DENTONS

IT Policy

Information Security Policy

Contents

Table of Contents

1 Purpose

The purpose of information security is to ensure and enforce confidentiality, integrity and availability of Firm systems and information. The Firm must protect information assets from unauthorized disclosure, modification or destruction. The Firm's electronic information systems encompass a wide variety of equipment, resources, files and databases in the Firm’s facilities.

2 Summary

These systems require adequate levels of protection to ensure their availability and the integrity of the information that is stored, processed, or transmitted via system use. The policies and responsibilities contained in this document were developed to ensure that these information resources are adequately protected and safeguarded. It is the responsibility of all Systems users to read and comply with this document. Active support and compliance with these policies is essential and is a requirement for employment by the Firm.

3 Scope

This policy covers Firm systems and related activities within the Firm. This includes but is not limited to communications, networks, systems, and the data stored and processed on systems owned and managed by the Firm. Individuals covered under the policy include all Systems users such as employees, partners, officers, directors, associates, consultants, contractors, temporary staff and third-party processors of Firm data.

4 Policy

4.1 Roles and Responsibilities

4.1.1 Structure

The Firm’s Information Security function includes a combination of Firm leadership and Information Technology professionals. This team supports the Information Security process and provides resources dedicated to information security.

4.1.2 Employees and Third-Party Partners

All Systems users, are responsible for adhering to the Firm’s Information Security standards and policies. Systems users must ensure they comply with, at a minimum, the tasks below:

- Understand and comply with the provisions of this policy. Confirm compliance with all policies and procedures using applicable signoff procedures (e.g., hard copy signature page, electronic confirmation program, etc.).
- Maintain the privacy and confidentiality of Firm and client data.
- Be accountable and responsible for all activities associated with individual user IDs.
- Do not allow use of individual user IDs by personnel other than the assigned user.
- Use computer systems for authorized business purposes only.
- Do not set up or use unauthorized network devices, such as wireless access points (WAP).

- Immediately report any suspected incidents involving information assets or policy violations to Information Security or Human Resources.
- Do not test or attempt to compromise or circumvent access controls.
- Do not use code-breaking software or hardware that allows illegal copying of proprietary software, discovery of passwords or decoding encrypted data unless specifically authorized by Information Security in consultation with Office of General Counsel as appropriate.
- Adhere to endpoint threat protection control procedures.
- Do not use client production data, personally identifiable information (PII) or Firm confidential data in any external publication, including on-line help, system documentation, procedures documentation, training guides or any other type of electronic or printed format.
- Confidential and/or PII that is stored in or viewable and/or printable from Firm systems must not be left accessible to non-authorized personnel. Authorized personnel who have a requirement to print this type of information will not leave it in any area that is accessible to unauthorized resources.
- Do not transmit or remove sensitive information from Firm systems unless appropriate encryption methods are used and this activity is explicitly approved. See *Encryption Policy* for further details.
- Unauthorized equipment must not be physically or wirelessly connected to the Firm internal (protected) network.
- Response Teams
    - Incident response, disaster recovery and business recovery plans are regularly tested to verify the capability of critical computer systems to continue processing in the event of an emergency or disaster. Please refer to the *Incident Management Policy* and *Incident Management Standards* for details on incident response plans and responsibilities.

Please refer to the *Acceptable Use Policy* for further details on these responsibilities.

4.1.3 Management

- Ensure that Systems users understand their responsibility have received and understand this Information Security Policy.
- Promote security awareness.
- Promptly report all significant changes in employee duties, data access needs, or employment status to Human Resources.
- Ensure that Firm Systems are returned when Systems user ends employment or has their job responsibilities changed in a fashion that no longer require the property.
- Evaluate Information Security risks and, where appropriate, take necessary action.
- Note variances from this policy and promptly initiate corrective action.
- Authorize and approve access to Firm Systems for Systems users under their responsibility based on position requirements and responsibilities.
- Ensure the segregation of duties with regard to administrative tasks and responsibilities.

4.1.4 Information Owners

- Approve access requests based on position requirements and responsibilities.

- Apply appropriate controls for data based on Firm policy.

4.1.5 Information Technology Department

- Establish, configure, and maintain Information Security controls for the Firm Systems under their responsibility.
- Coordinate the assignment or termination of user IDs and access privileges for Firm Systems.
- Monitor access control logs and report any access-related problems or incidents to Information Security.
- Ensure that emergency response plans and disaster recovery plans are organized, maintained, tested and coordinated with the business recovery plan.
- Establish, maintain, implement and enforce this policy.
- Monitor the effectiveness of Information Security controls.
- Contribute to annual review of this Information Security policy and propose improvements where appropriate.
- Evaluate new technology and systems to ensure proper implementation of security controls.
- Investigate and report system-related security incidents and contribute to the documentation of those incidents and their resolution.
- Establish control override procedures to include audit controls.

4.1.6 Human Resources

- Notify the Information Technology Department of all new hires, terminations, promotions, demotions, transfers, reassignments, short or long-term absences or other significant changes in employee status that might require a change in information access privileges.

4.2 Information Security Practices and Procedures

4.2.1 Administrative Security Controls

- Security Violations and/or Problems
  - Employees violating the Information Security Policy are subject to the disciplinary action described in the regional Policy & Procedure Manual or applicable HR policies. Consultants and contractors violating the Information Security Policy may be in breach of their contractual agreement and subject to the actions specified in that contract and/or applicable legal action.
- Security Standards for Systems under Development
  - For new systems or significant new functionality under development, formal security and architectural reviews will be included as part of the standard software development lifecycle and facilitated by the Project Leader and conducted in the early stages of the project.
  - Vulnerability scans will be run as appropriate against major revisions or new system implementations, and formal signoff obtained from Information Security prior to implementation into a Production environment.

4.2.2 Access by Authorized Third Parties

- Access by authorized third parties to Firm information resources and Firm Systems should be restricted to only least privilege use. Examples of third parties that may require access include vendors, contractors, external auditors and regulatory agencies. Contracts and agreements with these groups will address the issue of information and system access controls. Access needs will be restrictively granted, closely monitored and terminated once no longer needed. Please refer to the *Access Control Policy* for more detailed information.
- Contracts and Agreements
  - All non-employees needing access to Firm information or Firm Systems must contractually agree to protect the Firm's Information resources and abide by the provisions outlined in this Information Security Policy.
- Access to Systems and Resources
  - Access needs by authorized third-parties to Firm information or Systems must be communicated to the Information Technology Department via the HRIS system or agreed upon on-boarding process.
- Completion of Work or Contract Termination
  - HR must be notified at the completion of work by a third-party or upon cancellation of the contract. The request for deletion of access rights is communicated to the Information Technology Department via the HRIS System or agreed departure procedures.
  - Information Technology Department terminates access rights at the time determined and communicated by HRIS.
- Review of Access Requirements
  - The person who requests access to Firm information and Firm Systems is also responsible for monitoring the access activities of third-parties for compliance with established policy.
  - Non-compliance issues must be immediately communicated to the Information Security Team. Please refer to the *Access Control Policy* for more detailed information.

4.2.3 Information Safeguards

- The Firm employs numerous safeguards to protect client and Firm information. Those safeguards are outlined within this policy and are supported by numerous documented procedures.
- Security Controls & Objectives
  - Security control objectives, as well as the specific controls required, are evaluated and established based on information sensitivity and classification. Procedures for identifying, implementing and monitoring those controls have been created and documented. They encompass all platforms and operating systems within the Firm enterprise and provide standards for various information sensitivity levels and a framework for:
    - Identifying the level(s) of protection required
    - Specific controls required based on the level of protection required
    - Identifying potential threats to determine their relative importance and the timeframe in which they must be addressed
    - Identifying appropriate responses in order to ensure information is secure and risk is mitigated.
- Security Awareness
  - The Firm has implemented security education and training programs for all employees and contractors. All members of the Firm and long-term contractors are required to complete Security Awareness Training with a retention assessment given at the conclusion of each training session on an annual basis.

4.2.4 Risk Management

(a) Responsibility for Risk Management

The Firm's Board is ultimately responsible for managing risk but delegates responsibility for the identification, assessment, reporting and management of Information Security Risks to the Information Security Team. Effective risk management is, however, also the responsibility of every Partner, director and employee in the Firm.

(b) Risk Register

The structure of the Risk Register is taken from the ISO standard for risk management, risk registers that are publicly available and general best practice. These were then adapted to suit the needs of the Firm and its current approach and thinking on risk. It is not a fixed document and may change as current thinking on risk management or the Firm's risk needs change.

Recording a risk on the Risk Register does not necessarily mean that a risk has actually manifested itself. An important function of the register is to anticipate risks that may occur and consider the Firm's exposure to those risks if it did nothing to manage or avoid them. The probability rating for each risk is therefore an assessment of the Firm's exposure to an actual or potential risk occurring in the absence of risk controls and responses. If a risk is given a high probability rating it therefore does not mean the risk has or is happening. Once mitigated or avoided, that risk exposure is likely to be significantly reduced. Many of these risks will be inherent to the business and unavoidable.

The Information Security Team and Office of General Counsel reviews all of the risks recorded on the Risk Register at least once annually, including the effectiveness of mitigation strategies. People responsible for specific risks report any updates and give their assessment of mitigation strategies to the Information Security Team to assist it in its review. The team reports its findings and the updated Risk Register to the Board for approval. This annual review date is recorded on the tracking page of the Risk Register.

(c) Risk Assessment and Analysis

The Information Security Team has developed a Risk Assessment Process and uses a Risk Register to help to meet the Firm's Risk Management Objective and to fulfil its purpose and discharge its responsibilities. In time, the Information Security Team intends this risk management process to evolve to include the identification of opportunities as well as threats.

Understanding exactly how the Firm records and analyses risk is crucial to the use and utility of the Risk Register. Interpreting the identification of a risk on the register as an admission of guilt, will inhibit the Firm fully and frankly identifying and recording risks. If risks are not identified and systematically dealt with, the Firm may find themselves exposed. That said, the Risk Register deals with sensitive information and its circulation and access needs to therefore be limited to Firm management, Information Security and the Office of General Counsel

Once identified, risks are then entered onto the Risk Register, which records:

- the asset and criticality;

- the threat type and threat actor;
- the vulnerabilities in play;
- the likelihood of a risk occurring and the potential impact of that risk;
- who is responsible for the risk, both in terms of mitigating and reporting; and
- where mitigation measures are needed, what policies, process or procedures are in place to adequately address the risk.
- whether a risk should be accepted, avoided, transferred or modified (e.g. measures taken to reduce the risk);

(d) Risks Treatment

The actions assigned to a risk are taken from the International Standard on risk management and include modify, accept, avoid or transfer. These terms summarise the Firm's general approach to a risk. They are explained below:

- Accept – This means the Firm accepts the risk without doing anything. A risk can be accepted because it is low or because resources are currently allocated to higher risk issues.

- Remediation – This means the Firm tries to put in place measures, systems or controls to minimise its exposure to risk or the impact of the risk if it happens. This is how the Firm responds to most of the risks it has identified.

- Avoid – This means the Firm acts or refrains from acting so that the risk no longer applies to it. An example may be refraining from providing a particular service because of the risks it poses.

- Transfer – This means the Firm transfers the impact of all or part of the risk to a third party. An example of this is the use of professional indemnity insurance to displace exposure to negligence claims.
  The risk action (accept, remediate, avoid, or transfer) and treatment must be approved by an appropriate level of management based on the risk score. The following table establishes the necessary management level for approving risk actions.

Risk Level	Management Level Required for Acceptance
Insignificant or Minor	Director of Information Security
Moderate	Office of General Counsel
Major	Chief Operating Officer or Chief Executive Officer
Critical	Board

4.2.5 Periodic Independent Reviews

- Risk assessments of security policies, procedures and standards are conducted on a periodic basis both internally and by approved third-parties engaged by the Firm as appropriate. Inputs into the assessments should include, at a minimum, the following information:
  - The status of current preventive and corrective actions if applicable
  - Changes that could impact the organization's approach to managing Information Security, including changes to the organizational structure, business circumstances, resource availability, contractual, regulatory and legal conditions or changes to the technical environment
  - Trends related to threats and vulnerabilities, as well as reported security incidents.
- The results from those assessments must be documented by the reviewer and discussed/evaluated with Firm management. Remediation and mitigation steps should be taken as appropriate based on the specific findings.
- Summaries of external penetration tests may be provided to a third-party (e.g. client) upon request.

5 Definitions

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

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

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 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.

Appendix 1 - Document control

Ownership and responsibility

Document Owner	Information Security Team
Service Owner	
Author	Fishnet & Andrey Zelenskiy
Contact for amendments	Information Security Team

Amendment History

Date Issued	Issued by	Reason for Change
2/1/17	Michele Gossmeyer	Updated to include reference info for Acceptable Use Policy & TOC details for section 4
2/27/17	Information Security Team	Updated for annual security team review & expanded exception section per Feb 2017 OGC review for all policies.
6/28/18	Michele Gossmeyer	Updated to adjust signature options for policy signoff based on South Africa question/feedback
9/14/18	Information Security Team	Updated for annual security team review with wording adjustments for consistency and to align with other policy modifications.
3/20/2019	David Beck	Updated for annual security team review with minor wording changes. Added section regarding Risk Management.
4/16/19	Michele Gossmeyer	Updated “Employee Handbook’ reference to Regional Policy & Procedure Manual or applicable HR policies
8/21/20	Information Security Team	Annual review and minor updates for language clarification / grammar accuracy.

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	Global Chief Security Officer	R

Related Documentation

Reference	Docs Reference
Acceptable Use Policy	83519612
Incident Management Policy	83422670
Incident Management Standard	83519528
Access Control Policy	83422548
Encryption Policy	106406599
Information Risk Management Process	109917103

Approval

Name	Role	Date	Comments
Michele Gossmeyer	Director, Information Governance & Compliance	29-Dec-2015	
Michele Gossmeyer	Director, Information Governance & Compliance	27-Feb-2017	

Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	28-June-2018	
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	7-March-2019	
David Beck	North America Information Security Director	20-March-2019	
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	16-April-2019	
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	21-Aug-2020	