**ANCHOR CORPORATION**

**COMPUTER USE GUIDELINES**

**1. General**

Anchor Corporation provides computing services to employees and contractors. This document provides guidelines for confidentiality and privacy, copyrights, computer accounts and passwords, computer and data security, electronic communications, and networks.

**2. Confidentiality and Privacy**

Everyone, including managers, supervisors, and systems administrators, shall respect and protect the privacy of others. This documentdefines the limited conditions under which access to information and files can be obtained**.** Although Anchor Corporation is committed to protecting individual and information privacy, correspondence and information stored and transmitted through company computer networks and systems cannot be guaranteed to be private. Since confidential information is often stored on desktop computers, displayed on screens, or printed on paper that could be in public view, users need to control access by:

* using passwords;
* turning screens away from public view;
* logging out of systems when leaving the work area;
* shredding reports containing private information prior to disposal; and
* clearing confidential information off desks in public areas.

**3. Copyrights**

Laws that protect owners of intellectual, textual, music, sound, photographic, artistic, and graphic property apply to all computer media such as software, electronic library material, and paid subscriptions. Anchor Corporation is committed to protecting copyrights.

**3.1. Software Copyrights**

Commercial programs produced for use on computers are protected by copyright. Copying computer software without authorization violates federal copyright law. Payment for a software product represents a license fee to use a designated number of copies. The buyer does not own the software, but merely buys a license to use the software. The license is not a blanket authorization to copy.

**3.1.1. Site Licenses**

Anchor Corporation enters into site license agreements with commercial vendors for company-wide use of certain software products. Anchor Corporation currently has site licenses for products, including word processing, spreadsheet, and database management applications software. Before buying a particular product, departments should contact the Technical Support Department to determine if Anchor Corporation has a site license or volume purchase discount for the software in question.

**3.2. Software Developed Internally**

Anchor Corporation personnel may develop computer programs using company resources. Such software may be subject to the company’s Intellectual Property Policy.

**4. Computer Accounts and Passwords**

Anchor Corporation provides computer accounts to authorized users for access to various company systems. These accounts are a means of operator identification and passwords are used as a security measure. Account use is a privilege, not a right.

**4.1. Account Authentication**

Passwords, PINs, and other identifiers authenticate the user's identity and match the user to the privileges granted on company computer networks and systems. A password is a security measure designed to prevent unauthorized persons from logging on with another person's computer account and reading or changing data accessible to that user. Users should create passwords carefully and handle them with care and attention. For this security feature to be effective the user must protect the secrecy of his/her password. Each user should:

* change his/her password regularly and at any time the user feels the password may have been compromised;
* avoid writing the password down;
* not disclose or share the password with anyone; and
* choose a password that is easy to remember but hard to guess.

Similar measures apply to all authentication methods such as PINs.

**4.2. Account Termination and Locking**

When an individual leaves Anchor Corporation, his or her account(s) will be locked and eventually deleted. If misuse or theft is detected or suspected, account(s) will be locked according to the company's procedures.

**5. Computer and Data Security**

Everyone at Anchor Corporation shares responsibility for the security of computer equipment and information.

**5.1. Physical Security**

Everyone is responsible for the proper use and protection of company computer equipment. Examples of protection measures include:

* locking areas after business hours or at other times when not in use;
* taking special precautions with high-value, portable equipment; and
* following company policies for taking computer equipment off site.

**5.2. Information Security**

Security of information is an essential responsibility of computer system managers and users alike. For example, users are responsible for:

* ensuring the routine backup of their files;
* using data only for approved company purposes; and
* ensuring the security and validity of information transferred from company systems.

**5.3. Computer Viruses**

Due to the proliferation of computer viruses and the damage they can cause, Anchor Corporation strongly recommends that users keep current anti-viral software active and scan frequently for viruses. For example, scan the following for viruses:

* attachments;
* downloaded files; and
* shared CDs, flash drives, and other media.

**6. Electronic Communications**

Electronic communications include information in any form such as data, audio, video, and text, that is conveyed or stored electronically, for example, by email, web pages, and in files. Electronic communications are used for furthering the education, research, and public service mission of Anchor Corporation and may be used for incidental personal use but may not be used for commercial purposes or profit-making. The following types of communication are prohibited:

* chain letters, pyramid schemes, and unauthorized mass mailings;
* fraudulent, threatening, defamatory, obscene, harassing, or illegal materials;
* non-work- or non-class-related information sent to an individual who requests the information not be sent;
* copyright law violation; and
* commercial or personal advertisements, solicitations, promotions, destructive programs, or any other unauthorized use.

Users should understand that, due to their nature, electronic communications can be intentionally or unintentionally viewed by others or forwarded to others, and are therefore inherently not private. In addition, addressing errors, system malfunctions, and system management can result in communications being viewed and/or read by other individuals and/or system administrators.