1. Introduction

These instructions set forth the guidelines and rules of using SEDCO Capital's information technology resources and services. All users must adhere to these guidelines. Failure to comply may result in disciplinary action, including the revocation of access privileges and/or legal action.

2. Responsible Use

2.1. General Guidelines

Users of SEDCO Capital's IT resources must use them in a responsible, ethical, and legal manner. This includes but is not limited to:

a) Complying with all applicable laws and regulations.
b) Respecting the privacy and confidentiality of data and communications.
c) Avoiding any activities that could harm the integrity, availability, or security of IT resources.

2.2. Prohibited Activities

The following activities are strictly prohibited:

a) Unauthorized access to, use of, or tampering with computer systems, networks, or data.
b) Distribution of malware, viruses, or other malicious software.
c) Downloading or installing unauthorized software.
d) Violation of copyright, trademark, or intellectual property rights.
e) Harassment, hate speech, or any form of discrimination in electronic communications.
f) Unauthorized sharing, distribution, or downloading of confidential or sensitive information.
g) Unauthorized use of IT resources for personal or non-business-related activities.
h) Attempts to compromise the security or confidentiality of SEDCO Capital's IT resources.

3. Network and Internet Usage

3.1. Network Access

Access to SEDCO Capital's network and internet services is provided for business-related purposes. Users are expected to use these resources responsibly and avoid activities that may overload or disrupt network performance.

3.2. Bandwidth Management

Large downloads, streaming, or excessive use of bandwidth-consuming applications for personal use may be restricted during business hours to ensure network availability for critical business operations.

3.3. Social Media and Web Usage

The use of social media and web browsing during business hours should be limited to work-related tasks. Personal use should not interfere with job responsibilities.

4. Email Usage

4.1. Business Communication

Email is primarily intended for business-related communications. Users must refrain from using email for personal or non-business purposes that could lead to excessive use or the spread of unsolicited emails.

4.2. Phishing and Spam

Users should exercise caution and promptly report any suspicious or unsolicited emails. Do not engage with or click on links or download attachments from unknown or suspicious sources.

5. Data Security

Users must take all necessary precautions to protect the confidentiality, integrity, and availability of data.

6. Enforcement

Violations of these guidelines may result in disciplinary action, including but not limited to:

a) Temporary or permanent revocation of IT resource access.
b) Termination of employment or contractual relationships.
c) Legal action, where applicable.

7. PC and Equipment Care

7.1. Physical Handling

a) Users are responsible for handling company PCs and related equipment with care to prevent physical damage.

b) Users should keep their work area clean and free of dust and debris that may affect the performance of company PCs.
c) Do not stack heavy objects on top of PCs or place them in areas prone to spills or extreme temperatures.
d) When transporting company laptops, use protective cases or sleeves to prevent damage during transit.
e) Do not leave laptops or other company equipment unattended in vehicles, as extreme temperatures can damage the equipment.

7.2. Security

a) Ensure that company PCs are physically secure and protected from theft or unauthorized access.
b) Follow company policies and procedures for securing data and confidential information stored on company PCs.
c) Report lost or stolen company PCs immediately to the IT department and relevant authorities.

7.3. Software and Updates

a) Users should promptly install software updates and security patches as directed by the IT department to protect against vulnerabilities and security threats.

7.4. Access Control

a) Protect login credentials and use strong, unique passwords for company PCs. Do not share passwords with colleagues or external individuals.
b) Log out or lock company PCs when leaving them unattended to prevent unauthorized access.

7.5. Reporting Issues

a) Users must promptly report any hardware or software issues, damage, loss, or theft of company devices to the IT department.
b) Do not attempt to repair or modify company PCs without proper authorization from IT personnel.

By adhering to these guidelines, users help ensure the reliability, security, and longevity of company PCs. Failure to comply with these provisions may result in disciplinary/legal actions.