No. CS001 Reporting an IT Security Incident

July 2009

Introduction

Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems on campus. Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals and the campus as a whole. This document outlines the procedure individuals should follow to report potentially serious IT security incidents and the actions the Computing Services Department will take upon notification of an IT security incident.

Section I – What to Report

For the purposes of this policy an "IT security incident" is any accidental or malicious act with the potential to:

- Result in misappropriation or misuse of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual or individuals

- Significantly imperil the functionality of the information technology infrastructure of the ASC campus

- Provide for unauthorized access to College resources or information

- Allow ASC information technology resources to be used to launch attacks against the resources and information of other individuals or organizations

Section II - How to Report

ASC faculty and staff should report all suspected computer security incidents to the Computing Services Help Desk at 587-7741. A help desk representative will record the caller’s contact information and data about the incident and forward it to the Computing Services Security Working Group (SWG). It’s recommended that the telephone be used for reporting purposes, rather than e-mail or other electronic means.

If the person reporting the incident wishes to maintain anonymity, the information may be sent via the college mail system to the Chief Information Officer. However, be advised that the effectiveness and timeliness of the response may be hampered if additional necessary information cannot be attained.

If a security incident is suspected, take the following steps to minimize any potential damage:

- Don’t turn the computer off

- Isolate the computer by disconnecting the (blue or yellow) network cable connecting the computer to the data port on the wall

- Don't continue to use the affected computer - don't move or alter files on the computer
- Preserve all pertinent evidence, as appropriate
- Notify your supervisor of the potential security incident

Section III - Computing Services Response

- Upon receipt of a call reporting a suspected computer security incident, the Computing Services Help Desk will review the above steps with the caller to minimize potential damage
- An "Emergency" Security Incident Work Order will be created by Help Desk personnel and assigned to the CIO and members of the SWG (Table 1)
- The SWG will review the information and make an initial determination as to the severity of the incident (Table 2)
- The incident will be assigned to a Computing Service IT professional for further analysis and resolution and/or forwarded to the Chief Information Officer for further action. The SWG will contact the individual who reported the incident to explain the steps being taken
- Based on an initial analysis and assessment, the assigned IT professional will focus on remediation of mission critical information and telecommunications systems, as well as those systems whose loss would constitute an immediate threat to the College
- Based on the severity and potential threat to the College, the CIO will inform appropriate College, legal and state officials

Table 1 - Security Working Group

(As of 01 July 2009)

Department or Function	**Primary Contact**	**Alternate Contact**
1. Banner Programmer	Bhargavi Pulavarti	Michael Rael
2. Banner/System Administrator	Alan Carbutt	Bob Mulqueen
3. Network/System Administrator	Randy Smith	Logan Hansen

4. Student Labs/Desktop	Chris Olance	Christine Wright
5. CIO	Mike Nicholson	Cameron Miller, Kevin Daniel, Tom Fuller

Table 2 - Incident Severity

Severity	**Symptoms**
1	A. Network or system outage with significant impact to the user population or operation of the College B. High probability of propagation. C. Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.) D. Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities. E. Notification of entities outside of the College is required.
2	A. Some adverse impact to the operation of the College B. Adverse effects are localized or contained, or minimal risk of propagation. C. No apparent release or compromise of sensitive data. D. Remedial but not immediate action is required. E. Notification of entities within the College is required.
3	A. Minimal impact to small segment of user population or operation of the College B. Completely localized, with few individuals affected, and presenting little or no risk to other entities. C. No loss or compromise of sensitive data. D. Remedial action is required. E. Individual notification is required.