Technology Use Policy

1.0 Overview

Schafer's intention in establishing a Technology Use Policy is to protect its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

For the purposes of this policy, Internet/Intranet/Extranet-related systems include but are not limited to computer equipment, software, operating systems, storage media, and network accounts providing email, web browsing, and other services. These systems are the property of Schafer and are to be used for business purposes in service to the positive interests of the company, its clients and customers in the course of normal operations.

Effective security is a team effort and involves every Schafer employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

This policy outlines the acceptable use of computer equipment at Schafer. The practices shown below are in force to protect employees and Schafer. Inappropriate use of technology exposes Schafer to risks including malware attacks, compromise of network systems and services, data breaches, and legal/regulatory issues.

3.0 Scope

The scope of this policy includes employees, third party contractors, consultants, and other workers at Schafer, including all personnel affiliated with third parties who access Schafer technology using company resources.

4.0 Policy

4.1 General Use and Ownership

1. The Schafer corporate IT staff routinely monitors and inspects information stored, transmitted and manipulated by Schafer IT systems. The use of these systems constitutes acknowledgement of this fact. Additionally, users acknowledge that data they create on corporate systems is the property of Schafer. Data received, created, or sent on Schafer's electronic communication systems are Schafer's property and are subject to review. Schafer cannot guarantee the confidentiality of information stored or transmitted on any network device belonging to Schafer.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within Schafer may monitor equipment, systems and network traffic at any time.
4. Schafer reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorized access to information contained on Internet/Intranet/Extranet-related systems. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended.

4. Because information contained on portable computers is especially vulnerable, laptops should be equipped with encrypted hard drives. Each division is responsible for providing employees with encrypted laptops for use. Laptops should not be left in unattended vehicles or common areas.
5. All hosts used by employees connected to Schafer trusted network segments shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
6. Employees should exercise extreme caution when opening e-mail that is received from unknown or unsolicited senders, which may contain malware.
7. Employees should report any and all suspicious activity (email, virus alerts, unusual system behavior, etc.) to the local IT staff or FSO immediately.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances are employees, third party contractors, consultants, and other workers at Schafer, including all personnel affiliated with third parties authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Schafer-owned resources.

The lists below are not exhaustive, but provide a framework for activities, which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Schafer.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Schafer or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Schafer media or electronic asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any Schafer account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology team is made.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" "Ponzi" or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

All users are expected to report any suspected infiltrations of Schafer systems to the Infrastructure team responsible for their work site immediately. In addition, any potential exposure of sensitive information should be reported to the Facility Security Officer responsible for their worksite.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Infrastructure Team	A Team of individuals that are directly responsible for managing networked equipment for the business.
Facility Security Officer	The FSO manages the company's security program, which includes processing security clearances, management of facilities, personnel and ensures the Corporation's Security Program is compliant with all government regulations and requirements.
Internet	An electronic communications network that connects computer networks and organizational computer facilities around the world.
Intranet	A collection of private computer networks within an organization. An intranet uses network technologies as a tool to facilitate communication between people or work groups to improve the data sharing capability and overall knowledge base of an organization's employees.
Extranet	A computer network that allows controlled access from the outside for specific business or educational purposes. Extranets are extensions to, or segments of, private intranet networks that have been built in many corporations for information sharing.

7.0 Revision History