Policy Title:	Information Security Incident Response Policy
Issue Date:	January 1, 2011
Effective Date:	November 21, 2016
Last Reviewed:	November 18, 2016
Responsible Office:	Chief Information Officer
Contact Information:	University Information Technology Services/ Information Security Office Phone: (470) 578-6620 Email: iso@kennesaw.edu

1. Purpose Statement

The Kennesaw State University (KSU or the University) Information Security Incident Response Policy establishes responsibilities associated with the coordination of the University's information technology (IT) incident response. The policy is necessary in order to ensure the timely remediation of campus IT incidents as well as in post-incident information gathering and reporting of infrastructure-affecting and security-related events. This policy is aligned with the University System of Georgia's (USG) requirement that KSU establish an internal capability for handling security incidents.

2. Background

The Kennesaw State University Information Security Incident Response Policy complies with the USG information technology policies. Pursuant to the USG *Information Technology Handbook*, Section 5.1.2, KSU is required to establish and maintain "appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated, paper file, or database."

3. Scope

The KSU Information Security Incident Response Policy applies to all computer systems and networks connected to the KSU network and any remote access (e.g., dial-up connections, VPN connection, etc.) onto the campus network or associated domains.

4. Exclusions or Exceptions

The Kennesaw State University Information Security Incident Response Policy may be exempted only via approval from the Chief Information Officer.

5. Definitions

Definitions are available via the IT Glossary on the KSU Policy Portal at policy.kennesaw.edu.

6. Policy

Understanding that no controls are perfect, policies and procedures must be in place to address the compromise of a University system. The first priority in such a situation is to prevent the attacked system from doing additional damage, either to its own system and files or to the campus network. Second is to protect the confidentiality, integrity, and availability of the data on the system. Third is to restore the compromised machine to functionality in a timely manner. Fourth is to analyze the factors that led to the compromise and introduce safeguards to mitigate risk in the future. During all four of these steps, the Information Security Office (working closely with the respective system administrator) will retain management and control of the compromised system.

7. Associated Policies/Regulations

a. USG *Information Technology Handbook*, 5.3 Incident Management

8. Procedures Associated with this Policy

a. Antivirus Standard
b. System Compromise Procedures

9. Forms Associated with this Policy

a. As required by information in Sections 7 and 8.

10. Violations

Servers connected to the KSU network found to be in violation of the Information Security Incident Response Policy may be disconnected from the network without notice and may result in disciplinary action.

11. Review Schedule

The Information Security Incident Response Policy is reviewed annually by the Office of the CIO or his/her designee.