LITS Incident Response Process

Anyone

Start

Identify Event

Report event

Perform initial triage

Is event an incident?

yes

no

Notify LITS incident manager

Ongoing triage

Is incident resolved?

no

yes

Inform IMT

Incident Responder(s)

Open ticket & activate IMT

Campus level and/or info security?

no

yes

Notify HERT* and/or Grey Castle**

Incident Manager

Provide leadership & direction

• Actions during incident
• Finalizing incident

Conduct notifications

Manage incident response

Oversee internal and external resources

Post-incident tasks

Conduct post-mortem

Document & close ticket

LITS Incident Management Team (IMT)

EDUCAUSE 2017; Debby Quayle & Beth Bohstedt, Hamilton College
Library & Information Technology Services (LITS)
dquayle@hamilton.edu; bbohsted@hamilton.edu

*Hamilton Emergency Response Team
**Information security consultant
Hamilton College Library & Information Services (LITS) Incident Management Team Members

The LITS Incident Management Team (IMT) is a small group of people who oversee the communication and resolution of a LITS incident, defined as an unplanned interruption of services that falls within the purview of LITS to resolve. A full instantiation of this team includes the positions defined below. Depending on the nature of the emergency, at a minimum the Incident Manager, Resolution Manager and Communications Manager will be involved.

The following is assumed for anyone who is filling the roles defined below:
- Must own a cell phone
- Must be willing to be called or come to campus during off-hours (if deemed essential)
- Must be willing to step away from regular work responsibilities on a moment's notice and have a backup in place who can cover critical aspects of their work for them.
- It is recommended that the Incident Manager and backup take and pass the FEMA Incident Command System introductory course.

Incident Manager - the leader of the LITS Incident Management Team. This person is responsible for ensuring that all aspects of an incident are addressed in a coordinated and timely manner and will call together as many members of the IMT as is deemed necessary. The Incident Manager is also responsible for making certain a chronology of events is recorded for each service interruption, regardless of whether it rises to the level of a “declared incident.”

Resolution Manager - the person best qualified to oversee the resolution of the incident (not necessarily a member of the standing IMT). This person identifies and oversees the individuals who need to contribute to the resolution of the incident in accordance with the incident action plan. For very low level incidents, the Resolution Manager may be the person who actually resolves the incident.

Communications Manager - responsible for communicating the incident details to those affected. This person is responsible for ensuring that adequate internal and external communication is maintained. At all levels of the incident, the Communications Manager will work closely with the Incident Manager and the IMT (as necessary) to coordinate communications.

Logistics/Finance Manager
This person is responsible for securing and tracking the use of facilities, services, and materials in support of the incident response as well as managing/recording all costs associated with the incident, including the production of financial reports and cost accounting.

Security Officer - responsible for managing the response to an incident that threatens information security. During an incident, the Security Officer is responsible for recognizing, monitoring and assessing security hazards or unsafe conditions related to the incident. The Security Officer is responsible for developing measures to mitigate an insecure situation to ensure the security of campus information. In the event of a serious information security incident that requires the campus emergency response team and our cybersecurity services provider to step in, the Security Officer will serve as a liaison.

Incident Scribe
When the Incident Manager deems it to be necessary, an Incident Scribe will assume responsibility for logging the events of the incident in chronological order and may also record the Incident Action Plan (IAP).