Allegany College of Maryland

BREACH REPORTING PROCEDURE

Adopted date 6/18/2018
Revised Date 6/22/2022
Reviewed by Board of Trustees 6/18/2018
Implementation Date 6/18/2018
Type of Policy: Operational

BACKGROUND AND PURPOSE

The purpose of this procedure is to outline the steps that must be followed once a possible breach of personal privacy is identified.

PROCEDURE

I. SCOPE OF THE PROCEDURE

This procedure applies to information safeguarded both by Allegany College of Maryland and/or by third-party vendors and contractors working with ACM.

II. PROCEDURE STATEMENT

When a possible privacy breach has occurred, immediate action should be taken. The following steps will assist in controlling the situation and ensuring that, if a breach of privacy occurs, actions will be taken to minimize the risks of a similar breach from happening again.

III. Steps

1. Confirm and Contain

Confirm the validity of the suspected information breach. If the breach can be reasonably ascertained, containment should occur immediately. Containment includes, but is not limited to, disconnection of the host (e.g., server or another device) from the network or shutting down an application. Care should be taken not to destroy data, but to preserve it without any form of network connection. Re- connection of the device to the network is not allowed until such time as remedial steps have been completed and re-connection is specifically approved by the Dean of Information Technology or designee.

2. Report

The following individuals are required to be informed as soon as possible:

- Dean of Information Technology or designee
- Vice President of Finance and Administration or designee
- Department head from which the information was breached

The report should indicate whose personal information was disclosed, to whom it was disclosed, when it was disclosed, how it was disclosed/accessed, and what steps have been taken in response to the disclosure.

Employees and students can report a security breach from the helpdesk portal at https://www.allegany.edu/it-helpdesk by email at ithelpdesk@allegany.edu or by calling the helpdesk at 301-784-5444.

3. Retrieve.

Any documents or contents of electronic documents that have been disclosed to, or taken by, an unauthorized recipient should immediately be retrieved and/or secured (electronic documents or paper documents in facsimile form or printed e- mail messages) or taken offline. Documents, in any form, should not be destroyed until specific instruction is received. This may require personal attention to obtain the documents and return them to their original location, remove them permanently from electronic storage, or send them to the intended authorized recipient.

4. Remove.
Private information taken offline may still be accessible and discoverable on the Internet via Internet Search engines (e.g., Google). The usual time periods for information to be removed by the search engines through routine web crawling techniques is too elongated (e.g., weeks) and requests must be made to remove the information from search engine indexes and cache directly to the Internet Search engines companies. These requests must be made as quickly as possible. This step will be synchronized with the College ISP coordinator.

5. Notify.
In cases where the breach results in the disclosure of personal information, the College may be required to notify the individuals affected. Determination of the reporting requirements will be made by the Vice President of Finance and Administration or Designee on a case-by-case basis. All notification letters must be reviewed and approved by the Vice President of Finance and Administration prior to being sent. Notification letters should include the information sheet from the Federal Trade Commission entitled "What to do if your personal information has been compromised."

5. Investigate.
The Vice President of Finance and Administration, the Dean of Information Technology, and appropriate IT staff will investigate the details of any breach, for the purpose of determining and recording all the relevant facts concerning the breach and making recommendations. The objectives of this investigation should include: a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal private information.

6. Management Review.
The Vice President of Finance and Administration or Designee will document and report the details of the breach of privacy and remedial steps to the President of the College. The Dean of Information Technology will report on recommendations and actions to the appropriate parties within the President's office.

IV. Conclusion
A breach of private information is a serious matter. College staff, faculty and Office departments must make every reasonable effort to prevent breaches from occurring. If one does occur, staff and faculty must ensure that compliance with this procedure is followed.

V. Definitions

Confidentiality - Maintaining authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information and a loss of confidentiality is the unauthorized disclosure of information.

Integrity - Protecting against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity and a loss of integrity is the unauthorized modification or destruction of information.

Availability - Safeguarding timely and reliable access to and use of information and a loss of availability is the disruption of access to or use of information or an information system.

Information Technology Resources - includes all college-owned computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; communication services and devices, including electronic mail, voice modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.

Information Security Event - any situation that has the potential to threaten the confidentiality, integrity, and availability of the College's information and information technology resources. An event includes loss of control of information through unauthorized access, equipment loss, or theft.
Information Security Incident - any event that is known or suspected to have compromised the confidentiality, integrity, and availability of the College's information and information technology resources.

Breach - the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to events where persons other than authorized users have access or potential access to confidential or sensitive information, either electronically or physically.

VI. Administration of this Procedure

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining this procedure.

VII. Changes

Substantive changes to this procedure require approval by the Board of Trustees; editorial changes, title/position changes, and/or changes to its implementation procedures may be made as required by federal or state mandate and/or institutional need with timely notice to students and employees.