

**X Corp. Information Security Policy v. 1.3**

**Establishing Network Connections**

X Corp. computers or networks may be connected to third-party computers or networks only after the Information Security department has determined that the combined systems will be in compliance with X Corp. security requirements. Real-time connections between two or more in- house X Corp. computer systems must not be established unless Information Security has determined that such connections will not jeopardize information security. Connections of internal X Corp. computers to the X Corp. internal network do not require such permissions, unless the involved systems store sensitive information. Connections to the Internet through X Corp. firewalls do not require such permissions.

All X Corp. computers and networks that interface to external networks must keep system logs that indicate the identity and activity performed by each user who accesses these systems. These logs must indicate time of day, date, user ID employed, any privileges utilized, and other details associated with all connections. System administrators must review summaries of these logs. System administrators must employ automated intrusion detection systems approved by the Information Security department to immediately inform them of suspicious activity.

**Dial-Up Access**

With the exception of portable computers and telecommuting computers, the use of modems directly attached to, or integrated into, personal computers to establish communications sessions with X Corp. computers or networks is prohibited. All dial-up connections with X Corp. computers and networks must be routed through a modem pool that includes an extended user authentication security system approved by the Information Security department.

Sending Security Parameters—Users must not send any sensitive parameters such as credit card numbers, telephone calling card numbers, fixed passwords, or customer account numbers through the Internet unless the connection is encrypted. Users must not include sensitive parameters in electronic mail messages sent through the Internet unless these messages are encrypted with software approved by the Information Security department. It is not sufficient for a user to employ a virtual private network (VPN) to connect with X Corp. computers, even though the result is that the communications link between a remote computer and X Corp. computers is encrypted. Use of a VPN permits an electronic mail message sent to an outside party to travel over unencrypted links. Security parameters must not be sent through electronic mail to outside parties unless end-to-end encryption is employed.

International Transfer of Data—The movement of private information such as human resources records across international borders in some countries is illegal. Before transferring any private information across a border, users must check with the Information Security department to ensure that laws are not violated.

False Security Reports—All users in receipt of information about system vulnerabilities must forward this information to the Information Security department, which will determine what action is appropriate. Users must not redistribute system vulnerability information.

**Y2K, Viruses, Malicious Software**

Y2K—Any outside software being used by X Corp. should be screened for Y2K deficiencies. The Year 2000 Information and Readiness Disclosure Act, (\_\_\_U.S. C.\_\_\_) (P.L. 105-271).

Virus Checking Required—Virus-checking systems approved by the Information Security department must be in place on all personal computers with operating systems susceptible to viruses, on all firewalls with external network connections, and on all electronic mail servers. All files coming from external sources must be checked before execution or usage. If encryption or data compression has been used, these processes must be reversed before the virus-checking process takes place. Users must not turn off or disable virus-checking systems.

If A Virus Is Detected—If users obtain virus alerts, they must immediately disconnect from all networks and cease further use of the affected computer, and call the help desk for technical assistance. Users must not remove viruses on their own. If users believe they may have been the victim of other malicious software, they must immediately call the help desk to minimize the damage. User possession or development of viruses or other malicious software is prohibited.

**Reporting Problems**

What to Report—All workers must promptly report to the X Corp. Information Security department any loss of, or severe damage to, their hardware or software. Workers must report all suspected compromises to X Corp. information systems. All serious information security vulnerabilities known to exist must be reported. All instances of suspected disclosure of Confidential or Secret information also must be reported.

Further Information—Questions about this document should be directed to the X Corp. Information Security department manager:

Shana Angelosa

150 E. 4TH Street

Cincinnati, OH 45202

(918) 749-2879

*sangelosa@xcorp.com*