Information Security Management System Policy

Public

Version 3.3 Issued

Document Name P079A – ISMS Security Policy

Owner Information Security

Security Policies, Standards and Procedures emanate from the Information Security Policy which has been approved by the Security Committee. Drafting has been sanctioned by the Chief Security Officer subject to an approved ratification procedure.
Foreword

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

We must also recognise that information also resides in other than electronic forms which also require protection.

Information security is not just something we do; it is an organisational culture and one that is deeply embedded in IFDS’ business.

Therefore IFDS’ senior management, to protect the confidentiality, integrity and availability of our information, have approved an information security management system (ISMS) built on the ISO 27001 standard.

The Risk Management Committee and I as Chief Security Officer further endorse this information security policy.

Dennis Gregoris
Chief Security Officer
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 Associates employed by International Financial Data Services (Canada) Limited including part-time, full-time, temporary staff, consultants, contractors and vendors 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. Information Security Policies are located in our intranet, Inside IFDS 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 form 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 organisation’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.

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

ISO/IEC 27001 (formerly BS 7799-2:2002) 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:

- PIPEDA (2000) – in scope
- Ontario’s Occupational Health and Safety Act (OHSA) – in scope
- Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) – not in ISO27001 scope
- National Instrument 81-102 Mutual Funds - not in ISO27001 scope
**Information Security Manager** 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, Management’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;
- Assessing vulnerabilities or threats not adequately addressed in the previous risk assessment;
- Reporting on results from effectiveness measurements;
- Following-up on actions from previous management reviews;
- Checking on any changes that could affect the ISMS; and
- Providing recommendations for improvement.

Regular Management Reviews should result in the following:

- Improvement of the effectiveness of the ISMS.
- Update of the risk assessment and risk treatment plan.
- 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 Office** is responsible for ensuring compliance with any law, statutory, regulatory or contractual obligations.

**IT 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 IS policies for their business areas, and of compliance by their Associates.

**All Associates** are responsible for adherence to the Information Security Policy and sub-policies.

### 3. Objectives of ISMS Implementation and Certification

**To enhance customers’ confidence, stakeholders’ satisfaction and market perception of organization:**

With the increasing risk of identity and financial cyber thefts and unauthorized access to obtain confidential information, IFDS Canada has taken proactive measures to safeguard confidential information of our customers by implementing information security controls. This is to ensure that all risks are identified and...
proper counter measures and controls are carried out to protect the information at risk in enhancing customers, stakeholders and market perception and confidence.

To identify areas of improvements:

Improvements are an essential aspect in financial industry. IFDS Canada will continue to face the challenges and fulfil the needs of emerging technologies in the financial industry.

To develop ISMS Framework using International Standards as benchmark:

Standardization is an important part of an organization. Therefore, by adopting International Standards such as ISMS, IFDS Canada will be able to have the best technical application of consensual experience inclusive of processes for selection in making appropriate choices for ratification coupled with consistent decisions.

To align the IT processes and objectives with the overall business objectives:

It is crucial to ensure IT systems and infrastructures are able to fulfil the demands of the business and adapt to changes in the business. This to ensure IFDS Canada remains relevant and competitive in the challenging business environment today.

To improve management control and achieve consistency in operations:

The management will achieve a bird's eye view of the organization. Strategic decision can be made effectively to ensure smooth execution of decision thus contributed to business improvements, stakeholder’s requirements, regulatory and legislative requirements and in addition increasing customer's confidence.

To minimize costs by rationalizing internal systems, practices and processes.

All systems, practices and processes could be streamlined and resources could be utilized to their maximum potential.

4. Security Policy

IFDS has established a framework of controls, policies and standards, as laid out in the Information Security Management System (See ISO/IEC 27001 Information Security Management System, Statement of Applicability), 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 policies approved by the Information Security Committee. All policies are reviewed on an annual basis.

Senior Management, as commitment to the IFDS ISO/IEC 27001 information security model approves this document and policies within the ISMS.

This ISMS contains 11 domains (A5 – A15), Security Policy, Organising Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and...

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.

Every Associate 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.

Management will ensure attendance of associate IS induction training and on-going IS awareness training.

Managers are responsible for implementing effective processes consistent with these policies that protect IFDS’ information assets and monitor controls and compliance.

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 Associates are making choices consistent with security policies outlined in the Information Security Management System. All employees are responsible for minimising risk of loss of information. Where appropriate, Associates 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 Manager 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.

The Information Security Policies, which define a basic level of information security to meet the Business need and is consistent with industry best practice, are subject to annual review by the Information Security Manager.

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 a disciplinary offence which could lead to dismissal. In some cases breach of these policies may expose the user to personal liability, actioned by regulators and in serious cases, prosecution. 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 reserve the right to suspend the member of staff in accordance with Human Resources disciplinary procedures and carry out a full investigation and forensic analysis of associated equipment.

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