

East Georgia College Information Technology Incident Response Policy & Procedures Computer Services Department

I. Introduction

This policy addresses IT incident response issues involving the college's IT resources.

The policies and procedures listed in this document provide a mechanism for East Georgia College faculty, staff and students to report any potential IT-related security incidents.

II. Definitions

IT Resource: A system or application that consists of computer hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network infrastructure, E-mail and web based services.

Security Incident: An incident meeting one or more of the following conditions:

Any potential violation of Federal law, Georgia law or East Georgia College Policy or Plan involving an East Georgia College IT Resource.

A breach, attempted breach or other Unauthorized Access of an East Georgia College Information Technology Resource. The incident may originate from inside the East Georgia College network or via an outside entity.

Internet worms, Trojans, viruses and similar destructive files / services

Any action and/or conduct using in whole or in part an East Georgia College Information Technology Resource which could be construed as harassing, or in violation of any East Georgia College policy or state / federal regulation.

Unauthorized Access: Any action or attempt to utilize, alter or degrade an IT resource owned or operated by East Georgia College in a manner inconsistent with the college policies.

III. Reporting and Response Procedures

All incidents involving East Georgia College's IT resources will be handled via the following procedures:

1. Department or Division Manager will be notified of incident.
2. Department or Division manager will communicate incident to Director of Computer services. If it is unclear as to whether an issue / situation should be considered an IT security incident, the Department or Division manager should contact the Director of Computer Services for assistance.
3. The Director of Computer Services, Department or Division Manager will communicate incident to college's senior administration. The college's

- Human Resources Officer, and if necessary, the college's campus security office will also be notified of incident.
4. Depending on scope of incident, the Office of Information and Instructional Technology (OIIT) will also be contacted.
 5. If warranted, local law enforcement officials will be notified.
 6. All issues (cause, scope, resolution) relating to the security breach incident will be documented by and retained in the offices of the college's senior administration. Any costs associated with the security breach will also be documented.
 7. Individuals (faculty, staff or student), who report a breach of security incident will receive appropriate feedback and updates regarding the incident from one or more of the following areas: college's senior administration; human resources department; campus security department; department / division manager; director of computer services.
 8. Individuals reporting a breach of security incident will be assured of confidentiality, and if necessary, appropriate protection.

Additional items regarding Reporting and Response:

With the exception of items listed below, it is imperative that any investigative or corrective action be performed ONLY by a member of East Georgia College's Computer Services Department.

1. When faced with a potential IT-related security situation, faculty and staff should do the following:
If the incident involves a compromised computer system, do not alter the state of the computer system. The computer system should remain powered on and all currently running computer programs should be left as is. Do not power down the computer or restart the computer.
2. Immediately disconnect the computer / laptop or other IT connected device from the campus network by removing the patch cable from the back of the computer. If the computer, laptop or device is utilizing wireless network connectivity, the system's wireless network hardware should be disabled via the Network Settings in the Control Panel or via the appropriate system configuration tool.