Georgia Southern University

Incident Response Procedures

Purpose

All authorized users have an interest in the security of the computer resources at Georgia Southern University, and share in the responsibility for protection of those resources, prevention of problems, and incident detection and response. The purpose of this document is to describe the general procedures that will be followed in response to a security incident involving University resources. Cooperation of personnel with these procedures is mandatory. A security incident is defined as a threat to the legitimate use and/or operation of any University computing resource as defined in the Computer Use Policies, or the actual occurrence of any situation identified as a potential risk to those resources. Threats may be internally or externally generated.

Security Incident Response Team

Security incidents will be responded to by a specially-formed team of individuals from across the University, the Security Incident Response Team (SIRT). This team will be comprised of technical resources with the appropriate skills to identify, assess, respond to and communicate the effects of security incidents. SIRT members will be designated by the Director of Information Technology Services who is authorized as the designee of the Chief Information Officer, as per the Computer Use Policies, to take any and all necessary actions, including immediate confiscation and/or disabling of a University computer resource or the temporary termination of a computer account, to protect, investigate, and ensure the security and proper use of the computer resources. Full cooperation with the SIRT is required of all authorized users of Georgia Southern University computer resources.

Security Incident Response

Generally speaking, security incidents will be responded to by removing or deactivating the threat or cause of the problem as soon as possible and as completely as possible while investigative and corrective actions are taken. In addition, appropriate measures to support investigation of the incident will be taken. Cooperation of authorized users with these steps is required. Specifically, incident response procedures will include the following practices as appropriate.

1. Internal notification. All users and units are responsible for reporting any discovered unauthorized access attempts or other improper usage of University computing and network resources. If a security incident is discovered or reported, a user must take immediate action to ensure the protection of University resources and notify the following individuals:
    a. the technical support person for your area (if one exists);
    b. the unit head; and
    c. the office of Information Technology Services (681-5429).

2. Protection. If not already executed, appropriate measures will be taken as soon as possible after the discovery and identification of an incident to prevent additional loss of or harm to University resources. These measures will be completed by a member of the SIRT, in concert with the owner or administrator of the resource affected and his department head.
3. Investigation. Appropriate measures to determine the nature, scope and cause of the incident will be taken. These should be a cooperative effort between the SIRT and the owner or administrator of the computer or network resource. It should be understood that investigation of an incident is intended to uncover information that will help to
    a. resolve the problem at hand; and
    b. help the University to improve its practices and prevent or minimize the occurrence of such incidents in the future.

    As such, the full cooperation of all parties is expected and required.

4. Correction. Once the nature and scope of the incident is understood, the appropriate corrective actions to be taken must be identified and completed. These should include requirements for system administration activities in the future that will prevent a recurrence of similar problems.
5. Documentation of incident. Information about each security incident must be logged and maintained by the Security Incident Response Team. Information to be recorded includes:
    a. a description of the computer or network resource(s) involved;
    b. individual responsible for the resource(s);
    c. nature of the attack or incident;
    d. source of the attack or incident;
    e. University resources compromised or placed at risk;
    f. an assessment of actual harm or loss;
    g. a general estimate of time spent responding to the incident; and
    h. a description of corrective measures taken.
6. Notification. Persons whose accounts are known to have been accessed or compromised as a result of a breach or the response to a breach will be notified in a timely manner and as appropriate of the actions taken.

External Notification of Security Incidents

Release of information regarding a security incident beyond the offices and individuals named above must be coordinated through the Office of Public Relations and Office of Legal Affairs. If the security incident involves an attack from a known outside entity, that entity should be contacted by a representative of the SIRT with notification that the incident occurred and a request for information on what measures will be taken to prevent subsequent incidents.