Title:	IT Acceptable Use Policy			
Type:	Corporate Policy	Version:	10/20/25 (v.7)	
Function:	General	Last Reviewed:	10/20/25	
Dissemination:	Internal only	Original Issuance:	1/31/14	
Owner:	Chief Information Officer			IT-01

1. PURPOSE

To define acceptable use, procurement, and possession of the information technology (IT) resources of Expand Energy Corporation and its subsidiaries (the "Company").

2. SCOPE

This policy applies to all Company employees and contractors ("Company Personnel") who use Company IT Resources, as defined in Section 5.

3. POLICY

Policy Summary

- **Business Use Priority:** IT resources are for business use, with limited personal use allowed if it doesn't interfere with work or violate policy.
- **Monitoring & Privacy:** All IT activity is monitored; users have no expectation of privacy when using Company systems. Personal legal communications will not be intentionally monitored, but it should not be assumed that such communications will be treated as private.
- **Security & Confidentiality:** Company Personnel must protect non-public company data and follow the Information Security Policy.
- **Password Management:** Potentially compromised passwords should be changed immediately and reported to Cybersecurity.
- **Privileged Access:** Access is granted only for job-related tasks and must follow strict standards.
- **Lost or Stolen Equipment:** Must be reported to the Help Desk; theft requires a police report.
- **Email & Messaging:** Mass non-work-related emails are prohibited and storing email or messages must comply with the Records Retention Schedule.
- **Copyright Compliance:** Company Personnel must follow copyright laws.
- **Personal Equipment:** Use of Personal Devices is limited to devices complying with the Bring Your Own Device Policy.
- **Hardware & Software:** Modifying hardware or installing software without IT approval is prohibited; all software must be properly licensed by the IT department.
- **AI/ML Tools:** Only IT-approved AI/ML tools may be used for work; use of AI/ML tools must be transparent and used in a way that protects Company data.
- **Data Handling:** Data must be managed according to the Information Security Policy and not shared with unauthorized parties or platforms.
- **Recording & Transcription:** Meeting recording/transcription is restricted to Microsoft Teams and Company Personnel must ensure any recording/transcription follows published guidelines and policy restrictions.
- **Policy Violations:** May result in disciplinary action, including termination and legal consequences.

3.1. General Policy

Company IT Resources are provided for official and authorized business purposes serving the interests of the Company.

3.2. Incidental Personal Use

Incidental personal use, including, but not limited to, e-mail access, texting, instant messaging, temporary personal file storage (e.g. documents, pictures, music, other media, etc.), personal calls or Internet use, is permitted if it: a) does not interfere with job responsibilities or professional duties; b) is of reasonable duration and frequency; c) is limited in nature such that productivity, performance and costs are not impacted; and d) does not violate Company policy. Please remember, though, that you should have no expectation of privacy, confidentiality, or privilege as to any such communications or use of Company resources for personal or other purposes.

3.3. Acceptable Use

The use of Company IT Resources in any manner that is disruptive, intimidating, hostile, obscene, unlawful or encourages unlawful conduct, threatening, defamatory, vulgar, pornographic, hateful, racially or ethnically offensive, insensitive, or violates Company policy is prohibited.

3.4. Privacy

The Company may, at its discretion and without notice, monitor and access all information transmitted using or stored on Company IT Resources. Company Personnel have no expectation of personal privacy with respect to any file, email, text or digital communication, document, attachment, program, voicemail or other material or communication transmitted using or stored on Company IT Resources. Internet usage, irrespective of the time of use, is monitored and usage reports routinely provided to Company management. Company Personnel are prohibited from removing monitoring capabilities from any Company IT Resource. All Company Personnel, by their use of Company IT Resources, consent to monitoring and auditing of their use of Company IT Resources without notice.

3.5. Security

3.5.1. Company Information and Data

Non-public Company data is inherently sensitive and should be treated as Confidential Information under the Information Security Policy.

Information regarding Company IT Resources is potentially sensitive, and any disclosure should align with the Information Security Policy.

3.5.2. Passwords

Company Personnel are required to maintain unique confidential passwords for Company IT Resources in compliance with the Information Protection Standard. If a password is compromised or thought to be compromised, Company Personnel are required to change the password immediately and notify Cybersecurity. Contact information is listed in Section 4.

3.5.3. Privileged Access

Privileged Access to certain systems or data is granted for the purpose of performing a designated job responsibility. Use of privileged Access should adhere to the Information Protection Standard and the Zero Standing Privilege Procedure.

3.5.4. Lost, Stolen or Damaged Company IT Resources

Company Personnel are required to report lost, stolen, or damaged Company IT Resources to the Help Desk. Stolen Company IT Resources will require a police report. Fines may be applicable and will not exceed the replacement cost. Contact information is listed in Section 4.

3.5.5. Additional Restrictions

Additional restrictions to Company IT Resources may be necessary to maintain performance or mitigate security risks as determined and communicated by the IT department.

3.6. E-mail & Messaging

3.6.1. Non-Work Related

Sending nonwork-related e-mail or other digital communication to a large number of recipients (e.g. 25 or more) is prohibited. Furthermore, in the interest of maintaining network performance and complying with copyright laws, Company Personnel are prohibited from sending large, nonwork-related e-mail attachments such as photos, music files, or movie files.

3.6.2. Storage

It is prohibited to store e-mail or other digital communication (e.g., .MSG, .PST files) outside of an approved application or storage area. E-mail and messaging storage is limited to maintaining official records in accordance with the Records Retention Schedule. Personal files should not be stored within e-mail or messaging platforms. Refer to the Records Retention Schedule for details.

3.7. Copyright

Company Personnel are responsible for complying with applicable copyright laws. Questions related to copyright should be directed to the Legal department.

3.8. Personal Equipment

Other than pursuant to the Bring Your Own Device Policy or using Company provided channels (e.g., websites authenticated with Single Sign-On like Microsoft 365), connecting Personal Equipment to Company IT Resources is prohibited. Company data-bearing devices, including but not limited to SIM cards provided with a Company Device, may not be inserted into Personal Equipment without prior authorization. The Company does not provide technical support for Personal Equipment or third-party software. Company Personnel violating this provision by connecting their Personal Equipment to the Company's network without prior approval, acknowledge the Company has the ability to access that device, as needed, to retrieve Company data.

3.9. Hardware

Computer systems must connect to the Company's network for four (4) consecutive hours every ninety (90) days at a minimum.

Computer hardware is configured based on a standard. It is prohibited to modify Company hardware with personally purchased/owned components. This includes, but is not limited to, the removal or addition of components such as RAM, Hard Drives, Video Cards, SIM cards, etc. The IT department is responsible for adding or removing components as necessary.

3.10. Software

Prior consent of the IT department is required to 1) download or install software onto Company computers and 2) initiate service for Internet-based software or other IT services. Contact information is listed in Section 4.

All software installed on Company computers and networks must be used and properly licensed by the IT department in accordance with the software license terms, copyright laws, or other applicable agreements. This includes all off-the-shelf and custom-developed software as well as "shareware," "freeware" and "public domain" software. No software should be downloaded or installed onto Company computers without the prior consent of the IT department.

All Internet-based software used for Company business must be used and properly licensed in accordance with the software license terms, copyright laws or other applicable agreements. This includes all web-based applications, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), and Internet-of-Things (IoT) platforms.

3.11. Artificial Intelligence and Machine Learning Tools and Platforms

The Company recognizes the need for Company Personnel to utilize Artificial Intelligence (AI) and Machine Learning (ML) tools and platforms to increase productivity, enable innovation, and aid decision making. The intent of this policy to enable these tools and platforms to be used in a secure, ethical, and responsible manner, while recognizing the unique risks presented by such tools.

3.11.1. Work Use

Company personnel are required to review the AI/ML Guiding Principles provided at the AI page on The Point. Only Company approved AI/ML tools can be used for work-related activities in a manner that ensures all Company data remains protected. No unapproved AI/ML tools may be used to perform any work, integrated into any workflows, or used to process Company data. AI/ML training and additional resources are available at the AI page on The Point and may be required by Company as communicated to Company Personnel.

Company Personnel must be transparent with stakeholders and communicate when AI/ML tools are used in decision-making processes. The AI page on The Point includes guidance for using an AI/ML disclaimer and how to appropriately mark documents. Company Personnel utilizing AI/ML tools are responsible for ensuring the accuracy and integrity of any work product developed with AI/ML assistance. All AI/ML-generated materials must be validated by Company Personnel and justifiable upon review.

3.11.2. Permitted AI Tools

Only Company approved AI/ML tools may be used on Company IT Resources or for any work-related tasks. A list of approved AI/ML tools is provided at the AI page on The Point and updates will be made as new technologies are vetted and approved. No AI/ML tools should be downloaded, installed, or utilized on Company IT Resources, nor used with any Company data on any device, without prior approval of the AI Committee.

All Company Personnel must seek prior approval from the AI Committee for the use of new AI/ML tools in their work. Anyone wanting to use a new AI/ML tool must submit the new tool to the AI Committee for review. The Company's AI Committee which includes representation from Legal, Operations, IT, and Cybersecurity, will review all submissions to ensure the AI/ML tool meets the Company's security, legal, and technical standards before use.

Any existing software or enterprise tools that introduce AI/ML tools must be brought into compliance with this policy. The AI Committee will regularly review existing software and enterprise tools to ensure any new AI/ML tools are properly reported and approved. Company Personnel who suspect, discover, or receive notification that any Company approved software is upgraded to include any AI/ML capabilities must promptly inform the AI Committee. Contact information is listed in Section 4.

3.11.3. Unauthorized Use

Any unauthorized use of non-Company approved AI/ML tools on Company IT Resources, or misuse or abuse of Company approved AI/ML tools, by Company Personnel must be promptly reported. Additionally, any security concerns raised by the use of AI/ML tools for work on Company IT Resources must be submitted immediately to Cybersecurity. Contact information is listed in Section 4.

3.12. Data

Data creation, retention, disposition, or transfer is subject to the Company's Information Security Policy. Company data may only be downloaded, uploaded, or otherwise transmitted within Company IT Resources or with third parties having a legitimate Company business purpose. Non-public Company data may not be uploaded to any publicly accessible service, including, but not limited to, artificial intelligence (AI) and machine learning (ML) services.

3.13. Vehicle Safety

Text messaging and other distracting uses of Company IT Resources are strictly prohibited while operating any vehicle.

3.14. Equipment Return

Supervisors and department heads must return all Company IT Resources assigned to departing Company Personnel to the IT department prior to reassignment to other Company Personnel.

3.15. Recording and Transcribing Communications

The Company has a substantial interest in maintaining trust, securing Company confidential, proprietary, or legally sensitive information, and protecting Company Personnel privacy in recording and transcribing communications for work-related activities.

3.15.1. Permitted Use

Upon completion of the Company's Recording/Transcribing Training, available through the Company's training platform, Company Personnel may initiate Microsoft Teams recording and transcription functionality for telephone or video communications on Company IT Resources. Use of the recording or transcribing functionality is limited to work-related activities on Company IT Resources and is subject to the Company's Recording/Transcribing Guidelines. Transcriptions and meeting summaries generated by the Microsoft 365 Platform are provided as a productivity enhancing tools but should not be relied on for accuracy.

3.15.2. Restrictions

Use of any recording devices, software, or applications other than the Company's Microsoft 365 Platform during any communications is prohibited. If Company Personnel become aware that a third party is virtually recording or transcribing a communication without the Company's prior authorization, they must request the recording stop, move the meeting to the Company's Microsoft Platform, or reschedule the call for when it can meet the Company's Recording/Transcribing Guidelines.

Recordings or transcriptions should not be made of the following types of meetings and conversations:

- Discussions involving confidential, proprietary, or legally sensitive content
- Conversations regarding private personnel information such as compensation or performance evaluations
- Events with Executive Vice Presidents or higher-ranking executives as participants

This restriction on executive participation does not include formal Company presentations such as quarterly company-wide meetings or department-wide meetings.

3.15.3. Storage

It is prohibited to store recordings and transcriptions outside of the Microsoft 365 Platform. Refer to the Records Retention Schedule for details.

3.16. Policy Violations

Company Personnel who violate this policy may be subject to disciplinary action, up to and including separation of employment, and if applicable, prosecution to the full extent of the law.

3.17. Limited Exception

Notwithstanding the foregoing, nothing in this policy prevents employees from engaging in concerted activities permitted by applicable law (such as engaging in collective bargaining to improve working conditions or discussing the terms or conditions of employment) for the mutual aid and protection of

employees. Any other deviation from this policy must be approved by the Chief Information Officer and General Counsel.

4. CONTACTS

- AI Committee – ai@expandenergy.com
- Cybersecurity – cybersecurity@expandenergy.com
- Legal department – legal@expandenergy.com
- Reporting lost/stolen equipment – helpdesk@expandenergy.com | 405-935-9311
- IT approval for software – helpdesk@expandenergy.com | 405-935-9311

5. DEFINITIONS

5.1. Company IT Resources

Company provided voice communications services, voicemails, the Company Intranet and Internet connections, the local area network ("LAN"), the wide area network ("WAN"), wireless network, e-mail, messaging and other multimedia services, mobile devices, server and personal computing devices and their peripherals, and Company-related IT services and software, including approved artificial intelligence and machine learning platforms.

5.2. Company Device

Includes, but is not limited to, Company-issued desktop and laptop computers, tablets, smartphones, mobile phones, and mobile hotspots.

5.3. Microsoft 365 Platform

Microsoft applications including, but not limited to, Teams, OneDrive, SharePoint, and Outlook, which are installed on Company IT Resources or hosted within the Company's Microsoft tenant (a private, access controlled environment) provided as part of the Company's Microsoft 365 enterprise license.

5.4. Personal Equipment

Any device that is not owned by the Company that may access Company information, including, but not limited to, computers, smartphones, tablets, mobile phones, thumb drives, and external hard drives.

5.5. Privileged Access

Any special access level beyond that of a standard user account. Often, but not always, this includes administrative access or an account distinct from the standard user account.

5.6. Single Sign-on (SSO)

Websites, web applications, software, or tablet/mobile device applications which authenticate through the Company's identity service provider (i.e. Okta).

6. RELATED DOCUMENTS

Information Security Policy
Bring Your Own Device Policy
Protection of Expand Energy Assets Policy
Records Retention Schedule
Information Protection Standard
Zero Standing Privilege Procedure
Recording and Transcription Guidelines