Information Security Handbook

PRAIRIE LAND ELECTRIC

Standards, Procedures and Guidelines

Version: 1.0

CONTENTS

CORPORATE INFORMATION SECURITY

Security Statement

The purpose of this handbook is to outline standards and procedures used to protect the company's information assets whether stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on electronic or optical media, or spoken from all threats, whether internal or external, deliberate or accidental.

It is the policy of Prairie Land Electric to ensure that:

- **Information** will be protected against accidental unauthorized access.
- **Confidentiality** must ensure the protection of valuable and/or sensitive information from unauthorized disclosure or intelligible interruption.
- **Integrity** of information will maintain the accuracy and completeness of information by protecting against unauthorized modification.
- **Regulatory** requirements will be met.
- **Business Continuity plans** will be produced, maintained, and tested to ensure that information and vital services are available to users when they need them.
- **Information Security training** will be available to all employees.

All breaches of information security, actual or suspected, will be reported and investigated by the **IT Department**.

The IT Department has direct responsibility for maintaining this handbook and providing guidance and advice on its implementation.

It is the responsibility of **EACH** employee to adhere to this Information Security Handbook.

INTRODUCTION

About this Handbook

This handbook outlines information security standards, procedures and guidelines that are utilized by Prairie Land Electric employees - they form the foundation for the Prairie Land Electric Information Security Program.

Compliance with the contents is mandatory.

The manual is the responsibility of the Prairie Land Electric IT Department, which will ensure that the statements within it reflect changing business and technological needs. Further detail on the responsibilities and the process of change control are given later.

Using the Standards

The manual is intended as a reference document to ensure that our practices and procedures are implemented in a consistent fashion across the enterprise.

Change Control

The manual is intended to be a "living" document and will be managed by the IT Department. All requests for amendments/additions must be approved by the IT Department.

The manual will be subject to version control and when sufficient changes have been received, a full reissue will occur. All amendments will be circulated to the appropriate staff and will ensure that copies held within Prairie Land Electric are updated and the amendment record noted.

STANDARDS

RISK MANAGEMENT

Use of Computing Resources

- Computer resources may only be used by authorized individuals and authorized purposes.
- Reasonable personal use of computer systems is allowed (e.g.: email, internet browsing).

Software Installation

- All software licenses will be maintained by the IT Department.
- The introduction of software into Prairie Land Electric computer systems by persons other than the IT Department is not allowed.
- Only licensed copies (if not open source) of software can be installed. Open source software will need to be evaluated by IT Department prior to install.
- Anyone suspecting unauthorized software present within a system must immediately inform the IT Department. Upon notification:
    - The incident will be logged.
    - Appropriate follow-up action will be carried out to remove the software.

Copyright and Software Piracy

- Regular reviews are carried out to ensure the terms of software licenses are being complied with.
- Any unauthorized software will be isolated and access disabled.
- The copying of software other than for legitimate backup purposes is not allowed.

Remote Computing

- Remote connectivity into the enterprise infrastructure will be available via SSL–VPN and Logmein only using 2 factor authentication.
- All Prairie Land Electric computers connecting to the company infrastructure must have anti-threat measures installed and in place:
    - Anti-virus software is installed and enabled.
    - Personal firewall is installed and enabled.

Internet Access

Prairie Land Electric, through the Internet, provides computing resources to its staff to access information, communicate, and retrieve and disseminate organization and business related information.

Use of the public Internet by Prairie Land Electric employees is permitted and encouraged where such use is suitable for business purposes and as part of the normal execution of an employee's job responsibilities.

Security:

- All connections must be made via a firewall protected, managed gateway.
- Never download files from unknown or suspicious sources.

Unacceptable Use:

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- The following widely-used Internet programs represent significant potential security risks and are **not allowed** on any Prairie Land Electric computer. Many of these programs are packaged for download with spyware or dangerous malware which may seriously compromise your computers' security.
  - Peer-to-peer(P2P) file sharing services such as Gnutella, Kazaa, Bit torrent, eDonkey
  - Video games, particularly any that might be downloaded from the Internet
  - Shareware utilities such as so called "Internet Accelerators"
  - Internet based Internet Relay Chat (IRC)

Email

Prairie Land Electric maintains electronic communication systems (email, voice mail, etc.) to assist in company business both internally and externally. These systems, including the equipment and the data stored in the system, are and remain the property of Prairie Land Electric.

Employees should be aware that even when messages are deleted or erased, it may still be possible to recreate the message; therefore, the ultimate privacy of message control may not be assured.

While electronic communication systems may accommodate the use of passwords for security, this control does not ensure message confidentiality.

Security:

- DO NOT send confidential information when using email or any other messaging method that could be intercepted.
    - Credit card information: account number, PIN/PAN
    - Bank information: account number, routing information
    - Username & password combination

- When using email, don't open attachments unless you are expecting them. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.

- Check any embedded links within emails to verify they point to the expected location before clicking the link. Generally, hovering your mouse cursor above the link will display a "popup" indicating the target location – if the displayed link and the popup link differ, the intent might be malicious.

- Designated anti-virus software must remain installed and active at all times. Do not disable or remove the anti-virus software.

Unacceptable Use:

- Employees and other authorized users must not use offensive or obscene, derogatory or slanderous remarks in any electronic mail messages.
- The propagation of chain e-mail messages is not allowed.

Monitoring:

- Prairie Land Electric is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary, as authorized by management, to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

- Prairie Land Electric reserves the right to retrieve and review any messages composed, sent or received.

ACCESS CONTROL

User Identification

- All Prairie Land Electric domain user IDs must be allocated by the Prairie Land Electric IT Department.
- Unauthorized use of user IDs is prohibited.

Password

- Passwords must:
  - Not be displayed by the system on entry
  - Not be disclosed to others or written down
  - Not be recorded in audit trails
  - Not be the same as the user ID
  - Not be manufacturer supplied
  - Be changed immediately if it is thought that someone else may have discovered it
- Prairie Land Electric domain group policy "password standards" will enforce the following:
  - Be a minimum of 10 characters long
  - Contain characters from three of the following four categories:
    - English uppercase (ex: A-Z)
    - English lowercase (ex: a-z)
    - Base 10 digits (ex: 0-9)
    - Non alpha characters (ex: !, $, #, %, etc.)
  - Cannot contain the user's account name or parts of the user's full name
  - Be changed at least every 60 days
  - Minimum password age: 1 day (cannot change your password twice in one day)
  - Cannot be one of the last 12 passwords used
  - Your account will lockout after 5 invalid login attempts

Access Timeout

- Unattended computers must enforce a timeout not exceeding 20 minutes.
- Resumption of access must require the revalidation of the user's identity.
- Lock your account out after 5 invalid login attempts

Mobile Devices

- Must have at least a 4 digit passcode or 4 digit passcode with fingerprint sensor.
- Any device that has a Prairie Land email account will automatically require a 4 digit password even if it is not a company owned device.

PHYSICAL AND ENVIRONMENTAL SECURITY CONTROLS

Server Rooms

- All visitors must be accompanied by authorized personnel *while* in controlled areas.
- All third party contractors, visitors, etc. **must not** be left alone in the computer rooms or other sensitive locations.

Network Security

- Access to network equipment is restricted to authorized personnel only.
- Only authorized personnel are allowed to connect management-approved devices to the network. Such devices include workstations and servers owned by Prairie Land Electric that comply with the configuration standards of Prairie Land Electric, routers, hubs, firewalls, managed wireless access points and network management/monitoring devices. Installation and maintenance of these devices are restricted to the Prairie Land Electric IT Department.
- When a third party contractor's device (i.e. laptop) is to be connected to the network, it must be authorized by the Prairie Land Electric IT Department to ensure it is properly patched and anti-virus software is running.
- Users are not allowed to attach devices or PCs running host port scanning, "sniffers", or network filtering software.

DATA SECURITY

Information Classification

Information needs to be protected from unauthorized access, modification, disclosure and destruction. Classification of information into categories is necessary to help identify a framework for evaluating the information's relative value and the appropriate controls required to preserve its value to Prairie Land Electric.

- Two basic classifications of information have been established:
  - *Public*: Information that has been made available for public distribution through authorized company channels.
    Examples:
    - Corporate annual report
    - Public service bulletins, marketing brochures and advertisements
  - *Prairie Land Electric Internal Use*: Information that is intended for use by employees when conducting company business. *Examples:*
    - Proprietary information
    - Operational business information and reports and non-company information that is subject to nondisclosure agreement
    - Company phonebook and announcements
    - Company policy, standards and procedures unless stated otherwise
    - Personnel records, Prairie Land Electric Member/Customer data or Prairie Land Electric Member/Customer consumer personal identifying information, and health insurance records.
- Specific operating plans and business strategies. Where no classification is apparent, information will be assumed to be *Prairie Land Electric Internal Use.*

Sensitive Information Use & Handling

- Sensitive information for which access has been authorized may only be used for the purposes identified to and authorized by the information owner.

Email

- Users must not originate or forward *Prairie Land Electric Internal Use* information from/to a personal account (yahoo, hotmail, gmail, etc.)
- Users must not forward or further distribute company confidential information, inside or outside Prairie Land Electric, without the authorization of the originator or appropriate management.

PROCEDURES & GUIDELINES

PRAIRIE LAND ELECTRIC PORTABLE DEVICE SECURITY PROCEDURES

Physical Security

- **To report a missing portable device, call Shane Schumaker in the IT Department.**
- Users must protect Prairie Land Electric-owned (or authorized) portable computing devices and portable media from unauthorized access. Physical security measures shall, at a minimum, include the following:
  - Devices **must not** be left unattended without employing adequate safeguards such as simply taking it with you.
  - Portable computing devices and portable media must remain under visual control while traveling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device and portable media.
- Safeguards shall be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.
- When you travel or commute, the following guidelines can help guard against portable device and portable media thieves:
  - **Never** leave your laptop, laptop bag, portable device or portable media unattended.
  - If possible, carry your laptop in an inconspicuous bag (ex: backpack)
  - Keep your arm (or leg, if you set the bag down) through the strap.
  - Never leave your laptop, laptop bag or portable device or portable media in a visible area of a car. It is best to take it with you out of the car whenever possible.
  - If you place your laptop in the trunk of your car, place it there before you leave for your destination, not after you are parked at your destination. Thieves watch for people who place items in the trunk and then walk away from their car.
  - Take extra care at times and places where you can be easily distracted, such as:
    - At an airline or rental car counter
    - While going through airport X-ray
    - While speaking to someone, whether in person or on the phone
    - When a stranger distracts you by asking for assistance or bumping into you - it could be a decoy

INFORMATION SECURITY HANDBOOK ACKNOWLEDGEMENT FORM

As an employee of Prairie Land Electric, I________________________________ have read and fully understand the Prairie Land Electric Information Security Handbook.

I am aware that violations of this guideline may subject me to disciplinary action, up to and including discharge from employment. In particular, I understand that all information transmitted by, received from, and stored by Prairie Land Electric equipment are the property of Prairie Land Electric and that I have no expectation of privacy in connection with the use of the e-mail system, company-provided access to the Internet or with the transmission, receipt or storage of information in any of those systems.

I understand that this signed document will be retained in my personnel file.

NOTE*: This document will be revised periodically to reflect changes in security process and procedure - you may be required to acknowledge your acceptance of the revised document.*
If you wish to discuss an aspect of this agreement you may do so by contacting the IT Department.

___________________________________ ______________________

Signed Date