## Incident Response – Technical Procedures

### Reference USG IT Handbook Section 5.3

#### Level

<table>
<thead>
<tr>
<th>US-CERT Incident Reporting Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cat 0 – Exercise / Network Defense Testing</td>
</tr>
<tr>
<td>Cat 1 – Unauthorized Access</td>
</tr>
<tr>
<td>Cat 2 - Denial of Services (DoS)</td>
</tr>
<tr>
<td>Cat 3 – Malicious Code</td>
</tr>
<tr>
<td>Cat 4 – Improper Usage</td>
</tr>
<tr>
<td>Cat 5 – Scans/Probes/Attempted</td>
</tr>
<tr>
<td>Cat 6 – Investigation</td>
</tr>
<tr>
<td>Immediately Trigger Level 2 Access for breach involving...</td>
</tr>
<tr>
<td>PII – Personal Identifiable Information</td>
</tr>
<tr>
<td>PHI – Protected Health Info</td>
</tr>
</tbody>
</table>

#### Engagement

<table>
<thead>
<tr>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access, misuse, or other inappropriate behavior by an employee, or the security breach involves personal identifiable information? (Reference Incident Categories)</td>
</tr>
</tbody>
</table>

**Yes**

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

**No**

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

#### Level 2

<table>
<thead>
<tr>
<th>USG Cyber Incident Management Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity: <a href="https://www.usg.edu/cybersecurity/incident_management">https://www.usg.edu/cybersecurity/incident_management</a></td>
</tr>
</tbody>
</table>

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.

### 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 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 preserved?

### 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.

### Reference Guides

- **USG IT Handbook**  
  [https://www.usg.edu/assets/information_technology_services/documents/IT_Handbook.pdf](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](https://www.us-cert.gov/government-users/reporting-requirements)

- **Gordon State College Incident Response Collaborative Model**