COMPLIANCE

SECURITY GUIDELINE I MOBILE DEVICE

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

JANUARY 2017

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

OVERVIEW - PURPOSE

This Guideline has been developed by the Information Security Office to assist in understanding how to secure *personally managed* mobile devices used for professional business. Its purpose is to ensure that the use of such mobile devices does not result in the loss, theft or compromise of Company information, or adversely affect Company infrastructure. The company represent Optimal Financial Centre Inc. and it's division including insurance and investment company that we have contracted business relationship.

This Guideline describes the most common security features of mobile devices. Not all possible features are covered. Nor are all features described available on all mobile devices.

SCOPE

This Guideline is intended to apply to *personally managed* mobile devices (i.e., mobile devices normally purchased by the employee) where approved for Company business.

This Guideline specifically addresses the use of *personally managed* mobile devices including cell phones, smart phones and tablets. It is not meant to deal with laptops, although some features may also be available on laptops and if they are, the Guideline should apply.

AUDIENCE

This Guideline applies to the following persons:

- all broker 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 Guideline to refer to any of the foregoing persons who are using personally managed mobile devices for business purposes. Corporate information is not only valuable to the Company, but also to other unauthorized individuals.

INTRODUCTION

Stolen corporate information could allow someone to open bank accounts, get credit cards or passports, share or sell product or governance information and commit other criminal activities.

What information might be stored on a mobile device?

- Contact details for everyone in your address book.
- Call history (outbound and inbound).
- Text messages or chat sessions.
- Location history based on GPS or cell tower history.
- Web browsing history and cached web pages.
- Photos, videos, audio recordings and email messages.
- Stored passwords, documents, Company records or other sensitive files.

This Guideline is intended to help you use mobile devices securely. It does not, however, provide in-depth information on how to enable various features.

SECURE CONFIGURATION RECOMMENDATIONS

The following security features are available on most mobile devices and should be enabled for proper mobile device protection:

Password Management

- **Password Strength**: Most mobile devices will support either a simple 4 digit PIN code or the use of longer passwords. Ideally, a strong password (including upper and lowercase letters, numbers and symbols) should be used instead of a weaker 4 digit PIN. The password should expire or be changed regularly. Likewise, some mobile devices support drawing a pattern to unlock the mobile device. Again, the longer and more complex the pattern, the better.

- **Auto Lock**: The mobile device should be configured to auto lock after a few minutes of inactivity. Your password should be required to unlock it.

- **Password Wipe**: The mobile device should be set such that if the password is entered incorrectly too many times, the mobile device erases all user data to protect against brute force guessing.

- **Tethering/Hotspot Password**: If your mobile device allows you to connect other Wi-Fi enabled mobile devices to it to share Internet services (called tethering or hotspots), ensure you have a strong password (including upper and lowercase letters, numbers and symbols) on the connection. Others could use your connection or steal your data if the password is easy to determine. Also be mindful of any data usage restrictions or expectations.

Encryption

- **Hardware Encryption**: Most mobile devices support built-in hardware encryption. All user data is automatically protected. Encryption protects the data should someone try to access storage areas directly.

- **Removable Media Card Encryption**: If your mobile device supports removable media cards, then you should enable encryption on those as well to protect any sensitive data you may store there.

- **Backup Encryption**: To ensure the protection of any backup files you create, enable encryption of your backups. Again, you must set a strong password on your backup files. **Malware Protection**

- **Mobile Security Services**: Comprehensive security is as important and necessary for your mobile device as for your PC or laptop. If your personal mobile device supports it, install an antivirus solution as well as a firewall.

SECURE USE RECOMMENDATIONS

In addition to the configuration recommendations above, there are also safe user behaviors you should follow that align with the corporate *Acceptable Use of Technology Standard*:

App (Software) Installation

- **Use only official App stores**: Shop at reputable App stores (e.g., iTunes, Google Play, Blackberry). Official Apps undergo a minimum level of quality control by the manufacturer of your mobile device. While this isn't perfect, it does reduce the chances of malicious applications ending up on your mobile device.

- **Scrutinize Apps before you install them:** Check other users' reviews and ratings to see if an application is safe. Check to see how much of your data the App accesses, if it will share your information with third parties and if there is a privacy policy. Check the permissions that the App requires. Does it really need to track your every move? If you are at all suspicious or uncomfortable, don't download the App.

- **Apply App and operating system updates**: Periodically, updates will be available for your Apps and for the operating system on your mobile device. These updates are meant to patch vulnerabilities and bugs and should be applied in a timely manner. Failure to patch can leave your mobile device open to malware and hackers. Always allow updates to proceed.

- **Do not hack your mobile device:** Do not "jailbreak" or "root" your mobile device. These terms refer to the act of hacking your mobile device so that it can go beyond the intended walls it was

designed to stay behind. Those walls offer protection you won't otherwise get. If you jailbreak your mobile device you open it up to malware and hackers.

Data Management

- **Only store what you need**: Be conscious of what you are storing on your mobile device. Do you really need it? The less you store, the better. Also, keep track of what's stored on your mobile device so that you will have a record if the mobile device is lost or stolen.

- **Perform regular back-ups**: Most mobile devices have the ability to back up your data and applications. Just like your computer, it's good to do this with your mobile device on a regular basis in case you lose access to your data for any reason.

- **Practice safe surfing and email**: Spam and phishing occur on mobile devices just like a PC or laptop. Don't click on links or attachments in unsolicited emails or text messages. Avoid disclosing any confidential information through texts, emails, or web browsers on your mobile device. Remember to use your Internet best practices. Delete unsolicited or suspicious messages as soon as you receive them. Think before you click!

Networking

- **Be cautious of public Wi-Fi hotspots**: Someone may be eavesdropping on public Wi-Fi hotspots. Avoid banking, shopping online, or accessing corporate resources from such connections. It's best to save sensitive transactions for when you're on a network that you trust. Also be wary of using your mobile device outside your home country. Eavesdropping and traffic analysis maybe more prevalent on a foreign network.

- **Ensure wireless encryption**: If you use a Wi-Fi or Bluetooth connection, ensure it is done over a secure connection. For example, the connection should be protected with at least WPA2 encryption for Wi-Fi.

- **Disable wireless capabilities (when not in use)**: Turn off Wi-Fi and Bluetooth when not in use. Open, unattended wireless connections are easy targets for criminals. When these are enabled, set them to prompt for connection instead of automatically connecting to anything available.

Physical Protection

- **Label your mobile device**: Attach a label or ID to your mobile device in case it is lost or stolen. That way it can be returned should someone find it or the police recover it. Also, keep your mobile device's brand, model, serial number, IMEI number and SIM card details stored in a safe place.

- **Never leave your mobile device unattended**: Mobile devices are easily stolen in an instant when you are not looking.

- **Dispose of your mobile device securely**: Your mobile device stores far more sensitive information then you may realize. You need to ensure that information is removed from the mobile device before you get rid of it. Backup any information you want to save and then wipe the mobile device. Simply deleting information is not secure. Also, don't forget the SIM card and or any removable media cards. Either remove them or wipe them too.

General Use

- **Log out**: Just like on a PC or laptop, log out of any websites or programs when you are finished using them. And remember, don't "save" your information so that you can automatically log in the next time—if your mobile device is lost or stolen, someone may be able to access your accounts or files.

- **Be wary of QR Codes**: Quick Response (QR) codes are those funny little square pictures that look like a fuzzy TV screen that you see in ads and on posters. These codes are designed to be scanned by a mobile device's camera and automatically send your browser to a website for more information. However, you have no way of knowing where a QR code may take you ahead of time. Someone may have generated a QR code to take you to malicious website. If in doubt, do not scan!

- **Take care during repairs**: If the mobile device should need to be serviced, you need to ensure the data is protected. You should remove any data and any removable media from the mobile device before releasing it for repairs. If that's not possible, then ensure all password protection mechanisms are enabled. Never give anyone your passwords. If you are receiving a replacement, then ensure all data is wiped from the original mobile device. And ensure when you return any loaner mobile devices that the data is wiped from them too.

- **Report lost or stolen mobile devices immediately**: If you think you have lost your mobile device or it has been stolen, contact your service provider to report the incident. Also, contact the Service Desk and the Chief Compliance Officer to receive any further directions.

CONCLUSION

Mobile devices are convenient and easy to transport. However, they can store huge amounts of corporate data that could be lost or exposed if not properly protected. It is important for you to understand the protections available, which ones are mobile device settings and which ones are best practice behaviors to keep your mobile device secure.