Information Security Policy

The Library will take every reasonable precaution to ensure that any confidential information that is kept by the Library for any purpose is safeguarded from unauthorized access. The Library has a responsibility to ensure that the accessing, handling, sharing and disposing of confidential information complies with the **Confidentiality of Library Records and Privacy Policy, NYS Civil Practice Law and Rules, Section 4509, NYS Civil Practice Law and Rules, Section 2307.**

In general, this policy applies to all East Greenbush Community Library employees, volunteers, and contractors with access to East Greenbush Community Library systems, networks, East Greenbush Community Library information, nonpublic personal information, personally identifiable information, and/or customer data.

Roles and Responsibilities

The Library's administration is assigned the goal of implementing a secure technology infrastructure using the appropriate vendors and products. These assets must be protected from unauthorized access, theft, and destruction. All workers must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

The Library Director is responsible for developing and maintaining a comprehensive suite of information security policies, standards, procedures, and guidelines that are to be mandated and/or endorsed by management where applicable.

The Head of Digital Services is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organization's and the organization's customer's information assets. They will address potential risks to the security, confidentiality, and integrity of confidential information that could result in a compromise. The Head of Digital Services must ensure that the following standards are met on every computing system, equipment, or network with access to confidential information:

- Secure computing systems, equipment, and networks with confidential information.
- Restrict physical and login access to authorized users.
- Maintain up-to-date software patches and antivirus software.
- Ensure and maintain complete system backups.
- Enable and use firewalls.
- Perform regular security scans on computing systems, equipment, and networks.
- Provide training to staff, volunteers, and contract workers who have unsupervised access to the network, in the appropriate use of the network, awareness of the possible effects of misuse or unauthorized use of computer resources, and the consequences of any unauthorized use.

All Department Heads are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness training and educational activities where appropriate and required. Department Heads are responsible for ensuring that Information Security Policies and Procedures are clearly communicated to staff and adequately followed. Department Heads are responsible for informing the Head of Digital Services of any changes in the status of staff, volunteers, or contract workers who use library technology or have access to confidential information. This could include a position change (providing greater or more restricted access privileges) or termination of library employment.

It is the responsibility of all staff members to protect the technology and information assets of the Library. Staff IT Guidelines (included in the Staff Manual) will be distributed to all staff upon hire. Staff will complete assigned security awareness training at least annually, with ongoing phishing training throughout the year. All workers must be informed about relevant, current information security matters, and be motivated to fulfill their information security obligations. All Staff are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

This policy also applies to third parties working or volunteering for the Library, whether they are explicitly bound (e.g., by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

Security Awareness Training Requirements

The information security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

Additional training is appropriate for staff with specific obligations towards information security that are not satisfied by basic security awareness. Such training requirements must be identified and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.

The East Greenbush Community Library will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

All awareness training must fulfill the requirements for the security awareness program as listed below:

- Upon hire, and at least annually thereafter, all employees must successfully complete a General Security Awareness Course.
- Awareness training should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.

- Employees whose specific job requirements require access to increased levels of confidential information must complete additional training modules depending on their specific job requirements.
- Staff will be given a reasonable amount of time to complete each course so as to not disrupt business operations.
- The Library Digital Services department will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. These will be conducted at random throughout the year with no set schedule or frequency.

Breach of Security

Any actual or suspected security breaches involving confidential information must be reported immediately to Digital Services Staff and the Library Director. The IT Incident Response Plan will be initiated to identify the suspected breach, remediate the breach, and notify appropriate parties.

Enforcement

When users fail to comply with this policy, confidential information that is stored, processed, or transmitted on the East Greenbush Community Library network or property may be exposed to the unacceptable risk of loss of confidentiality, integrity, or availability. Violations of security guidelines and procedures established to support this policy will be promptly investigated and could result in disciplinary action up to and including termination of employment, or termination of rights to use the computer resources or have access to confidential information.