Stevens Memorial Community Library
146 Main Street • Attica, NY 14011 • (585) 591-2733

Cybersecurity Policy

This policy defines the circumstances under which the Stevens Memorial Community Library ("the Library") shall provide notice regarding a security breach that results in unauthorized access to confidential Library information. This policy applies to information stored by the Library. Suspected or confirmed information breaches must be reported immediately to the Library Director.

Upon notification of a suspected information breach, the Library will:

● Investigate the breach and report it to the appropriate internal and/or external officials and parties (such as administrative members of the OWWL Library System);

● Block, mitigate, or de-escalate the breach, if possible;

● Implement processes and procedures to prevent similar breaches from occurring in the future.

1. Internal Notification: The employee who discovers the breach will report it to the Library Director, who will establish an appropriate response strategy. If it is determined that criminal activity has taken place, the Library Director will notify law enforcement, the President of the SMCL Board of Trustees, and the OWWL Library System.

2. External Notification: The Executive 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 § 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.

Adopted by the SMCL Board of Trustees on September 21st, 2026