

Written Information Security Policy of the George Hail Free Library

1. Introduction and Purpose

This Written Information Security Policy (WISP) outlines the framework for protecting the confidentiality, integrity, and availability of sensitive information processed, stored, or transmitted by the library. This policy applies to all library staff, volunteers, contractors, and any third parties with access to the library's information systems or data.

2. Scope

This policy covers all information assets, including:

- **Patron Information:** Names, addresses, contact details, borrowing history, and any other personally identifiable information (PII).
- **Employee Information:** Personnel records, payroll data, and other sensitive employee data.
- **Library Operational Data:** Financial records, vendor contracts, system configurations, and other administrative information.
- **Hardware and Software:** Computers, servers, network devices, applications, and operating systems.

3. Policy Statements

3.1 Data Classification and Handling

All data will be classified based on its sensitivity and criticality.

- **Public:** Information readily available to the public.
- **Internal:** Information for internal library use only.
- **Confidential:** Sensitive information requiring protection, such as patron and employee PII.

Confidential data must be handled with the utmost care, in accordance with all applicable privacy regulations and laws.

3.2 Access Control

Access to information systems and data will be granted on a "need-to-know" basis.

- **User Accounts:** Each individual will have a unique user account. Generic or shared accounts are prohibited.
- **Strong Passwords:** All users must create and maintain strong, complex passwords that are changed regularly.
- **Role-Based Access:** Access permissions will be assigned based on job roles and responsibilities.
- **Least Privilege:** Users will be granted the minimum necessary access to perform their duties.

3.3 Network Security

The library's network will be protected against unauthorized access and cyber threats.

- **Firewalls:** Network firewalls will be implemented and configured to restrict unauthorized inbound and outbound traffic.
- **Intrusion Detection/Prevention Systems:** Systems will be deployed to detect and prevent malicious activity.
- **Wireless Network Security:** All wireless networks will be secured using strong encryption protocols (e.g., WPA2/WPA3).
- **Network Segmentation:** The network may be segmented to isolate sensitive data and systems.

3.4 Data Encryption

Confidential data will be encrypted both in transit and at rest where feasible.

- **Data in Transit:** All sensitive data transmitted over public networks (e.g., internet) will be encrypted using secure protocols (e.g., SSL/TLS).
- **Data at Rest:** Confidential data stored on servers, databases, and portable devices will be encrypted.

3.5 Incident Response

A formal incident response plan will be in place to address security breaches.

- **Reporting:** All suspected security incidents must be reported immediately to tech services at Ocean State Libraries (tech@oslri.net)
- **Containment and Eradication:** Steps will be taken to contain the breach and remove the threat.

- **Recovery:** Systems and data will be restored to their normal operational state.
- **Post-Incident Review:** A review will be conducted to identify the root cause and implement preventative measures.

3.6 Employee Training

All employees will receive regular security awareness training.

- **Initial Training:** New employees will receive security training during onboarding.
- **Ongoing Training:** Annual refresher training will be provided to all staff.
- **Phishing Awareness:** Training will include recognizing and reporting phishing attempts.

3.7 Third-Party Vendor Management

Third-party vendors with access to library data or systems must adhere to this policy.

- **Security Requirements:** Vendor contracts will include specific security requirements and obligations.
- **Audits:** The library reserves the right to audit vendor security practices.

3.8 Physical Security

Physical access to library facilities and information assets will be controlled.

- **Restricted Access:** Server rooms and other sensitive areas will have restricted access.
- **Surveillance:** Security cameras may be used in appropriate areas.
- **Asset Management:** All library hardware will be inventoried and tracked.

3.9 Data Backup and Recovery

Regular backups of critical data will be performed and stored securely.

- **Backup Frequency:** Backups will be performed regularly, as defined in the library's backup procedures.
- **Offsite Storage:** Critical backups will be stored offsite for disaster recovery purposes.
- **Recovery Testing:** Backup restoration procedures will be tested periodically.

4. Policy Enforcement

Any violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

5. Policy Review

This policy will be reviewed and updated annually by the Director and the George Hail Board of Trustees as needed to address changes in technology, regulations, or business practices.

6. Definitions

- **Confidentiality:** Protecting information from unauthorized access and disclosure.
- **Integrity:** Ensuring the accuracy and completeness of information.
- **Availability:** Ensuring that authorized users can access information when needed.
- **PII:** Personally Identifiable Information.
- **WISP:** Written Information Security Policy.