

Incident Response Plan

Policies & Procedures



Preparing people to lead extraordinary lives

Table of Contents

Organizational Details	3
Code of Conduct	6
Information Classification and Disclosure	7
Information Requests	8
Other requests	9
Human Error.....	10
Internal Contact List	11
Testing and Policy Review	12
Incident Handling	13
Definitions	16
Appendix	17

Organizational Details

Mission Statement

The mission of the Loyola University Chicago Information Security Incident Response Team (LISIRT) is to promote a computing environment which ensures the confidentiality, availability, and integrity of the University's data and systems. LISIRT will handle all information security incident analysis and response for systems managed by Information Technology Services (ITS), and will offer to assist with any information security incidents on systems within the Loyola network that are not managed by ITS. LISIRT will investigate reports of violations of Loyola ITS policies (<http://luc.edu/its/policies.shtml>). LISIRT will strive to consistently provide quality service in a timely fashion.

Constituency

The constituency of the LISIRT can include all persons accessing and using computing, networking, telephony and information resources through any facility of the University. These persons include students, faculty, staff, persons retained to perform University work, and any other person extended access and use privileges by the University given the availability of these resources and services, and in accordance with University contractual agreements and obligations.

Authority

When a security incident has been declared, the LISIRT team takes on the ownership and responsibility of the incident handling process. This can include directing key members of ITS staff on incident handling decisions and taking the necessary actions to remediate the issue without first discussing it with affected constituents. This includes the possibility of taking temporary action to mitigate a threat posed against the entire network by a segment of the network that is not managed by ITS. Any actions taken without previous discussion will be discussed with affected departments after the issue has been mitigated. The LISIRT will maintain open lines of communication with the affected constituents during the incident handling process.

Organizational Placement

LISIRT is housed within Loyola University Chicago's ITS division. The team will be headed by the Information Security Officer, or his or her appointee, referred to as the LISIRT lead in this document. The team will include members of the Information Security Department, as well as the Director of Enterprise Architecture and PMO.

The LISIRT may recruit key members within the University to aid in the handling of an incident. These members will run all communications, technical and logistical decisions through the LISIRT.

Services

LISIRT will provide the following services to its constituents:

- Incident handling
- Investigations of potential violations of Loyola policies

Incident Handling

The first step in the incident handling process begins when an [event](#) is detected by or reported to LISIRT. The LISIRT Lead will evaluate the event and determine if the Incident Response (IR) is appropriate. If the Incident Response is enabled, all the authority granted within this plan will be granted to the LISIRT and a [security incident](#) will be declared. Logging of the incident begins, and the incident is triaged in accordance with the procedures defined within.

If the LISIRT lead is unavailable during the time of the event, the LISIRT's backup, or any member of the LISIRT team, may declare a security incident and enable Incident Response after an evaluation of the event. The LISIRT team member that has escalated the incident will become the LISIRT Lead for the duration of the incident. At the time the LISIRT lead becomes available, he or she may decide to transition the LISIRT lead role.

Incidents will be brought to the attention of the ITS Directors, as well as the CIO, when they are first classified. All incidents will be detailed in a monthly report that is sent to the ITS Directors and to the CIO.

Investigations of potential violations of Loyola University policies

LISIRT serves a supporting role for Human Resources, Office of the General Counsel, Student Affairs, and other departments. Requests from departments not specifically identified previously must be authorized by Human Resources or the Office of the General Counsel. LISIRT will perform technical investigations at the request of these bodies, while appropriately respecting the privacy rights of all individuals involved. This can include accessing electronic and voice mail, in accordance with the ITS policies (<http://luc.edu/its/policies.shtml>).

Code of Conduct

All members of the Incident Response Team (LISIRT) are expected to adhere to the code of conduct detailed in this plan. Violations of the code of conduct may be grounds for dismissal from the LISIRT, and possible disciplinary action following standard University procedures for such actions, depending on the nature of the violation.

The code of conduct is designed to ensure that LISIRT members are professional, consistent, and service oriented, while exercising appropriate care and providing quality service.

Individuals covered

This policy covers all members of the Loyola University LISIRT. Any members of ITS assisting with LISIRT business are also covered.

Policy

All members of the LISIRT are expected to be familiar with and follow all LISIRT policies. A copy of all LISIRT policies will be provided when an individual joins LISIRT. Revisions to LISIRT policies will be provided to all LISIRT members for comments, and updates to any policies will be provided to all current LISIRT members.

All LISIRT members are expected to perform LISIRT tasks to the best of their ability. All LISIRT members are expected to communicate LISIRT information only with individuals who have a need to know, and who should have access to the information based on its classification under the [Data Classification Policy](#). When communicating LISIRT matters, all LISIRT members are expected to be constructive, to communicate with an appropriate level of technical detail based on the audience, and to project a professional image. LISIRT members should not hesitate to say that they “do not know the answer” if that is the case. LISIRT members will refer any inquiries from media representatives to University Marketing & Communications instead of providing an answer.

Information Classification and Disclosure

All information received by LISIRT is initially shared only within LISIRT. Once the information is properly classified, it may be possible to share the information with a wider audience.

Individuals covered

This policy covers all members of the Loyola University LISIRT. Any members of ITS assisting with LISIRT business are also covered.

Policy

Information received by LISIRT can be classified as one of two types of data:

- Sensitive
- Non-sensitive

Sensitive information is information that will only be shared with LISIRT, the ITS Directors and the CIO, Office of the General Counsel, Human Resources and any individuals designated by the Directors or the CIO. Any information which can easily be tied back to an individual is classified as Sensitive. In keeping with existing Loyola policies (<http://luc.edu/its/policies.shtml>), a user's right to privacy must be respected as much as possible even when they are suspected of violating Loyola policies. Sensitive materials may be reclassified if identifying information has been sanitized. Any materials which contain Loyola Protected data or Loyola Sensitive data, as defined under the Loyola Protected Data and the [Loyola Sensitive Data Identification Policy](http://luc.edu/its/pdfs/gov_PIIP/Loyola%20Protected-Sensitive%20Data%20Identification.pdf) (http://luc.edu/its/pdfs/gov_PIIP/Loyola%20Protected-Sensitive%20Data%20Identification.pdf) will be treated as Sensitive by LISIRT.

Non-sensitive information is information that can be shared with individuals within ITS as needed. Non-sensitive information is not easily tied back to an individual. Non-sensitive information typically includes IP addresses, timestamps, and similar technical information. Non-sensitive information can be shared with other Loyola groups as metrics concerning the incidents and trending information. Non-sensitive information may be shared with any individuals within ITS and any system administrators within the University community who need to know about the incident.

Data is classified by the LISIRT member who initially receives it. If an item is classified as Non-sensitive, any LISIRT member can change the classification to Sensitive. If an item is classified as Sensitive, only the LISIRT lead can change the classification to Non-sensitive. If a member of the LISIRT is unsure of the classification assigned to a particular piece of information, they should assume that the information has been classified as Sensitive.

Information Requests

Various external groups may request information from LISIRT. The requestor and the type of information requested will determine if the information can be released, and what steps need to be followed to release the information.

Individuals covered

This policy covers all members of the Loyola University LISIRT. Any members of ITS assisting with LISIRT business are also covered.

Policy

Requests from Loyola University Medical Center (LUMC)

The Loyola University Medical Center (LUMC) shares a number of electronic resources with Loyola due to shared history. LUMC will contact Loyola's LISIRT with technical information regarding possible incidents. LISIRT members are allowed to share any information that has been classified as Non-sensitive with LUMC. If LUMC is requesting information that has been classified as Sensitive, the request must be approved by the LISIRT lead. All communications with LUMC concerning incidents should carbon copy the LISIRT lead.

Requests from Internet Services Providers (ISPs), Incident Response Teams (IRTs), and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)

ISPs, IRT's, and REN-ISAC may contact Loyola's LISIRT with technical information regarding possible incidents. Any messages of this nature should be forwarded to the LISIRT lead. The LISIRT lead will determine the appropriate response. The LISIRT lead may designate a member of the team to serve as the primary point of contact for communications concerning a particular incident, but all communications should carbon copy the LISIRT lead.

Requests from the media

All responses to requests for information made by members of the media must be approved by University Marketing and Communications.

If approached by a member of the media for a quote, LISIRT members should only reply with "no comment", and direct the media representative to contact University Marketing and Communications.

If approached by a member of the media for trending information, LISIRT members should direct the media representative to contact the LISIRT lead. The LISIRT lead

will work with University Marketing and Communications to determine if the requested trending information can be provided.

Requests from Law Enforcement

All responses to requests for information made by law enforcement must be approved by the Office of the General Counsel. The only exception to this is if a subpoena or a warrant is issued to ITS or the LISIRT. The warrant or subpoena must be honored, however immediate contact to the Office of the General Counsel must be made. The other exception is requests for trending data

If approached by a member of law enforcement, LISIRT members should only direct the law enforcement agent to contact the LISIRT lead. The LISIRT lead will bring the request to the CIO and the Office of the General Counsel for approval, and then work with the law enforcement agent as appropriate.

If approached by a member of law enforcement for trending information, LISIRT members should direct the law enforcement agent to contact the LISIRT lead. The LISIRT lead will work with the Office of the General Counsel to determine if the requested trending information can be provided.

If a member of LISIRT discovers activities that are believed to violate local, state, or federal laws, they should bring the activities to the attention of the LISIRT lead. The LISIRT lead will work with the CIO and the Office of the General Counsel to determine if the information should be turned over to a law enforcement agency. If that is the case, the LISIRT lead will serve as the primary liaison between Loyola and the law enforcement agency.

Other requests

Requests from non-ITS groups within Loyola for any additional information will need to be approved by either an ITS Director or the CIO, and may be subject to sanitizing before the information is released.

Information requests from outside of the University community will be evaluated individually. Requests for information from members of the media community will be forwarded to University Marketing and Communications. Requests for DMCA-related information will be forwarded to the DMCA agent as identified in the University [Digital Millennium Copyright Act Policy \(http://www.luc.edu/its/policy_dmca.shtml\)](http://www.luc.edu/its/policy_dmca.shtml).

Decisions regarding other requests for information will be considered by the LISIRT lead.

Human Error

During a security incident, there is the possibility that a LISIRT member will make a mistake. The emphasis should be placed on correcting the mistake when it is detected, and working to improve the procedures to prevent similar mistakes after the incident has been resolved.

Individuals covered

This policy covers all members of the Loyola University LISIRT. Any members of ITS assisting with LISIRT business are also covered.

Policy

If any member of LISIRT believes that they identified a possible mistake in the investigation, all members of LISIRT who are working on the issue should be notified of the perceived mistake, why it is believed to be a mistake, and what effect this may have on the incident response.

After the incident has been resolved, the LISIRT members involved in the incident will meet to determine what factors lead to the mistake. This is not an attempt to assign blame, but rather an attempt to refine the incident response process to prevent similar mistakes in the future.

If a LISIRT member repeatedly makes the same or similar mistakes across a number of incidents, the LISIRT lead may ask the LISIRT member to resign their membership in the LISIRT.

If the mistake constitutes a violation of a University policy (<http://luc.edu/its/policies.shtml>), the disciplinary procedure from that policy may apply. If that is the case, the LISIRT lead will be available to speak on the LISIRT member's behalf, if needed.

Internal Contact List

The ITS Helpdesk will maintain a list of all contacts within ITS. Access to this list may be accomplished by calling the 24/7 support line (773.508.7190) or internally at 4-4444. This list will contain off-hours contact information for all ITS functional areas, and will be maintained by the ITS helpdesk process owner.

Individuals covered

This policy is the responsibility of the ITS Helpdesk, which is a member of the Academic Technology Services department.

Policy

The LISIRT will utilize the after hours support list in the event additional resources need to be contacted. In addition to this list of ITS contacts, the after hours support list will also contain contacts for:

- Office of the General Counsel
- University Marketing and Communications
- Human Resources
- Campus Safety
- Facilities Management

The list of individuals will include their name, email address, Loyola telephone number, and emergency contact number.

Testing and Policy Review

The LISIRT will test the procedures in this plan and review the entire plan every 12 months.

Individuals Covered

This policy is the responsibility of the LISIRT lead.

Policy

The LISIRT lead will create a test scenario every 12 months. This scenario will then be treated as an incident and the appropriate groups will be activated. The LISIRT lead will ensure that this plan is maintained in accordance with the [Information Security Policy](#).

Incident Handling

Summary

This document provides an overview of the procedure for incident handling at Loyola.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources

The LISIRT will work to identify the scope of the incident. In this case, the scope involves evaluating the event, or events, identifying what resources might be affected, how many resources are affected, if any services are unavailable as a result of the incident, if any sensitive information might have been accessed and similar information that will be collected and analyzed. As the investigation progresses, the scope may be modified as appropriate.

2. Begin documentation of the incident

The LISIRT assigns each incident a unique incident number. Incident numbers are generated by combining the four digits of the current fiscal year with a four digit counter. So the first incident of 2008 would be 20080001, the next would be 20080002, etc. All steps taken by the LISIRT from this point forward will be documented. After the incident has been resolved, all of the available documentation will be collected for a final report (step #10).

Documentation includes a brief description of any actions taken, along with the time that action was taken. This is especially important if the actions are being taken on a resource which may be compromised.

3. Assess incident

An assessment of the impact of the incident will be done. This impact will be brought to the attention of the ITS Directors and the CIO.

4. Assign responsible LISIRT members

Based on the affected resources and the impact, ITS members with the appropriate knowledge will be assigned to the incident to aid the LISIRT team.

5. Contain the incident

If specific steps are available to contain the incident, the LISIRT will consider the consequences of those actions. If the benefits outweigh the costs, the containment steps will be performed. LISIRT has the authority to take necessary actions to mediate the issue without first discussing it with affected constituents.

6. Collect evidence

The LISIRT will collect evidence of how the incident occurred on the affected resources. Any digital evidence, such as log files and suspicious files, will be preserved by the LISIRT. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. So the first piece of evidence in the first case of 2008 would be 200800010001, the second piece would be 200800010002, etc. All collected digital evidence will be documented. This information will be logged in the security_metrics.xls spreadsheet located on \\sharedfs\data4\its\IT-Security\Incident documents\security_metrics.xls.

7. Determine vulnerability

The LISIRT will work to determine how the incident occurred. If a vulnerability is found on the resource, the LISIRT will determine if a patch or workaround is available.

8. Determine malicious actions taken

The LISIRT will work to determine what malicious actions may have been performed on the resource. Determining what actions might have been taken will influence the recommended recovery steps. Depending on the incident, forensic analysis may be required to determine what actions were taken on the resource.

9. Provide recovery steps / Take recovery actions

LISIRT is empowered to take the necessary steps to secure the resource and bring it back online. The resource will not be allowed back onto the network until it has been secured. Depending on the extent of the compromise, it may be necessary to restore the resource from tape backup, or to rebuild the resource from scratch.

10. Create final report

The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports will be provided to the ITS Directors. Reports and the CIO.

11. Archive evidence and report

The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.

12. Process improvement

The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Incident Handling process that require improvement.

06/23/2008 – Version 1.0, Included in Incident Response Plan

11/4/2008 – Version 2.0, removed incident levels and added evidence collection location.

Definitions

Electronic resources - All computing, networking, telephony and information resources procured through, operated or contracted by the University. Such resources include computing and networking systems including those that connect to the University telecommunications infrastructure, other computer hardware, software, data bases, support personnel and services, physical facilities, and communications systems and services.

Event – Any event that can be logged from any server, network device, or security device that contains suspicious activity. Examples of an event include the replacement of a system-level file, or the notification of a virus on a workstation. Events may or may not be malicious and must be evaluated to determine their impact.

(Security) Incident – An event, or combination of events, that alerts on real or risky activities that compromise the confidentiality, integrity and availability of information resources. Examples of incidents could include:

- attempts (failed or successful) to gain unauthorized access to a system or it's data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent
- violations of the information security policy and University usage policies

Security Breach – Any successful unauthorized access to a Loyola University Chicago computer or system or network.

LISIRT – An Information Security Department team that receives, triages, resolves, assigns and tracks incidents of technology abuse or security breaches for all Loyola University Chicago campuses. This staff coordinates with various University offices as well as with external resources (Internet Service Providers, law enforcement, etc).

Server – A software program, or the computer on which the program runs, that provides service to *client* software running on the same computer or other computers on the network.

Workstation – Any personal computer or laptop.

Malware – Any type of malicious code, such as viruses, worms, trojans, bots, spyware.

Appendix

For details on specific Incident Response Procedures, please see the [ITS Incident Response Plan - Appendix](#).