

# Incident Escalation Procedures for Employees

This procedure describes the various steps to be taken at the time of computer or physical security incidents occurring within the <Organization> premises.

The computer security incidents that are covered in this procedure include: suspected computer breach (both internal and external), loss of sensitive files such as password files, suspected illegal system access (includes account sharing), and computer malware and viruses.

The physical security incidents that are covered in this procedure include: property destruction (major or minor), illegal building access, and theft (major and minor).

The types of incidents have been classified into three levels depending on their severity:

- **Level one incidents:** These incidents are regarded as less harmful or least severe. They can be handled within one working data post occurrence. For these incidents, the Computer Security Officer and/or the Security Analyst must be contacted.
- **Level two incidents:** These incidents are regarded as being more harmful and they must be handled the same day the event occurs. These incidents must be escalated to the ISO and possibly some outsiders such as CIAC or CERT.
- **Level three incidents:** These incidents are regarded as most harmful and must be handled as soon as possible.

## List of terms:

ISO - Installation Security Officer

CSO - Computer Security Officer

CSA - Computer Security Analyst

LSA - Lead System Analyst

Computer Security Incidents		Check
<b>A. Loss of Password File (Level One Incident)</b>		
1. Notify the CSA within one working day.		<input type="checkbox"/>
2. The CSA will decide if a password change is necessary.		<input type="checkbox"/>
<b>B. Suspected Sharing of User Accounts (Level One Incident)</b>		
1. User Services document all pertinent information on a CMS report. If unable to contact CSA within two working days, disable appropriate accounts and inform the ISO and CSA.		<input type="checkbox"/>
2. The CSA calls the person(s) suspected of account sharing and determines damage that could have been caused by the incident. In most cases, people who share accounts have a valid need to have their own accounts.		<input type="checkbox"/>
3. The CSA escalates the issue to higher management (if necessary).		<input type="checkbox"/>
<b>C. Unfriendly Employee Termination (Level Two Incident)</b>		
1. Notify ISO and CSA within two hours. If neither can be reached within two hours, contact the backup ISO or CSA person.		<input type="checkbox"/>
2. Upon request from ISO or CSA, all user accounts for terminated employee are disabled by a member of System Control Accounts Section.		<input type="checkbox"/>
3. CSA ensures building access is disabled and confiscates card key, if possible.		<input type="checkbox"/>
4. If appropriate, the CSA will change systems passwords.		<input type="checkbox"/>
5. If necessary, the ISO will escalate issue to Division Office.		<input type="checkbox"/>
<b>D. Suspected Violation of Special Access (Level Two Incident):</b> The misuse of Special Access is defined in the document "Special Access Guidelines Agreement," which is signed by each person having Special Access at <Organization>		
<b>Minor Violations - No Threat to Organizational Security</b>		
1. Notify CSA within one working day. If unable to reach <Organization> CSA within that time, contact the ISO or the backup person for the CSA. You should also inform the group leader and manager of the person suspected of violating the policy.		<input type="checkbox"/>
2. The CSA or designated backup will determine who is involved in the violation and the extent of the violation.		<input type="checkbox"/>
3. Notify the ISO within two working days.		<input type="checkbox"/>
4. If necessary, the NSA CSA will escalate issue to Division Office.		<input type="checkbox"/>

<b>Major Violations - Possible Threat to Organizational Security</b>	
1. Notify CSA within one hour. If neither can be reached within two hours, contact the backup person listed for the CSA.	<input type="checkbox"/>
2. Notify ISO within four hours. If unable to reach him/her within ten minutes, contact the backup person.	<input type="checkbox"/>
3. If possible threat exists for organizational security, notify organizational ISO within 24 hours.	<input type="checkbox"/>
4. Disable all user accounts for involved people.	<input type="checkbox"/>
5. Begin process of changing all system passwords.	<input type="checkbox"/>
7. Take further action as deemed necessary by CSA.	<input type="checkbox"/>
<b>E. Suspected Computer Break in or Computer Virus (Level Three Incident)</b>	
1. Isolate infected systems of the organizational network as soon as possible. The System Control Section support staff should consult the LAN/WAN teams to determine the best method to isolate the infected systems from the remaining organizational network.	<input type="checkbox"/>
2. If a computer virus/worm is suspected, isolate organizational network from outside networks as soon as possible. The LAN and WAN teams should be consulted before the disconnect takes place to discuss the best method and feasibility for doing a full disconnect from the Internet.	<input type="checkbox"/>
3. Notify CSA as soon as possible. If unable to reach him/her within ten minutes, contact the backup person.	<input type="checkbox"/>
4. Notify ISO within one hour. ISO escalates to higher level management, if necessary.	<input type="checkbox"/>
5. Notify all involved LSA's within two hours.	<input type="checkbox"/>
6. While waiting for LSA's and the 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 which may be pertinent to incident.	<input type="checkbox"/>
7. CSA will decide what further actions are needed and assign appropriate people to do perform the tasks.	<input type="checkbox"/>
8. The CSA will escalate the incident to the physical security office, if necessary	<input type="checkbox"/>
9. Upon completion of the investigation, the CSA will write an incident summary report and submit to the appropriate levels of management.	<input type="checkbox"/>

Physical Security Incidents		Check
<b>A. Unauthorized Building Access (Level Two Incident)</b>		
1. If during regular working hours an unauthorized person is in a controlled area, call or message the ISO immediately. If after working hours, call the physical security/duty office first and then inform the ISO via phone call/SMS.		<input type="checkbox"/>
2. Escort the person outside the building or controlled area. Log incident and report to the ISO.		<input type="checkbox"/>
3. The ISO and/or the physical security office will decide upon the appropriate action to take.		<input type="checkbox"/>
<b>B. Organization Property Destruction or Personal Theft (Level Two or Three Incident)</b>		
1. Unless the theft or destruction is major, notify the ISO and CSA within one working day. If unable to reach ISO within one working day, contact the backup person listed on page one.		<input type="checkbox"/>
2. For major theft or property destruction, notify ISO immediately. If he/she cannot be reached within one hour, call or page the backup person.		<input type="checkbox"/>
3. If destruction involves a computer, notify LSA for that system within 24 hours.		<input type="checkbox"/>
4. If incident involves theft of property, contact the Property Custodian within two working days. The Property Custodian will contact the Property Custodian, if necessary.		<input type="checkbox"/>
5. The ISO will escalate the incident to the Division Office as necessary.		<input type="checkbox"/>