Weatherford College Information Resources Security Management Program

14.2.1 Acceptable Use Procedure

14.2.1.1 Overview

Technology Services' intentions for publishing an Acceptable Use Procedure are not to impose restrictions that are contrary to the Weatherford College established culture of openness, trust and integrity. Technology Services is committed to protecting Weatherford College's employees, students, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Information resource-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of Weatherford College. These systems are to be used for business purposes in serving the interests of the organization, and of our clients and students in the course of normal operations. Please review Weatherford College personnel procedures for further details.

Effective security is a team effort involving the participation and support of every Weatherford College employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

14.2.1.2 Purpose

The purpose of this procedure is to outline the acceptable use procedure at Weatherford College. These rules are in place to protect the employee and Weatherford College. Inappropriate use exposes Weatherford College to risks including virus attacks, compromise of network systems and services, and legal issues.

14.2.1.3 Scope

This procedure applies to employees, students, contractors, consultants, temporaries, and other workers at Weatherford College, including all personnel affiliated with third parties. This procedure applies to all equipment that is owned or leased by Weatherford College.

14.2.1.4 Procedure

1. **General Use and Ownership**
    a. While Weatherford College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the campus systems remains the property of Weatherford College. Because of the need to protect Weatherford College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Weatherford College.
    b. 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 rules, employees should be guided by departmental procedures on personal use, and if there is any uncertainty, employees should consult with their supervisor or manager.

c. Technology Services recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see the Data Classification Procedure. For guidelines on encrypting email and documents, see the Encryption Procedure.
d. For security and network maintenance purposes, authorized individuals within Weatherford College may monitor equipment, systems and network traffic at any time, per Technology Services' Audit Procedure.
e. Weatherford College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this procedure.

2. Security and Proprietary Information

a. The user interface for information contained on information resources-related systems should be classified as either Confidential, Weatherford College-Sensitive, or Public, as defined by organizational confidentiality guidelines, details of which can be found in the Data Classification Procedures. Examples of confidential information include but are not limited to: Weatherford College private information, educational strategies, private and confidential student, staff, and faculty information, potential student or donor lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
b. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed every 90 days; user level passwords should be changed every 90 days.
c. All computing devices including laptops, workstations, and tablets should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by either locking the computer screen or logging-off when the computer will be unattended.
d. Use encryption of confidential information in compliance with the Encryption Procedure.
e. Because information contained on portable computers is especially vulnerable, special care should be exercised. Never leave a laptop unattended in a public place like an airport, restaurant, or classroom. Laptops should always be in your possession especially when you are off-campus. Do not leave a laptop inside the passenger department of a vehicle when you are not present. Laptops should be placed in a locked trunk of your vehicle if you cannot carry the laptop with you when away from your vehicle.
f. Postings by employees from a Weatherford College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Weatherford College, unless posting is in the course of business duties.
g. All computers used by the employee that are connected to the Weatherford College Internet/Intranet/Extranet, whether owned by the employee or Weatherford College, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group procedure.

h. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

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., Technology Services staff may have a need to disable the network access of a computer if that computer is disrupting production services).

Under no circumstances is an employee of Weatherford College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Weatherford College-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

a. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

I. Violations of the rights of any person or organization 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 Weatherford College.

II. 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 Weatherford College or the end user does not have an active license.

III. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. An appropriate management member should be consulted prior to export of any material that is in question.

IV. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

V. 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.

VI. Using a Weatherford College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment workplace laws in the user's local jurisdiction.

VII. Making fraudulent offers of products, items, or services originating from any Weatherford College account.

VIII. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

IX. 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, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

X. Port scanning or security scanning is expressly prohibited unless prior approval is received from Technology Services.

XI. Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.

XII. Unauthorized circumventing of user authentication or security of any computer, network or account.

XIII. Interfering with or denying service to any user other than the employee's computer (for example, denial of service attack).

XIV. 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.

XV. Providing information about, or lists of, Weatherford College employees to parties outside Weatherford College without the express written permission of the Weatherford College Administration.

b. Email and Communications Activities

I. 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).

II. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

III. Unauthorized use, or forging, of email header information.

IV. 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.

V. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

VI. Use of unsolicited email originating from within Weatherford College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service connected via Weatherford College's network.

VII. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).