COLLEGE of COASTAL GEORGIA
UNIVERSITY SYSTEM OF GEORGIA

Incident Response – Technical Procedures

Reference USG IT Handbook Section 5.3

Level

Engagement

Incident Identified
1. Confirm and document incident and identify system(s) involved
2. Identify business process and/or application(s) affected
3. Investigate system for known exploits

Incident Remedied / Resolved
End Process

Incident Categories
IT Handbook – Section 5.3.6.4

Cat 0 – Exercise / Network Defense Testing
Cat 1 – Unauthorized Access
Cat 2 - Denial of Services
Cat 3 – Malicious Code
Cat 4 – Inappropriate Usage
Cat 5 – Probes and Recon Scans
Cat 6 – Investigation
  PII – Personal Identifiable Information
PHI– Protected Health Info

Level 1

unauthorized access, misuse, or other inappropriate behavior by an employee, or the security breach involves personal identifiable information? (Reference Incident Categories)

Does incident involve: — No →

Yes ↓

Remediation Actions
- Clean machine using appropriate methods
- Apply appropriate patch(s)
- Apply any available updates (OS and App)
- Ensure anti-virus and firewall are installed and configured
- Ensure SCCM agent is configured/alerts set
- Restore data from backups as necessary
- Change system and user passwords
- Document actions taken in ticketing system & SCCM
- Monitor system(s)

Level 1 Incidents
Before re-imaging answer these questions:

- Is there a management concern?
- Has management been notified?
- Instead of re-imaging, can the original hard drive be perserved?

Level 2

Report Incident to CCGA Info Security Officer (ISO)

Report Incident to CCGA Executive Incident Response Team Point of Contact (Chief Information Officer)

USG Cyber Incident Management Protocol
(Reference Section 5.3 of USG IT Handbook)
Info Sec: http://www.usg.edu/infosec/incident_management

1. Immediately call the ITS Helpdesk, **706-583-2001** or **1-888-875-3697** (Toll free within Georgia).
2. Step away from the computer; do not touch it or take any other action until advised by TSS or Information Security & ePrivacy.
3. Do not attempt to login, or alter the compromised system or power it off. These actions will delete forensic evidence that may be critical to your incident.
4. Do not talk about the incident with any other parties until you are authorized as part of the process outlined in this document.
5. From another computer, download the following file: Abuse Notification (04-21-2014) and USG INSTITUTION INFORMATION SECURITY INCIDENT REPORT and email the completed form to with details of the suspected exposure.

Reference Guides

USG Sensitive Data Exposure Incident Checklist Flow Chart
http://www.usg.edu/infosec/documents/USGSensitive_Data_Exposure_Incident_Checklist_Flow_Chart.pdf

Abuse Notification (04-21-2014)
http://www.usg.edu/infosec/documents/USG_Security_Incident_Report.pdf

USG Instition Information Security Incident Report
http://www.usg.edu/infosec/documents/USG_Security_Incident_Report.pdf

Level 2 Incidents
Incidents include, but are not limited to:
(anything that is not malware)

- Anything that is not readily identified as malware.
- Incidents that may require coordination with USG ISO, Police, USG Legal or external agencies such as the FBI, GBI, etc.
- Situations which could result in employee or legal action.

Tech Advisory Committee Approved
2/18/16

Cabinet Approved
3/1/16