



QUICK REFERENCE GUIDE:

When an IT Security Incident Occurs

What type of incident should be reported?

A **serious incident**, meeting one or more of the following criteria:

- involves potential unauthorized disclosure of **sensitive information**
- involves **serious legal issues**
- may cause **severe disruption** to critical services
- involves **active threats**
- is **widespread**
- is likely to **raise public interest**

Sensitive information includes (but is not limited to) personally identifiable information such as:

- Social security number
- Credit card number
- Driver's license number
- Student records
- Protected health information (PHI)
- Human subject research

Passwords and other security-related information should also be treated as sensitive.

For more information on the University's incident reporting policy, visit:

<http://spg.umich.edu/pdf/601.25.pdf>

When an incident occurs...

1. **Stay calm.** There is an established protocol for handling incidents, and ITSS is equipped to guide the process.
2. **Sacrifice speed for correctness.** Don't act rashly.
3. **Involve your leadership early**, reminding them that all information, especially early in the investigation, should be limited to a need-to-know basis.
4. **Every detail is important.** Share everything you know with the ITSS incident coordinator(s).

FIRST TEN MINUTES

Unit Determine the severity of the incident.
In the case of a serious incident, please note that continued interaction with a compromised machine can severely affect later forensic analysis. When an incident is discovered, the unit should:

CONTAIN THE INCIDENT BY:

- restricting network access
- disabling all remote access
- keeping the machine out of use

AND NOT:

- run anti-virus software
- power down the machine
- attempt any kind of unilateral mitigation procedure

FIRST 24 HOURS

Unit Report all serious incidents to: security@umich.edu, except:

- incidents involving PHI report to: UMHS-Compliance-IT-Sec@med.umich.edu
- incidents involving human subject research report to: OVPR.JLG@umich.edu

Alert business owners and leadership, advising them to keep all details confidential until further notice. Consult safecomputing.umich.edu/umonly/im_guidelines.php for further information

ITSS Contact the unit and develop a plan for further containment

FOLLOWING DAYS

ITSS Convene the Computer Security Incident Response Team (CSIRT), which may include such University resources as the Office of the Vice President for Communications, the Department of Public Safety and others.

ITSS &

Unit Address the incident through a series of steps that will vary in length depending on the details of the event. In general order, these steps include:

- **Information gathering:**
 - Conduct forensic analysis or live examination
 - Collect network logs
 - Conduct interviews to gather information from multiple sources
- **Analysis/Investigation:**
 - Perform additional vulnerability analysis
 - Determine cause and effects of incident
- **Decision Support:**
 - Share relevant information with unit/business owners/CSIRT
 - Identify potential further action, such as notification of affected parties
- **Service Restoration:** Performed if services have been taken offline during the forensic acquisition.

CONCLUSION

ITSS & Unit Create an executive summary and incident report, and lead a lessons learned session with the unit and CSIRT

QUICK REFERENCE GUIDE: High-Level Incident Life-Cycle

