DENTONS

IT Policy

Mobile Device, Portable Computing, and Remote Access Policy

Contents

1 Purpose

The purpose of this policy is to define the rules for connecting to the Firm's network from external devices (including smart phones and laptops) or networks. These standards are designed to minimize the potential exposure to the Firm from damages which may result from unauthorized remote access or use of the Firm resources from a remote location. Damages include the loss of sensitive client or Firm confidential data, intellectual property, damage to public image; damage to critical Firm internal systems, etc.

2 Summary

The damage caused by unsecure remote access and the improper use or loss of unsecured mobile devices with Firm data can be serious, for both the Firm and the person responsible for the loss or improper use. It can result in damage to our clients, who expect the Firm to maintain the confidentiality of its information. Improper use can also result in a regulatory breach, which could lead to fines or civil claims against the Firm or individual.

3 Scope

This policy applies to Systems Users with Firm-owned or personally-owned Mobile Devices or workstations used to access Firm data. This policy applies to remote access connections used to do work on behalf of the Firm, included but not limited to reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to Virtual Private Network (VPN) and Secure (Secure Shell - SSH).

4 Policy

4.1 Mobile Device Requirements

All mobile devices, whether Firm-owned or personally owned, that connect to the Firm Systems must comply with the following:

- Devices must store any user-saved passwords in an encrypted password store.
- Devices must be configured with a secure password that complies with the Firm’s *User Password Policy & Authentication Standard*.
- Only devices owned by the Firm and managed by IT are allowed to be connected directly to the Firm production network. Personal or visitor devices may only connect via the Firms' public and visitor networks.
- Mobile devices holding information about, or belonging to, the Firm or its clients must be approved by the IT department. Hand-held Mobile Devices must be managed through the Firm’s MDM (mobile device management) system.
- Requests for a mobile device will be reviewed on a per-case basis, considering business needs, risk and suitable alternatives. If the request is denied, the reason for refusal will be communicated to the requestor.
- Firm Hand-held Mobile Devices must be procured using approved procedures available either on the Mobility page of the Local Portal or via local office procedures.

- The IT department will configure all approved Hand-held Mobile Devices for access with the Firm’s MDM policy. This enables the Firm to enforce policies, including the ability to remote wipe/factory data reset the device.
- Mobile Devices will have encryption enforced.
- Users are strictly prohibited from disabling, modifying or tampering with the Firm’s configuration.
- Mobile devices are subject to inspection and monitoring by the IT department on behalf of Firm management in accordance with the *Acceptable Use Policy*
- Secure data containers/compartments on Hand-held Mobile Devices containing data used for Firm business will be wiped by the IT department when no longer used to process Firm data (e.g., approved to be taken by a departing user). In certain situations, the whole device will need to be wiped/factory data reset (e.g. when lost, disposed of, exchanged, swapped, upgraded, traded in, donated, sold).

4.2 Mobile Device User Requirements

The mobile device user must comply with the following:

- Users must report all lost or stolen devices to Firm IT immediately.
- If a user suspects that unauthorized access to Firm data has taken place via a Mobile Device, the user must report it to the IT Department immediately, in alignment with the Firm’s *Incident Management Policy*.
- Devices must not be “jailbroken” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load illegal software or content onto their devices.
- Applications must only be installed from official/approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact the Firm's IT Department.
- Users should use reasonable judgment when connecting mobile devices to external sources for the purpose of charging or transferring data. For charging purposes, power outlets should be used, rather than USB ports when possible, to reduce the risk of unintended data transport/interception.
- Users must be cautious about co-mingling personal and work email accounts on their devices. They must take particular care to ensure that Firm data is only sent through the Firm email system.
- Users must not use Firm computers to back up or synchronize device content, such as media files, unless such content is required for legitimate business purposes.
- Systems Users may be responsible for reimbursing costs incurred as a result of personal use.
- Prior to receiving a Firm-owned Mobile Device, the employee must sign the Acknowledgement and Receipt of firm Property form or follow the office’s equipment procurement procedures.
- Lost, damaged, stolen or missing Firm mobile devices should be immediately reported to the IT Department. Systems Users may be responsible for damage and replacement costs for Firm equipment.
- Systems Users are prohibited from using mobile devices (other than when utilizing a hands-free function) while driving when the Hand-held Mobile Device is being used for the purpose of conducting Firm business or while in transit for Firm purposes.

4.3 Laptops/Netbooks Data Storage

- Use of full disk encryption products is standard on Firm-issued laptops. Personally-owned laptops may only be connected to the Firm's internal network through the Virtual Desktop Environment.
- Storage of personal data on Firm-issued devices should be limited to ensure adequate space, connectivity and usability of equipment for business purposes.
- Firm data must not be stored on personal (non-Firm) computers.

4.4 Removable Media Storage

- The Firm restricts the transfer of data between Firm systems and Removable Media in most instances.
- Requests for approval or guidance should be directed to the IT Department. Those granted approval should follow the exception criteria in our *Removable Media Policy*.

4.5 Remote Access Requirements

- Firm-approved multi-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by Systems Users.
- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the *User Password Policy & Authentication Standard*.
- At no time should any the Firm employee provide their login or device password to anyone, including family members or co-workers.
- Systems Users with remote access privileges must ensure that their Firm-owned workstation, which is remotely connected to the Firm's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Non-standard hardware configurations must be approved by exception and Information Security must approve security configurations for access to Firm's systems.
- All devices, including Mobile Devices and personally-owed desktops that are connected to Firm internal networks via remote access technologies must use the most up-to-date anti-virus/anti-malware software. Third-party connections must comply with requirements as stated in the *Third-Party Risk Management Policy*.

5 Definitions

Mobile Device - a portable computing device such as a laptop, tablet or smart phone.

Hand-held Mobile Device - a Mobile Device with a form factor small enough to be used while holding in your hand (i.e. smart phone)

Systems Users - individuals who utilize Firm computer networks, hardware, applications, tools, and systems (collectively, “Systems”) to facilitate communications, store information, and support the business of the Firm.

Jail Broken (or rooted) - a Mobile Device that has had the manufacturer limitations removed by unapproved measures. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

Removable Media - storage device which can be connected to, inserted in and/or removed from a computer. Examples include CDs, DVDs, Blu-Ray discs, as well as diskettes, USB flash drives, external hard drives, and various types of memory cards (SD, Memory Stick, Compact Flash, etc.).

6 Violations and Enforcement

Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Non-compliance with or breach of this policy will be reported to the violator's immediate manager and/or appropriate Firm management.

7 Exceptions

Exceptions to this policy must be requested via email to the IT Security Team and/or the Office of the General Counsel or equivalent Risk Management Leadership. Requests must include:

- Clear business justification for the exception
- Duration of exception request
- Any appropriate details regarding compensating controls or information that reduces the risk of the exception.

Exceptions, approved or denied, will be logged in our IT ticket tracking system for follow up and/or control purposes as appropriate.

Document control

Ownership and responsibility

Document Owner	IS Security Team
Author	Fishnet / Andrey Zelenskiy
Contact for amendments	IS Security Team

Amendment History

Date Issued	Issued by	Reason for Change
23-Sept-2016	Michele Gossmeyer	Expand section 4.3 to include 3rd bullet to strengthen 4.5
12-Dec-2017	IT Security Team	Language updates and minor edits to clarify technical components. Also update of exception language to standardize with new format.
6-May-2019	IT Security Team	Updated to better clarify mobile device definitions and better align remote access and mobile device usage.
24-Aug-2020	IT Security Team	Updated with minor language clarifications.

Distribution List

This document has been issued to the following people for information (I) and / or review (R):

Name	Position	I / R
Eddie Reich	US General Counsel	R

Related Documentation

Reference	Doc Reference
Acceptable Use Policy	83519612
Removable Media Policy	100399960
User Password Policy & Authentication Standard	83670388
Third-Party Risk Management Policy	83670553
Incident Management Policy	83422383

Approval

Name	Role	Date	Comments
Michele Gossmeyer	Director, Information Governance & Compliance	26-Jan-2016	
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	12-Dec-2017	

Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	6-May-2019	With OGC collaboration
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	24-Aug-2020	