LITS Incident Management Structure

Purpose & Objectives

Hamilton College LITS is committed to providing excellent library and information technology services in support of the mission of the college. We strive to act responsibly and proactively to anticipate and avoid incidents before they may occur. To this end, the division has numerous service standards, policies and procedures which typically permit problems to be resolved quickly and with minimal impact to the business processes or academic program of the college. However, there is always the potential for more serious disruptions of LITS services which require a quick and methodical response that involves the coordination of several individuals across various LITS teams. To make such response a smooth and minimally disruptive as possible, we have developed these procedures and organizational structures.

SCOPE

This plan will address and review the following topics in order to achieve its objectives:

Incident Management

Definition of an Incident

For the purposes of this document, an incident is an unplanned interruption of services that falls within the purview of LITS to resolve. Unplanned interruptions can occur with varying levels of impact and urgency for resolution. In general, the following factors should be considered in assessing the level of urgency and the appropriate response required.

Factors to be considered

- The number of people affected (or who, in some cases);
- The extent to which college business (academic or administrative) is disrupted;

    - For example, when more than one campus-wide system is involved.
- The timing of the problem: Is the affected process or service in its critical state?
    - For example, if a large format printer is down in January it is not urgent; at the end of the semester, it is;
- Anticipated or experienced[1] length of time to resolve or whether there is a viable workaround for the affected work process or service; "Viability" is more strongly related to moving the work forward in a timely manner and less strongly tied to user inconvenience;
- The level at which sensitive information is at risk.

Examples of critical LITS service interruptions that rise to the level of an incident include (but are not limited to) the following:

- Failure of campus network equipment, servers, or the Internet connection, making it impossible for a significant number of users to access information resources including ESS, SSS, Academic Server, Blackboard, e-mail , the Colleague system, library catalog (ALEX), web access (my.hamilton.edu, www.hamilton.edu, WebAdvisor,), Citrix, and campus-wide printing;
- Failure of the campus telephone system making it impossible for a majority of users to make outgoing calls, receive incoming calls, or retrieve voice mail;
- Facility problems in Burke, and the Music Library, including air conditioning failures, power failures, flooding, etc.. This also extends to buildings in which network core services are housed.
- Security breach, denial of service attack, widespread virus/malware attack, network intrusion;
- Problems in the Technology Enhanced classrooms or computer labs that interfere with the ability to conduct activities related to the academic program.

Initial Reporting

For any unplanned interruption of services, the LITS staff member who discovers the issue or is first informed of the issue will immediately notify the service provider, their supervisor, or the Incident Manager (IM). If the Incident Manager is notified first, she/he will immediately inform the Help Desk, and through them, the Circulation Desk. These units should be made aware of any unplanned service interruptions, even if it is not declared an incident. Employees should report service outages and building problems following current guidelines, which should result in either a LITS service provider or a LITS director being contacted. An incident reporting guide is provided below.

NOTE: Business hours are defined as 8:30 am - 4:30 pm, M-F (academic year) or 8 am - 4 pm (between the end of the spring semester and the beginning of the fall semester).

[1] "Experienced" refers to prior experience with a similar incident.

Any problem considered to be life threatening (e.g. fire) should be reported immediately to Campus Safety at 315-859-4000

Problem	**Service Provider-** **during business hours**	**Service Provider-** **non-business hours**
A suspected or confirmed service outage. For example: · Wireless · Phone · Web service	Help Desk 315-859-4181 or Circulation 315-859-4479 Network Services 315-859-5638	Help Desk 315-859-4181 or Circulation 315-859-4479 Network on call - refer to monthly email from NS
A suspected or confirmed problem with Library information services. For example: · Library Catalog · LibGuides · Databases	Help Desk 315-859-4181 or Circulation 315-859-4479 Library Information Systems 315-859-4487	Circulation 315-859-4479 or Research 315-859-4735
A suspected or confirmed problem with equipment. For example: · Scanners · Printers · Copiers	Digital Media Tutors 315-859-4735 Circulation 315-859-4479 or Research 315-859-4735	Digital Media Tutors 315-859-4735 Circulation 315-859-4479 or Research 315-859-47351.
A building problem. For example: · Elevator · Heating/cooling · Doors	Circulation 315-859-4479 Help Desk 315-859-4181	Circulation 315-859-4479 or Research 315-859-4735 Campus Safety 315-859-4000

The top number(s) listed in each column are the primary numbers to call. Those listed below are secondary.

Once notified, the IM will evaluate the situation in consultation with the appropriate team(s) and the factors that define an incident. A LITS incident will be declared if s/he believes it is warranted.

This flow chart (called LIMT Flow Diagram -V2.pdf) depicts the process - from a suspected incident reported to an incident declared.

Incident Declared

Once the IM declares a situation to be an incident, s/he will immediately notify the Communications Manager (CM). From this point, all internal and external communication will be managed by the CM. The IM will activate the remaining roles of the IMT as s/he deems necessary. The role of Incident Scribe will be assumed by either the IM or CM (as appropriate) until it is determined that the IS needs to be called.

Incident Concluded

Once the incident is resolved, the IM develops a draft summary of the event that includes the IAP (Incident Action Plan) and the event log as supporting documents. This will be shared with the participating members of the IMT for comment.The IM will also facilitate a “post mortem” meeting of the IMT for the purpose of improving procedures.

LITS Incident Management Team (IMT)

The LITS IMT is a small group of people who oversee the communication and resolution of a LITS incident. A full instantiation of this team includes an Incident Manager (IM), Resolution Manager (RM), Communications Manager (CM), Security Officer (SO) Logistics/Finance Manager (L/FM), and an Incident Scribe (IS). Each of these positions is defined below. Depending on the nature of the incident, at a minimum the Incident Manager, Resolution Manager and Communications Manager will be involved.

Members of LITS will be identified to fill these roles on an ongoing basis. Each will be responsible for naming a team member to cover their responsibilities in the event of an incident. In addition, each role will also have a named backup person who will assume the responsibilities of the role should the primary person be unavailable.

Incident Action Plan (IAP)

The IAP is a brief document that outlines the primary objectives to be achieved during the course of the incident. It is developed by the Incident Manager in coordination with members of the IMT. These include, but are not limited to:

- Identifying the nature of the incident,
- Prioritizing how it will be contained, and
- Identifying the actions required to resolve the incident.

The IAP is a living document that may be altered as the incident unfolds. It must be shared with all those who are involved in its implementation.

Back to top

Definitions of Roles

Requirements for filling these roles

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 IM and the backup IM take and pass the FEMA Incident Command System introductory course.

Incident Manager (IM)

The Incident Manager is the leader of the LITS Incident Management Team (IMT). The IM is the person 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 IM 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.” This log may evolve into the incident action plan (IAP).

Resolution Manager (RM)

This is the only role not filled on a “standing” basis. This person identifies and oversees the individuals (Incident Responders) who need to contribute to the resolution of the incident in accordance with the incident action plan. For very low level incidents, the RM may be the person who actually resolves the incident. This role will be filled by the person best qualified to oversee the resolution of the incident.

Communications Manager (CM)

The Communications Manager is responsible for communicating the incident details to those affected. The CM is responsible for ensuring that adequate communication is maintained. Other people may also be involved in the communication process at the discretion of the CM. At all levels of incident, the CM will work closely with the Incident Manager and the IMT (as necessary) to coordinate communications.

Logistics/Finance Manager (L/FM)

The L/FM 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 (SO)

The SO position is responsible for managing the response to an incident that threatens information security. During an incident, the SO is also responsible for recognizing, monitoring and assessing security hazards or unsafe conditions related to the incident. The SO is also responsible for developing measures to mitigate an insecure situation to ensure the security of campus information. The SO may have assistants if necessary. In the event of a serious information security incident that requires the HERT and GreyCastle to step in, the SO will serve as a member of the HERT and will serve as a liaison between the HERT and GreyCastle. The SO may also call on members of the LITS IMT to assist in the incident response if he/she deems it necessary.

Incident Scribe (IS)

When the IM 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).

LITS Incident Management Team (as of May, 2016)

(BU)=Backup

Position/Call Order	Name	Office	LITS Team
Incident Mgr.	Debby Quayle	315-859-4031	Help Desk & Training
Incident Mgr. (BU)	Beth Bohstedt	315-859-4485	Acquisitions & Access Services
Security Officer	Marty Sweeney	315-859-4164	Central Information Services
Security Officer (BU)	David Swartz	315-859-4918	Network & Telecommunication Services
Communications Manager	Kristin Strohmeyer	315-859-4481	Research & Instructional Design
Communications Manager (BU)	Katrina Schell	315-859-4479	Acquisitions & Access Services
Finance/Logistics & Scribe (BU)	Linda Lacelle	315-859-4994	Central Information Services
Finance/Logistics (BU) & Scribe	Terry Lapinski	315-859-4352	Administrative Services

Back to top