

Information Technology Services Security Incident Response Plan

Information Technology Services Incident Response Team (IRT) will respond to security incidents, reports, and complaints about abuse of information technologies at The University of Findlay.

The IRT will investigate the problems reported and take appropriate action to protect the members of the community and the University's resources. Members of the IRT team include the Information Technology Officer, the Network Systems Manager, the Programming Services Manager and the Technology Support Services Manager. Whenever appropriate, the team may be expanded to include select members from each of these manager's teams, the UF Office of Safety and Security, the Office of Academic Affairs, the Office of Student Affairs, and/or the Office of Business Affairs and/or Human Resources, depending on the specific nature of the incident.

Each member of the IRT recognizes the often sensitive nature of both reports received and what is found during the course of an investigation. All members of the team will hold both reports and findings confidential, consistent with both the letter and the spirit of the procedure described in this document, federal and state laws, and the rules of the disciplinary bodies involved.

Review of incidents frequently begins with reports received at the Technology Support Services (techsupport@findlay.edu or 419-434-4357) or by e-mail directed to the Information Technology Officer. Information Technology Services (ITS) is neither an investigative nor a disciplinary unit in its primary responsibilities. However, in cases where University resources and privileges are abused or otherwise threatened, the department will take appropriate steps to support this plan.

ITS managers who are members of the IRT may disable user accounts, interrupt computing processes or disable services at any time to safeguard University resources and protect University privileges. They may take these actions without prior approval if, in their best professional judgment, they need to do so to deal with immediate circumstances. These actions must be reported to, and are subject to timely review by the Information Technology Officer and the Vice President for Academic Affairs. The vice president may authorize extending such actions to longer terms if necessary to safeguard University resources.

Generally, the team will work rapidly and collaboratively, mostly using e-mail to its members, to establish the nature of the incident and to develop an appropriate response that protects the University's resources and interests while eliminating (to the degree possible) the threat of recurrence. Sometimes, to accomplish this goal, the technical staff may have to temporarily leave a vulnerable system open in order to identify the malicious person(s) behind the incident. In all cases, the team will assume that it must notify appropriate authorities and preserve evidence.

How Investigations Work

Incidents that involve the University's on-line environment sometimes lead to investigations, which include the gathering of technical evidence. Those investigations may be managed by law enforcement officers, authorized government officials, or others outside of the University community; by the vice president(s) whose areas are involved in the investigation (per the University's Acceptable Use Policy); or by other University administrators depending on the nature of the incident and the role of the persons suspected of improper behavior. In such investigations, investigating officials may call on the IRT to provide technical information that may become evidence from computers owned and managed by Information Technology Services.

Information that can be requested

Evidence in these investigations may involve computer usage information about individuals that is maintained on centrally-managed servers. Computer usage information about individuals includes two major types:

- log information (generally referring to when a user's account was used in various contexts); and
- content information (generally referring to content of materials stored in storage space tied to the account as well as "live" content generated or received by a person currently using the account).

After investigative officials have completed appropriate processes to authorize their requests per the University's Acceptable Use Policy, the IRT may be able to provide pertinent log information. Such records may show the connection of individual accounts to UF host computers (called a connection log), and they may show delivery of a message from one individual's account to another or other similar usage information. These logs usually are available for a limited period of time before they are overwritten with more current log data. Providing content information such as the contents of a mailbox, a file or a copy of a specific message within a mailbox raises more complex policy issues of privacy and academic freedom. From a technical perspective, it is also important for investigating officials to know that:

- ITS keep backup copies of mailboxes for a limited period of time - while some individuals keep copies of all messages received on servers, others keep some messages there, and still others store no messages on servers after they have been delivered to a local machine. In any case, if a message was received by the recipient sufficiently long before the request, ITS may not be able to find a copy of it.
- A message must reside in a mailbox or a file on one of our systems overnight for it to be available on a backup device - if someone routinely reads and deletes messages from the server or keeps a file on the system for only a short period of time, it is possible that we have no record of the contents of that message/file.

Data ITS can provide from servers in almost all cases will not establish with certainty the physical location of any person at any time. What it may establish is when an account was used and from what location.

How to request information

The procedures below reflect the sequence of steps necessary for investigating officials seeking computer usage information about individuals. All requests for access to the specific subtype of computer usage information that involves "content" may require additional review by the office of the University's counsel.

Law Enforcement, Government Officials, and Others Outside the University Community

- Law enforcement, government officials and others outside the University community usually will need to provide legal orders (normally search warrants) to obtain computer usage information. These documents should be delivered to:

Information Technology Officer
The University of Findlay
1000 N. Main St. Room 122A
Findlay, OH 45840

Any such legal documents will be forwarded immediately to other appropriate University officials. The University and its employees will comply in timely fashion with any conditions included in a legal order. To ensure the IRT preserves information that may be needed, those reporting the need for investigation should notify the Information Technology Officer or any other member of the IRT as far in advance as possible about the request. When possible and feasible, advance discussion about the type of computer-usage information sought before a legal order is delivered may help to ensure that language included in the order is precise and appropriate to the technical environment at the University.

- Requests should be specific. A specific request may speed delivery of information and provide information that is pertinent to specific circumstances. This is especially important for requests for information covering a large time period. Generally, the more specific the investigatory time period the faster the electronic records in question can be identified, assuming the request is made within a time when ITS still has the records being sought.
- The IRT will release computing usage information to law enforcement, government officials, or others outside the University community only after it has been reviewed by the University's counsel, except in conditions where immediate delivery is mandated by legal order.
- Unless otherwise instructed in the legal order, the IRT will inform the persons whose accounts were associated with the requested information with the name of the investigating entity and the nature of information requested and provided.

Judiciary Investigations and Faculty Conducting Individual Student-Academic-Issue Investigations

- Per the University's Acceptable Use Policy (AUP) Section III B. "Procedures for Gathering and Reporting Evidence," any office receiving a complaint about a suspected violation of the Acceptable Use Policy will report this to the Information Technology Officer in writing or e-mail. The Information Technology Officer will ensure the report is forwarded to the most appropriate IT staff member for initial investigation. Authorizations are required before specific evidence can be gathered about an individual's activity unless required by law or it is necessary to respond to a perceived emergency situation. Authorization for monitoring an individual's use of resources or the gathering of evidence from an individual's assigned account, network storage space or a University-owned computer must be granted by the appropriate authority. In the case of student accounts, authorizations come from the Vice President for Student Affairs or his/her designee. In the case of members of the faculty, authorizations come from the Vice President of Academic Affairs or his/her designee. In all other cases, authorizations come from the Director of Human Resources or the Vice President of Business Affairs. Authorizations must be specific and delivered in writing or by e-mail to the Information Technology Officer before any evidence is gathered from an individual's accounts.
- Requests should be as specific as possible (see above).
- The IRT will not provide computer usage information to faculty or staff conducting individual student-academic-issue investigations until the IRT is notified by the appropriate vice president that the request has been granted. Requests for content information may require additional review by the University's counsel.
- Unless otherwise instructed in the request the IRT receives from a University's vice president, the IRT will inform the persons whose accounts were associated with the requested information with the name of the investigating entity and the nature of information requested and provided.

University Administrators in Faculty or Staff Disciplinary Investigations

- University administrators investigating incidents as part of faculty or staff disciplinary processes will need to obtain appropriate authorization cited in the University's AUP (cited above).
- The IRT will not provide log or other electronic information to University administrators investigating incidents as part of faculty or staff disciplinary processes until appropriate approval has been received.
- Unless otherwise instructed in the request the IRT receives from a University's vice president, the IRT will inform the persons whose accounts were associated with the requested information with the name of the investigating entity and the nature of information requested and provided.