IT SECURITY AND INFORMATION MANAGEMENT POLICY

Approved by: Peter Scott, Senior Vice President and Chief Financial Officer
Date Effective: December 2019

INTRODUCTION AND APPLICATION

Obsidian Energy is committed to providing a secure yet open network that protects the integrity and confidentiality of electronic information from unauthorized intrusions, malicious 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 (“IT department”). All Users of Obsidian Energy information systems are responsible for the security and protection of electronic information resources in their control.

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.

The IT Department is responsible for assisting Users and Representatives in all aspects of information security including; protection and prevention against malware/viruses, security stewardship of enterprise-wide systems and network authentication and improving general security awareness around our technology and systems. The IT Department reserves the right to monitor email and internet activity in order to ensure compliance with this policy.

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 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 information technology services are the property of Obsidian Energy. All Company software, hardware, and IT assets are to be used for Obsidian Energy business purposes. All non-public corporate information is confidential. You must ensure an appropriate level of security when transmitting data. All official Obsidian Energy corporate work should be conducted through corporate email and/or procurement systems.

Personal use of IT assets is permitted if it is not excessive, costly or interfering with performance. Any personal use must comply with Obsidian Energy policies, guidelines and standards. Any personal data, information or communications stored, relayed or addressed on an Obsidian Energy device is the property of Obsidian Energy and users must not have any expectations of privacy.

Use of personally owned equipment to connect to corporate systems whether for remote access or to store and utilize corporate data including email, files, and other data types, may be permitted with prior authorization of the IT Department. Personal devices capable of wireless email, calendar and/or contact synchronization require the same security policies to be applied as those owned by Obsidian Energy and will be applied without notice.

All electronic data and communications created on any device issued by Obsidian Energy are deemed to be records that belong to Obsidian Energy. This includes messages and information on mobile devices, voicemail, and/or data saved in folders and directories whether or not it is personal in nature. You should not expect personal 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 (for the IT Department to collect all applicable data).

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 conduct official corporate business is prohibited as is forwarding Company information to personal email accounts.

SOFTWARE PURCHASES AND LICENSING

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

Users are not permitted to purchase or install software. 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.

For maximum flexibility, software will always be registered in the name of Obsidian Energy. The IT team will install all software and store the original media in a safe storage area.

USER RESPONSIBILITIES

Users will take all necessary precautions to protect the confidentiality of personal, customer and sensitive information encountered in the performance of their jobs. Users are responsible for:

- complying with Obsidian Energy’s password and remote access authentication process;
- maintaining the integrity of their logon account credentials, and not sharing individual email accounts between multiple individuals;
- complying with Obsidian Energy’s obligations under the licensing agreements of the software purchased by Obsidian Energy;
- logging off and locking down all desktops and laptops when unattended. All smartphone devices must also use password protection, to protect Company information in the event the device is lost or stolen;
- storing all Obsidian Energy related files, particularly those of a confidential nature or those which have a material value to the Company, on Obsidian Energy network drives;
- ensuring that any files transported or stored on USB drives are encrypted and/or password protected;
- maintaining the physical security of portable Obsidian Energy computer systems;
- not modifying, adding or altering the corporate network and or network components;
- immediately reporting the loss of laptops and smart phones to the Service Desk so steps can be initiated to limit further risk to Obsidian Energy systems or information; and
- immediately alert the Service Desk and/or IT Manager of any suspected Phishing attempts, or if you believe your system is infected with a virus or spyware.

CORPORATE SECURITY

All Obsidian Energy computers and servers must employ the Company’s standard, supported anti-virus/malware software installed and scheduled to run at regular intervals. Obsidian Energy maintains firewalls and software to maintain network traffic integrity. Suspected virus/malware-infected systems will be removed from the network until they are verified as virus/malware-free. Anti-virus systems will be updated monthly at minimum.