

Montana Tech Escalation Procedures for Security Incidents

1.0 Introduction

This procedure describes the steps which are to be taken for physical and computer security incidents which occur within the Montana Tech facility. The physical security incidents covered in this procedure are: theft (major and minor), illegal building access and property destruction (major or minor). The computer security incidents covered in this procedure are: loss of personal password sheet, suspected illegal system access (includes account sharing), suspected computer break-in (both internal and external) and computer viruses. For additional information on incident response and handling refer to the "Montana Tech Security Incident Handling Procedures." The types of incidents have been classified into three levels depending on severity. The Level One incidents are least severe and should be handled within one working day after the event occurs. Level One incidents usually require that only the Montana Tech Computer Security Officer and/or the Montana Tech Security Analyst be contacted. Level Two incidents are more serious and should be handled the same day the event occurs (usually within two to four hours of the event). Level Two incidents must be escalated to the Montana Tech ISO and possibly some outside groups such as the CIAC or CERT. Level Three incidents are the most serious and should be handled as soon as possible.

2.0 List of Terms:

ISO - Installation Security Officer
CSA - Computer Security Analyst
LSA - Lead System Analyst
CIRC - Computer Incident Response Center

3.0 List of Contacts

1. Computer Security Incidents

4.1 Loss of Personal Password Sheet (Level One Incident)

- Notify the Montana Tech CSA or resource manager within one working day.
- The Montana Tech CSA will decide if a password change is necessary.
- Suspected Sharing of Montana Tech Accounts (Level One Incident)
- Suspected Sharing of Montana Tech Accounts expect where authorized (Level One Incident)
- Montana Tech Network Services and/or Information Services or appropriate resource management will document all pertinent information and Network Services will disable appropriate accounts.
- The Montana Tech CSA will call person(s) suspected of account sharing and determine severeness of the incident. In most cases, people who share accounts have a valid need to have their own Montana Tech accounts. In these cases, the Montana Tech user's account will remain disabled until account request forms are received and processed for the person who was using the Montana Tech user's account.
- The Montana Tech CSA will escalate the issue to higher management if necessary.

4.2 Unfriendly Employee Termination (Level Two Incident)

- Notify Montana Tech ISO and CSA within two hours. If neither can be reached within two hours, contact the backup CSA or ISO person.
- Upon Human Resource (HR) is ISO notification, the Montana Tech CSO will request all Montana Tech accounts for the terminated employee be disabled by a member of Network Services.
- The Montana Tech ISO will ensure building access is disabled and will confiscate all keys, if possible.
- If appropriate, the Montana Tech CSA will change systems passwords.
- If necessary, the Montana Tech ISO will escalate issue to HR.

4.3 Suspected Violation of Special Access (Level Two Incident)

The misuse of Special Access is defined in the document "Special Access Guidelines Agreement" which is signed by each person having Special Access at Montana Tech.

Minor Violations - No threat to Montana Tech Security

- Notify Montana Tech CSA within one working day. If unable to reach Montana Tech CSA within that time, contact the appropriate resources. You should also inform the group leader and manager of the person suspected of violating the policy.
- The Montana Tech CSA and appropriate resource managers will determine who is involved in the violation and the extent of the violation.
- Notify the Montana Tech ISO within two working days.
- If necessary, the CSA will escalate issue to Montana Tech Administrative Offices.

Major Violations- possible threat to Montana Tech computer security

- Notify Montana Tech CSA within one hour. If unable to reach Montana Tech CSA within that time, contact the appropriate resource manager. You should also inform the group leader and manager of the person suspected of violating the policy.
- If possible threat exists for computer security, notify the Montana Tech ISO within 24 hours.
- Disable all Montana Tech accounts for involved people.
- Begin process of changing all system passwords.
- Take further action as deemed necessary by Montana Tech CSA.

4.4 Suspected Computer Break-in or Computer Virus

- Isolate infected systems from the remaining Montana Tech network as soon as possible. The College support staff should consult the Montana Tech Network Services to determine the best method to isolate the infected systems from the remaining Montana Tech network.
- If a rampant computer virus/worm is suspected, at the discretion of Network Services, network isolation from outside
- Notify Montana Tech CSA as soon as possible. If unable to reach him/her within ten minutes, contact the backup person.

- Notify Montana Tech ISO within one hour. Montana Tech ISO will escalate to higher level management if necessary.
- Notify all involved LSA's within two hours.
- While waiting for LSA's and the Montana Tech CSA to respond, attempt to trace origin of attack and determine how many systems (if any) have been compromised. Save copies of system log files and any other files that may be pertinent to incident.
- Montana Tech CSA will decide what further actions are needed and assign appropriate people to do perform the tasks.
- The Montana Tech CSA will escalate the incident if necessary.
- Upon completion of the investigation, the Montana Tech CSA will write an incident summary report and submit to the appropriate levels of management.

5.0 Physical Security Incidents

5.1 Illegal Building Access (Level Two Incident)

- If during regular working hours an unauthorized person is in a controlled area (e.g. MDF, IDF's), call or page the Montana Tech ISO and CSO immediately. If after working hours, call the Physical Security office first and then page the Montana Tech ISO or attempt to call his home phone number.
- Escort the person outside the building or controlled area. Log incident and report to Montana Tech ISO.
- The Montana Tech ISO and/or the Security office will decide upon the appropriate action to take.

5.2 Property Destruction or Personal Theft (Level Two or Three Incident)

- Unless the theft or destruction is major, notify the Montana Tech ISO and Montana Tech CSA within one working day. If unable to reach Montana Tech CSA within one working day, contact the backup person listed on page one. Otherwise, for major theft or property destruction, notify Montana Tech ISO immediately. If he/she can not be reached within one hour, call or page the backup person.
- Security Office within 24 hours.
- If destruction involves a Montana Tech computer, notify LSA for that system within 24 hours.

Montana Tech System Control Section Escalation Procedures for Security Incidents

- If incident involves theft of Montana Tech property, contact the Montana Tech Security immediately.
- The Montana Tech ISO will escalate incident to Montana Tech Division Office as necessary.

Montana Tech System Control Section Escalation Procedures for Security Incidents

-