

Information Security Breach Notification Policy

This policy defines the circumstances under which the Library shall provide notice regarding a breach in security of sensitive information.

This policy applies to information safeguarded by Hauppauge Public Library. Suspected or confirmed information security breaches must be reported immediately to the Chief Executive Officer. A breach is defined as unauthorized access of library information. The Library will investigate all reports of security breaches of private and/or otherwise sensitive information. Based on the results of the Library's investigation, internal and/or external parties may be notified, as necessary and appropriate.

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

- 1) Report the breach to the appropriate officials
- 2) Block, mitigate, or de-escalate the breach, if possible.
- 3) Implement processes and procedures to prevent similar breaches from occurring in the future.

Internal Notification

The person/department discovering the breach will report it to the Chief Executive Officer, and will work with them to establish an appropriate response strategy. If the Library's investigation determines that criminal activity has taken place, the Chief Executive Officer will notify the Board of Trustees.

External Notification

The Chief Executive Officer will determine if external notification will be required. External notification is required if any of the following conditions are met:

- 1) Access has been gained to sensitive information
- 2) A physical device that contains sensitive information has been lost or stolen
- 3) There is evidence that sensitive 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: May 18, 2017

Reviewed: June 2021