It is our responsibility as employees of and contractors to Total Energy Services Inc. and its subsidiaries and affiliates worldwide (each a "**Division**"), where each Division and its subsidiaries and affiliates and Total Energy Services Inc. are collectively and individually, as the case may be, the "**Company**") to conduct our business in a professional manner, to properly utilize Company assets provided to us in order to do our jobs more efficiently and to understand the effects of our actions on the Company's operations, financial performance and reputation.

This policy guides users of the Company's Information Technology (IT) infrastructure. It balances the employee's ability to benefit fully from information technology with Company's need for secure and effectively allocated IT resources. Any violation of this policy may lead to disciplinary action, up to and including dismissal for cause.

1. Policy

The use of Company information systems, including computers, fax machines, cellular devices and all forms of internet/intranet access, is for company business and for authorized purposes only.

Electronic communication should not be used to solicit or sell products or services that are unrelated to Company's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of Company computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Signing up for email notification to work account for non-work related activities;
- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail (ie. spam) that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Sharing of passwords or any other measure given to a user to grant him or her access to data, hardware or buildings - ie network passwords, keys, security access cards / FOBS
- Making unauthorized copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;
- Misrepresenting oneself or Company;
- Violating the laws and regulations of Canada, city, province, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;

- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs (ie. blogs), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games or videos; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Using Company information systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates Company anti-harassment policies and is subject to disciplinary action. The Company's electronic mail system, mobile phone systems, internet access, and computer systems must not be used to harm others or to violate the laws and regulations of Canada or any other city, province, or other local jurisdiction in any way. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

Unless specifically granted in this policy, any non-Company business use of Company's information systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal for cause. In addition, any excess fees or charges that are incurred as a result of inappropriate use of the Company's computers, networks, phones or internet access will be the responsibility of the employee.

2. Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy

The Company owns the rights to all data and files in any computer, network, or other information system used in the Company and to all data and files sent or received using any Company system or using the Company's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The Company also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content.

Employees must be aware that the electronic mail messages sent and received using Company equipment or Company-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times.

The Company has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with Company policies and provincial and federal laws. No employee may access another employee's computer files, or electronic mail messages without prior authorization from an appropriate Company official.

The Company uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on Company electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Company use at any time. Further, employees who use Company systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than Company systems or Company-provided Internet access.

No employee may use Company hardware or software for work outside of the Company. The Company has licensed the use of certain commercial software application programs for business purposes only. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.

3. **Internet/Intranet Browser(s)**

The Internet is to be used to further the Company's business, to provide effective service of the highest quality to the Company's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are Company resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements. Employees are also responsible for all costs incurred by the Company from inappropriate use of computer systems, mobile phones, smartphones, or other third party charges.

All Company policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

4. **Approved Equipment**

The proper selection and use of equipment is critical to maintain the integrity of our communication systems. Using the incorrect hardware or software can have severe, unintended consequences on the functionality of the Company information systems.

All equipment (e.g. computers, laptops, smartphones, cell phones, tablets, etc.) used on the Company's IT systems or used to access the Company's networks are to be approved by the Information Technology group prior to use. Any equipment not receiving prior approval will be removed from the Company computer system immediately.

Regarding all mobile devices (e.g. smartphones, handheld computers, etc.), only authorized mobile devices and apps may be used to store Company data or connect to the Company's computers and networks. This includes the forwarding of email, telephones or other information to personal devices. Any non-approved device will be disabled immediately.

5. **Cell Phones and Portable Computers**

All portable electronic equipment, which may include cell phones, computers, laptops, radios, etc. and all associated equipment such as chargers, cords, holders, bags, etc. are assets of Total.

Employees are responsible for the appropriate care and use of any and all assigned Company property. Employees must immediately inform their supervisor of the loss or damage to company property. If the loss is due to negligence or abuse, the employee may be held responsible for repair or replacement costs.

6. **Personal Electronic Equipment**

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, iPods, or other data storage media) or other electronic equipment (cameras, tablets, etc.) to the workplace or connect them to Company electronic systems unless expressly permitted to do so by Company. Any employee bringing a personal computing device, data storage device, or image-recording device or any other electronic equipment onto Company premises thereby gives permission to the Company to inspect the device at any time with personnel of Company's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal computer or image-recording device in question. Employees who do not wish such inspections to be done on their personal devices should not bring such items to work at all.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment for cause, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from Company, from law enforcement officials, or from individuals whose rights are harmed by the violation.

These policies are for the protection of Company, its shareholders, and its employees. It is the Company's belief that its interests, and those of its stakeholders, can best be served by managing our activities pro-actively, clearly, and safely.

This corporate Information Technology Use Policy approved this 30th day of November, 2023

Brad Macson
Vice President, Operations
Total Energy Services Inc.