IT SECURITY AND INFORMATION MANAGEMENT POLICY

Approved by: Peter Scott, Senior Vice President, and Chief Financial Officer
Date Effective: December 2025

INTRODUCTION AND APPLICATION

This policy establishes a baseline for information security in order to protect the reputation of the Company with respect to Obsidian Energy's ethical and legal responsibilities. Obsidian Energy is committed to providing a secure environment that protects the confidentiality, integrity, and availability of electronic information from unauthorized intrusions, misuse, or inadvertent compromise, while maintaining accessibility for authorized Users (as defined below) to perform their work. This policy applies to all authorized users that utilize the company information systems. A User is considered authorized when they are issued a valid User ID and password by the Obsidian Energy Information Technology Department ("IT Department"). All Users of Obsidian Energy information systems are responsible for the security and protection of electronic information resources in their control.

The Information technology "IT" Department holds the responsibility for ensuring robust information security, providing support to Users and Representatives in all related areas including: protection and prevention against malware/viruses, stewardship of enterprise-wide systems and networking, and improving general security awareness around our technology and systems. The IT Department reserves the right to monitor email, internet, and network access activity in order to ensure compliance with this policy.

Where activities are outsourced to external representatives, the measures taken to protect Obsidian Energy data and infrastructure must meet or exceed Obsidian Energy security requirements.

Violation of this policy may result in disciplinary action. This may include termination of employment, contract, or consulting services. Representatives who are aware of a violation of this policy must inform the IT Department Manager. Violations can also be reported using EthicsPoint at 1-877-309-9397 or at:

www.obsidianenergy.ethicspoint.com.

In this Policy, Obsidian Energy Ltd. and its subsidiaries are referred to as "Obsidian Energy" or "the Company." Unless stated otherwise in the Policy, this Policy applies to the Directors, Officers, Employees, and contractors (where applicable) of Obsidian Energy (referred to collectively as "Representative(s)").

ACCEPTABLE USE

All Company information, records, files, data, electronic communications, software, hardware, and IT services are the exclusive property of Obsidian Energy. All Company software, hardware, and IT assets should be used for business purposes. All non-public corporate information is confidential. You must ensure an appropriate level of security when transmitting data. All corporate work product should be conducted using corporate Obsidian Energy-approved email and IT assets.

Limited personal use of IT assets is allowed only if it does not incur excessive costs, hinder network performance, or violate Company policies, guidelines, and standards. Personal data or communications stored, transmitted, or addressed on Obsidian Energy devices are considered Company property, and users should have no expectation of privacy.

Use of personally owned laptops or tablets to connect to corporate systems, whether for remote access or to or store and utilize corporate data including email, files, and other data types, may be permitted with prior authorization from the IT Department. Users are expected, where possible, to segregate personal and business data wherever feasible, report any changes to authorized personal devices promptly, and comply with all security policies. Authorized personal devices are subject to the same security requirements as Company-owned devices, and these policies will be enforced without notice.

All electronic data and communications created, stored, or transmitted on Obsidian Energy systems are considered Company records and property. This includes all messages, voicemails, and stored data, regardless of content. Users should have no expectation of privacy for communications or electronic data that you send, receive or store within Obsidian Energy systems and may be asked, in connection with an investigation, to provide all access codes and passwords upon request during investigations, as approved by department head, to ensure compliance with Company policies.

PROHIBITED USE

Prohibited usage of IT assets includes violating laws; harassing or discriminating on the basis of gender, race, disability, age, religion, etc.; viewing, transmitting, saving storing or printing sexually explicit material; copyright infringements, placing wagers and bets or inciting violence. Personal text messages to authorize official corporate business is prohibited as is forwarding Company information to personal email accounts.

Confidential company data should not be uploaded, entered or filtered on artificial intelligence-based platforms and/or tools. If you are unsure whether the information is confidential, please speak to your supervisor or line manager.

USER RESPONSIBILITIES

All members of staff are required to:

Access and Credentials:

- Follow the Company's password and remote access protocols.
- Protect login credentials and avoid sharing email accounts.

System Security:

- Apply monthly, or as requested, security patches to all Company and home-based devices.
- Use the corporate Citrix portal or VPN for remote access.
- Store company files, especially confidential ones, on approved network drives.
- Encrypt or password-protect files stored on USB drives.
- Avoid modifying or altering the corporate network or components.

Physical and Remote Security:

- Secure portable devices and avoid unsecure public Wi-Fi.
- Lock or log off computers when unattended.
- Use password protection on smartphones.
- Immediately report lost devices to the Service Desk.

Cybersecurity Awareness:

- Complete mandatory cybersecurity training.
- Report phishing attempts and suspected malware infections to the Service Desk or IT Manager immediately.

Software Compliance:

- Follow licensing agreements for company-purchased software.

Artificial Intelligence Usage:

- Please refer to the Generative AI Acceptable Usage Policy for usage guidelines. This policy can be found via this link: AI Usage Policy

CORPORATE CYBERSECURITY AND MALWARE PROTECTION

The AAA Framework guides Obsidian Energy’s cybersecurity strategy—Authentication, Authorization, and Accountability—to ensure comprehensive protection of all systems and data. All systems are required to utilize the Company’s standard, supported anti-virus and malware software, configured for automatic execution at regular intervals. Firewalls and advanced network security software are deployed to ensure the integrity of network traffic. Any system suspected of virus or malware infection will be immediately isolated from the network until verified as virus- and malware-free. Anti-virus systems must be updated at least monthly (or as soon as practical in the case of critical updates) to maintain protection against evolving threats.

Authentication

- Access to all systems, including anti-virus management consoles, is restricted to authorized personnel using multi-factor authentication (MFA), passkeys, and/or biometric authentication.
- All networked devices must authenticate with the Company's directory services to maintain access privileges and ensure system compliance.

Authorization

- Only authorized personnel are permitted to configure, update, and maintain anti-virus and firewall systems.
- Control system architectures and Linux-based platforms are subject to specific authorization protocols due to their operational sensitivities.

Accountability

- All security events, including malware detections, unauthorized access attempts, and system isolations, are logged and monitored in real-time.
- IT personnel are accountable for ensuring that isolated systems are thoroughly verified as malware-free before reconnection to the network.
- Regular audits are conducted to verify compliance with anti-virus update schedules and the overall effectiveness of security controls.

PLATFORM CENTRIC EXCEPTIONS

Control System Architectures: Human Machine Interface (HMI) and Supervisory Control and Data Acquisition (SCADA) platforms may operate without standard anti-virus software, as recommended by vendors to prevent operational interference. These systems are maintained through periodic, controlled updates, with access strictly limited to authorized personnel.

Linux Operating Systems: Linux-based applications are exempt from standard anti-virus requirements due to the operating system's inherently secure architecture. However, access to these systems is restricted and monitored to ensure compliance with security policies.

To mitigate risks associated with platform exceptions, the IT Department implements enhanced firewall rules and robust management controls. All access to control systems and Linux platforms is authenticated and logged, ensuring accountability and maintaining compliance with cybersecurity best practices.

CYBERSECURITY AWARNESS TRAINING

It is a requirement for all Users to complete Obsidian Energy Cybersecurity awareness training. The training curriculum emphasizes the importance of vigilance, verifying sender identities, and exercising caution when interacting with suspicious emails or links. Further to the potential disciplinary actions noted above, corrective actions, including stricter access controls and/or temporary restrictions to sensitive systems, will be implemented for Users who repeatedly fall victim to phishing emails and/or fail to comply with the internal phishing escalation processes. Fostering a culture of accountability and continuous learning is essential to mitigate the impact of cybersecurity incidents while cultivating a more resilient workforce.

SOFTWARE STEWARDSHIP AND LICENSING

It is our policy to respect all computer software copyrights and to adhere to the terms of all software licenses. Unauthorized duplication or utilization of software may subject Users and/or Obsidian Energy to both civil and criminal penalties.

Users are not permitted to purchase or install software on Obsidian Energy equipment. Any software requiring a license for which Obsidian Energy does not currently hold a licensing agreement may not be installed on any Obsidian Energy equipment. All software purchase requests are the responsibility of the IT Department. Adhering to this requirement facilitates the accurate inventory of software license agreements, terms and provisions, and ensures software availability and license requirements for all Users.

Software will be registered in the name of Obsidian Energy with clearly defined management ownership and oversight. The IT Department will install all software and store the original media in a safe storage area.

QUESTIONS

If you have any questions or concerns about the application of this policy, please contact the IT Department Manager.