Gordon State College — Incident Response – Technical Procedures

Reference USG IT Handbook Section 5.3

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

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 → Report to IT Helpdesk
helpstar@gordonstate.edu
678-359-5008

Yes → Report Incident to Information Security Officer
678-359-5907 (preferred)
cybersecurity@gordonstate.edu

Remediation Actions
- Clean or reimage machine using appropriate methods (See Level 1 Incidents)
- Apply appropriate patch(s)
- Apply any available updates (OS and App)
- Ensure anti-virus is installed and configured
- Ensure LANDesk agent is configured
- Restore data from backups (if applicable)
- Change system and user passwords
- Document actions taken in Helpstar ticketing system
- Monitor system(s)

Level 2

Report Incident to Ad-Hoc Incident Response Team Point of Contact (Director of IT)

Formally notify President and/or Cabinet officials as appropriate

USG Cyber Incident Management Protocol
(Reference Section 5.3 of USG IT Handbook)
Cybersecurity: https://www.usg.edu/cybersecurity/incident_management

1. USG organizations' must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information and report cybersecurity incidents to USG Cybersecurity.

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 GSC IT or other Cybersecurity officials.
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. Remove the system from the network by unplugging the network cable or disconnecting from the wireless
5. Do not talk about the incident with any other parties until you are authorized as part of the process.

Reference Guides

USG IT Handbook https://www.usg.edu/assets/information_technology_services/documents/IT_Handbook.pdf
Federal Incident Reporting Guidelines https://www.us-cert.gov/government-users/reporting-requirements
Gordon State College Incident Response Collaborative Model

Level

US-CERT Incident Reporting Guidelines

Cat 0 – Exercise / Network Defense Testing
Cat 1 – Unauthorized Access
Cat 2 - Denial of Services (DoS)
Cat 3 – Malicious Code
Cat 4 – Improper Usage
Cat 5 – Scans/Probes/Attempted Access
Cat 6 – Investigation
Immediately Trigger Level 2 Procedures for breach involving…
PII – Personal Identifiable Information
PHI– Protected Health Info

Level 1 Incidents
Before re-imagining 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 Incidents
Incidents include, but are not limited to:

- Incidents affecting systems or data categorized as moderate or high for any of the security objectives of confidentiality, integrity, or availability.
- 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.

09/18/2018