Samuels Public Library IT Security Incident Response Plan

Summary

This policy defines the reporting and response to any computer security incident that threatens the security or privacy of confidential data ("Data" or "Information"). This policy applies to all users. Computer security incidents apply to all computing or network devices and information systems owned, leased, contracted, or otherwise controlled by Samuels Public Library ("Library").

Definitions

1. **Attack or Breach -** The attempted or actual acquisition, access, use, or disclosure of Information in a manner not permitted under existing law or Library policy (actual and implied) that compromises the security or privacy of the individual and/or Library.

2. **Computer Security Incident -** Any attack or breach. Examples of computer security incidents:
   - **Email** - An attack executed via an email message or attachment (e.g. malware infection).
   - **Web** - An attack executed from a website or a web-based application (e.g. drive-by download).
   - **External/Removable Media** - An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
   - **Attrition** - An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
   - **Improper Usage** - Any incident resulting from violation of the Library's acceptable usage policies by a user.
   - **Loss or Theft of Equipment** - The loss or theft of a computing device or media used by the Library, such as a laptop or smartphone.
   - **Breach of a Library Vendor or Contractor** ("Third Party") in which Library Information is compromised.

3. **Information System -** A set of information resources, procedures and/or techniques, organized or designed, for the classification, collection, accessing, use, processing, manipulation, maintenance, storage, retention, retrieval, display, sharing, disclosure, dissemination, transmission, or disposal of Information. An information system can be as simple as a paper-based filing system or as complicated as a tiered electronic system.

4. **Personally Identifiable Information ("PII") -** An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following Data elements: a social security number; a driver's license number, state identification card number, or other individual identification number issued by a unit; a passport number or other identification number issued by the United States government; an individual taxpayer identification number, or a financial or other account number; a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account; payroll Data; donor Data.

5. **Protected Health Information ("PHI") -** Any information created, maintained or received, via any communication or record retention format, by the Library that identifies an individual and any services regarding their health care or health payments relating to their past, present, or future health status. In addition, any Protected Health Information (PHI), as the term is defined in 45 Code of Federal Regulations 160.103 (HIPAA).

6. **User –** Any Library staff, consultant, contractor, patron, or other individual using computing or network devices owned, leased, or otherwise controlled by the Library.

Policy and Reporting

All users are required to immediately report to the Library IT Systems Technician ("IT Systems Technician") any:

- Suspected or actual incidents of a breach, loss, inappropriate disclosure, or inappropriate exposure of Information - whether in printed, verbal, or electronic form - including but not limited to those incidents involving the following Information, systems, or processes:
    - Critical Information such as PII, PHI, credit card numbers, Social Security numbers, driver's license numbers, or bank account numbers.
    - Lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives.
    - Viewing of Information without a demonstrated need to know (e.g., snooping).
- Systematic attempts to compromise Information - whether in printed, verbal, or electronic form - or Library information systems, such as:
    - Unsuccessful login attempts, probes, or scans.
    - Repeated attempts by unauthorized individuals to enter secured areas.
- Suspected or actual weaknesses in the safeguards protecting Information - whether in printed, verbal, or electronic form - or Library information systems, such as:
    - Weak authentication processes.
    - Ability to access Information users are not authorized to access.
    - Weak physical safeguards such as locks and access controls.
    - Lack of secure transport methods.

If it is unclear whether a situation should be considered a computer security incident, the IT Systems Technician should be contacted to evaluate the situation.

With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by the IT Systems Technician or authorized personnel.

If the suspected incident involves a potentially compromised computer system - e.g., a suspicious email attachment was opened, a computer begins responding abnormally, files become inaccessible, etc. - staff should proceed as follows:

- Do not alter the state of the computer system, the computer system should remain on and all of the currently running computer programs left as is, do not shutdown or restart the computer.
- Immediately disconnect the computer from the network by removing the patch cable from the back of the computer.

- Document any information you know while waiting for the IT Systems Technician to respond to the incident. This may include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response

Upon receiving a report, the IT Systems Technician will:

1. Attempt to determine if the computer security incident justifies a formal incident response. In cases where a computer security incident does not require an incident response, the situation will be handled by the IT Systems Technician to ensure that all technology support services required are rendered.
2. Ensure appropriate information and evidence is collected and logged.
3. Immediately assess initial actual or potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of Information.
4. Immediately advise and assist in containing and limiting the loss, corruption, inappropriate disclosure, inappropriate exposure, or breach.
5. Invoke incident response procedures commensurate with the situation.
6. Inform the Operations Director and/or the Library Director of the initial situation and update throughout the investigation.
7. As appropriate, contact outside law enforcement for assistance.
8. As appropriate, assemble an Incident Team to advise and assist in ongoing investigation and decision making. The nature of the incident and the type(s) of Information involved will determine the make-up of the Incident Team.
9. As appropriate, perform forensics or other specialized technical investigation or recommend a third party to assist in the investigation.
10. Initiate steps to warn other departments if the situation has the potential to affect other Library Information or information systems.
11. Confirm actual or probable events from investigatory information and facilitate decision-making by the Incident Team.
12. In coordination with the Incident Team and following internal procedures, determine if notification to individuals and/or regulatory or governmental authorities is required and/or desired, and invoke breach notification procedures commensurate with the situation.
13. Ensure appropriate Library management approvals are obtained prior to any notifications to individuals or regulatory and government officials.
14. Document decisions and any notifications made to individuals or regulatory and government officials.
15. Schedule a debriefing meeting with the department and Incident Team after the response, to ensure appropriate corrective action in the affected department is taken, to identify any actions that could be taken to reduce the likelihood of a future similar incident, and to continuously improve the response processes.

Incident Confidentiality

Information regarding computer security incidents will be kept confidential by all parties involved. Only authorized personnel may disclose such information.

Prevention

In an effort to proactively combat the occurrence of a computer security incident, the Library will employ the following defensive measures:

- Maintain up-to-date anti-virus software on all computers and servers, as well as keep all network systems behind a monitored firewall.
- Regularly backup servers and management personnel computers.
- Keep Server Room locked at all times.
- Store all backup media, computer information, passwords, and security system documentation in a fireproof file cabinet in the locked Server Room.
- Change Active Directory user passwords every 6 months.
- The Operations Director will change the accounting software password every 3 months.
- Terminate the email account, Active Directory user account, and security code of former employees within 12 hours of their departure.
- Turn wireless network access off from 9:00 p.m. to 8:00 a.m.
- Staff shall refrain from clicking any links or opening attachments contained in suspicious emails.
- Utilize Sucuri (or similar) website security monitoring and firewall service for all Library related websites.

Dealing with a Third Party

Where Library vendors or contractors have access to Library Data protected under this policy, the IT Systems Technician shall work with the Third Party to be sure it has in place policy to protect such Data. Upon notice of, or otherwise becoming aware of, a breach at or caused by a Third Party the IT Systems Technician shall consider said breach as a breach hereunder and shall take such action as is appropriate and possible to limit further dissemination of said Data.