NEUSE REGIONAL LIBRARIES
Inspiring Creativity. Fostering Learning. Engaging Community.

# Information Security Policy

### Policy #2025-22

## PURPOSE

This Information Security Policy establishes the framework for setting up an effective information security program at Neuse Regional Libraries. It defines the program, assigns responsibilities, demonstrates the strategic and tactical value of security, and outlines enforcement procedures to protect the confidentiality, integrity, and availability of library information assets.

## SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at Neuse Regional Libraries, including all personnel affiliated with third parties. It covers all information assets, systems, networks, and data owned or managed by Neuse Regional Libraries.

## POLICY

**Information Security Program**

This policy is the program's foundational document and permits the implementation and enforcement of the program based on the established roles and responsibilities.

The Library will maintain the following procedures:

1. Account Security/Password Procedures
2. Onboarding Procedures
3. Resignation/Termination Procedures
4. Backup Procedures
5. Application Update Procedures
6. Workstation Default Configuration
7. Disaster Preparedness Plan

**Roles & Responsibilities**

**Leadership Team -** The Leadership Team is responsible for providing strategic direction and support for the information security program. They must ensure that the necessary resources are allocated for the effective implementation and maintenance of the program. Additionally, they are required to review and approve the information security policy and any major updates.

**Information Technology Specialist -** The Information Technology Specialist is responsible for implementing controls as outlined in the security framework. They also maintain and monitor the security of information systems and networks while responding to security incidents and conducting root cause analysis when necessary.

**Employees and Contractors -** Employees and contractors must adhere to the information security policy and related procedures. They are also expected to participate in security awareness training programs. Additionally, they must immediately report any observed or suspected security incidents to the IT department.

**Non-compliance**

Non-compliance with this policy will result in disciplinary action, which may include termination of employment, contract termination, and/or legal action, depending on the severity of the breach.

## Adopted by the Neuse Regional Library Board
## June 17, 2025