

Oakville, Milton and District Real Estate Board

1.0 General

The Oakville, Milton and District Real Estate Board (“OMDREB” or “the Board”) has adopted this Information Security Policy to ensure that adequate protection measures are taken to assure the confidentiality and integrity of the information held by OMDREB and the security of the networks and computers used to store and access that information.

This Policy applies to Users with respect to their access to, and use of, OMDREB-held information as well as access to hardware, software or network facilities owned or controlled by OMDREB. With respect to employees, this Policy is also to be read in conjunction with and form a part of OMDREB’s *Employee Handbook*. All new employees and contractors shall receive a copy of this Policy upon employment or engagement.

In the event of questions about this Policy, please contact:

Executive Privacy Officer
Oakville, Milton and District Real
Estate Board
125 Navy Street
Oakville, Ontario L6J 2Z5

E-mail: mponder@omdreb.on.ca
Telephone number: 905-844-6491
Fax: 905-844-6699

2.0 Definitions

“Availability” means information being accessible as required.

“Confidential Information” means Personal Information; OMDREB business, tax or accounting information; employee information and disciplinary files, and archived information pertaining to former members or employees.

“Confidentiality” means the restriction of access to information only to those having a business reason to have such access as authorized by the appropriate manager within OMDREB or the client concerned.

“Disruption of network communication” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

“Integrity” means the information in question has not been modified in an unauthorized manner.

“Internet communications” means existing and future communication protocols and services including but not limited to the World Wide Web; electronic mail (“e-mail”); Instant Messaging; Internet Relay Chat; any intranet that OMDREB establishes or participates in; any proprietary data transfer protocols utilized by OMDREB in communications with others; File Transfer Protocol, TELNET and Usenet news groups.

“Members” mean a sales agent, broker or other type of member of OMDREB.

“Personal Information” means any information, recorded in any form, about an identified individual, or an individual whose identity may be inferred or determined from the information.

“Security breaches” means accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these activities are within the scope of regular duties.

“User” means (1) an individual, whether an employee, officer, director, a sales agent, broker or other type of member of OMDREB who creates or accesses information on OMDREB-owned or controlled Computer System; (2) a computer program or application operating pursuant to an individual or organization (e.g. electronic agent).

3.0 Information Security Requirements

3.1. Privacy & Confidentiality

Users with access to Personal Information shall respect the confidentiality of that information and adhere to the requirements of OMDREB’s *Privacy Policy* and OMDREB’s *Employee Privacy Policy*.

Users with access to other types of Confidential Information shall respect the confidentiality of that information and not disclose such information unless specifically authorized to do so.

Each User that accesses information held by OMDREB, whether owned by the OMDREB or not, regardless of form (e.g. paper or electronic) or format, shall protect that information against accidental or deliberate disclosure or destruction. Any modification of such information shall be only as authorized and required for business reasons.

Confidential Information shall be:

- Physically protected through the use of locked cabinets or offices and/or technologically protected using Computer System access controls;
- Accessible for review by employees as authorized by OMDREB management;
- Corrected or marked with appropriate notation in the event inaccuracies in the information are identified; and
- Retained for such retention periods as required by law or as identified by OMDREB management.

3.2. OMDREB Property

All information and/or messages composed, sent or received using OMDREB's computers are the property of OMDREB and may be reviewed, audited, accessed and disclosed for any purpose considered appropriate by OMDREB management. **USERS SHOULD NOT HAVE ANY EXPECTATION OF PRIVACY WITH RESPECT TO SUCH MESSAGES.** See also [Section 3.10 Monitoring](#) below.

Unless contractual or licensing arrangements govern, any data or software downloaded using Internet communications into OMDREB computers becomes the property of OMDREB and may be retained, removed or destroyed at the sole discretion of OMDREB management.

3.3. Identification & Authentication

Each User shall be assigned a unique identifier ("User ID") and will be required to authenticate themselves prior to gaining access to OMDREB computers or networks. Users shall not log on to OMDREB computers using another User's User ID. **EACH USER SHALL BE RESPONSIBLE FOR ALL ACTIVITY CONDUCTED UNDER THEIR ASSIGNED USER ID.**

Associated with each User ID will be a password generated to authenticate a User prior to accessing any application, system, network or remote connection. A User shall adhere to the requirements of [Annex A Password Standard](#). All default passwords and access codes on vendor-supplied hardware and software shall be changed prior to use by Users.

The System Administrator shall have a separate Administrator User ID and password. Administrator User IDs shall only be used for system administration purposes.

The Administrator's User ID and password shall be changed immediately upon (a) the installation of any system; and (b) immediately after use by service personnel. The administrator's password shall be documented and stored in a secure location.

Where non-specific User accounts are required, they shall be assigned to a specific User for accountability purposes. The purpose of the account shall be documented and the password associated with the account changed when a User who knows the password is no longer an employee or a contractor of OMDREB.

User IDs shall be deleted from an OMDREB computer upon the termination of a User's employment or, in the case of contractors, contract. User IDs that are inactive for thirty days shall be disabled and removed.

3.4. Use of OMDREB Computers

The OMDREB shall provide employees and managers, and may (but is not required to) provide other Users, with workstations for the purposes of their activities with the OMDREB. **USERS SHALL BE RESPONSIBLE AND ACCOUNTABLE FOR THEIR ACTIONS while using OMDREB hardware, software or networks, or components thereof, including desktop or laptop computers or personal digital assistants (PDAs) owned, leased or controlled by OMDREB including, but not limited to, the MLS® network.**

Users shall use OMDREB computers primarily for business purposes. Limited and reasonable personal use of the OMDREB computers permitted provided such use:

- a. Is not for non-OMDREB commercial purposes or personal gain;
- b. Does not:
 - i) Adversely affect the primary business use of the computer or OMDREB network;
 - ii) Conflict with a OMDREB business objective or policy;
 - iii) Consume a large amount of OMDREB computer resources;
- c. Complies with applicable law.

OMDREB management shall be solely responsible for any determination as to what constitutes limited and reasonable personal use.

Under no circumstances is a User authorized to engage in any activity that is illegal under the laws of Ontario and Canada while utilizing the OMDREB computers.

Users shall not harm or destroy, or attempt to harm or destroy, hardware, software or data on any OMDREB computer, other than their own data in the course of editing such material.

Users shall not load, install or activate, or attempt to load, install or activate onto OMDREB computers any unauthorized hardware, including, but not limited to, modems, data scopes, line monitors, nodes, gateways or bridges of any kind.

Users of OMDREB-owned or controlled portable devices (e.g laptops, PDAs), if supplied with such equipment, shall not leave such equipment unattended when outside OMDREB offices. Information contained on such devices must be protected from unauthorized access using power-on passwords or passphrases and password or passphrase-enabled time-out or lock-out features.

3.5. Access to OMDREB Information or Computers

User access to OMDREB information or to OMDREB computers shall be on an “as authorized” basis in order to accomplish OMDREB business objectives. Networks shall have routing controls to ensure connections and information flows do not have unauthorized access to OMDREB information. External users accessing the MLS® network (e.g. sales agents or brokers) shall be distinguishable from OMDREB employees during their use of OMDREB computer resources. Access by external users shall be provided only for the use of the MLS® network.

Any computer or portable device with a modem operating in “inbound mode active” (permitting external callers to connect to the device using that modem) shall not be simultaneously connected to both an OMDREB network and any external network.

3.6. Software

Only software approved for deployment by OMDREB management is permitted on any OMDREB computer or network. Downloading software programs (e.g. screen savers, audio software and messaging software) from the Internet is not permitted. All other file

types downloaded from the Internet must be scanned with anti-virus software before being stored on OMDREB computers. If a User has a business requirement to download software from the Internet or to otherwise load non-OMDREB standard software, [Section 4.0 Exceptions to Policy](#) will govern.

Virus detection software shall be installed and regularly updated on OMDREB computers and networks. Users are required to report any known or suspected virus incidents to the System Administrator.

Opening e-mail attachments with “.exe” or “.com” extensions (including trial versions of software) is not permitted.

Any application to be purchased, whether custom-developed or commercially available, shall have authentication and access controls. The application should ensure that, with respect to the information it stores, the application shall maintain the integrity of the data.

Users shall report any observed or suspected software malfunctions but shall not attempt to remove the software in question unless authorized to do so.

3.7. Internet Communications

OMDREB may provide all Users with Internet access for business and limited personal purposes. OMDREB may also provide e-mail addresses with “@omdreb.on.ca” to employees. Accordingly, the use of OMDREB resources that identify a user with OMDREB must be done in a manner that reflects well on the organization. All access to the Internet shall be done via approved OMDREB gateways and in a manner consistent with this Policy. Managers and employees must understand that Internet access is to be treated as a privilege that may be revoked at any time in the event of a failure to comply with this Policy. Withdrawal of access to the OMDREB network or the Internet may occur whether or not disciplinary action is taken.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use of OMDREB’s computers. In the absence of applicable OMDREB policies or if there is any uncertainty, Users should consult their General Manager.

The following system and network activities are expressly prohibited:

1. Installing or distributing "pirated" or other software products that are not appropriately licensed for use by OMDREB;
2. Copying and/or distributing material not authorized by OMDREB management including, but not limited to, music, text or photographs from magazines, books or other copyrighted sources;
3. Providing information about, or lists of, OMDREB employees to parties outside OMDREB;
4. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Using an OMDREB computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws under the laws of Ontario and Canada.
6. Making fraudulent offers of products, items, or services;

7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties;
8. Causing security breaches or disruptions of network communication;
9. Intercepting data not intended for the User's host computer, unless this activity is a part of the employee's normal job/duty;
10. Circumventing User authentication or security of any computer or network account;
11. Interfering with or denying service to any user other than the User's host (for example, denial of service attack);
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's use of a computer; and
13. Exporting or importing software, technical information, encryption software or technology, in violation of applicable Canadian import and export control laws.

The following communication activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material;
2. Harassing OMDREB employees or employees of members or third parties via email, telephone or paging, whether through language, frequency, or size of messages;
3. Forging email header information;
4. Soliciting email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type; and
6. Posting the same or similar non-business-related messages to large numbers of newsgroups or web sites.

Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

3.8. Physical Security

Computers located within OMDREB are to be located in areas that have appropriate physical security controls, including but not limited to, keys or combination locks, access logs and alarms. Users whose employment or contract is terminated shall return all keys assigned to them. A log of office keys shall be maintained by the General Manager who shall also have responsibility for the issuance and retrieval of keys.

Storage media shall be protected from environmental threats such as temperature, humidity and magnetism. All media containing Confidential Information shall be sanitized or destroyed before release for disposal to ensure that data recovery from such media is not possible.

Equipment shall be not removed from the OMDREB offices or facilities without permission.

3.9. System Risk Management

Any new computer system or modification to existing OMDREB computers or network shall be assessed for risk prior to deployment. Such a risk assessment shall examine any potential consequences of a loss of confidentiality, integrity or availability of OMDREB information or other assets, and the realistic likelihood of a loss occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented. This risk assessment may be completed by the System Administrator or such person(s) as the General Manager believes appropriate to conduct such an assessment.

3.10. Monitoring

The OMDREB reserves the right to monitor computers or networks to ensure compliance with this Policy. For security and network maintenance purposes, authorized individuals within OMDREB may monitor and access equipment, systems and network traffic at any time.

Such access may include:

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on OMDREB computers or property;
- Access to work areas (offices, cubicles, storage areas, etc.).

For OMDREB computers important to the activities of OMDREB, at a minimum, the following information shall be recorded either electronically or manually:

- Login and logout attempts;
- Unauthorized attempts to access system files;
- Attempts to create, remove, set passwords or change the system privileges of system administrators;
- System alerts or failures; and
- System configuration changes and maintenance information.

All logs, whether electronic or manual, must contain the date and time of the event and the User ID which caused the event and are to be reviewed, at a minimum, on a monthly basis.

Where a computer records information that is required to be logged and operates a clock, that computer's clock should be set, as required, to Standard Time or Daylight Savings Time in Ontario. Computer system clocks shall be checked every 60 days as to their accuracy.

Logs are to be protected against unauthorized changes or operational failures (e.g. logging media exhausted; failing to record events or overwriting itself).

Monitoring tools and systems audit processes are to be configured so as to only allow designated personnel to change such tools and processes.

Audit logs shall be archived monthly and retained according to OMDREB's *Records Retention and Destruction Policy*.

Security processes and controls are to be audited annually.

4.0 Exceptions to Policy

Exceptions to any policy requirement stated in Section 3 may be permitted if:

- An appropriate business reason is provided;
- The request is approved by the General Manager; and
- The User making the request accepts all responsibility for any additional risk created by the exception.

5.0 Non-compliance With Policy

While records of communications can be created for monitoring and review purposes, OMDREB will not actively monitor the communications of Users. However, the OMDREB may do so upon suspicion or evidence of a breach of any law or the OMDREB policy and any past communication may be examined in the course of an investigation of a security breach or in the course of disciplinary action. See Section [3.2](#).

Any User who disregards, disobeys, disables or circumvents any element of this Policy or any security mechanism, or who attempts to do so, shall be subject to disciplinary action, up to and including termination of employment or, in the case of contractors, termination of contracts. Users should also note that, if circumstances warrant, an incident may be referred to the appropriate authorities for prosecution.

OMDREB reserves the right to restrict any User's access to OMDREB information or computers.

Agreements with external vendors or suppliers shall require compliance with this Policy in the event of use of OMDREB computers or networks by such vendors or suppliers, or employees or agents, thereof.