration Management Plan<br>SA-10 Developer Configuration Management<br>SC-10 Network Disconnect<br>SC-15 Collaborative Computing Devices |

| | |
|---|---|
| **Regulations and Requirements** | <table><tr><th>Name</th><th>Reference</th></tr><tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process</td></tr></table> |
| **Supporting Standards and Procedures** | |

# POL- 23 – Systems Acquisitions and Development Policy

**PURPOSE**

The purpose of this policy is to define a framework for acquiring information technology hardware and acquiring or developing new software at ISH.

**SCOPE**

This policy applies to all hardware and software systems utilized by ISH. It applies to any purchased or leased hardware and software, as well as licensed software, Software as a Service (SaaS), and proprietary software developed by ISH or for ISH by a third party.

**POLICY**

Information Technology involvement and approval is required for any software/systems acquisition or development. This is important for reasons including:

- Ensuring that the hardware and software are consistent with the overall information technology strategy, standards and best practices and will operate effectively in the IT infrastructure
- Evaluating the hardware and software interface requirements to existing systems
- Evaluating the security capabilities, deficiencies and/or vulnerabilities
- Ensuring there are not already existing hardware and software products owned, leased or licensed by the company that provide equivalent functions
- Ensuring that any hidden costs of provisioning/licensing/ownership are accounted for including integration with existing systems and support costs
- Ensuring that the company takes advantage of preferred and volume pricing from vendors by centralizing technology acquisitions. The best pricing is received through consolidation of purchasing power
- Ensuring that there is proper review of licensing agreements for all software
- Accounting for any internal costs for programming, systems administration, training, networking and other support requirements
- Ensuring the software/system meets compliance requirements for any laws, regulations or industry requirements
- Ensuring all proprietary software developed and maintained by developed by ISH or for ISH by a third party is developed according to ISH's System Development Life Cycle (SDLC) and must follow ISH's Project Management Methodology (PMM)

**REFERENCES**

**Frameworks**

| Name | Reference |
|---|---|
| **NIST** | CA-2 Security Assessments<br>CA-6 Security Authorization<br>CM-9 Configuration Management Plan<br>MA-1 System Maintenance Policy and Procedures<br>MA-2 Controlled Maintenance<br>MA-3 Maintenance Tools<br>MA-4 Non-Local Maintenance<br>SA-1 System and Services Acquisition Policy and Procedures<br>SA-3 System Development Life Cycle<br>SA-4 Acquisition Process<br>SA-5 Information System Documentation<br>SA-8 Security Engineering Principles<br>SA-12 Supply Change Protection<br>SA-13 Trustworthiness<br>SC-2 Application Partitioning<br>SC-3 Security Function Isolation |

| | |
|---|---|
| **Regulations and Requirements** | <table><tr><th>Name</th><th>Reference</th></tr><tr><td>**HIPAA**</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy</td></tr></table> |
| **Supporting Standards and Procedures** | |

# POL- 24 – Change Management Policy

**PURPOSE**

The purpose of this policy is to ensure that changes at ISH to information technology hardware, software and services are introduced in a controlled and coordinated manner to reduce the risk of errors and of malicious software or hardware being introduced by any changes. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

**SCOPE**

All changes to ISH's Information Technology resources that affect customers, partners, vendors or staff such as: operating systems, network devices (firewalls, routers, switches, etc.), network cables, servers, workstations, and application software are subject to the Change Management Policy and must follow the Change Management Procedures.

**POLICY**

All changes shall be planned, approved, tested and documented.

- Only authorized staff shall perform changes, with the changes endorsed by the application or system owner(s).
- Assessment of the potential impact of such changes shall be conducted.
- Audit trail of all changes, configuration changes made, person who performed the change, date of the change, purpose of the change, whether the change was a success or failure and other relevant information shall be retained.
- Procedures for testing and approval of changes shall be implemented prior to promotion to production as applicable.
- A staff member, other than the implementer of the change, tests the changes prior to installation into a production environment to ensure the identified components of the change has been met.
- A process for aborting and recovering from unsuccessful changes shall be documented as part of the change process.
- Information users shall be notified regarding how these changes shall impact them. If system availability will be affected while the change is being made, affected individuals will be notified letting them know what to expect and when to expect it. They should also know whom to contact in case they experience difficulty as a result of the change.
- Changes to the environment that could affect data will not be made until there is a known current backup of that data.
- For changes requested directly by the TechOps department, the Executive Vice President will approve and sign those change requests.
- For changes other than break/fix (where a change is needed to correct an issue or broken system), changes will be reported out to the IT Steering Committee.
- The application or system owner may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- In certain circumstances emergency changes can be made with approvals being documented after-the-fact. System failures or the discovery of a critical vulnerability affecting security may necessitate emergency changes.
- From time to time, information technology infrastructure components may require an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning. Whenever possible and where applicable, maintenance windows will be defined to limit the impact to productivity.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>CM-9 Configuration Management Plan<br>MA-1 System Maintenance Policy and Procedures<br>MA-2 Controlled Maintenance<br>MA-3 Maintenance Tools<br>MA-4 Non-Local Maintenance<br>MA-5 Maintenance Personnel<br>SA-10 Developer Configuration Management<br>SA-11 Developer Security Testing<br>SI-7 Software, Firmware, and Information Integrity</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(4)(ii)(B): Access Authorization<br>§ 164.310(a)(2)(iv) Maintenance Records</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 25 – Patch Management Policy

**PURPOSE**

The purpose of this policy is to minimize security vulnerabilities and keep pace with updates to minimize system interruptions and down time on ISH's hardware and software.

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software which can disrupt normal business operations in addition to placing data at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability. Patches are also made available to correct malfunctioning software and hardware not related to security vulnerabilities.

## SCOPE

This policy applies to all equipment that is owned or leased by ISH such as servers, workstations, laptops, software and network devices.

## POLICY

Due to the importance of the confidentiality, integrity and availability of ISH's systems and information, it is vitally important that Information Technology be proactive in implementing security measures designed to reduce the risks of impaired productivity, increased costs, and damage to the business reputation due to malfunctioning system components or system components with security vulnerabilities. In order to ensure the security of the network and protect the company's data, all computers and network devices must be maintained at vendor supported levels and critical security patches must be applied in a timely manner consistent with an assessment of risk.

- Computers and devices must be properly patched with the latest appropriate updates to reduce the vulnerability of all workstations and the entire network to malicious attacks
- Information Technology will implement and maintain appropriate controls and take the necessary measures to ensure all servers, workstations, and network components have available security patches and updates installed
- The computers and network components on the network must have a regular schedule or automated process for identifying and loading appropriate security updates for the operating system or other software
- In the case that automated updates are not configured, Information Technology will set up a notification process from the vendor, from US-CERT, or from some other security vulnerability reporting organization to identify patches to be applied to its environment
- Critical security patches and updates will be installed within 30 days of release by the vendor and receipt by the organization
- Non-critical security patches and patches not related to information systems security and updates available from vendors will be reviewed monthly and applied when appropriate by Information Technology staff. In an emergency situation, expedited application of new security patches may be required

In addition to ensuring that patches are applied times to limit vulnerability exposure, ISH shall also undertake the following proactive steps to detect, assess, rank, and remediate system and network vulnerabilities:

- Internal network vulnerability scans will be run at least quarterly
- External vulnerability scans will be run be run at least annually or after any significant change on the network.
- External and internal penetration testing will be performed at least once per year and after any significant infrastructure or application upgrade or modification. Penetration testing will include network-layer and application-layer penetration testing where applicable. Penetration testing will be conducted by personnel independent of implementing the security controls either with internal staff or contracted to a third party.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AU-2 Audit Events<br>CA-1 Security Assessment and Authorization Policy and Procedures<br>CA-2 Security Assessments<br>CA-5 Plan of Action and Milestones<br>CA-6 Security Authorization<br>CA-7 Continuous Monitoring<br>RA-1 Risk Assessment Policy and Procedures<br>RA-3 Risk Assessment<br>RA-5 Vulnerability Scanning<br>SA-12 Supply Chain Protection<br>PM-9 Risk Management Strategy<br>PM-10 Security Authorization Process<br>PM-11 Mission/Business Process Definition</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(5)(ii)(B) Protection from Malicious Software</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 26 – Backup and Recovery Policy

**PURPOSE**

The purpose of this policy is to define the criteria for the backup, archival storage and restoration of critical data and systems at ISH.

Backup data is defined as information that can be restored to a point in time in the event of a disruption of business, and then used in the daily operations of the company. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

## SCOPE

The scope of this policy includes all data and systems required to conduct company business and to support company business.

## POLICY

- Data and systems to be backed up and archived will be identified by business owners and information technology based on business need and on legal, regulatory, and business requirements.
- At a minimum all systems and data must be backed up on a nightly (at least incremental or differential) basis
- Business owners and IT will identify any systems and data that needs to be backed up more frequently for approval by Management
- Full backups shall be performed at least on a weekly basis with backups stored in Google's cloud platform in Iowa and a secondary DR site which is in South Carolina.
- At a minimum all confidential and sensitive data shall be encrypted.
- Backup media must be properly identified by filename and description to be easily identifiable.
- Backup of non-critical data is at the discretion of the TechOps Department
- Recovery procedures must be tested at least every three (3) months to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery
- Backup and recovery documentation must be reviewed and updated as needed at a minimum on an annual basis to account for new technology, business changes, and migration of applications to alternative platforms
- Backups and archives will be treated with the same level of criticality and sensitivity as the data and applications stored on them
- Errors in backups will be reviewed daily, and if possible corrected in real time. If not possible, notation will be made and will be resolved with the next scheduled nightly backup.

## REFERENCES

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AU-6 Audit Review, Analysis and Reporting<br>CP-4 Contingency Plan Testing<br>IR-1 Incident Response Policy and Procedures<br>IR-2 Incident Response Training<br>IR-3 Incident Response Testing<br>IR-4 Incident Handling<br>IR-5 Incident Monitoring<br>IR-6 Incident Reporting<br>IR-7 Incident Response Assistance<br>IR-8 Incident Response Plan<br>PE-10 Emergency Shutoff</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(7)(i) Contingency Plan<br>§ 164.308(a)(7)(ii)(A) Data Backup Plan<br>§ 164.308(a)(7)(ii)(B) Disaster Recovery Plan<br>§ 164.308(a)(7)(ii)(C) Emergency Mode Operation Plan<br>§ 164.308(a)(7)(ii)(D) Testing and Revision Procedure<br>§ 164.310 (d)(2)(iv) Data Backup<br>§ 164.310(a)(2)(i) Contingency Operations<br>§ 164.312(a)(2)(ii) Emergency Access Procedure</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 27 – Business Resiliency Policy

**PURPOSE**

The purpose of this policy is to define how ISH will plan and prepare for the recovery from a business interruption or disaster.

**SCOPE**

A Business Continuity Plan (BCP) can be defined as the ongoing process of planning, developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

This plan is designed to reduce the risks of the company's ability to operate successfully in the face of various crisis situations. It is recognized that the probability of a severe disaster is low; however, this plan is considered vital should such an emergency occur.

**POLICY**

ISH recognizes that a significant threat exists to its ability to continue normal business operations following a serious unexpected disruptive incident. A high level of dependency upon its automated systems and processes poses risks that need to be mitigated. The company further recognizes that it needs to recover from disruptive incidents in the minimum possible time and that this necessity to ensure a speedy restoration of services requires a significant level of advanced planning and preparation.

Although the primary focus of the company's BCP is to restore the ability to conduct business, regardless of the nature of the disruption, different types of disruptions may require a variety of responses in order to resume business. Many types of disasters may impact not only the company but also the surrounding community. The company realizes that its employees and their families could be affected as significantly as, or more significantly than, the business. In the event of a business disruption, the safety of our employees and their families is of highest priority.

The BCP will be developed after performing a detailed Business Impact Analysis of all company business processes and functions to identify critical systems and recovery times as defined by the line of business heads and senior management.

The BCP will ensure that information security is maintained to protect non-public information as required in normal operations during the recovery process and while operating in alternate facilities and using alternate processes.

A high-level recovery plan will be documented and communicated to personnel on at least an annual basis. The plan should include the process to declare an emergency and the logistics of contacting key individuals that will be responsible for recovering the systems. Recovery procedures should be maintained in at least two separate, secure, facilities so that plans are available when needed.

When enacted, the plan achieves the following objectives:

- Address all possible disasters, emergencies, or disruptive incidents which could have a negative impact on the operations of the business

- Identify staff necessary to perform critical functions defined within the plan
- Contain a call tree with information on emergency contact details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to a critical, serious, or irritating disruptive event
- Take inventory of information systems assets such as computer hardware and software
- Require all contact information be kept confidential and only allow access to staff responsible for maintenance, review and execution of the plan
- Provide the means necessary to handle all incidents in a controlled and structured manner
- Help ensure employee and customer safety
- Assist management in providing swift and decisive leadership for a successful recovery
- Minimize disruptions of service to the company and its customers
- Reduce the risk of the company's ability to operate in the face of various crisis situations, thereby limiting losses to earnings and capital
- Afford the employees the means to efficiently and effectively carry out their tasks and responsibilities
- Prioritization of key business functions
- Creation of a public relations plan to assist with effective handling of an incident
- The plan will be reviewed at least annually, and when a restructuring of the business occurs, new products or services are introduced or significant changes in the information technology architecture takes place to ensure appropriate systems, staff, assignments, and contact information are all accurate
- Training for all staff regarding the business continuity plan and their responsibilities based on their roll will take place at a minimum on an annual basis and when there are significant changes to the plan
- Testing of the plan will be coordinated by the Information Security Program Officer and will be tested at a minimum on an annual basis
- Testing of the plan should take place in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed
- Test results will be documented indicating successes, deficiencies, and improvements with a plan developed to remediate the deficiencies

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-14 Permitted Actions Without Identification or Authentication<br>CA-5 Plan of Action and Milestones<br>CP-1 Contingency Planning Policy and Procedures<br>CP-2 Contingency Plan<br>CP-3 Contingency Training<br>CP-4 Contingency Plan Testing<br>CP-6 Alternate Storage Site<br>CP-7 Alternate Processing Site<br>CP-8 Telecommunications Services<br>CP-9 Information System Backup<br>CP-10 Information System Recovery and Reconstitution<br>PE-17 Alternate Worksite<br>SA-12 Supply Chain Protection<br>PM-5 Information System Inventory</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.312(c)(1): Integrity<br>§ 164.316(a): Policies and Procedures<br>§ 164.316(b)(1): Documentation</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 28 – Asset Management Policy

**PURPOSE**

The purpose of this policy is to ensure that an asset management program is maintained to ensure proper control, management, assessment and planning regarding information technology assets at ISH.

No information technology asset may be placed in service in the company network/infrastructure without being inventoried. Inventory records of an asset must be maintained so long as ISH continues to own or lease the asset.

**SCOPE**

The scope of this policy includes all information technology assets owned or leased by ISH. Assets must be properly tracked from acquisition through useful service lifetime to the point at which each asset is disposed of – either through sale, gift or destruction.

This policy applies to all computers, laptops, servers, firewalls, routers, printers, faxes, scanners, credit card readers, swipe devices, other hardware devices and any other information technology asset that is either directly or indirectly connected to the company network (e.g., a dedicated printer connected to a computer).

Additionally, information technology assets temporarily or permanently removed from service are included in the inventory. A log of information technology assets disposed of will be kept for a minimum of 1 year from the disposal date.

**POLICY**

- An Approved Product List must be maintained containing information technology assets that can be purchased or leased for use on the network and by staff
- Newly acquired assets must be inventoried before they are placed into service on the company network/infrastructure
- Only IT staff may move, connect or disconnect information technology assets with the exception of explicit authorizations to IT staff for troubleshooting purposes
- Periodic inventories at a minimum on an annual basis of assets are conducted to ensure that all assets are accounted for, installed in their designated location and that no unknown assets are detected
- Any “rogue” or unanticipated assets found during inventory will immediately be taken out of service and result in a security incident report and, as appropriate, quarantined, scanned, and an investigation involving the company, police and legal
- Any missing or unaccounted-for assets will result in a security incident report and may involve the company, police and legal if a suspected/actual theft has occurred
- Results of the periodic asset inventories are documented and made available as input to depreciation schedules, obsolesce planning and IT/general budgeting initiatives
- All information technology asset acquisitions must follow a formal process that involves appropriate IT staff in the decision-making process. If none of the assets on the approved

products list meet the criteria the asset (make/model) must be added to the list before funds are committed to its purchase

## REFERENCES

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>CA-2 Security Assessments<br>CA-6 Security Authorization<br>CM-9 Configuration Management Plan<br>MA-1 System Maintenance Policy and Procedures<br>MA-2 Controlled Maintenance<br>MA-3 Maintenance Tools<br>MA-4 Non-Local Maintenance<br>SA-1 System and Services Acquisition Policy and Procedures<br>SA-3 System Development Life Cycle<br>SA-4 Acquisition Process<br>SA-5 Information System Documentation<br>SA-8 Security Engineering Principles<br>SA-12 Supply Change Protection<br>SA-13 Trustworthiness<br>SC-2 Application Partitioning<br>SC-3 Security Function Isolation</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 29 – Vulnerability and Penetration Testing Policy

**PURPOSE**

The purpose of this policy is to define the guidelines for conducting vulnerability testing and penetration testing of systems within ISH.

**SCOPE**

The scope of this policy applies to all information technology assets owned or leased by ISH.

**POLICY**

Vulnerability testing and penetration testing is required for restricted systems. Optionally, non-restricted systems may also apply these standards.

Vulnerability Testing

- ISH must conduct vulnerability testing on all public-facing systems and internal systems with testing of restricted systems occurring on a regularly scheduled basis
- External vulnerability testing (scans) of restricted systems must be conducted on a regularly scheduled basis, at least twice a year.
- Internal vulnerability testing (scans) of restricted systems must be conducted on a regularly scheduled basis, at least quarterly
- Upon configuration change to the system, an internal scan must be performed
- Upon identification of new vulnerability issues, system and network configuration standards shall be reviewed and updated accordingly

Penetration testing

- External and internal penetration testing shall be performed at least once a year
- External and internal penetration testing shall be performed after any significant infrastructure or application changes
- Penetration testing shall minimally consist of network-layer and application-layer penetration tests
- Exploitable vulnerabilities noted during penetration testing shall be corrected and an adequate retest performed to demonstrate that identified exploit is addressed

**REFERENCES**

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>CA-2 Security Assessments<br>CA-6 Security Authorization<br>CM-9 Configuration Management Plan<br>MA-1 System Maintenance Policy and Procedures<br>MA-2 Controlled Maintenance<br>MA-3 Maintenance Tools<br>MA-4 Non-Local Maintenance<br>SA-1 System and Services Acquisition Policy and Procedures<br>SA-3 System Development Life Cycle<br>SA-4 Acquisition Process<br>SA-5 Information System Documentation<br>SA-8 Security Engineering Principles<br>SA-12 Supply Change Protection<br>SA-13 Trustworthiness<br>SC-2 Application Partitioning<br>SC-3 Security Function Isolation</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(A) Risk Analysis<br>§ 164.308(a)(1)(ii)(B) Risk Management<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(6)(i): Security Incident Procedures<br>§ 164.308(a)(6)(ii) Response and Reporting</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 30 – Data Breach Policy

**PURPOSE**

The purpose of this policy is to define the actions required for responding to security incidents involving ISH information and/or information technology resources to ensure effective and consistent response and handling of such events.

**SCOPE**

The scope of this policy applies to all members of the ISH community and any affiliates using ISH's information technology resources or data.

**POLICY**

All members of ISH are responsible for reporting known or suspected information security breaches. (See Policy 12 Incident Response Policy) Incident response will be handled appropriately based on the type and severity of the incident.

Incident severity-Incident response is based on the level of severity of the incident. The level of severity is based on its impact on or threat to the operation or integrity of ISH.

High: (Immediate Response)

- Threatens to have a significant adverse impact on a large number of systems or people
- Poses a potential large financial risk or legal liability to ISH
- Threatens confidential data
- Adversely impacts an enterprise system or service critical to the operation of a major portion of ISH
- Poses a significant and immediate threat to human safety
- Has a high probability of propagating to other systems and causing significant damage or disruption

Medium: (Response within 4 hours)

- Adversely impacts a moderate number of systems or people (department, unit or building)
- Adversely impacts a non-critical enterprise system or service
- Adversely impacts a departmental system or service
- Disrupts a building or departmental network
- Has a moderate probability of propagating to other systems

Low: (Response within next business day)

- Adversely impacts a very small number of systems or individuals
- Disrupts a small number of network devices or segments
- Has little or no risk of propagation or causes only minimal disruption

NA:

- This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found.

## REFERENCES

<table>
<tr><td>Frameworks</td><td>N/A</td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(6)(i): Security Incident Procedures<br>§ 164.308(a)(6)(ii) Response and Reporting</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 31 – Personal Device Policy

**PURPOSE**

ISH grants its employees the privilege of using tablets and smartphones of their choosing at work for their convenience. ISH reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below. This policy is intended to protect the security and integrity of ISH's data and technology infrastructure.

**SCOPE**

The scope of this policy applies to all members of the ISH community and any affiliates connecting to ISH's network.

**POLICY**

Personal device acceptable use is defined as:

- Business use: activities that directly or indirectly support the business of ISH
- Personal use: reasonable and limited personal communication or recreation, such as reading or game playing
- Employees are blocked from accessing certain websites during work hours/while connected to the company network at the discretion of the company
- Devices may not be used at any time to: store or transmit illicit materials, store or transmit proprietary information, harass others; engage in outside business activities.
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- ISH has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted
- The following apps are not allowed:
    - No unsigned apps
    - No apps that allow root access
    - No apps that could be used for malicious intent

Devices and support:

- Smartphones including iPhone, Android, Windows phones are allowed
- Tablets including iPad and Android are allowed
- Connectivity issues are supported by IT
- Devices must be presented to IT for proper job provisioning and configuration of standard apps before they can access the network

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network
- The device must lock itself after idling for 5 minutes
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps

- The employee's device may be remotely wiped out if 1) the device is lost, 2) the employee terminates his/her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification
- Lost or stolen devices must be reported to ISH within 24 hours
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use guidelines
- The employee is personally liable for all costs associated with his or her device
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable
- ISH reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy

**REFERENCES**

<table>
<tr><td>Frameworks</td><td></td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA/HITECH</td><td>§ 164.310(a)(1): Facility Access Controls<br>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.310(a)(2)(ii): Facility Security Plan<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(5)(ii)(B) Protection from Malicious Software<br>§ 164.308(a)(6)(i): Security Incident Procedures<br>§ 164.310(b): Workstation Use</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 32 – Third Party Access Policy

**PURPOSE**

The Purpose of the ISH Third-Party Access Policy is to establish the rules for third-party access to ISH information systems and the computer room, third-party responsibilities, and protection of ISH's information.

**SCOPE**

This policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to ISH information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of ISH personnel responsible for the contracting and/or supervising of the third party.

**POLICY**

Computer Room and Third Policy Guidelines:

- All third-party access to the computer center should be scheduled to occur during regular business hours
- When third parties are scheduled to have access to the computer center, the IT staff must be notified in advance of the date, time, and type of work to be performed
- When the third party arrives, he/she will report to a staff contact that scheduled the visit. The staff contact will escort the third party to the IT area. At this point, the third party is to be informed that he/she will take further direction from the IT staff point person in relation to their activity in the computer center
- Prior to the onset of any work, the third party will describe the activities that are planned
- The IT staff point person is responsible for explaining what measures need to be taken to protect the computer hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the IT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the IT staff to do what needs to be done to protect the computer systems before starting their work
- The third party will report to and receive instructions from the IT staff point person regarding their work in the computer center. The IT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed before leaving the area

Information Systems Third Party Policy Guidelines:

1) Any third-party agreements and contracts must specify:

    - The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software
    - ISH information that the third party should have access to

- The minimum security requirements that the third party must meet (i.e., method for remote access)
- How ISH information is to be guarded by the third party. Signing of a non-disclosure agreement is typically required
- Strict use of ISH' information and information resources for the purpose of the business agreement by the third party. Any other information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others
- Feasible methods for the destruction, disposal, or return of ISH information at the end of the contract. The return of company property such as laptop, PDA, or cell phone after the completion or termination of the agreement

2) Third party must comply with all applicable ISH standards, agreements, practices and policies

3) ISH will provide an IT point of contact for the third party. This point of contact will work with third party to ensure compliance

4) Third party will provide ISH with all additional third parties working on project

5) Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with ISH' password policy

6) Any third-party device that is connected to ISH systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage incurred to ISH in the event of an incident

7) Each third-party employee that has access to ISH' sensitive information should be cleared by IT to handle that information

8) Third-party employees must report all security incidences to the appropriate IT manager

9) Third party must follow all applicable change control procedures and processes

10) All third-party employees are required to comply with all applicable auditing regulations

11) All third-party maintenance equipment on ISH' network that connects to the outside world will remain disabled except when in use for authorized maintenance

12) Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to ISH or destroyed immediately upon departure. The third party will also provide written certification of that destruction within 24 hrs. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by ISH

13) ISH will eliminate third-party access to facilities after the contract has been completed or terminated. The following steps must be performed: Remove third party authentication and all

means of access to systems; Make sure that incoming e-mail is re-routed to an appropriate person; Archive any third-party software configuration, and transfer ownership to designated internal staff; Get a written statement from the third party that any software created and/or installed by the third-party is free of viruses and any other malicious code

**REFERENCES**

<table>
<tr><td>Frameworks</td><td></td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA/HITECH</td><td>§ 164.312(a)(1): Access Control<br>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy<br>§ 164.308(a)(3)(i): Workforce Security<br>§ 164.308(a)(4)(ii)(B): Access Authorization<br>§ 164.308(a)(4)(ii)(C): Access Establishment and Modification<br>§ 164.308(a)(8): Evaluation<br>§ 164.310(b): Workstation Use<br>§ 164.308(b)(1): Business Associate Contracts and Other Arrangements<br>§ 164.308(b)(3): Written Contract or Other Arrangement</td></tr>
</table>
</td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>

# POL- 33 – Social Media Policy

## PURPOSE

Social media can bring significant benefits to ISH particularly for building relationships with current and potential customers. However, it's important that employees who use social media within the company do so in a way that enhances the company's prospects. A misjudged status update can generate complaints or damage the company's reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively.

## SCOPE

This policy applies to all staff, contractors and volunteers at ISH who use social media while working — no matter whether for business or personal reasons. It applies no matter whether that social media use takes place on company premises, while travelling for business or while working from home.

Social media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Yelp and Trip Advisor**
- Sharing and discussion sites like **Reddit**
- Photographic social networks like **Instagram**
- Question and answer social networks like **Google** and **Yahoo Answers**
- Professional social networks like **LinkedIn**

## POLICY

General Advice:
Regardless of which social networks employees are using, or whether they're using business or personal accounts on company time, following these simple rules helps avoid the most common pitfalls:

- **Know the social network.** Employees should spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.

- **If unsure, don't post it.** Staff should err on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or offence — or be otherwise unsuitable — they should not post it. Staff members can always consult the IT Manager for advice.

- **Be thoughtful and polite.** Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.

- **Look out for security threats.** Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.

- **Keep personal use reasonable.** Although the company believes that having employees who are active on social media can be valuable both to those employees and to the business, staff should exercise restraint in how much personal use of social media they make during working hours.
- **Don't make promises without checking.** Some social networks are very public, so employees should not make any commitments or promises on behalf of ISH without checking that the company can deliver on the promises. Direct any enquiries to the IT Manager.
- **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communications via the most appropriate channel — usually email or telephone.
- **Don't escalate things.** It's easy to post a quick response to a contentious status update and then regret it. Employees should always take the time to think before responding, and hold back if they are in any doubt at all.

**Use of company social media accounts:**

Authorized users: Only people who have been authorized to use the company's social networking accounts may do so.

Authorization is usually provided by the IT Manager. It is typically granted when social media-related tasks form a core part of an employee's job.

Allowing only designated people to use the accounts ensures the company's social media presence is consistent and cohesive.

Creating social media accounts: New social media accounts in the company's name must not be created unless approved by the IT Manager.

The company operates its social media presence in line with a strategy that focuses on the most-appropriate social networks, given available resources. If there is a case to be made for opening a new account, employees should raise this with the IT Manager.

Purpose of company social media accounts: ISH's social media accounts may be used for many different purposes. In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the company's overall objectives.

For instance, employees may use company social media accounts to:

- Respond to **customer enquiries** and requests for help
- Share **blog posts, articles and other content** created by the company
- Share **insightful articles, videos, media and other content** relevant to the business, but created by others
- Provide fans or followers with **an insight into what goes on at the company**
- Promote **marketing campaigns** and special offers
- Support **new product launches** and other initiatives

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it, and to put those ideas to the IT Manager.

Inappropriate content and uses: Company social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the company into disrepute. When sharing an interesting blog post, article or piece of content, employees should always review the content thoroughly, and should not post a link based solely on a headline.

**Personal social media rules:**

Acceptable use**:** Employees may use their personal social media accounts for **work-related purposes** during regular hours, but must ensure this is for a **specific reason** (e.g. competitor research). Social media should not affect the ability of employees to perform their regular duties. Use of social media accounts for non-work purposes is **restricted to non-work times,** such as breaks and during lunch.

Talking about the company:

- Employees should ensure it is clear that their social media account **does not represent** ISH's **views** or opinions.
- Staff may wish to **include a disclaimer** in social media profiles: 'The views expressed are my own and do not reflect the views of my employer.'

Safe, responsible social media use:

The rules in this section apply to:

- Any employees using company social media accounts
- Employees using personal social media accounts during company time

Users must not:

- Create or transmit material that might be **defamatory or incur liability** for the company.
- Post message, status updates or links to material or **content that is inappropriate**.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use social media for any **illegal or criminal activities**.
- Send **offensive or harassing material** to others via social media.
- Broadcast **unsolicited views** on social, political, religious or other non-business related matters.

- Send or post messages or material that **could damage ISH's image or reputation**.
- Interact with ISHs' competitors in any ways which could be interpreted as being **offensive, disrespectful or rude**. (Communication with direct competitors should be kept to a minimum.)
- Discuss **colleagues, competitors, customers or suppliers** without their approval.
- Post, upload, forward or link to **spam, junk email or chain emails and messages**.

Maintain confidentiality:

Users must not: Share or link to any content or information owned by the company that could be considered **confidential or commercially sensitive**. This might include sales figures, details of key customers, or information about future strategy or marketing campaigns; Share or link to any content or information owned by another company or person that could be considered **confidential or commercially sensitive**. For example, if a competitor's marketing strategy was leaked online, employees of ISH should not mention it on social media; Share or link to data in any way that could breach the company's **data protection policy.**

Protect social accounts:

- Company social media accounts should be **protected by strong passwords** that are changed regularly and shared only with authorized users.
- Wherever possible, employees should use **two-factor authentication** (often called mobile phone verification) to safeguard company accounts.
- Staff must not use a new piece of **software, app or service** with any of the company's social media accounts without receiving approval from the IT Manager.

Avoid social scams:

- Staff should watch for **phishing attempts**, where scammers may attempt to use deception to obtain information relating to either the company or its customers.
  Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.

- Employees should **avoid clicking links** in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.

**REFERENCES**

<table>
<tr><td>Frameworks</td><td></td></tr>
<tr><td>Regulations and Requirements</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>HIPAA/HITECH</td><td>§ 164.308(a)(1)(i): Security Management Process<br>§ 164.308(a)(1)(ii)(C): Sanction Policy</td></tr>
</table>
</td></tr>
</table>

| | | |
|---|---|---|
| | | § 164.308(a)(3)(i): Workforce Security<br>§ 164.310(a)(1): Facility Access Controls<br>§ 164.310(b): Workstation Use |
| **Supporting Standards and Procedures** | | |