# IT SECURITY AND INFORMATION MANAGEMENT POLICY

**Approved by: David Hendry, Vice President, Finance**
**Date: Effective December 12, 2016**

## INTRODUCTION

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 Representatives to perform their work.

This policy applies to any "Representative" or individual provided access to Obsidian Energy data, hardware, software, or networks.

All Representatives of Obsidian Energy are responsible for the security and protection of electronic information resources in their control including data, computers, software, and networks.

The Obsidian Energy Information Technology ("**IT**") Department is responsible for assisting Representatives in all aspects of information security including protection and prevention against malware/viruses, input into the security of enterprise-wide systems, authentication and authorization, researching new security technologies, and raising general security awareness around our technology and systems.

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.

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)").

## SCOPE

This policy addresses the following topics:

1. Acceptable Use of Systems and Information
2. Email, Messaging and other Communications
3. Remote Access
4. Virus/Malware Protection
5. Information Protection
6. Breaches of this Policy

This policy should be read in conjunction with Obsidian Energy's other corporate policies including the Code of Business Conduct and Ethics and the Records and Information Management Policy.

## POLICY DETAILS

### 1. Acceptable Use of Systems and Information

**a. Access to systems and information** at Obsidian Energy must be authorized by your manager. You must not share your User ID and password with any other individual. You are responsible for the use of your account and will be held responsible for any issues arising from the misuse of your User ID and password. You must lock or turn off your workstation when you are not using it.

**b. Use of information systems** within Obsidian Energy is for the purpose of performing your job responsibilities. Internet and e-mail access is provided for business purposes only. Inappropriate use of internet or e-mail may result in breaches of security or confidentiality, legal risk and/or negative publicity to the Company. Limited personal use is acceptable subject to the terms of this policy.

**You must not:**

- Engage in any activities which compromise the availability, integrity, accuracy, authenticity, or confidentiality of Obsidian Energy data and/or systems. This includes:
    - Accessing or distributing restricted or confidential information which you have no job-related need to access;
    - Use of another Representatives' account;
    - Erasing, renaming or making unusable any software or essential data;

  - Deliberate attempts to breach the security of the IT infrastructure; or
  - Deliberate introduction of malware to the infrastructure (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
- Participate in chain letters or other forms of mass mailing or marketing.
- Connect your own personal devices including portable storage devices of any kind, (e.g. flash drives, USB keys, cameras, MP3 players, or other portable devices) within the Obsidian Energy network.
- Install software on any devices, including portable devices that connect to the Obsidian Energy network without approval and assistance from IT.
- Establish any service or presence using Obsidian Energy's IT infrastructure or name that has not been approved by management.
- Set up your Obsidian Energy e-mail account to automatically forward e-mail to an external e-mail address such as a personal Internet e-mail account.
- Intentionally access, view, download or redistribute sexual, pornographic, racist, or other offensive material, or any material prohibited by law.

**c. Use of Obsidian Energy equipment including portable devices**: All equipment provided by Obsidian Energy remains the property of Obsidian Energy. This includes desktop equipment and portable devices such as laptops, smart phones and tablets.

Only devices supplied by Obsidian Energy may be used in the Obsidian Energy IT environment. You must take extra precautions to protect the physical safety of portable devices by properly securing them at all times. Portable devices must be kept in a secured location such as a locked office or desk drawer when not in use. Only Obsidian Energy issued mobility devices will be connected to our mobility server environment. Personal mobility devices will only be provided access to email via our Outlook Web Access environment.

**d. Privacy**: 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 on Obsidian Energy systems.

Authorized personnel may access all information related to user accounts. Monitoring, collection, use and disclosure of personal information shall comply with Obsidian Energy's Privacy Policy and applicable laws.

Representatives should recognize that personal information on devices issued by and on the Obsidian Energy network may not be made available to or sent to the Representative upon their departure from Obsidian Energy.

**e. Security** is everyone's responsibility. All non-public corporate information is confidential. You must ensure an appropriate level of security when transmitting data.

Forwarding corporate information to personal email accounts is prohibited. Copying or retaining corporate information following termination of employment, service agreement or appointment with Obsidian Energy is also prohibited.

You are required to notify the Helpdesk if you suspect security breaches (i.e. unauthorized file access, viruses, loss or theft of any device, compromised passwords, etc.). You may also submit your concern confidentially using the Obsidian Energy EthicsPoint hotline (refer to section 6 for more information).

**f. Intellectual Property**: You must comply with Obsidian Energy's obligations under the licensing agreements of the software purchased by Obsidian Energy. You must not duplicate, or reproduce in any manner, software that is licensed for use at Obsidian Energy.

Information published on the Internet is not by default public domain. Copyright laws, whether expressed or implied, may apply to logos, trademarks, and other materials that may appear on the Internet. The use of third-party or Obsidian Energy intellectual property or logos is forbidden without the express consent or appropriate licensing from the owner.

## 2. Email, Messaging and other Communications

Business-related electronic messages must be sent through an electronic messaging method which is appropriate in the circumstances, considering such factors as the sensitivity or confidentiality of the message contents, the relative security levels of various electronic communication methods, and the need for a permanent, recoverable record of such communication. Formal communications (for example, requests for and granting of approvals, correspondence with counterparties or working interest partners, negotiations, and any post-incident inquiries or investigations) or communications including confidential or sensitive corporate information should sent by email; or where email is unavailable or impractical, must be otherwise preserved or confirmed.

## 3. Remote Access

Access will only be granted to Representatives and third parties that have a valid business need for remote access. Remote access requires management approval.

## 4. Virus /Malware Protection

All Obsidian Energy computers and servers must have 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 integrity. Any suspected virus-infected computers will be removed from the network until they are verified as virus-free.

## 5. Information Protection

Representatives are responsible for maintaining records generated in the ordinary course of business. See also Obsidian Energy's Records and Information Management Policy, which can be found on the Intranet.

All corporate information must be stored on a corporate drive rather than an individual workstation or laptop hard drive. The Obsidian Energy IT department will ensure that all Obsidian Energy data and applications stored on corporate drives are periodically backed up.

## 6. Breaches of 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 a manager within the Obsidian Energy Information Technology Department.

Violations can also be reported using EthicsPoint at:

1-877-309-9397 or at www.obsidianenergy.ethicspoint.com.

For more information, please see Obsidian Energy's Code of Business Conduct and Ethics, which is posted on the Intranet as well as at www.obsidianenergy.com.