

Reporting and Handling Security Incident Response Policy

Policy

Information security incidents occurring on the institution network or attached devices will be managed centrally by the Institution Chief Information Officer (CIO) and will include other campus resources as determined by the CIO.

Rationale

Centralized notification and control of security incident investigation is necessary to ensure that immediate attention and appropriate resources are utilized to control, eliminate and determine the root cause of events that could potentially disrupt the operation of the institution or the compromise of institution data or sensitive information.

Standards & Procedures

Standards

Computer Security Incident Response Team (CSIRT). The CIO, with the advice and assistance of college and departmental IT representatives, will have the capability to establish a CSIRT to respond to security incidents.

Campus-wide Outage. A campus-wide outage is a fault, event or other unforeseen issue causing failures to all or large portions of the campus communication and computing infrastructure, services and devices or key communication and computing resources such as a DNS failure or a loss of campus Internet access. This type of incident would be treated as a Critical Incident.

Incident Types. An incident is defined as an adverse event in an information systems and/or network device or the threat of the occurrence of such an event. Events may be characterized as unauthorized use of another's user account, unauthorized use of system privileges or execution of malicious code. Events characterized as environmental (such as natural disasters, electrical outages, heat damage, etc.) are not within the scope of this policy. The most identifiable types of event are:

Malicious code attacks—Attacks by programs such as viruses, Trojan Horse programs, worms, and scripts to gain privileges, capture passwords, and/or modify audit log to hide unauthorized activity.

Unauthorized access—Includes unauthorized users logging into a legitimate account, unauthorized access to files and directories or operation of "sniffer" devices.

Disruption of services—Includes erasing of programs or data, mail spamming, denial of service attacks or altering system functionality.

Misuse—Involves the utilization of computer resources for other than official purposes.

Espionage—Stealing information to subvert the interests of a corporation or government entity.

Hoaxes—Generally an e-mail warning of a nonexistent virus.

Incident Severity. Incidents will be classified by the CIO based on the perceived impact on institution resources:

Critical—Severe risk to the institution network and/or external systems over the Internet. May be characterized by widespread risk of compromise of multiple systems or high risk of compromising sensitive information. Criteria for determining if an incident is critical include but are not limited to: health and safety of personnel, legal issues, possible harm to the institution's reputation.

Medium—Medium risk to the institution network and low risk to external systems over the Internet. May be characterized by risk of compromising more than one system, no risk to sensitive data, or isolation to a single system.

Low—Low risk to the institution network and no risk to external systems over the Internet. May be characterized by compromise of a system that does not host or process critical/sensitive information, does not pose a risk to other systems or types of devices.

DARTON COLLEGE TECHNOLOGY INCIDENT REPORT

Department of Campus Information Services

TO: Margaret Bragg, Director, OIT/CIO
Brian Anderson, Systems Analyst II/DBA
Ashley Coates, Network Analyst

Emergency Contact Numbers
Mobile 229-291-2465
Pager 229-431-6261
Mobile 229-894-9688

Personnel Reporting Incident: _____ DATE _____

Location: _____

Time: _____ a.m./p.m. Security Called? Yes No
 Police Called? Yes No

Summary: _____

Name(s) of person(s) involved (including witnesses)	- Student: ID Number - Employee: Department - Visitor	Other Information (Relative, telephone number, etc)

OIT Personnel must complete other side of this form for report to be complete Revised: 03/2009

