Title: Incident Response  
ID: CSS002  
Revision: 1.0

Purpose  
This procedure defines how security incidents should be identified, investigated, and resolved.

Scope  
This procedure applies to all systems within the Computer Science Department.

Incident Detection  
● Possible incidents may be detected using either internal alert systems or notifications provided by external entities via an email to abuse@cs.odu.edu.

Incident Investigation  
● Upon identification of a possible incident, the offending system or a network may be monitored or scanned to determine if an incident has occurred.  
● In the event that a possible incident involves systems or network which may contain confidential information, the offending systems will be taken offline and quarantined so that forensics can be performed locally.

Incident Response  
● In the event that an incident has occurred, the offending system or network will be investigated to determine the effects of the compromise. These effects include (but are not limited to): information disclosure, internal compromise attempts, and data loss.  
● In the event that an incident has occurred, the offending system or network will be investigated to determine the possible mechanism of compromise.  
● Upon completion of investigation, a compromised system or network will be either repaired or erased at the discretion of the Network Security Administrator.

Definitions  
Incident - an incident is defined as an event in which information or system access is obtained by parties who are not authorized to have or view such access or information.

Revision History