

MCLS Policy Breach Notification Policy

Statement

The MCLS will investigate and provide notice of information security breaches to affected individuals and/or Federal and State agencies in accordance with applicable Federal and State requirements.

Purpose

The purpose of this policy is to outline how the MCLS will respond to incidents involving data breaches. It will identify and define steps and procedures that will be followed when those breaches occur and will address how affected individuals will be notified as required by relevant state and/or federal laws.

Scope

This policy applies to all MCLS information assets or information assets under the care of the MCLS, and applies to all individuals who interact with, access, or store MCLS electronic information regardless of storage device, medium, or physical location.

Data Breach

A *Data Breach* is defined by the MCLS as an incident of unauthorized access of data in electronic form containing personal information. Protected personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, and does not include information made lawfully available to the general public from federal, State, or local governments.

Reporting Responsibility

All individuals affiliated with the MCLS in any capacity, including but not limited to member library staff, vendors, and contractors, should report suspected or actual data breaches immediately to the Manager of Library Automation Services. The MCLS will investigate all reports of breaches related to information maintained by the MCLS.

MCLS Procedures

MCLS administration will initiate the following procedures upon notification of a suspected breach:

- Containment - If MCLS Library Automation Services determines there was a data breach, the MCLS will work with the affected department or location to contain the breach.
- Director Notification – The Director of the MCLS will be notified when determination of an actual breach is made.
- Assessment - Once the breach is contained and eradicated, MCLS Library Automation Services will assess the extent and impact of the breach, and provide documentation.
- Data preservation - All available evidence related to the breach will be preserved by MCLS Automation Services for future analysis.
- Reporting and legal obligations – The MCLS Director or Assistant Director will consult with legal counsel to determine specific legal obligations relating to the breached information and relevant reporting obligations.
- Internal response strategy – the MCLS Director will establish an appropriate response strategy. If it is determined that criminal activity has taken place, the Director will notify law enforcement, MCLS Board of Trustees and MCLS Director's Council.

External Notification

The MCLS Director will determine if external notification is required. External notification is required if any of the following conditions are met:

- Access has been gained to private information as that term is defined in New York State Technology Law Section 208(1)(a);
- A physical device that contains private information has been lost or stolen;
- There is evidence that private information has been copied or removed from a physical device containing sensitive information.

External notifications will go to anyone affected by the breach, or whose data may have been compromised, as well as to government officials, as required by law. Notification contents will include, at minimum:

- A description of the incident in general terms and a timeline of the data breach, including any notification delays and reasons (e.g., law enforcement request).
- A description of the type of personal information that was subject to possible unauthorized access and acquisition.
- A description of the actions taken by the MCLS to protect the personal information from further unauthorized access.
- A contact that affected individuals may reach for further information.

Monroe County law department will review the proposed notification prior to being sent and will assist in drafting as required. A copy of the notification will also be provided online at www.libraryweb.org at the time it is posted or sent to affected individuals.

Resolution

Based on the assessment of the breach, corrective and/or preventative actions may be implemented within a timeframe agreed to by the Manager of Library Automation Services and MCLS Director. Where a systemic issue is identified, an improvement plan should be developed to address policy and/or process improvement. The MCLS Director shall report to the MCLS Board of Trustees and MCLS Director's Council of the corrective actions completed.

*Approved by the Monroe County Library System Board of Trustees
March 18, 2019*

*Endorsed by the Webster Public Library Board of Trustees
June 12, 2019*