Security Incident Response Framework (External)

It is the responsibility of the entire University community to respond in a consistent manner, with appropriate leadership and technical resources, to any security incident. The MSU IT Service Desk and MSU Office of Information Security are available to facilitate and provide guidance with any computer security incidents that affects University IT resources or threatens the availability, confidentiality, and integrity of university information.

Security incidents involving restricted personally identifiable information (PII) or confidential information as defined by the Data Classification and Handling Policy must be reported immediately to the Office of Information Security (security@montclair.edu)

What is a Security Incident?
An incident is an adverse event in an information system, including the significant threat of an adverse event. In other words, it implies harm or the attempt to harm. An incident can be defined as any act that violates MSU Information Security policies and/or the MSU Guidelines for Responsible Computing. The following activities are common incidents and should be reported to the Office of Information Security:

- Attempts to gain unauthorized access
- Unwanted disruption of services or denial of resources
- Unauthorized use of a system
- Changes to a system without the owner’s knowledge, instruction, or consent
- Theft or loss of University computing equipment

What is not an incident?
Spam is not considered an incident as the high volume of spam e-mails makes it difficult to investigate every case. Only when the spam is a sign of a compromised MSU account, or if the spam contains criminal content will it be considered an incident. If you are interested in reporting unsolicited email (Spam) please contact the MSU IT Service Desk at itservicedesk@montclair.edu. You are encouraged to read this page prior to making a complaint to help you distinguish activities which do not violate the law or policy.

How can I report an incident?
If you would like to report an incident that meets the criteria for a violation please contact the appropriate agency. Please do not submit personally identifiable information such as your CWID, passwords, or financial information via e-mail. This contact matrix provides guidance in the event you observe or experience the following:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts or behavior indicating possible infection on a University provided client (computer)</td>
<td>MSU Service Desk or your local college technical team</td>
</tr>
<tr>
<td>Network scanning, probing, or system compromises</td>
<td>MSU Service Desk, E-mail Office of Information Security</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Found a lost mobile device</td>
<td>University Police</td>
</tr>
<tr>
<td>Lost or stolen University provided mobile device</td>
<td>University Police, E-mail Office of Information Security, and inform your supervisor</td>
</tr>
<tr>
<td>Discover you have incorrect access rights to a shared University file repository (MSUFILES, Google Drive, etc.)</td>
<td>E-mail IT Office of Information Security</td>
</tr>
</tbody>
</table>

What are some signs of common Security Incidents?

If you are experiencing issues with your computer or a resource located on the network it is recommended to first check with the MSU IT Service Desk or your local technical team to rule out common problems.

**Signs of a Denial of Service Attack**
- The network appears to be running slower than usual or there is no connection at all (opening files or visiting websites)
- Unable to reach a University website, resource, or any public website or resource available through the internet.
- Mailbox is inundated with spam to the point that no legitimate e-mails can be delivered.
- The hard drive has suddenly become full

**Signs of Malicious Code (Virus, Malware, Spyware, Rootkits)**
- Computer is running abnormally slow or crashes for no apparent reason
- Files are being deleted or becoming corrupt
- Internet homepage is different and/or there are additional components added to the browser
- Pop-up ads are always appearing on the desktop
- Random Windows error messages appear
- The mouse cursor moves around without any interaction

**Signs of Unauthorized Access**
- Computer is not in the same physical condition that it was left in
- Files and folders have been added, deleted, or changed
- You witness someone using a system or using credentials that do not belong to them

**Investigation**

Once the initial response is performed and the incident is classified and contained, further investigation may be required to determine the cause. All actions taken should be fully documented within an incident in ServiceNow. Report incidents by logging into our ServiceNow self-service portal and submitting an ISIM “Security Incident Reporting Form” ticket.
Recovery

Recovering from an incident occurs when the investigation process is complete and the machine can be returned to normal operation. Lessons learned will be identified and any implementation to protect from any future incidents of the same kind will be taken. A final report to communicate findings with MSU IT Security Office, IT staff, and other affected parties will need to be developed and shared.

Information Security Breach Notification Guidelines

Breach of restricted personal or confidential information requires special handling. Refer to the MSU Breach Response Protocol for an appropriate response. The Information Security Breach Reporting Form must be used to report a security breach to the Office of Information Security.

Request for Computer Forensic Examination

Computer forensics is the analysis of data from a computer system in response to a security incident. A computer forensic examination may be needed when it is suspected that a computer was misused, violating MSU’s Guidelines for Responsible Computing or used to commit a crime. To learn more and to request a computer forensic examination, please contact security@montclair.edu.