Policy Name – IT Assets Acceptable Use	Policy Reference #: 2.0
Information Services	Last Updated: May 29, 2019
Approval: SVP & Chief Administrative Officer	

1.0 Purpose

The purpose of this policy is to define the expectations of all who utilize Gibson Energy's IT assets (collectively, the "IT Assets") to protect the organization from the impact of cyber risk.

2.0 Scope

The policy establishes cybersecurity requirements for accessing the IT Assets.

The intended audience includes all staff, vendors, external contractors who utilize the IT assets (collectively the "Users").

3.0 Policy

General Use

All IT Assets are to be utilized for supporting the business functions at Gibson Energy. Users shall not utilize these assets for activities that would be considered damaging to the organization or potentially illegal. All activities conducted using IT Assets must comply with the Code of Conduct and Ethics.

If a User believes that the integrity or confidentiality of Gibson Energy digital systems or information has been compromised, such User must immediately report this incident to his or her manager, department head or IS security (GibsonITSecurity@gibsonenergy.com).

Users may access, use or share Gibson Energy proprietary information only to the extent it is authorized and necessary to fulfill his or her assigned job duties.

Hardware and Software Use

Users must take proper care and ensuring appropriate use of all IT Assets assigned to them. IT Assets shall not be used to conduct a personal business.

All software on IT Assets must be approved by IS to be installed and used. All software must be used per its valid licensing agreement.

All software usage must comply with copyright, licensing and contractual obligations governing the downloading, storage, reproduction and use of software, information (such as proprietary databases or subscription newsletters), music, images and other intellectual property.

Electronic Communications

The use of electronic communications (e-mail, text, instant messaging, teleconference) services must not be used in a way that may damage the organization. All messages sent via electronic communications must comply with the Respectful Workplace Policy, Corporate Communications Policy, and Commercial Electronic Message and Anti-Spam Policy.

Any transmission or sharing of confidential information must follow the Confidential Information Policy.

Users shall not automatically forward Gibson Energy e-mail to a non-Gibson Energy email account.

Internet Usage

Gibson Energy uses the Internet as a key business tool. This use is intended to support and satisfy a User's work responsibilities with Gibson Energy. Use of the Internet from Gibson Energy systems must comply with the Respectful Workplace Policy and Corporate Communications Policy.

User Accounts and Passwords

Users will be given a unique user account and for which they will create a password that adheres to Gibson Energy password standard. Users are responsible for all actions taken with their account.

Users must not share their account information including with their supervisors or administrative assistants.

Protect Devices

Users are responsible to secure any device in their possession that has access to IT systems from being accessed or stolen from external parties.

All lost or stolen devices including personal devices used to access Gibson Energy's systems must be reported to IS Desktop Support immediately.

Mobile Devices

To enable Mobile devices to access Gibson Energy IT systems, the device must meet the current mobile device configuration standard and be managed by Gibson Energy's Mobile Device Management system.

Information Protection

IT Assets are to enable users in delivering on their role in the organization. They must be used responsibly and protected from external threats.

Access to IT Assets will be assigned to support business activities in accordance with the authorization requirements set by the Information Asset Owner.

Utilization, sharing and storage of confidential information assets needs to comply with the Confidential Information Policy.

It is all Users' responsibility to report access to IT Assets that they do not need and request access to the IT Assets they need to complete their role.

Gibson Energy is respectful of applicable privacy laws, but all IT systems and communications may be monitored for performance and security reasons.

Unacceptable Use

- Activities in general prohibited (unless exempted as part of job responsibility):
- Port Scanning or security scanning is expressly prohibited unless authorized.

- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan Horses, email bombs etc.).
- Providing information about or lists of Gibson employees to parties outside Gibson.
- Introducing honeypots, honeynets, or similar technology on Gibson Network.
- Attempting or accessing data of which the employee is not intended recipient or logging into IT Assets or accounts that the employee is not expressly authorized to access.
- Causing disruptions (e.g. network sniffing, ping floods, packet spoofing, denial of service etc.) for malicious purpose.
- Execute any type of network monitoring which will intercept data, unless authorized.
- Circumventing user authentication or security of any host network or account.

Roles and Responsibilities

Leader	Employee	Information Services
• Present and ensure employees have reviewed and signed the policy • Set expectations within the team • Uphold the terms of the policy • Seek additional guidance from IS	• Uphold the terms of the policy • Seek additional guidance from IS if required	• Review and maintain the policy at least annually • Lead and facilitate the administration of the policy • Provide policy guidance and interpretation to leaders, employees and other stakeholder groups • Investigate and report violations of the policy

5.0 Process

Policy Enforcement

Non-Compliance (Individual Policies)

If a User demonstrates willing non-compliance with this policy, then disciplinary action will be taken.

Violations of this policy are grounds for disciplinary action up to and including termination of employment, civil action, and/or criminal prosecution. Gibson Energy will also pursue and prosecute, where deemed appropriate, any non-employee who accesses or uses, or attempts to access or use, the IT Assets and its components without proper authorization.

Policy Management

Content

This policy shall be followed for all IT Assets.

Policy Review and Changes

This policy will be reviewed for compliance and relevance on an annual basis.

6.0 Relevant Documents and Helpful Resources

Definitions

Phrase/Word	Definition
IS	Information Services
IT Assets	There are three types of assets that this policy refers to including: • **Information Assets** Every piece of information about the organization falls in this category. This information has been collected, classified, organized and stored in various forms. • **Software Assets:** Application software and system software. • **Physical assets:** These are the visible and tangible equipment and the devices that make up the network.
Electronic Communications	Electronic communications consist of mechanisms to communicate information in a recorded manner. Electronic communications may include: • E-mail • Instant Messenger • Text Message/SMS/iMessage • Teleconference/Web conference • Social Media • Web sites
User Device	A physical IT asset that is in the possession of Users.
Mobile Devices	Mobile devices consist of devices that are regularly transported with Users and typically consist of mobile phones or tablet computing devices.
Personal Devices	A personal device is a computing device that is not owned by Gibson Energy but is used to access assets that exist within the Gibson Energy IT environment.

The Company maintains the exclusive right to amend, adjust or terminate this policy at any time. Revisions or additions to the information contained in this policy document will be made as required.

Change Record

Date	Reason for Change	Owner
05/29/19	Added Unacceptable Use Examples	