Allegany College of Maryland
Breach Notification Policy

Issued: 7/18/2017 **Approved**: 6/18/2018

Purpose
To define the circumstances under which Allegany College of Maryland (ACM) shall provide notice regarding a breach in security of college information.

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

Definition
A breach is defined as any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of protected college information.

Policy
Upon notification of a suspected information security breach the Information Technology department will: investigate reports of a security breach, report the breach to the appropriate officials, block, mitigate, or de-escalate the breach, if possible, implement processes and procedures to prevent similar breaches from occurring in the future and based on the results of the investigation, notify internal and/or external parties as necessary and appropriate. Suspected or confirmed information security breaches must be reported immediately to the campus Helpdesk by phone: 301-784-5444, email: ithelpdesk@allegany.edu, or by web request: at https://www.allegany.edu/it-helpdesk/student-helpdesk-form.html.

Notification

Internal
The College Information Technology department will report all suspected cases of significant information breaches to the Vice President of Finance and Administration, and will work with him/her to establish an appropriate response strategy. If the College information technology department's investigation determines that criminal activity has taken place, the Vice President (or designee) will report the breach to public safety and/or College legal advisors. The College community at large will be notified of the results of the initial investigation.
External
The Dean of Information Technology in consultation with the Vice President of Finance and Administration will determine if external notification will be required in the event of an information breach. External notification is required if any of the following conditions are met: has access been gained to unencrypted PII and/or ePHI, has a physical device that contains unencrypted PII and/or ePHI been lost or stolen, is there evidence that unencrypted PII and/or ePHI has been copied or removed, is there evidence that the intrusion was intended to acquire unencrypted PII and/or ePHI, the breach results in a significant loss of data, system availability, or control of systems, the intrusion involves a large number of victims or Indicates unauthorized

access to, or malicious software present on critical systems, local, state, or federal laws or College policy require notification in this instance.

Parties to be notified may include:

- Anyone affected by the breach, or whose data may have been compromised.
- US Department of Education
  - By email: cpssaig@ed.gov)
  - By phone EdSoc: 202-245-6550.
- Law enforcement officials (as needed).
  Cumberland Police
  - By phone 301-777-1600

  Maryland State Police
  - By phone 301-729-2101
- Government officials as required by law, such as the attorney general of Maryland.
  - By mail: Office of the Attorney General
    Attn: Security Breach Notification
    200 St. Paul Place
    Baltimore, MD 21202
  - By fax: Security Breach Notification (410) 576-6566
  - By email: Idtheft@org.state.md.us

What to report:

- Date of the breach (suspected or known)
- Impact of the breach (# of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information security point of contact (email and phone details)
- Remediation status (complete, in-progress with details) and next steps (as needed)

Enforcement

Users found to have violated this policy may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Any corrective measures taken shall be administrated in accordance with appropriate disciplinary procedures applicable to the relevant user.

Related Policies/Standards:

Technology Security Policy, Technology Security Standard, Breach Reporting Procedures

Revision History

Version Number	Date	Author	Description
1.0	3/07/2017	Rich Crawford	Initial Draft
2.0	5/8/2018	Rich Crawford	IT Governance Committee approved
2.1	5/18/2018	Rich Crawford	President's Advisory Team reviewed
3.0	6/18/2018	Rich Crawford	Board of Trustee's approved