



Information Security Standards

Introduction

The intent of these information security standards is to ensure employees understand their role in the protection of Grand Valley Power's sensitive information and systems. All employees must read this document and sign the Agreement to Comply on the last page. This document is reviewed and updated annually or when new security standards are implemented.

1. Acceptable Use

Grand Valley Power adheres to professional standards and prohibits illegal or damaging computer activities. Therefore, employees are expected to:

- Use company resources responsibly.
- Keep passwords secure and do not share them.
- Lock workstations and devices when unattended.
- Inspect equipment regularly and report any issues to IT.
- Avoid using company resources and the Internet for offensive or illegal actions (e.g., discrimination, pornography, etc.).

2. Data Classification

Information is classified based on its sensitivity:

- Confidential Data: Legally protected data (e.g., member information, employee information, proprietary company documentation, payment cardholder data). Disclosing it can cause severe harm.
- Sensitive Data: Important data that must be protected (e.g., internal emails, day-to-day work, and project documents).
- Public Data: Can be shared without restrictions but get permission first if you are not sure.

3. Physical Security

To protect sensitive data:

- Restrict access to areas where sensitive information is stored (both digital and physical).
- Ensure that visitors are escorted in sensitive areas.
- Shred sensitive documents rather than throw them away.

4. Payment Cardholder Data

No member payment card data is stored on Grand Valley Power systems. All card data is encrypted during the payment process. Employees assisting with payment cards must:



- Regularly inspect payment devices for tampering.
- Report any suspicious behavior or device issues to the IT department.
- Complete PCI training every year.

5. Security Awareness and Procedures

Employees are responsible for maintaining information security. These responsibilities include:

- Following department procedures for handling sensitive data.
- Completing cyber training as assigned by the IT department.
- Exercising caution when sending or receiving email or messages.
- Ensuring third-party vendors comply with Grand Valley Power standards.

6. User Access Management

Access to Grand Valley Power's systems is based on job roles and responsibilities. Each employee gets a unique ID that only they should use. When an employee leaves, access is revoked immediately.

7. Access Control

To secure our systems:

- Employees are granted access only to the systems necessary for their job.
- Access is limited to the minimum necessary to complete job duties.
- Remote access must be approved by IT and treated with care.
- Prior to using any personal devices (tablets, smart phones, USB thumb drives, etc.), on the Grand Valley Power network or systems, ask the IT department for assistance first.
- Company-owned computers, tablets, phones, and other technology assigned to employees may be inspected at any time to ensure compliance.
- There is no expectation of privacy when using company equipment. All technology provided by Grand Valley Power should always be used professionally and appropriately.

8. Associated Policies

The [Electronic Communications Systems Policy](#) found on the Grand Valley Power Intranet provides additional details regarding acceptable use of Grand Valley Power systems as well as other important information you should be aware of as an employee.



Agreement to Comply

I, the undersigned, have read and understood the Grand Valley Power Information Security Standards. I understand the importance of protecting sensitive data and agree to abide by the guidelines outlined in this document as well as those found on the [Grand Valley Power Intranet](#). I also understand that failure to comply with this policy may result in disciplinary action, including termination of employment.

By signing this form, I acknowledge that:

- I will not disclose sensitive or confidential information without proper authorization.
- I will follow all security procedures, including protecting passwords, securing workstations and mobile devices, and reporting any security incidents promptly.
- I understand my responsibilities regarding acceptable use of Grand Valley Power's resources.
- I will report any information security concerns to the IT department.

Employee Name (printed): _____

Department: _____

Employee Signature: _____

Date: _____