DENTONS

## IT Policy

# Acceptable Use Policy

**Table of Contents**

# 1 Purpose

The Firm utilizes various computer networks, hardware, applications, tools, and systems (collectively, “Systems”) to facilitate communications, store information, and support the business of the Firm. This policy reflects the Firm’s commitment to have a formally documented procedure for the appropriate use of the Firm Systems and data developed, created, stored, transmitted and otherwise managed in support of the Firm’s organizational objectives.

# 2 Summary

The Firm Systems and data are valuable assets that must be protected. If you have access to Firm Systems or information, you are responsible for their security. If you discover that the security of Firm Systems or information has been compromised, you must immediately contact your manager and the IT Security Team. By using Firm Systems, you accept and understand the terms of this policy and all announced modifications to this policy. This policy does not give you contractual rights to Firm Systems or computer information. The Firm reserves the right to modify or terminate this policy at any time for any reason.

# 3 Scope

This policy applies to all System’s Users and all equipment that is owned or leased by the Firm.

# 4 Policy

## 4.1 General Use and Ownership

- Systems’ Users must be aware that the data they create or access using the Firm Systems or assets remains the property of the Firm.
- Information must be stored on the Firm's Document Management System (DMS) or authorized network storage locations to safeguard the confidentiality, integrity and availability of such information.
- The Firm prohibits the use of unapproved third-party cloud services (e.g., DropBox, Google Docs) to store Firm or client documents. The Firm provides secure cloud-sharing options to collaborate with external parties such as clients, co-counsel, etc. The Service Desk can provide options for access to these resources.

## 4.2 Privacy Expectations and Monitoring

- Privacy Monitoring
    - The Firm has authorized specific individuals or groups, including contracted third-parties, to actively monitor equipment, devices, systems, network traffic and message and file content. The Firm reserves the right to review and/or audit all information and technology assets at any time without notice and on a periodic basis to ensure compliance with this and other Firm policies.
- Privacy of Stored Personal Information and Personal Electronic Communications
    - Systems’ Users shall have no expectation of privacy in data they store, send or receive on Firm Systems. Systems’ Users should exercise caution when storing and processing personal and sensitive information not directly related to Firm business. The Firm reserves the right to actively monitor, restrict, use and

dispose of data, email messages, other electronic communications and/or personal files stored on Firm Systems.

- Electronic Monitoring Areas
    - Individuals may be subject to electronic monitoring while on the Firm premises and in secure areas in accordance with the requirements of the *Physical and Environmental Controls Policy*. This monitoring is used to measure policy compliance as well as to protect the Firm, its clients, and others.
    - In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no visual or audio monitoring will be performed.
- Oversight of Monitoring
    - The Firm reserves the right to monitor all use of the computer network and Systems.
    - To ensure compliance with Firm policies, monitoring may include the interception and review of any emails or other messages sent or received and inspection of data stored on personal file directories, hard disks and removable media. Investigations of alleged policy violations will be conducted in accordance with the requirements of the *Incident Management Policy* and applicable statutes.
- Excessive System Usage
    - Actions detrimental to the computer network or other corporate resources or that negatively affect job performance are not permitted. Systems' Users must refrain from acts that waste Firm technology resources or limit others from using them.
    - Excessive use of the Firm network bandwidth, including streaming media, is not permitted. Business-related large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance should be performed during non-business hours as much as possible or with the assistance of IT Support.

### 4.3 Mobile Device Usage

- General
    - Firm-owned mobile devices may be issued to Systems' Users as needed to conduct Firm business.
    - Mobile devices, whether Firm-owned or personally-owned, that connect to the Firm environment must comply with strong password, encryption, connection and Mobile Device Management (MDM) requirements outlined in the *Mobile Device, Computing and Remote Access Policy*.
    - Devices holding Firm data are subject to Firm inspection and monitoring.

- Privacy and Security
    - Systems Users must exercise caution when using mobile devices to avoid inadvertent disclosures of sensitive or protected information (e.g. Client or Personally Identifiable Information).
    - ~~o~~ Mobile device recording capabilities such as voice, image or video should be used with extreme caution to protect sensitive information. Recording sensitive or protected information using mobile device voice, image or video capabilities is prohibited.

### 4.4 Copier, Printer, Facsimiles Usage

- General
    - Physically damaging or vandalizing copiers, printers and fax machines owned, operated, leased or contracted by the Firm is strictly prohibited.

    - Copier access codes must be used ONLY by the assigned user and must be kept secure at all times.
    - Employees are responsible for the safeguarding of material originating from their copier code.
- Unacceptable Use
    - Unacceptable use of copiers, printers and fax machines owned, operated, leased or contracted by the Firm includes, but is not limited to:
        - Offensive content of any kind, including pornographic, profane, defamatory, obscene, adult-oriented, harassing, inappropriate or "X-rated" material
        - Discriminatory information based on race, gender, national origin, age, marital status, sexual orientation, religion or disability
        - Unauthorized duplication of proprietary or confidential information regarding Firm business
        - Messages of a religious, political or racial nature
        - Gambling or sports-related betting pools/squares/chain letters
        - Material protected under copyright laws, patents and trademarks
        - Business or individually identifiable health information, social security numbers, passwords, access codes or any other confidential information or sensitive data for non-business purposes
        - Information that asserts or implies that personal views or opinions are the views or opinions of the Firm

### 4.5 Software Usage

- The Firm Information Technology (IT) department is designated as the manager of all software and is charged with the responsibility for enforcing this procedure.
- Users of Firm software can expect IT personnel to troubleshoot and assist with standard software issues.
- The Firm IT department is responsible for ensuring the software is appropriate to the user assigned after the transfer or re-assignment of workstations.
- Purchasing of software shall be centralized within the Firm IT department to ensure conformity to applicable software standards.
- Software purchased and provided by the Firm for use by Systems' Users must be used for Firm business or education-related purposes only.
- Users of Firm software will abide by the terms of applicable licenses, notices, contracts and agreements as it pertains to the use of software on Firm Systems.
- Software acquired for or developed by Systems' Users on behalf of the Firm for associated business-related purposes shall be deemed Firm property.
- Unauthorized software should not be installed, loaded or used on Firm Systems.
- Software should not be reproduced or duplicated, except as provided by the license agreement between the Firm and the software manufacturer.
- Any use of copyrighted materials in violation of copyright laws or software manufacturer licensing agreements is prohibited.

### 4.6 Workstation Usage

- Firm workstations shall be used primarily for business-related purposes. It is recognized that, for convenience, Systems' Users may wish to utilize Firm Systems for limited personal use. This is acceptable provided that such usage is not excessive and conforms to all Firm policies.

- No Firm or client data should be stored on unencrypted workstations. The Firm's Information Security team must approve encryption methods to be used.
- Data created or otherwise used in support of Firm business must be placed on systems that are appropriately protected and controlled.
- Systems' Users will not use Firm Systems to engage in any activity that is illegal under local, state, federal or international laws or that violates other Firm policies.
- Systems' Users with the appropriate authority and business need may obtain copy, modify, remove or erase data from Firm Systems.
- Systems' Users will not remove, disconnect, corrupt, circumvent, deny or otherwise interfere with any physical components, safeguards, authorized user services, user identification and/or authentication schemes on Firm Systems.
- Deliberate introduction of malicious software onto workstations/laptops (e.g., viruses, worms, Trojan horses) is strictly prohibited.
- Deliberately causing security breaches, including, but not limited to, accessing data or logging into an account that the Systems' User is not authorized to access, is strictly prohibited.
- Performing any form of network monitoring that will intercept electronic data is strictly prohibited unless a part of the Systems' User's defined job function.
- Firm approved antivirus software will be installed and configured by the IT Department on workstations to prevent transmission of malicious software. This will include:
    - enabled real-time scanning features
    - centrally managed, regularly updated antivirus software/definitions/signatures
    - weekly scans with the results of the scan recorded in a log that will contain at least the last 3 months of antivirus scans.
- Deliberately circumventing any security or authentication systems is expressly prohibited.
- By default, Systems' Users will use non-privileged accounts to access workstations or laptops.
- By default, all Firm-issued workstations require an active firewall to be running when connected to an untrusted network.
- Systems' Users must never leave their laptop unattended in an unsecured area.
- In the event of a stolen laptop, contact the Service Desk immediately.
- Upon return of a shared resource (such as a loaner laptop), the system must be wiped and reinstalled.
- Workstations/laptops removed from Firm premises will be protected with security controls equivalent to those for on-site workstations.
- Firm laptops will be carried as carry-on (hand) baggage when using public transport. They must be concealed and/or locked when in private transport (e.g. locked in the trunk of an automobile, safe at a hotel, etc.)

### 4.7 Email Usage

- Email messages contribute to our professional image. Therefore, Systems' Users should be aware of the following best-practices:
    - When sending emails on a client matter, it is very easy for others to forward your messages.
    - Copyright and defamation laws also apply to emails.
    - Email "threads" contain conversation history which may not be suitable for forwarding internally and/or externally.
    - When sending personal emails, that email will still be associated with the Firm when coming from your Firm email address. You must therefore avoid any content which could cause embarrassment for the Firm if it became public.
- Client email communication

    - Clients and other correspondents are usually accepting of email-based communications, but there may be occasions or types of information for which it is not appropriate. Consequently, you should agree on an approach for each matter.
- Use the Firm email system
    - Always use the Firm email system for business emails, even when you are working outside the office.
    - Do not forward your business email to another external address, as this can compromise its confidentiality.
- Personal use of Firm email system
    - Personal use of the Firm's email system is permitted if:
        - it is occasional and reasonable
        - the content will not cause embarrassment to the Firm
        - it does not interfere with the performance of your duties
    - As indicated above, personal use of email can still affect the Firm's reputation and cause significant damage. In such an event, actions in breach of the Firm's policies will be taken extremely seriously and considered as misconduct, which may result in disciplinary action, including termination.
    - Keep storage of personal emails to a minimum.
- Use of browser-based email programs
    - For security reasons, the use of browser-based email programs, such as Hotmail and Yahoo, is not permitted unless specifically authorized by the Information Security Team and/or Firm Leadership.
- Proper storage of Firm email as client records
    - All business-related emails should be systematically filed in the Firm’s Document Management system.
- Double-check addressees before sending an email
    - Remember that email is an instant form of communication and messages cannot be recovered once they are sent.
- Think twice before sending confidential information or documents by email
    - Email containing sensitive or protected information must be sent using a secure method. If a client asks for details, or if you are exchanging sensitive or protected messages, please contact the Service Desk for more information.
- Outgoing attachments
    - Always check that you have attached the correct document or version of a document. Ensure that any amendments you want to make to the document are saved in the Document Management System.
    - In order to enhance system performance, the maximum size of both inbound and outbound messages (including file attachment) has generally been set to 100 Mb. If you have any questions that relate to email size, please contact the Service Desk.
- Treat any incoming attachments carefully
    - All inbound messages are systematically scanned for viruses and SPAM by the Firm's selected provider. However, the handling of incoming email still requires vigilance and you should contact the Service Desk if you have any concerns in this regard.
- Check that time-critical emails have been received
    - As a rule, email is a very reliable and fast form of communication. However, delays can happen and if a message is time-critical, you should use an alternate method (e.g. telephone) to confirm receipt. Internally, you can ask for electronic confirmation that an email has been received and/or read. However, when sending emails to external recipients, you cannot rely on this electronic confirmation.
- Use of other Systems’ User email accounts

- Access to employees mailbox content must be requested through the Service Desk and approved by the mailbox owner and either Office of General Counsel, equivalent risk management leader or Human Resources. You should review who has been granted delegated access rights at regular intervals to ensure they are still relevant. Password sharing is not an appropriate method for sharing access to a mailbox.

### 4.8 Instant Messaging Usage

- It is possible to transfer files using IM. A size limit may be applied to ensure Systems' Users do not negatively impact Firm Systems.
- Discussing specific client/matter information with colleagues outside any information barriers / Ethical Wall is prohibited.
- Discussions about specific matters must be added to matter records to allow for appropriate time-keeping and complete client files.
- All communications via IM may be actively monitored and or recorded; abuse of IM will be referred to the HR department for appropriate handling.

## 5 Definitions

Policy – The guiding principle used to set direction in an organization that outlines security roles and responsibilities, defines the scope of information to be protected and provides a high level description of the controls that must be in place to protect information.

Firm Systems - Computer networks, hardware, software/applications and tools used to facilitate communications, store or transmit information and support the business of the Firm.

Systems' Users - Firm's partners, employees, contractors, consultants, vendors, agents and those affiliated with third-parties who access the Firm's Systems.

Limited Personal Use - occasional personal use of Firm Systems such as correspondence, scheduling appointments, accessing news media sites, on-line purchasing, social media access, and other similar activities

## 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 supervisor and/or appropriate Firm management.

## 7 Exceptions

Exceptions to this policy must be requested via email to the IT Security Team and the Office of the General Counsel or equivalent regional 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 / Scott Saundry |
| **Contact for amendments** | IS Security Team |

### Amendment History

| Date Issued | Issued by | Reason for Change |
|---|---|---|
| 22-Feb-2018 | IT Security Team | Annual policy review with various updates to make references to Systems users consistent and align language with current technology terms. |
| 26-Oct-2019 | IT Security Team | Annual policy review with minor language updates for consistency and/or clarity. |

### 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 |
| Karl Hopkins | CSI | I |
| Jason Najacht | North American CIO | I |
| | | |

### Related Documentation

| Reference | Docs Reference |
|---|---|
| Incident Management Policy | 83422670 |
| Mobility portal page (for US region) | http://portal.us.dentons.com/administration/is/mobility/Wiki/Home.aspx |
| Policy & Procedure Manual | US region: http://portal.us.dentons.com/administration/ppm |
| Mobile Device, Computing and Remote Access Policy | 83670438 |

### Approval

| Name | Role | Date | Comments |
|---|---|---|---|
| Michele Gossmeyer | Director, Information Governance & Compliance | 14-March-2016 | |
| Michele Gossmeyer & Eddie Reich | Global Director, Information Governance, Risk & Compliance & US General Counsel | 18-Sept-2018 | |
| Michele Gossmeyer | Global Director, Information Governance, Risk & Compliance | 14-Oct-2019 | |