Information Security Management Systems
Information Security Policy 2018

INTERNATIONAL FINANCIAL DATA SERVICES

Owner:	Chief Security Officer
Custodian:	Director, Information Security
Date of Review:	November 2017

Foreword

Information and Information Systems are critical to the efficient operation of IFDS' business and so IFDS must strategically and tactically direct operations for creating, processing, transmitting, and storing information ensuring its protection at all times.

IFDS also recognizes that information resides in electronic and paper formats which require protection. Information security is not just something we do; it is an organizational culture and one that is deeply in embedded in IFDS' business.

Therefore IFDS' senior management, to protect the confidentiality, integrity and availability of our information, has approved an Information Security Management System (ISMS) built on the ISO 27001:2013 standard.

Senior Management is committed to the IFDS ISO/IEC 27001:2013 information security model and approves this document and policies within the ISMS.

The Risk Management Committee and I as Chief Security Officer further endorse this Information Security Policy.

Dennis Gregoris
Chief Security Officer

November 7, 2017

Contents

1. Scope

Any Polices, Standards or Procedures in this document are explicitly set for International Financial Data Services (Canada) Limited and not globally under International Financial Data Services Ltd unless otherwise stated.

All policies, standards, procedures and controls apply to employees employed by International Financial Data Services (Canada) Limited including part-time, full-time, temporary staff, and third party resources based at 30 Adelaide Street East and, where appropriate, govern the use of all information assets including, but not limited to, buildings, computer processing facilities, computers, computer media, telephony (including mobile devices and fax) and paperwork. The Information Security Policies, which define a basic level of information security to meet the Business need and is consistent with industry best practices. Information Security Policies are located in SharePoint/ROCK under Information Security.

Offshore development and transfer agency operations and other third parties shall be deemed out of scope and governed by local polices and specific agreements.

2. Introduction

Information can exist in many forms, printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films and slideshows, or spoken in conversation. IFDS also relies heavily on computer systems to store, process and manage business and client information. Whatever forms the information takes, or means by which it is shared or stored, it must always be appropriately protected. Information in any form is a valuable IFDS company asset and shall be treated as such.

Senior Management's objective at IFDS is to protect against security problems that may have any adverse effects on the organization's operations or professional standing. Security problems include information being inappropriately obtained, accessed or disclosed, altered or erroneously validated whether deliberate or accidental or being unavailable when required. Management will ensure attendance of employee mandatory information security training and on-going information security awareness training.

ISO/IEC 27001:2013 is the standard adopted for setting out the ISMS. It identifies, manages and minimizes the range of threats to which information can be subjected. The standard is designed to ensure the implementation of adequate and proportionate security controls that protect IFDS' assets and give confidence to interested parties including regulators and customers.

Some aspects of information security are governed by law; the more notable Acts are as follows:

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) – not in ISO27001 scope
- National Instrument 81-102 Mutual Funds - not in ISO27001 scope

IFDS has established a framework of controls, policies and standards, as laid out in the Information Security Management System, to protect the Confidentiality, Integrity and Availability of all such held information. IFDS approves, issues, and maintains in a consistent format, official policies in a central policy library. Individuals engaged in developing and maintaining IFDS policies follow the requirements necessary to have changes to security policies approved by the Security Committee. All policies are reviewed on an annual basis.

This ISMS contains 114 controls in 14 groups: Information Security Policies, Organization of Information Security, Human Resources Security, Asset Management, Access Control, Cryptography, Physical and Environment Security, Operations Security, Communications Security, System Acquisition, Development and

Maintenance, Supplier Relationships, Information Security Incident Management, Information Security Aspects of Business Continuity Management, and Compliance. Each ISMS domain contains control objectives stating what is to be achieved and one or more controls that can be applied to achieve those objectives.

Responsibilities of Security Roles at IFDS

Chief Security Officer (CSO) - accountable for the development and oversight of policies and programs intended for the mitigation and/or reduction of compliance, operational, strategic, financial and reputational security risk strategies relating to the protection of people.

Information Security Director has direct responsibility for maintaining the policy and providing advice and guidance on its implementation.

Information Security Committee reviews ISMS and the ISMS policy on a regular basis which includes assessing opportunities for improvement and the need for changes to ISMS (including information security policies and security objectives). Reviews are documented and records maintained.

When reviewing ISMS, the Committee's responsibilities include:

- Assessing results of ISMS audits and reviews;
- Receiving feedback from interested parties;
- Identifying techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;
- Checking status of preventive and corrective actions;
- Review and acceptance of any exceptions;
- Review of internal and external issues;
- Assessing vulnerabilities or threats not adequately addressed in the previous risk assessment;
- Reporting on results from effectiveness measurements;
- Following-up on actions from previous committee reviews;
- Checking on any changes that could affect the ISMS; and
- Providing recommendations for improvement.

Regular Committee Reviews should result in the following:

- Improvement of the effectiveness of the ISMS.
- The update of the risk assessment and risk treatment plans.
- Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS.

Compliance Officer is responsible for ensuring compliance with any law, statutory, regulatory or contractual obligations.

IT Directors and Managers serve as the quality managers for all ongoing activities that serve to provide appropriate access to and protect the confidentiality, integrity and availability of client, employee, and business information in compliance with the ISMS policies and standards.

All Managers are directly responsible for implementing effective processes in-line with information security policies for their business areas, and of compliance by their employees. Managers are responsible for implementing effective processes consistent with these policies that protect IFDS' information assets and monitor controls and compliance.

All Employees are responsible for adherence to the Information Security Policy and sub-policies. Employees need to be vigilant when it comes to executing security policies in the workplace and to report any suspicious activities. A workplace security policy is effective only if it is used and practiced.

3. Objectives

The Objectives of the ISMS Framework and Information Security Policy are to:

1. Protect the information owned, created, stored and/or processed by IFDS Canada on behalf of its clients, affiliates, partners and staff from all threats – internal or external, deliberate or accidental.
2. Ensure that every staff member and third party resource is educated, informed and assumes responsibility in maintaining the security of information in all forms.
3. Prevent and minimize the impacts of security incidents to ensure business continuity – including access to information; upholding the integrity and authenticity of our information records; and reduce business damage.
4. Enhance client, affiliate, stakeholder, market perception and confidence through demonstrable security controls and procedures – protect business investments and opportunities.
5. Ensure compliance with information security-related regulatory and legal obligations.

4. Security Policy

Users of IFDS' computer systems and information must comply with all the policies, standards and procedures set out in the ISMS. Failure, by the user, to observe the policies and standards is deemed serious and may be subject to disciplinary action up to and including termination of employment. If a suspected Security incident has occurred which has indicated there may have been a case of improper use of IFDS' computer systems or information stored, IFDS reserves the right to suspend the member of staff in accordance with Human Resources disciplinary procedures and the IFDS Confidentiality Agreement and carry out a full investigation and forensic analysis of associated equipment.

Every employee of IFDS is responsible for maintaining security of information on the desktop, enterprise servers, across networks, and in all forms. Any security event or weakness must be reported to the Information Security Department to be addressed and corrective action taken in a timely manner.

Reasonable precautions for protecting IFDS' assets are the responsibility of all IFDS staff members. Situations of omission or commission regarding appropriate precautions and controls may result in disciplinary action up to and including termination.

Security policies are designed to protect all staff members in the effective use of company assets. Actively following and pursuing standards, guidelines and controls ensures that employees are making choices consistent with security policies outlined in the Information Security Management System. All employees are responsible for minimizing risk of loss of information. Where appropriate, employees are responsible for proactively addressing security requirements within their areas of responsibility. If in doubt staff members are encouraged to review and confirm actions and controls with their supervisor, manager or executive in consideration of these policies and their responsibilities within IFDS.

The Information Security Director takes overall responsibility for the development and implementation of security and will support the identification of controls. However, responsibility for resourcing and implementing controls remain with the relevant area.

To counteract interruptions to IFDS business activities and to protect critical processes from the effects of major failures of information systems or disasters, IFDS maintains and tests business continuity plans which address the information security requirements needed for business continuity.

This document forms an integral part of the Information Security Management System (ISMS).

Modification Date	Resultant Version	Change Description	Reviewer
12/20/2010	1.0	First Draft (Information Security)	ISO Project
	1.0	Issued	Information Security Manager
	1.1	Scope changes from ISO review 05/10/09	Information Security Manager
	1.2	Foreword by CIO	Information Security Manager
03/17/2011	1.3	Minor Revisions	Information Security Manager
01/16/2012	2.0	Change of Chief Security Officer; update location of security policies	Information Security Manager
09/05/2012	2.1	Changed name of the Senior Management Committee	Information Security Manager
11/09/2012	3.0	Include ISMS Objectives	Information Security Manager
07/22/2013	3.1	Annual Review	Information Security Manager
11/06/2013	3.2	Added: Policies are reviewed annually in Sec 4	Chief Security Officer
01/14/2014	3.3	Added: OHSA to scope Changed: Policies approved by Security Committee and Classification from Internal Use Only to Public	Information Security Manager
07/01/2014	3.4	Adjust to ISO 27001:2013	Information Security Manager
04/13/2015	3.5	Approval of Security Committee; minor updates to language	Security Committee
01/25/2016	3.6	General review and approval of the Security Committee	Security Committee
07/15/2016	3.7	New Objectives approved by the Security Committee	Security Committee
01/13/2017	3.8	Reference to PIPEDA and OSHA was removed	Risk & Bus. Cont. Manager
11/07/2017	3.9	Review for mandatory training; added CSO, moved ISO details to Introduction section	Risk & Bus. Cont. Manager