North Babylon Public Library
Incident Response Plan

The Incident Response Plan goal is to reduce cyber risks that can threaten patron and staff information, trust, liability and the library's survival.

The Incident Response Plan includes

- Detection and reporting
- Notification and recommendations
- Analyze, contain and validate
- Containment, recovery, remediation, and resolution
- Eradicate and enumerate
- Follow up reporting, after action review

Common Information Security Incidents

- Unauthorized Access: logical or physical access without permission to the Library's data, network, system, applications, etc.
- Denial of Service: an attack that prevents/impairs normal functionality of a network
- Malicious Code: software or scripts intended to breach, damage, steal, cause undesired effects, successful installation of malicious software
- Improper/Inappropriate Usage: violating acceptable computing policies
- PII Breach: personally identifiable information breach – unauthorized acquisition and/or disclosure of PII (physical or electronic)
- Protected Health information
- Financial information
- Theft/physical loss/brute force methods to compromise to degrade or destroy
- Suspected Loss of Sensitive Information: loss of information (not PII) occurring as a result of unauthorized access, malicious code or improper use

Cybercriminal access points

- E-mail
- Social engineering
- Unknown/malicious websites
- Phishing
- CD/DVD/USB/etc. and disks or other inserted media
- Strange cables/wires, rogue devices connected to network
- Tampered seals
- Piggy backing
- Shoulder surfing

Software Updates

- Operating systems, antimalware, firewalls, firmware and other applications are constantly patched, updated, and upgraded to protect against known exploits and vulnerabilities
- Keep all software updated with the latest versions
- Old or EoL applications are susceptible to exploits which can steal information, penetrate networks and cause damage.

Immediate Actions that May be Taken by the User

- Unplug computer from network, CAT5 cable
- Do *not* shut down or re-boot
- Contact key staff
- Isolate particular computer(s)

Back Up Data

A successful back up renders infected hardware expendable. Regular back-ups are the responsibility of the individual staff member with assistance from the Computer Technician.

Notification

- Library Director, Marc Horowitz
- Librarian III, Maureen Nicolazzi
- Computer Technician, James Jenkins
- Library Secretary, Denise Ledesma

Notification of anyone else, internal or external, only with Library Director's authorization. Do not share details of any breach with people outside the response team as defined by the Library Director.

Approved by the Board of Trustees, March 16, 2021