Security Incident Response Procedures
Office of Information Technology
Connecticut State Colleges & Universities

An IT security incident is defined as an event that impacts or has the potential to impact the confidentiality, availability, or integrity of IT operation and resources. The Security & Policy Program Office (S&PPO) of ConnSCU has primary authority in response decisions for IT security incidents and coordinates incidents from discovery through resolution and closure.

I. Security Coordinator

Each institution will appoint primary and secondary security coordinators. The security coordinator will coordinate all communications and activities between the Program Office of Security & Policy and institution IT team.

II. Notification

The IT leaders at colleges and universities must notify the Security & Policy Program Office immediately upon discovery of security incidents on their campus that impact mission critical services or involve the potential for unauthorized disclosure or acquisition of DCL3/Class A data. The S&PPO is in the process of developing a notification system and standard templates. Until the system is available, CSUS and Charter Oak should email security@ct.edu with the required information. The CCC should follow the document notification process and continue to send e-mails to security@commnet.edu and complete the malware tracking spreadsheet.

The Security & Policy Program Office will direct notification to senior administration, Office of the Attorney General, and other parties as appropriate. Each institution should also establish appropriate internal communication procedures regarding all incidents. The following incidents must be reported immediately upon discovery:

A. Incidents that seriously affect data center operation resulting in partial or complete shutdown of the data center:
    a. Physical Security – unauthorized access, loss of equipment
    b. Environmental – power failure, overheating, water damage
    c. Cyber Security – virus, intrusions

B. Incidents that affect network closets:
    a. Physical Security – unauthorized access, loss of equipment
    b. Environmental – power failure, overheating, water damage

C. Any security incidents that involve administrative departments with access to personal, financial, or FERPA data:
    a. Human Resources
    b. Registrar
    c. Admission
    d. Finance

e. Financial Aid
f. Bursar
g. Police
h. Athletics
i. Health Center
j. Institution Research
k. Other departments that may meet the criteria

The incidents include:

- ✓ Malware infections with the potential to compromise DCL3/Class A data
- ✓ Loss of paper documents containing DCL3/Class A data
- ✓ Loss of mobile devices (laptop, smartphone, USB drive, and tablet)
- ✓ Employee misconduct issue that may put DCL3/Class A data at risk

D. Notices from FBI, Homeland Security, or other law enforcement agencies about suspicious cyber activities.
E. Any other incidents that may involve personal, financial, or FERPA data.

The following information should be included in the notification:

- Institution Name
- Incident security coordinator
- Date & time of the incident/compromise, if known
- Date & time of the discovery
- Type of incident (Physical security, environmental, malware/virus, loss of mobile devices, loss of paper documents)
- Location of the incident, if applicable
- Name, Department, Job Title and contact information of the end user(s)
- A detailed description of the compromised host/device including maker, model, and OS.
- A brief description of the incident

Note: The S&PPO is in the process of developing a notification system and standard templates. Until the notification system is available, CSUS and Charter Oak should e-mail security@ct.edu with the required information. The CCC should follow the document notification process and continue to send e-mails to security@commnet.edu and complete the malware tracking spreadsheet.

III. Containment

A. For physical security or environmental incidents that involve data center or network closets, please notify Facilities and Police as well.

B. For incidents involve loss of mobile devices or paper documents:

- Notify Police as well.
- For mobile devices:
    - Perform a remote wipe of the device if possible
    - Lock user account until the password reset

C. For incidents involving malware, please follow the steps below to protect the evidence:
    a. When to shut the service or system off
        - Data is actively being compromised
        - System performance is at an unacceptable level
        - Files are actively being deleted or compromised
    b. When not to shut the service or system down:
        - The need to gather further evidence
        - Data may be lost when the service or system is shut off
        - Shutting the system down may tip our hand to the intruder
        - The need to add additional monitoring capabilities
        - Protecting evidence
        - The system needs to be secured until initial forensics are completed and the system can be quarantined

    Note: Malware detection by ePO or fake alert doesn't require the system to remain running.

    c. Evidence Protection – The system needs to be secured until initial forensics is completed and the system can be quarantined.
    d. Maintaining/collecting Monitoring Data – It is important not to lose any monitoring data that occurred during the incident. The following steps need to be taken to maintain log data:
        - If logs are not stored to a log server, backup logs for the duration of the event
        - Stop backup rotations for the system or systems in questions and archive tapes
        - If logging is not enabled, and can be, enable it for the affected systems
        - If logging is not enabled at the appropriate levels set it to the appropriate level for the event

IV. Incident Tracking

Upon receiving the notice, the Security & Policy Program Office will assign an incident ID and assign a point person to coordinate the incident response with institution's security coordinator. Regular status update will be entered by the S&PPO point person or security coordinator in the incident tracking system as updates are available. All related documentations will be stored in the incident tracking system for future reference.

Note: The S&PPO is in the process of developing an incident tracking system. Until the system is available, CSUS and Charter Oak will track incidents in the CCC incident tracking spreadsheets and send e-mail notifications on major updates. The CCC should continue to use malware tracking spreadsheets for their college.

V. Investigation

Investigation includes analysis, identification, prioritization, and evidence collection and retention.

A. Incidents involve malware or virus –
    a. Colleges and Charter Oak should engage the Office of Security & Policy immediately for all virus infection incidents on system that have the potential to compromise DCL3/Class A data

       Note: The CCC should follow the current notification process for all systems with potential access to DCL3 data. Charter Oak should send an e-mail to security@ct.edu for any system that has potentially compromised DCL3/Class A data.

    b. Prior to engaging the Security & Policy Program Office for investigation, University IT team should perform preliminary investigation and evaluate the potential security breach and determine the following
        - Verify that the malware or virus has the potential to exploit DCL3/Class A data
        - Scan the local and network mapped drive. Verify that the user(s) have access to DCL3/Class A data.

       If both criteria are met, university must contact the S&PPO at security@ct.edu immediately.

    In the event of a security investigation, the Security & Policy Program Office acts on behalf of Board of Regents and should be given complete and timely access to university network, systems, data, and personnel. All requests made by the Security & Policy Program Office should be treated as highest priority and be accommodated accordingly. There may be times that the S&PPO needs to use 3rd-party forensic service to perform advanced investigation. Any expenses incurred will be charged back to the institution.

    If forensic analysis is conducted and a determination is made that DCL3/Class A data is potentially compromised, the S&PPO will release an investigation report with recommendations.

B. The Campus Police will lead the investigation of all other incidents. The S&PPO will provide support upon request.

VI. Resolution

Compromises must be resolved as soon as possible, and within two weeks of the notification. Compromised hosts need to be maintained for forensic examination. Upon completion of forensic examination the host must be reformatted, rebuilt and have vulnerabilities resolved before reconnecting them to the network. Incidents must be resolved to the satisfaction of the Security & Policy Program Office. In some cases, the S&PPO may request privileged access to ensure the host is safe to resume network connectivity, or may require that it be evaluated for vulnerabilities before being placed back in service. The S&PPO must be informed of incident resolution details. The security coordinator must enter details about the incident resolution in the incident tracking system. The institution security coordinator must distribute to impacted users and their supervisors a summary of the compromise including:

- Impact on the user's work

- Remediation or preventative measures the users should take

In particular, if passwords have been compromised, they must be reset and changed by the users, once the system has been secured.

VII. Closure.

The Security & Policy Program Office reviews the tracking system and closes tickets when appropriate. In the event of a serious security breach, the Security & Policy Program Office will produce an executive summary report. The report will be shared with internal auditors, institution IT team, and senior management at both BOR and institution.

VIII. Personal Identifiable Information

The "personal identifiable information" means an individual's first name or first initial and last name in combination with any one, or more, of the following DCL3/Class A data:

- Social Security Number,
- Driver's license number,
- Financial account, credit card, or debit card number, , in combination with any security code, access code or password,
- Passport number,
- State identification card number,
- Alien registration identification number,
- Health insurance identification number.

Date: 03/20/12
Version: V1.0