COMPLIANCE

SECURITY GUIDELINE I OFFSITE WORKSPACE

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

JANUARY 2018

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

INTRODUCTION

Purpose

The purpose of this guideline is to help ensure reasonable security practices are in place in locations or workspaces outside of Optimal Financial Centre Inc. corporate-managed facilities. For policy purposes, we will refer to the term Optimal to identify the Optimal Financial Center Inc.

Your obligation to be fully compliant with regulatory and legislative requirements extends to all external sites of Optimal and services from which you may work. Simply put, risk should be minimized as much as possible in setting up such a workplace environment.

This guideline outlines the minimum required security measures you should implement for workplaces.

GENERAL GUIDELINES

1. Follow all applicable business practices and procedures

You must comply with all applicable policies, standards, business practices and procedures, including – but not limited to:

- The Acceptable Use of Technology Standard
- The Information Classification Standard Documents, and
- Optimal's Code of Conduct for advisors
- Client data protection-securing personally-owned hardware and media

2. Secure a location for the work space

Secure the location and equipment to be used for the workspace by following these guidelines:

- Handle all paper files securely, including keeping them locked away when not in use.
- If documents need to be destroyed at the offsite location, use cross-cu
- Consider confidentiality agreements for third-party service providers, such as technology support, cleaning services, etc.

3. Communicate securely

Ensure all communication channels between your location and other offices are secured:

- Use only approved means to connect computers to your network, including recommended routers, as required.
- When wireless connectivity, take appropriate steps to secure your computer from exposure to malicious use.
- Ensure clients understand email is not a secure means of transmitting personal information, unless appropriate measures are taken (i.e., using passwords).
- Consider using separate telephone and voicemail services to maintain confidentiality and privacy, and use appropriate professional scripts.
- Ensure all security features on fax machines are enabled and the unit is in a secure place.
- Only use a recognized, reputable, courier service with pre-set liability, tracking and service levels. Ensure all packages you send and receive are signed for and are not left at a door.
- Ensure you take appropriate measures to secure personal/confidential client information when transferring it from one location to another, it.

For example:

• Take only what information you need; document the information/files you've taken in the event there's a loss or theft; secure paper files or electronic devices storing information out of sight (in the trunk of vehicles); and use discrete bags to transport laptops.
• Fully shut down your laptop when not in use or when it's being transported to ensure hard drive encryption is activated.

4. Regularly-schedule backups.

Create and implement backup processes and procedures. These may include basic operational recovery needs and/or business continuity planning requirements.

- Apply the following according to your requirements for backup measures:
- Frequency (daily, weekly, etc.)
- Rotation (back to the corporate office, other offsite, etc.)
- Media (CDs, USB drives, backup tapes)
- Storage (home safe, locking cabinet, etc. and ideally fire-proof)
- Logging (keeping a record of backups)
- Testing (ensuring a backup is usable), and
- Destruction of backups in accordance with applicable retention schedules

5. Use of equipment and information

Use equipment in compliance with the Acceptable Use of Technology and Information Classification & Handling Standards. This includes but is not limited to the following items:

- Do not disable or alter security features on any equipment that's provided or configured for your use.
- Confidential information must always be stored securely, preferably on a server's network drive.
- Limit the amount of information stored on Personal Digital Assistants (PDAs), cell phones, and external storage devices to only what is necessary.
- Do not allow family, friends or anyone that does not have permission to use or access the equipment or client information under your care
- Ensure a password-protected screensaver is activated whenever you leave the computer unattended.

When purchasing or leasing a copier or other multi-function print devices, consider the following capabilities:

- Consider a vendor offering products with advanced data protection features.
- The unit's internal memory should be cleared when the unit is powered off.
- If the unit has a hard drive, it should be encrypted and securely erased.
- Disable the scanning or faxing to disk and network print functions if not required
- Consider having the hard drive of the device removed and destroyed prior to it being returned to the vendor at the end of the lease.

6. Immediately report any suspected or actual breach of security

Report any security incidents immediately.

Some examples of security breaches include:

- A theft of computer equipment including PDAs and smart phones containing client data

Security incidents and breaches must be reported to Optimal's Corporate Compliance Officer immediately in cases where client information could be exposed.

Please contact; Chief Compliance Officer – Optimal Financial Centre Inc.