Incident Management

Maturing of University IT Incident Management

The University has many groups and people involved with managing IT incidents or IT related incidents. (When we say IT incidents, we are primarily concerned with “IT security incidents” such as the loss of a mobile device that has unencrypted sensitive information stored on it or a virus attacking a University-owned computer that stores sensitive information.)But “IT incident” isn’t a clearly defined term and different types of “incidents” are managed by specific authorities across the University, often in isolation. Because so many people and groups are involved, there are potential conflicts of authority and the guidance about how to handle incidents can be confusing.

Everyone affiliated with UNC-Chapel Hill, including anyone with a University guest ID, could experience an IT incident. Currently, guidance on what steps to take after an incident occurs are not clearly defined, and in some cases, the guidance from schools and divisions conflicts with the official University guidance.

A trigger for this new project is a new regulation under the Gramm-Leach-Bliley Act (GLBA), which requires that financial institutions implement programs to safeguard private information. We may not think of the University as a financial institution, but it is because of the numerous financial accounts we have, including tuition payments and student loans. GLBA requires us to have these safeguards in place by December 2022. Adding new or revised policy, in isolation, would add to existing confusion.

Goals of the Project

The goals of the project are to:

- develop clear guidance for individuals who may have experienced an IT or IT related incident, so they know where to go and what steps to take to report the incident.
- ensure the University is compliant with the GLBA Act by the deadline, which means we need to update the ITS Incident Management policy and related documents.
- collaborate with staff who also have authority regarding incident management (for example Institutional Integrity and Risk Management and University Counsel) to develop an understanding of how to provide clear guidance for schools and divisions that doesn’t conflict with the University’s Incident Management policy.
- develop instructions for schools and divisions on how to remain in sync with the University’s Incident Management policy and procedures so that users aren’t provided conflicting information on IT and related incidents.

Who this affects

While everyone affiliated with the University could potentially be affected by changes to how we manage an IT or IT related incident (in that anyone could experience an incident and benefit from clear, unconflicted guidance), this project will mainly affect:

- anyone needing to report an IT incident
- anyone involved in managing incidents on campus, both in ITS and in the schools and divisions.
- anyone involved in creating departmental policies related to security.

Incident Management

Next Steps

A project team is being created that will include representatives from the Information Security Office, ITS Policy Office, Emergency Management and Planning, Office of Ethics and Policy Management and the University Controller’s Office.

The first steps the team will take are to

- identify and define what IT incidents are and what they are not, as well as incidents that appear to be IT related but are not (for example: an export-controls incident where a UNC staff member took the wrong thing out of the country and ITS has nothing to do with it.)
- Identify policies that overlap or conflict with the Incident Management Policy.

After there is a clear understanding of the scope of the work, the team will engage campus stakeholders with IT incident management authority to agree on an approach for how to update policies to remove conflicts and create and publish clear guidance so that anyone with a responsibility for Incident Management policies can more easily remain in sync with the University’s Incident Management Policy.

Resources

- Incident Management Policy at UNC-Chapel Hill
- FTC: Gramm-Leach-Bliley Act
- UNC Privacy Office