Purpose

This policy governs the actions required for reporting or responding to security incidents involving ACOM information and/or information technology resources to ensure effective and consistent reporting and handling of such events.

Scope

This policy applies to all members of the ACOM community, including students, personnel, units, and affiliates using ACOM information technology resources or data.

Effective Date

This policy became effective on August 1, 2013

Authority

For major incidents, which include a breach of personal identity information (PII), ACOM IT policy requires escalation to the top administration on campus and prompt notification of the Dean's Cabinet. Likewise,

Policy

All members of the College community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at ACOM must be promptly reported to ACOM's Director of Information Systems - ACOM and other appropriate authority(ies) Incident response will be handled appropriately based on the type and severity of the incident in accordance with the incident response summary table below and ACOM's IT Security Incident Management Procedures. Handling of security incidents involving confidential data will be overseen by the Dean's Cabinet.

All individuals involved in investigating a security incident should maintain confidentiality, unless the Director of Information Systems - ACOM authorizes information disclosure in advance.

Definitions

1. A security incident is any real or suspected event that may adversely affect the security of ACOM information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a ACOM security policy
- Security weakness such as an un-patched vulnerability

2. Personal identity information(PII) is an individual's name (first name and last name, or first initial and last name) in combination with one or more of the following: a) Social security number, b) driver's license number or state identification card number, c) passport number, or c) financial account number,

or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.

Roles and Responsibilities

1. The incident managers responsible for managing the response to a security incident as defined in the incident response summary table below.

2. The Security Incident Response Team (SIRT) will oversees the handling of security incidents involving confidential data (e.g., personal identity information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:

- Senior administrator for the affected unit
- Director of Information Systems - ACOM
- Security Officer
- Representative from the Office of General Counsel
- Director for Media Relations
- Others as needed (for example, Security Services for criminal incidents)

Implementing Procedures

1. Reporting Security incidents any member of the ACOM community who suspects the occurrence of a security incident must report incidents through the following channels:
    - All suspected high severity events as defined in Section below , including those involving possible breaches of personal identity information, must be reported directly to the Director of Information Systems - ACOM as quickly as possible by phone (preferred), e-mail, or in person. If the DIS-ACOM cannot be reached, contact the Dean of Student Services.
    - All other suspected incidents must also be reported to the DIS-ACOM. These incidents may be first reported to departmental IT support personnel, the unit's Security Incident Response Team (SIRT) representative. , or the unit head who can then contact the DIS-ACOM. Reports should be made by sending email to support@acomedu.org (preferred) or by notifying the DIS-ACOM by phone, email, or in person.
    - For detailed information about reporting IT security incidents, see the ACOM IT Security Incident Management Procedures.

2. Responding to Security Incidents

- Incident Severity

Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA ("Not Applicable").

- High

  The severity of a security incident will be considered "high” if any of the following conditions exist:

  - Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)
  - Poses a potential large financial risk or legal liability to the College
  - Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)
  - Adversely impacts an enterprise system or service critical to the operation of a major portion of the university (for example, e-mail, student information system, financial information system, human resources information system, learning management system, Internet service, or a major portion of the campus network)
  - Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
  - Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

- Medium

  The severity of a security incident will be considered "medium" if any of the following conditions exist:

  - Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
  - Adversely impacts a non-critical enterprise system or service
  - Adversely impacts a departmental system or service, such as a departmental file server
  - Disrupts a building or departmental network
  - Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruption

- Low

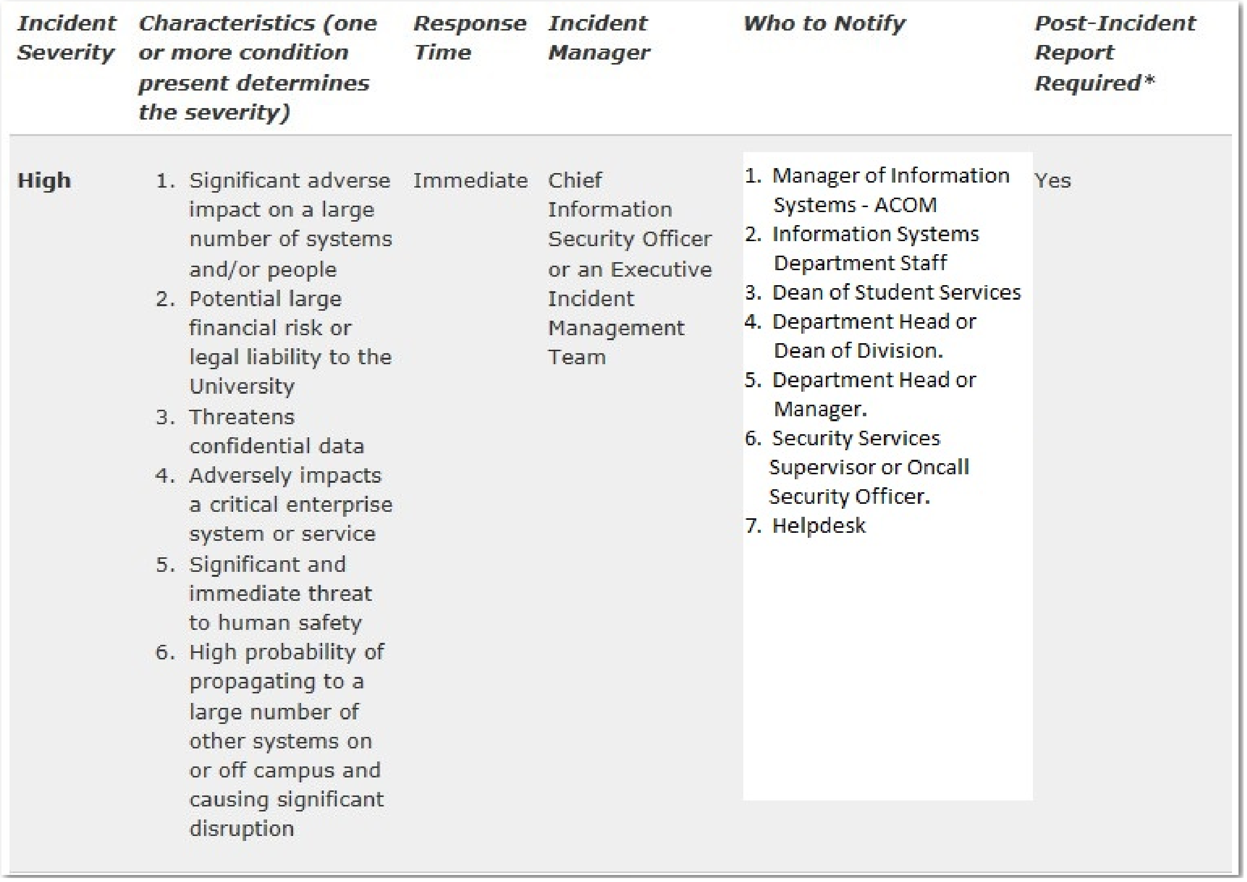
  Low severity incidents have the following characteristics:

  - Adversely impacts a very small number of systems or individuals
  - Disrupts a very small number of network devices or segments
  - Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate NA("Not Applicable")

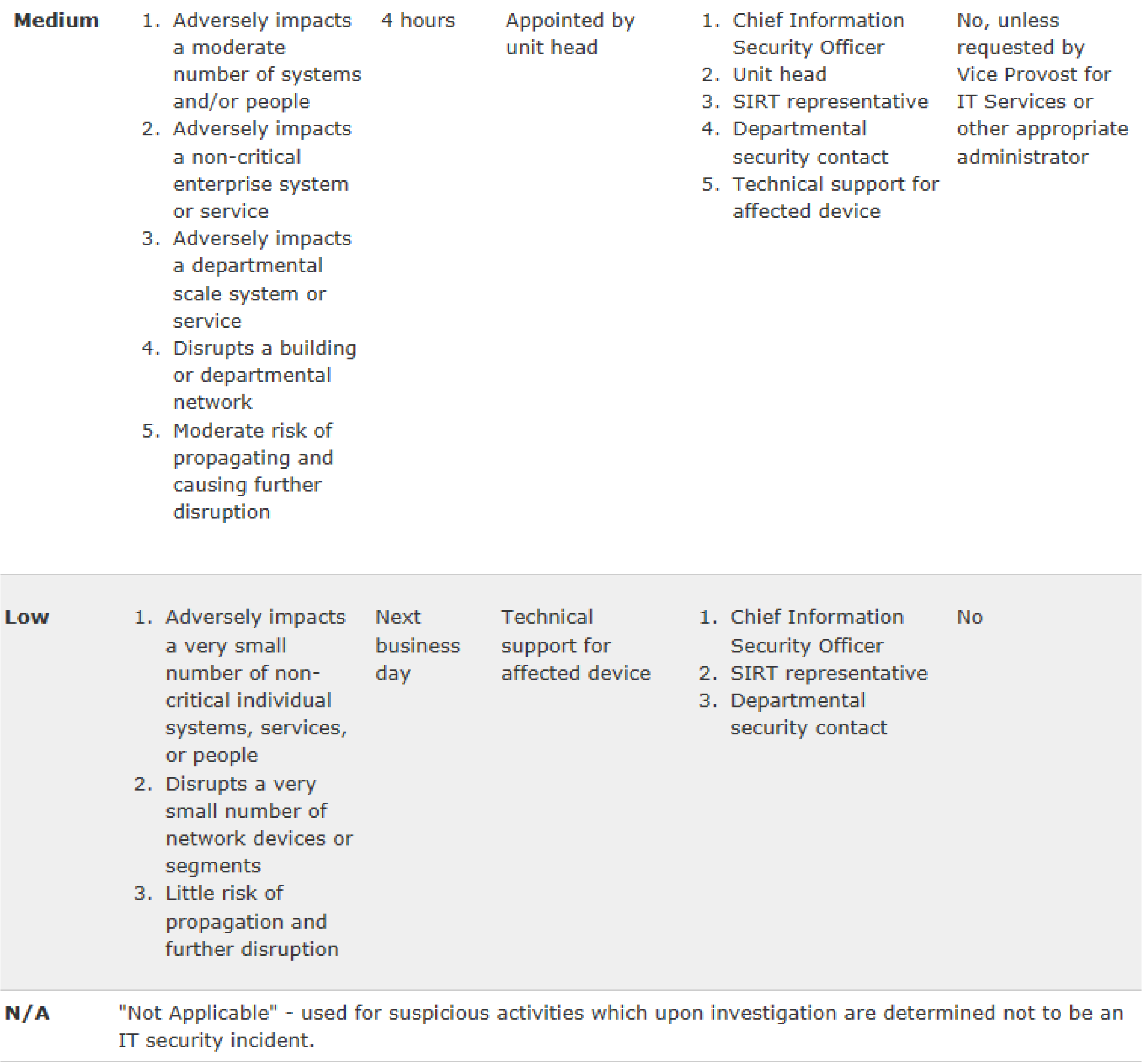
    This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found.

- Incident Response Summary Table

The following table summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements. Detailed procedures for incident response and management are further defined in the ACOM IT Security Incident Management Procedures.



Incident Severity	*Characteristics (one or more condition present determines the severity)*	*Response Time*	*Incident Manager*	*Who to Notify*	*Post-Incident Report Required**
High	1. Significant adverse impact on a large number of systems and/or people 2. Potential large financial risk or legal liability to the University 3. Threatens confidential data 4. Adversely impacts a critical enterprise system or service 5. Significant and immediate threat to human safety 6. High probability of propagating to a large number of other systems on or off campus and causing significant disruption	Immediate	Chief Information Security Officer or an Executive Incident Management Team	1. Manager of Information Systems - ACOM 2. Information Systems Department Staff 3. Dean of Student Services 4. Department Head or Dean of Division. 5. Department Head or Manager. 6. Security Services Supervisor or Oncall Security Officer. 7. Helpdesk	Yes



Medium	1. Adversely impacts a moderate number of systems and/or people 2. Adversely impacts a non-critical enterprise system or service 3. Adversely impacts a departmental scale system or service 4. Disrupts a building or departmental network 5. Moderate risk of propagating and causing further disruption	4 hours	Appointed by unit head	1. Chief Information Security Officer 2. Unit head 3. SIRT representative 4. Departmental security contact 5. Technical support for affected device	No, unless requested by Vice Provost for IT Services or other appropriate administrator
Low	1. Adversely impacts a very small number of non-critical individual systems, services, or people 2. Disrupts a very small number of network devices or segments 3. Little risk of propagation and further disruption	Next business day	Technical support for affected device	1. Chief Information Security Officer 2. SIRT representative 3. Departmental security contact	No
N/A	"Not Applicable" - used for suspicious activities which upon investigation are determined not to be an IT security incident.				

* See ACOM IT Security Incident Management Procedures for details about the Post-Incident Report

Related Laws, Regulations, or Policies

1. ACOM IT Security Incident Management Procedures

2. ACOM IT security team

3. ACOM Security Incident Response Team (SIRT)

4. ACOM Dean’s Committee Security Incident Policy and

Questions/Waivers

The Director of Information Systems - ACOM is responsible for this policy. The Dean or designee must approve any exception to this policy or related procedures.

Questions should be directed to the Director of Information Systems - ACOM.