I. Incident Reporting

Users of Goizueta IT Resources must promptly report all *information security incidents/violations*. This should be done as soon as possible, but no later than 24 hours.

IT security incidents/violations should be reported to the Goizueta Information Services (IS) department. All security incidents are reported to IT Help Desk via phone or email to Support_Desk@bus.emory. All security reports will be investigated.

**Security events include, but are not limited to:**

- Computer security intrusion i.e.
  - Virus/worms and denial of service attacks
  - Hacks and attempted hacks
  - Spam
  - Port scanning
- Unauthorized use of systems or data
- Theft of data and/or loss or theft of equipment used to store potentially sensitive information
- Interference with the intended use of the IT resource
- Compromised user account
- Copyright infringements (machines that are serving/distributing copyrighted material)

II. Incident Response

The IS team is responsible for receiving the notification of a suspected computer security violation, logging incidents, initiating trouble requests, coordinating response efforts for resolution and communicating incidents. The IS team is responsible for providing resources during investigations by local and federal law enforcement agencies. In some circumstances, the IS team investigates and remediates.

**Security Incident Response Process**

For all security incidents, the IS Team will perform the following steps:

- Verify that the report is not a duplicate by reviewing the Security Incident Log
- Open an IT HelpDesk request (GBS TractIT!) which will include at least a portion of the original complaint and/or logs
- Report the incident to the CIO is deemed a *serious incident*
- Inform appropriate parties – This may involve a school news alert
- Investigate the machine (if applicable) immediately during the normal business hours. If the incident occurs outside the normal business hours, the machine will be disabled on the network and notify the user.
- Once the issue has been resolved (in some cases a complete reinstall of the operating system, installing anti-virus programs and/or updates, loading system patches and upgrades, etc), the HelpDesk request will be closed.
III. Central Incident Reporting

The IS team is also responsible for reviewing and investigating computer security incidents and coordinating the incident response with the General Counsel’s office (when necessary), Emory Netcom, Emory AAIT HelpDesk, Academic Technologies (ATG), Emory Housing, local support and system administrators.

While the definition of security events covers numerous potential and actual incidents, the requirement for Central Incident Reporting is aimed at serious incidents as defined below:

A serious incident is any incident that poses a threat to University resources, stakeholders and/or services. Specifically, an incident is designed as serious if it meets one or more of the following criteria:

1. Involves potential unauthorized disclosure of sensitive information (defined below)
2. Involves serious legal issues
3. May cause severe disruption to critical services
4. Involves active threats
5. Is widespread
6. Is likely to raise public interest

Sensitive information is defined as information that “because of legal, ethical, or other externally-imposed constraints, may not be accessed without specific authorization or to which limited access may be granted. Sensitive information includes personally identifiable information such as student id, credit card numbers, Social security numbers, etc.