

- Prior approval of the IT Department will be obtained for communication configuration changes (i.e., network addresses or names). Typically such approval will be denied but access may be given on an "as needed" basis and access levels necessary to make said changes will be granted on a per episode basis.
- Before connecting to any system or network, the desktop system will have a "least privilege" access control configuration.
- <Company Name> maintains a vulnerability management system and will scan all systems each month to ensure most current software patches are installed. You may experience some inconvenience when patches and updates are installed.

Security Monitoring

- All <Company Name> systems and network activities are subject to security monitoring. Use of <Company Name> systems and networks constitutes consent to this monitoring.
- Disabling or interfering with virus protection software is prohibited.
- Disabling or interfering with logging, auditing, or monitoring software is prohibited.
- All <Company Name> desktop services are subject to inventory and inspection.
- Security irregularities, incidents, emergencies, and disasters related to <Company Name> information or systems will be reported to the IT staff immediately.

REPORTING SECURITY INCIDENTS

Any employee who determines that there may be misuse of any computer system, application, or software owned or operated by or for the Company should notify their supervisor or the **IT Department**. These individuals can make the determination to escalate the emergency response strategy.

Intrusions

An intrusion is defined as any unauthorized access to any data stored on <Company Name>'s computer system. This definition means that intrusions can occur from inside the Company or from outside. The following guidelines shall be followed upon discovery of any unauthorized deletions, alterations or additions of data or programs.

1. Employee Responsibilities

- Employees shall be responsible for the integrity of their personal files. Any changes made to their files without their consent are to be reported to their supervisor immediately. Shared files will be an exception to this guideline.
- Employees shall report to their supervisor if any new executable programs or suspicious data files appear on their workstations without their knowledge.

2. Supervisor Responsibilities

- It is the Supervisor's responsibility to ensure that all employees are aware of new software installations in order to avoid false intrusion reports.
- The supervisor must immediately notify the CTO when an employee makes an intrusion report. Notify the IT Department first and file the virus report after the IT department is aware of the potential attack.
- Supervisors will review operating unit risk assessments and provide input for risk review based upon the experience of their unit. Risk Assessments must be conducted at least once per year.

3. CTO Responsibilities

- The CTO must keep supervisors and Management aware of new software installations.
- The CTO must immediately investigate any intrusion reports.
- If an intrusion is found, the CTO must attempt to determine if the intrusion is from inside or outside the Company.
- If the intrusion is determined to be from inside the Company, the Management Team must be notified, and the employee must face disciplinary action up to and including termination.
- If the intrusion is from outside, the Management Team must be immediately notified with how the intrusion took place (if known), what was done, how to correct what was done, and how to repair the perimeter security.
- With any intrusion, law enforcement must be notified if warranted.

Handling Information About Security: Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the IT Department. Users are prohibited from utilizing our systems to forward such information to other users, whether the other users are internal or external to <Company Name>.

Intrusion Report

Note: This form is required for all intrusion/hacker incidents. Send completed form to the Information Security Officer

Type of Incident		Incident Date
Individuals Involved (Full Name and Title)		Report Date
Contact Information (Phone)	Department	Department Manager

Affected Systems Information	
Physical location of system(s)	
Hardware Configuration	
Operating System	
Security Software installed	
Other affected hosts/sites	

Damage or observations resulting from attack (Impact on Operations)	
---	--

Summary of Incident and Investigation Results (i.e. number of hosts attacked, how was access obtained, how was attack identified, was an Incident Response Organization contacted prior to submission of this report, etc...)	
---	--

Cost of this Incident (downtime, cost, etc)	
---	--

Report Completed by:

(Signature)

(Date)

IT Management Review signature:

(Signature)

(Date)