Digital Assets Acceptable Use Policy

Table of Contents

1 Overview

Gibson Energy Inc., hereinafter referred to as "**Gibson Energy**", is committed to protecting employees, contractors, third parties, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a concerted effort requiring the awareness, participation, and support of every employee, contractor, vendor and third party that interacts with company owned, operated and/or leased Industrial Control System (ICS)/Operational Technology (OT) assets, Information Technology (IT) assets and electronic files stored on Gibson Energy's systems (collectively, the "**Digital Assets**").

1.1 Purpose

This Acceptable Use of Digital Assets Policy (the "**Policy**") outlines the acceptable use of Digital Assets owned, operated and/or leased by Gibson Energy and to ensure that inappropriate or unauthorized use of digital technology are adequately managed to support business objectives.

Inappropriate use of Digital Assets can potentially expose Gibson Energy's Digital Assets to cybersecurity risks, including ransomware, malware, compromise of network systems and services, data breaches, operational disruption, potential degradation of industrial safety, and legal issues.

1.2 Scope

All users (employees, contractors, vendors, and other third parties, whether or not temporary) of our Digital Assets (collectively, the "**Users**," "**you**," or "**your**") are responsible for reviewing, understanding and implementing these requirements to govern their activities accordingly.

Digital Assets covered under the scope of this Policy include, but are not limited to, the following:

- Software
- Hosts (virtual or physical)
- Laptops and computers
- Mobile devices
- In-vehicle monitoring devices
- Electronic files (created and/or stored on Gibson Energy's systems)
- Emails
- Internet
- Artificial Intelligence ("**AI**") tools (e.g., Azure AI, Microsoft Co-Pilot)
- Voicemail
- Other Hardware, including but not limited to:
    - **Supervisory Control and Data Acquisition (SCADA) systems**: These systems are used for remote monitoring and control of industrial processes of facilities.
    - **Distributed Control Systems (DCS)**: These systems control complex processes and are used in industries like oil refining.

- **Programmable Logic Controllers (PLC)**: These are versatile control devices used in automation for crude oil terminals or pipelines.
- **Human-Machine Interfaces (HMI)**: These interfaces allow control room operators to interact with the control systems at terminals or refineries.
- **Flow Computers**: These devices measure and calculate the flow of liquids and gases in pipelines.
- **Sensors**: These devices detect changes in physical conditions like temperature, pressure, and flow.
- **Actuators**: These devices control a mechanism or system by moving or controlling a mechanism or system.

- Network and architecture diagrams
- Detailed system information
- Configuration Files
- Physical sites (e.g., plants) access

All use of Digital Assets must comply with the *Code of Conduct and Ethics*, the *Use of AI Tools in the Workplace Policy* and the *Confidential Information Policy*.

2 Ownership

All Digital Assets, including electronically created and/or stored data and email messages, are the property of Gibson Energy.

In the event the User's engagement is terminated for any reason, the User's account will be immediately deactivated and all electronic devices must be returned immediately to the Human Resources department.

3 Privacy

Users should be aware that use of all Digital Assets, including such activities as internet traffic, email communications, file transfers and system access is subject to monitoring and recording to ensure compliance with internal policies and security protocols and for other business purposes. As such, Users have no right to privacy or to the expectation of privacy with respect to their use of Digital Assets, subject to applicable laws.

Gibson Energy reserves the right to access all computers, workstations, email accounts and other Digital Assets, notwithstanding any passwords. Please be aware that deleting a file or email will most likely not destroy it completely.

4 Policy

1. Acceptable Uses

a) Digital Assets are to be used for business purposes in carrying out business functions at Gibson Energy and serving the interests of the company, of our clients and customers. Users are expected to exercise good judgment and professionalism in the use of all Digital Assets.

b) Incidental and occasional personal use of Digital Assets is permissible as long as such use: (i) does not interfere with workplace productivity or system/business

operations; (ii) does not pre-empt any business activity; (iii) is otherwise compliant with this policy; and (iv) is lawful.

c) You may use only the computers, mobile devices, computer accounts, computer files and any other applicable Digital Assets for which you have authorization.

d) You are individually responsible for appropriate use of your computer, account and all resources assigned to you.

e) Gibson Energy is bound by its contractual and license agreements respecting certain third-party resources; you are expected to comply with all such agreements when using such resources.

2. **Unacceptable Uses**

a) Users must not intentionally use Gibson Energy's Digital Assets to store, transmit or display information which:

a.1) violates or infringes on the rights of another person, including the right of privacy;

a.2) contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially, culturally or religiously offensive, or otherwise biased, discriminatory, or illegal material;

a.3) restricts or inhibits other Users from using the system or the efficiency of the Digital Asset(s);

a.4) use Digital Assets for any illegal purpose; or

a.5) embarrass Gibson Energy's personnel or jeopardize Gibson Energy's reputation.

b) Users must not intentionally disrupt any Digital Assets or obstruct the work of other Users such as by interfering with the accounts of others, introducing or spreading viruses or other destructive programs on computers or the network, sending chain letters or blanket e-mail messages, or knowingly consuming inordinately large amounts of system resources.

c) Users must not disable virus protection software, firewalls, internet screening programs or other security systems.

d) No software or hardware, including screen-savers, games, unauthorized AI tools or personal programs may be installed, deleted, replaced, repaired or updated on any machine by anyone other than the Information Services team or without Cybersecurity approval. All approved software must be used in accordance with their applicable licensing agreements and copyright laws which govern the downloading, storage, reproduction and use of the software. Downloading or distributing pirated software or data is prohibited.

3. **Electronic Communications**

a) Users must not send unsolicited electronic messages (e.g., email, text instant messaging), including "junk mail" or other advertising material to individuals who do not specifically request such material (e.g., spam).

b) Any form of harassment via email, telephone, text, social media or paging, whether through language, frequency or size of messages, is strictly prohibited.

c) Unauthorized use or forging of email header or email signature information is prohibited.

d) Such electronic communications must comply with the *Respectful Workplace Policy*, *Corporate Communications Policy*, and *Commercial Electronic Message and Anti-Spam Policy*.

e) Automatic forwarding of emails from Gibson Energy accounts to personal or non-Gibson Energy email addresses is not permitted. Forwarding individual emails for business purposes is allowed, but setting up rules to automatically forward all emails is prohibited.

f) Users must not use their email address or computer to subscribe to any email distribution lists for non-business purposes.

4. **Internet Usage and Network Connections**

a) Any Internet usage must also comply with the *Respectful Workplace Policy and Corporate Communications Policy*.

5. **Passwords**

a) Users may be given a unique Gibson Energy user account for which they will create a password that adheres to this Policy. Users must not use the *same* password for multiple accounts, devices, or networks and must not *reuse* passwords from personal accounts for accounts associated with Gibson Energy's Digital Assets.

b) Passwords must not be saved using application check boxes or software tools allowing online or internal password saving. For example, using "Remember Me" features or allowing your web browser, like Chrome, to remember company passwords for you.

c) Passwords must not be left on sticky notes posted on, near or under a computer, or left written down in an accessible location.

d) Passwords must be hard to guess and should not rely on predictable patterns, such as using a basic sequence of characters with minor changes for each new password. Instead, create passwords that are unique and not easily derived from previous versions.

e) All passwords must be immediately changed if they are suspected of being disclosed, compromised, or available to anyone besides the authorized user.

f) Users must not share account(s), passwords, Personal Identification Numbers (PINs), Security Tokens (i.e., Smartcards), or similar information or devices used for identification and authorization purposes or give others' access (physical or electronic) that they are not authorized to provide, including with their supervisors or administrative assistants.

6. **Lost/Stolen Devices.** Users are responsible for securing any device in their possession with access to Digital Assets from being accessed by external parties or stolen. All lost or stolen devices, including personal devices used to access Digital Assets must be reported

immediately to Information Services Desktop Support at actionline@gibsonenergy.com & GibsonlTSecurity@gibsonenergy.com.

7. **Mobile Devices.** Mobile devices with access to Digital Assets must meet the latest mobile device configuration standard and be managed by Gibson Energy's Mobile Device Management system. Users accessing Digital Assets on a personal device must either register their personal device or obtain approval for specific use cases. Users are required to keep their device operating systems and applications up to date with the latest versions, failure to do so may result in restricted access or disconnection from Digital Assets. For more information, please contact Information Services to ensure mobile device usage is compliant with this Policy.

8. **Access Levels.** Access to Digital Assets will be assigned to support business activities in accordance with the authorization requirements set by the Information Asset Owner. Users must not attempt to access data or Digital Assets which is not intended for the User or for which the User has not been granted authorization. All Users are responsible for reporting access to Digital Assets that are not required for their role and request access to Digital Assets needed to complete their role.

9. **Confidential Information/Security Sensitive Information**

    a) Utilization, sharing and storage of confidential information needs to comply with the Gibson Energy Confidential Information Policy.

    b) Users must not share or provide access to software, hardware, data, drawings, documentation, or Digital Assets with anyone who does not have authorization or need to know.

    c) Users are responsible for implementing appropriate physical security safeguards over confidential information.

    d) Information must be appropriately shared, handled, transferred, saved, and destroyed, in accordance with Gibson Energy's *Information Management Program*.

    e) Users are prohibited from providing information about or lists of Gibson Energy employees, customers, or other stakeholders to parties outside of Gibson Energy except as required for legitimate business purposes and all such disclosures must be in compliance with applicable privacy laws and Gibson policies.

10. **Removable Media.** Only removable media (e.g., USB, disk) that has been supplied, scanned and approved by Information Services may be plugged into Digital Assets. The use of personal removable media devices is prohibited. Personal use of company provided removable media devices is prohibited. All approved removable media devices that are no longer required must have all information stored on it securely deleted and returned to Information Services.

11. **Unattended Sessions.** Users must not leave their workstations or other devices unattended without either logging out or locking their device.

12. **Remote Access.** Users must not create any unauthorized remote access points to any ICS/OT environments or other networks.

    a) Users must not allow anyone other than themselves to access Gibson Energy's remote access system under their user account or password.

b) Personal use of any kind is prohibited on the OT remote access system.

c) Users must logon to the network to access email, download files or run applications remotely. Users must log off immediately upon completion of remote tasks.

d) Users must never leave remotely accessed computers unattended without logging off.

e) Users must have a current copy of Gibson Energy-provided anti-virus software installed and active on their work devices.

13. **Unapproved Devices.** Users must not connect unapproved personal or other electronic devices to any corporate Digital Assets.

14. **Use of Artificial Intelligence.** Gibson Energy recognizes that the use of AI tools can increase User productivity and innovation. At the same time, AI tools can pose risks to our information security, privacy, confidentiality, intellectual property and business operations.

a) Users may use pre-authorized AI tools in the course of performing their duties for Gibson Energy.

b) Users shall not use any AI tools outside of Authorized AI without the prior written approval from Information Services. Users must contact Information Services for approval to use any AI tools beyond those that provided directly by Information Services.

5 Training

To maintain the security of Gibson Energy's Digital Assets, all Users must complete mandatory cybersecurity training before receiving or using Digital Assets in the workplace and on an annual basis thereafter.

In addition to completing mandatory training, all Users are required to participate in periodic phishing simulation exercises to re-enforce security best practices. Failure to complete these simulations or demonstrate appropriate awareness may result in additional training, and if necessary, disciplinary action, up to and including termination of employment or contract, in accordance with Gibson Energy's policies.

6 Compliance

6.1 Reporting

Any User who becomes aware of a violation of this Policy must promptly disclose this to their Immediate Supervisor.

Users are responsible for reporting inappropriate access to Digital Assets, including Digital Assets that are not required for their role.

6.2 Consequences of Violation of this Policy

Violation of this Policy may result in disciplinary action, up to and including termination of employment or contract, as well as legal proceedings. Use of Digital Assets for illegal activity can also lead to criminal prosecution.

6.3 Policy Review and Changes

If Users have any questions regarding this Policy or any questions about using Digital Assets that are not addressed in this Policy, they may contact Information Services. Questions about the content of this Policy or suggestions for change should be reported to Information Services.

7 Document Governance and Revision History

Document #:	000000100
Revision #:	2
Effective Date (MM/DD/YYYY):	5/29/2019
Last Review Date (MM/DD/YYYY):	8/7/2025
Next Review Date (MM/DD/YYYY):	8/7/2030
Functional Area:	Information Services
OMS Element (N/A if not applicable):	N/A
Document Author:	Mohamed Borhot
Document Owner or OMS Driver:	Basim Abdalla
Governing Document(s):	

Revision History

Rev #	**Revision Date**	**Approver**	Revision Details (Describe changes)
01	5/29/2019	Sean Wilson	Issued for Use
02	7/23/2025	Curtis Philippon	Updated policy to include AI and OT; issued for use.