ADMINISTRATIVE PROCEDURES

Title: IT INCIDENT RESPONSE	Identification:	9.07
	Page:	1 of 3
	Effective Date:	March 26, 2013
Authority: SBE 6A-14.0261 FS 1001.64; 1001.65	Signature/Approval:	Dr. Ken Atwater

PURPOSE

The purpose of this procedure is to provide guidelines for the response to incidents that threaten the confidentiality, integrity, and availability of College information assets, information systems, and the networks that deliver the information. This procedure outlines the establishment and ongoing deployment of trained emergency response teams, formed with the purpose of managing the aforementioned incidents at the College. This effort is being taken to improve the response time to incidents, to provide consistent response, and improve incident reporting.

PROCEDURE

1. SCOPE

The Office of Information Technology is responsible for implementing incident responses related to all system and services for which it is responsible. Nothing in this Incident Response procedure should be taken to be in conflict with the following· policies and procedures which include but are not limited to the following:

- College Security
- Acceptable Use
- Federal/State mandates/Laws
- Memoranda from the Administration

These procedures specifically exclude the following:

- Non-electronic information including paper mail.
- Physical security or emergency response.
- Contingency planning, business continuity and disaster recovery are handled by different procedures. An event may initially be declared a "Critical Incident" and subsequently declared to be a "Disaster." In this case, a critical incident response team would implement the Disaster Recovery process.

2. DEFINITION OF CRITICAL INCIDENTS AND THEIR CONSEQUENCES

A critical incident is any adverse event that threatens the confidentiality, integrity, or availability of College information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident.

A critical incident may include adverse events that include denial-of-service attacks, loss of accountability, or damage to any part of the system. Examples include but are not limited to the insertion of malicious code (e.g. viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.

Incidents as defined above vary in their impact on the College and in the degree of threat they pose; consequently not all incidents require the same response. Incidents with high impact and high threat involve high risk and great vulnerability to the College;

such high risk impact and high threat involve and great vulnerability to the College; such high risk incidents are called 'critical incidents' and require that a Computer Systems Emergency Response Team (CSERT) be assembled to apply appropriate response. An incident can only be declared "critical" by the Vice President, Information systems/Chief Information Officer (CIO), the College Chief Information Security Officer (CISO) or his/her designee. The CISO or the designee will activate the CSERT in the event of such a declaration.

Notification

- Faculty, staff, students, contractors, consultants, temporaries, and other workers at HCC, including all personnel affiliated with third parties using HCC information technology resources should notify the IT Help Desk immediately of any real or suspected security incident.
- Criminal activity or immediate risks to the safety of individuals should be reported to the College Public Safety Office or 911 immediately.

3. DEFINITION OF APPROPRIATE RESPONSE TO CRITICAL INCIDENTS

The following items define appropriate responses of a CERT to a critical incident:

- Determine the extent of the incident
- Assume control of the incident and involve appropriate personnel, as conditions require
- Report to the CIO/CSO for the decision on how to proceed
- Document all actions and results
- Begin interviews
- Contain the incident before it spreads
- Collect as much accurate. and timely information as possible
- Initiate a chain of custody of evidence
- Preserve evidence
  - Protect the rights of clients, employees, and others, as established by law, regulations, and policies
  - Minimize business interruptions within the organization
- Restore the system
  - Conduct a post-incident critique
  - Revise response as require

4. ORGANIZATIONAL STRUCTURE AND DELINEATION OF ROLES, RESPONSIBILITIES AND LEVELS OF AUTHORITY.

Summary of Responsibilities

- CIO - The Chief Information Officer (CIO) is responsible for the administration and leadership of all administrative technology. The CIO will communicate status of critical incidents to the College leadership.

- **CISO** - The Chief Information Security Officer (CISO) is responsible for the security of all electronic data and telecommunications equipment and traffic. The CIO or CISO or designee has sole authority to declare a critical incident and form a CSERT.

  The CISO or designee will communicate to the CIO that a critical incident has been declared and a CSERT formed. The CISO will also communicate status of critical incidents to the CIO, select and train incident response team members/coordinators, and develop and promote policies and procedures.

- **CERTC** - The Computer Emergency Response Team Coordinator (CERTC) is an individual who is selected to oversee and direct the Computer Emergency Response Team actions as well as to act as the single point of contact for the given incident. The CERTC Will typically also be responsible for ensuring that specific information is communicated to the CISO in a timely fashion and that all evidence is preserved as indicated by policy.

- **CSERT –** The Computer System Emergency Response Team is a group of individuals who have been trained in incident management, each having distinct response roles. The CSERT works under the direction of the CERTC.

5. CLOSURE

Once an affected system is contained, the problem is eradicated, or the system is no longer needed for forensics discovery, the CERTC will forward a recommendation to the CISO to place the system back in production. The CISO will have sole discretion in the decision to place a system back into production once it has been taken out due to a critical incident.

HISTORY: New