COMPLIANCE

ACCEPTABLE USE OF TECHNOLOGY STANDARD INFORMATION SECURITY

This document is addressed to:
All Authorized Individual or Incorporated Brokers doing business under Optimal Financial Centre Inc.

APRIL 2016

425 NOTRE-DAME ST, DIEPPE NB E1A 9G4 | COMPLIANCE@OPTIMALCENTRE.CA | OPTIMALCENTRE.CA

TABLE OF CONTENTS SUMMARY

SUMMARY

Company Technology allows you to conduct your business or complete your work in a timely, efficient and productive way.

You can use Company Technology under the condition that you use it:

- for business purposes, and
- in accordance with the laws of your jurisdiction. Incidental personal use of Company Technology is allowed, subject to Management's discretion, provided that it in no way:
- interferes with the intended business uses of Company Technology,
- incurs unauthorized expenses,
- interferes with productivity, or
- breaches any applicable business practices or procedures, including this or any other applicable policy or standard.

It is your responsibility to ensure you remain in compliance with the Company's policies and standards. When in doubt, you must review specific activities with your manager/leader to ensure that you adhere to these standards. If you do not adhere to the Information Security Policy and its Supporting Standards (including this standard), you may be subject to disciplinary action, which may include the restriction or removal of access to Information Assets and networks, dismissal, termination of engagements or contracts, civil action and/or criminal prosecution.

DEFINITIONS

The Company means all companies, includes all insurance companies and investment companies and their respective subsidiaries, that Optimal Financial Centre Inc has a contract in place.
Information Assets means information everywhere it is stored or transmitted (i.e. paper and electronic files, physical equipment with electronic data memory and any other format) including employee, customer/client, Consultant/advisor and business partner, intellectual property, business processes, and proprietary information.
Accountability refers to the requirement that the responsibility for using all Information Assets can be assigned to and is assumed by authorized individuals.
Availability refers to the requirement that an Information Asset must be accessible, and usable upon demand by an authorized individual or entity.
Confidentiality refers to the requirement that all Information Assets not be made available or disclosed to unauthorized individuals or entities.
Integrity refers to the requirement that an Information Asset's accuracy and completeness must be safeguarded.
Supporting Standards are published pursuant to the Information Security Policy and provide specific instructions on the manner of compliance with the Policy
Cloud service is a form of outsourcing in which hardware and software are provided as a service by a vendor and accessed over the Internet.

SCOPE

Company Technology includes all computer systems, hardware and software, and all networks, which are
• owned by the Company,
• administered or operated by the Company, or
• not owned or operated by the Company (e.g. a laptop that you personally own) but only to the extent that they are used to process, store or transmit the Company's Information Assets (as defined in the Information Security Policy), including but not limited to the following types of technology:

- computers (e.g. desktops, laptops, tablets, servers, virtual servers and Smartphones),
- networks (wired & wireless) or any network enabled devices,
- telephones (e.g. stationary and cellular phones, pagers and voice mail systems),
- Company supplied or mandated software,
- portable media (e.g. USB / thumb drives, SD Cards, CDs, DVDs, tapes, any legacy storage devices),
- printers, scanners, fax machines and photocopiers,
- modems,
- closed circuit television (CCTV),
- email and Internet services and activities,
- Cloud Services,
- video conferencing, and
- any other third-party services supplied to, arranged by, or paid for by the Company.

See the Information Security Policy for definitions of Information Assets and other key terms.

AUDIENCE

This Standard applies to the following persons:
- all employees of the Company (regardless of employment status),
- consultants, advisors , brokers, dealers, and other independent contractor members of the Company's distribution channels and sales forces, and their respective employees,
- third parties who are contracted to provide services to the Company, and
- all persons who are authorized to access the Company's Information Assets.

You is used in this Standard to refer to any of the foregoing persons.

STANDARDS

1. Company Technology is monitored.
The Company monitors, examines, and retains information processed, stored, or transmitted on Company Technology, including personal files, emails, and Internet activity, while acting within the laws of each jurisdiction. The Company does so at its discretion without advance notice.

2. Company Technology is provided for business purposes.
Company Technology must not be used for soliciting or conducting outside business activities, including advertising any service or product not offered, supported or sponsored by the Company.

However, incidental personal use of Company Technology is allowed, subject to Management's discretion, provided that it in no way:
- interferes with the intended business uses of Company Technology,
- incurs unauthorized expenses, • interferes with productivity, or
- breaches any applicable business practices or procedures, including this or any other applicable policy or standard.

Company Technology must not be used for inappropriate purposes. Inappropriate use of technology includes but is not limited to:
- fraudulent or illegal purposes,
- gambling or betting,
- day trading not associated with your role within the Company,

- sharing Company resources with unauthorized third-parties (e.g. allowing family, friends or unauthorized employees to view/use Company systems, Internet access and email),
- destroying, altering, dismantling, disfiguring or disabling Company Information and systems without authorization,
- impersonating someone,
- attempting to circumvent security controls on Company Information and systems without authorization,
- faking, altering or "spoofing" messages, attachments or email,
- sending commercial electronic messages in contravention of anti-spam and/or do-not-call legislation,
- spying on/invading the privacy of any person who is using, or whose personal information is accessible using, Company Technology,
- distributing any political or religious messages,
- transmitting, downloading, storing, forwarding, sending, copying, circulating, creating, viewing , accessing, clicking-on, or browsing any materials or communications of any sites or links that are profane, hostile (i.e. bullying) or violent, obscene, pornographic or sexually explicit, and
- visiting or participating in or on any social media sites and/or forwarding, downloading or using any non-business multimedia for any of the above-noted inappropriate purposes or any other activity that may tend to bring the Company into disrepute or may affect its reputation adversely (as determined by the Company in its sole discretion).

3. Respect intellectual property rights

The Company respects intellectual property law and will not tolerate any copyright violations of its own intellectual property rights or those of a third party, including but not limited to: • downloading, storing, transporting or copying illegal and/or unlicensed data, music or video files, • photocopying or printing multiple copies of magazine and/or newspaper articles, books, or any other printed or online material without prior consent from the publisher, • using the Company's or another company's logos in Company marketing materials without permission, • making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others, and • revealing, sharing or copying the Company's intellectual property without explicit written permission, or outside the bounds of your documented responsibilities.

4. Use approved software and comply with all licensing requirements.

All software (e.g. applications, browsers, utilities, toolbars) installed on Company Technology must be properly reviewed and approved in advance. The Company reserves the right to remove any unapproved software.

5. Protect against viruses and other malicious code.

You are responsible to help safeguard Company Technology from viruses, spyware and other types of malicious code by: • not disabling, changing or interfering with protection software like antivirus software, • not opening suspicious email attachments, • not downloading unapproved software, • not creating or knowingly installing or distributing a virus or other malicious software on any computer system, • reporting suspected infections by viruses or other malicious code to the Service Desk/Help Desk.

6. Avoid activities that may degrade the performance of Company Technology.

You are expected to ensure that your activities do not unnecessarily consume network resources, interfere with productivity, or pre-empt any business activity. This can include but is not limited to viewing online animation, streamed videos or personal photos — basically any non-business related large files that consume large amounts of network capacity or bandwidth.

7. Do not connect unapproved devices to the network or to any workstations on the network.

Before connecting any device (any type of smartphone, USB drive, printer, etc.) to Company Technology, it must be approved by Information Services. Under no circumstances may a wireless access point be installed on any Company network without authorization.

8. Protect laptops and other mobile devices against theft and loss

Take steps at all times to protect the physical security of laptop computers, including against theft and loss, by using an anti-theft physical security device (e.g. locking cable) during the day and otherwise locking it away in a secure place when not using it.

9. Protect your password(s).

- ✓ **Never share your password with anyone**. This includes co-workers and especially anyone who calls and asks for your password. **No one from the Company will ever call and ask for your password.** •
- ✓ **Never leave a password written down in an easily accessible location.** If you must write down a password, protect it as you would personal, confidential and valuable documents.
- ✓ **Reset temporary passwords immediately**. If the Service Desk/Help Desk issues you a temporary password during a registration, reset it immediately to maintain its privacy.
- ✓ **Pick strong passwords**. Whenever possible, use strong passwords. Refer to the Strong Password Guideline for more information on how to choose strong passwords and keep them private.

10. Defend against attempts to manipulate you into revealing passwords or confidential information.

Attackers often use a technique known as Social Engineering to manipulate people into revealing information via the phone, email or websites. They may ask you for the names and numbers of in-house experts, software or system details or your identity and user ID/password. The attacker then uses this information to impersonate you or someone else authorized to receive confidential and sensitive Information Assets.

Do not provide any information about the Company, Company Technology, or processes to:

- anyone who has not adequately identified themselves (especially on the phone), or
- anyone who does not have an explicit business reason to know (acquaintances, friends, relatives, colleagues, etc.).

Be aware of Phishing attacks where an attacker will attempt to get you to click on links or open any attachments from emails. These can compromise the network and if you suspect an email as being suspicious, contact the Service Desk/Help Desk.

11. Use password-protected screensavers to prevent unauthorized access to unattended computers.

To help ensure no one accesses your computer without your knowledge or consent, always invoke your authorized, password-protected screensaver before leaving your computer (Ctrl-Alt-Delete / Lock Computer).

12. Protect the accountability of your user ID.

You should not allow anyone, including your manager/leader, to log on to any Company Technology using your user ID. You may be held responsible for all actions taken under your user ID (whether authorized by you or not) and those actions may be logged. Acceptable Use of Technology Standard Page 9 of 12 Information Security Office © April 2016 Standards (cont'd)

13. Follow all applicable Policies and Standards when providing third parties access to Company Technology or Information Assets.

The Company has minimum Supporting Standards to ensure secure access to Company technology in order to protect our Information Assets whenever external parties are provided access to them. If you are responsible for engaging third parties, including contractors, vendors, and business partners, who may require access to Company Technology or Information Assets, you must comply with the provisions of the Standards.

PROTECT INFORMATION IN YOUR CARE

Almost everyone in the Company can be considered to be an Information User and every Information User has a responsibility to safeguard the Information Assets they use or have in their possession.

For external service providers, consultants, advisors, brokers, dealers, and other independent contractors, a signed non-disclosure agreement at the start of their engagement is required.

1. Classification Levels

There are three information security Classification Levels for Information Assets with increasing requirements of Confidentiality, Integrity and Availability that Information Users should be aware of:

- Unrestricted,
- Confidential, and
- Restricted.

The Classification Level dictates the minimum level of protection that must be provided to that Information Asset.

a. Confidential

All Information Assets are deemed to be Confidential unless marked or otherwise formally communicated by the Information Owner as Unrestricted or Restricted.

b. Restricted

Restricted Information Assets are Confidential Information Assets that require a higher level of protection due to an increased requirement for Confidentiality, Integrity or Availability. Access to these Information Assets is restricted to a limited audience based on its need to know.

c. Unrestricted

Unrestricted Information Assets include those that may be disclosed to the general public with prior authorisation. They have Integrity and/or Availability requirements but the Confidentiality requirements have been removed.

2. Roles and Responsibilities

Information Users

- use Information Assets only in accordance with the Information Owner's approval and for the intended business purpose,
- have a responsibility to be aware of the Classification Level of the Information Assets they use,
- will only be granted access to Restricted and Confidential Information Assets if they:
  - have a "need to know" based on their role, and
  - have approved access from their leader/manager and/or the Information Owner or designate.
- protect:
  - all Information Assets they have been granted access to, and
  - all Information Assets in their possession or control, at all times according to their Classification Level, using approved methods to store, transport and prevent unauthorized disclosure of Information Assets. See the Information Classification and Handling Standard for further details,
- protect preliminary drafts, handwritten notes and any other form of temporary media during use,
- copy or distribute Information Assets only on a business need basis using appropriately secure communication channels. They ensure that all associated waste products (e.g., poor copies, extra copies) are destroyed in an appropriate manner and in accordance with record retention schedules,
- never engage in any practice that would increase the possibility of inappropriate disclosure of Information Assets, and

- inform their leader/manager if they have access to Information Assets that are not required to perform their role.

Information Owners

Information Owners are the heads of a business or Company unit who are accountable for the appropriate security of Information Assets in their units. They classify Information Assets and may delegate ownership responsibilities and/or give permission to use Information Assets (originals or copies) to other individuals or groups within the Company. They also grant permission to act on or with the Information Assets (e.g. view, copy, or modify).
Information Owners are subject to the provisions defined in the Information Classification and Handling Standard.

2.1 Handle Information Assets appropriately

Information Assets must be handled based on their Classification Levels, their medium (e.g., hardcopy or printed media, electronic format, verbal) and their stage in the information lifecycle (e.g., creation, storage, retirement). Such measures should be more stringent for Confidential and Restricted Information Assets.

See the Information Classification and Handling Standard for minimum handling requirements.

2.2 Only use the Company Technology and Information Assets you are authorized to use.

Never access Information Assets or Company Technology you are not expressly authorized to use or require to do your job or conduct your business.

If you discover you have been given access you don't require to do your job or conduct your business, you must immediately inform your manager/leader to have your access adjusted.

2.3 Use of personal devices.

Approved personal devices (e.g. smartphones, tablets) may be used to access Company Information Assets provided you are authorized to use them, that corporately managed security software (e.g. Good Technology or AirWatch) is installed on the device and that access to the Company Information Assets is only through the managed security software.

Unless authorized, devices which are not managed corporately cannot be connected to the network or used to download / store Company Information Assets. You must explicitly agree to mobile device terms of use before accessing internal resources of the Company.

2.4 Report suspicious activity related to the security of Information Assets, whether they are deliberate or accidental

Immediately upon discovery of an actual or suspected Information Security Event, you must report it to your AGA and MGA:

- ✓ Examples of Security Events include:
- ✓ Unauthorized access, use, alternation or destruction of electronic information.
- ✓ Password sharing or unauthorized use of another user's account
- ✓ All violations of the Information Security Policy, Acceptable Use of Technology Standard or the Information Security Standards
- ✓ Unauthorized access or use of computers or applications
- ✓ Unauthorized copying, altering or deleting of data
- ✓ The use of Company computers to commit illegal acts.
- ✓ Unsolicited SPAM email which appear to be originating within the Company environment.
- ✓ Unusual or unexpected behaviour on your desktop or laptop
- ✓ Unexplained Password lockouts
- ✓ Any phone calls or emails requesting passwords or other sensitive data.
- ✓ Suspicious or unexplained changes to Company web sites or other resources
- ✓ Viewing or having access to resources that are beyond your expected rights and privileges

- ✓ Unauthorized wireless access points.
- ✓ The loss of any of Technology or Intellectual Property, including misdirected emails outside of the Company.

2.5 Do not disclose any information about suspected or potential security incidents to anyone outside of the Company.

Unless specifically authorized by the Company, no one may disclose any information regarding an incident to the media or any third party outside of the Company. For more information, consult your applicable code of conduct.

If you have any questions about this Standard and how to enact it, please contact: Director of Sales @ Optimal Financial Centre Inc.