Information Security Incident Response Policy

Document ID:
Policy type: Administrative
Effective date:
Last revised:
External requirement for review:
Compliance reporting:
Policy owner: Gordon State College (GSC) Information Technology department
Policy contact: Troy Stout, System Administrator, troys@gordonstate.edu

1 Reason for Policy

The number of cybersecurity incidents causing disruption and damage continue to escalate across the globe. Preventive activities, such as limiting access to networks and computers through user access controls, security awareness training initiatives, mitigation of security risks, and implementation of emerging firewall technologies help to reduce security incidents, but not all incidents can be prevented. Therefore, it is imperative that organizations develop a strong incident response capability in order to rapidly detect incidents, minimize loss and destruction, mitigate weaknesses found, and restore IT services. This Information Security Incident Response Policy is maintained to properly respond in a consistent manner, with appropriate leadership and technical resources, to cybersecurity incidents and to comply with:

- **University System of Georgia (USG) Board of Regents (BOR) Policy 11.3 Information Security Policy**: *all USG institutions…shall create and maintain an internal information security technology infrastructure consisting of an information security organization and program that ensures the confidentiality, availability, and integrity of all USG information assets.*
- **USG Information Technology (IT) Handbook Section 5.3: Incident Management**

2 Policy Statement

All members of the Gordon State College community are responsible for reporting known or suspected information technology cybersecurity incidents. All cybersecurity incidents at Gordon State College **must** be reported to the Information Security Officer (ISO), or, in the ISO's absence, the Director of Information Technology. The institution **will** promptly investigate, document, recover from, and report such incidents involving loss, damage, misuse of information assets, or improper dissemination of information.

Incident management and response will be handled appropriately based on the type and severity of the incident in accordance with the procedures set forth in GSC's Incident Response Technical Procedures

and the Collaborative Model process flow charts. Cybersecurity incidents affecting systems or data categorized as moderate or high for any of the security objectives of confidentiality, integrity, or availability will be overseen by the *Incident Response Team*.

The lessons learned from the incident response will be used to enhance processes, methods, and capabilities in the future.

3 Scope

All Gordon State College IT resource users, and all Gordon State College IT resources, are covered by this policy.

4 Definitions

Term	Definition
Cybersecurity Incident	Any event that is a violation or imminent threat of violation of college cybersecurity policies, acceptable use policies, or standard security practices that may adversely affect the security of Gordon State College information or systems that process, store, or transmit information. Examples include, but are not limited to: a) Widespread infections from virus, worms, Trojan horse or other malicious code; b) Loss of a thumb drive containing sensitive data c) Unauthorized use/access of computer accounts and computer systems; d) Unauthorized, intentional or inadvertent disclosure or modification of sensitive/confidential data; e) Compromise of any server, including Web server defacement or database server; f) Attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or system or national security;
Incident management	Process of detecting, analyzing, and mitigating threats or violations of security policies and limiting their effect on business operations.

5 Plans

This policy is implemented in an associated plan.

Subject	Procedure
Incident Response Technical Procedures	(document locator/hyperlink)
Incident Response Collaborative Model	(document locator/hyperlink)

6 Responsibilities

This section establishes the roles and responsibilities necessary to manage GSC's Information Security Incident Response.

6.1 Information Security Officer (ISO)

The Information Security Officer is the college's primary escalation point of contact (POC) for cybersecurity incidents and is responsible for reporting the incident to the Director of Information Technology. The Information Security Officer is designated as the primary Incident Manager at Gordon State College. If the Information Security Officer cannot be reached in a timely manner, the Director of Information Technology should be contacted.

6.2 Incident Response Team

The Incident Response Team oversees the handling of security incidents involving loss, damage, misuse of information assets, or improper dissemination of information. This team has the authority to make decisions related to the incident and to notify appropriate parties. The team consists of:

- Director of Information Technology (Point of Contact)
- VP of Finance and Administration
- Compliance Officer
- Human Resources
- Information Security Officer
- Public Safety
- Public Information
- System Administrator
- President and Cabinet (Ex officio members)
- Others as needed (e.g. unit head of affected area)

6.3 Director of Information Technology

The Director of Information Technology is responsible for convening the Incident Response Team after notification from the Information Security Officer.

6.4 Users

All members of the Gordon State College community, including all college personnel (administrators, faculty, and staff), students, contractors, guests, and other affiliates that use the college's information technology resources or data are responsible for promptly reporting suspected or known cybersecurity incidents to the Information Security Officer.

7 Enforcement

Failure to report a suspected cybersecurity threat or take action upon such a report in a timely manner may result in the loss of privileges for the Gordon State College information system and network resources, and/or disciplinary action up to and including termination or expulsion as detailed in applicable Gordon State College policies. Cybersecurity incidents may or may not have legal and/or criminal implications as well.

8 Related information

Resource	Link
USG BOR IS Policy	http://www.usg.edu/policymanual/section11/C430
USG ITS IT Handbook	http://www.usg.edu/information_technology_services/it_handbook/
USG Cybersecurity Incident Management	https://www.usg.edu/cybersecurity/incident_management
NIST SP 800-61, Computer Security Incident Handling Guide	https://www.nist.gov/

9 Policy History

Revision date	Author	Description
2018-09-17	Troy Stout	Initial Version