FIERA CAPITAL

(« the Corporation »)

INFORMATION SECURITY POLICY

Version 3.0

Table of Contents

1. Introduction

To address information security, the executive management of Fiera Capital Corporation (‘FCC’, ‘Fiera’ or the ‘Corporation’) has sponsored a corporate information security program to protect the information assets of the firm and ensure the confidentiality, integrity and availability of information. With this mindset, a holistic approach is being taken and a stepping stone is the creation of an Information Security Governance Committee (the ‘iSGC’). This cross functional platform enables buy-in and commitment of executives across the firm.

In doing so, FCC is promoting a security culture whereby everybody is engaged in protecting informational assets, detecting incidents, and reacting promptly to unusual events as they unfold.

2. Scope and Objectives

This information security policy constitutes the foundation of good security practices that supports the achievement of business objectives and states the guidelines as per the management and operations of information assets.

This policy applies to all employees (permanent and temporary), business partners, contractors, and suppliers who have access to information systems and information assets (referred in this document as “Users”).

Information assets consist not only of FCC systems and infrastructures related to IT computing including hardware, software and infrastructure but also include information produced by FCC or its Users and kept on different media types (digital or non-digital).

3. Policy Framework

Information assets are among FCC’s key assets. In this respect, confidentiality, integrity and availability of information are critical to the firm. To be in line with these three key requirements, FCC has defined a framework that consists of four fundamental areas:

- “Governance”: establish the information security policy and enable appropriate strategies, policies and procedures to ensure alignment across all divisions.
- “Protection”: enable the required processes, technologies and resources to proactively protect information assets.
- “Detection”: enable the required processes, technologies and resources to detect any abnormal behaviour or event impacting the information assets.
- “Reaction”: enable the required processes, technologies and resources for quick response in case of any security breach.

The sections below outline each area and its corresponding domains with a set of guidelines that constitutes the information security policy.

4. GOVERNANCE

The objective of this area is to enable appropriate security strategies involving key stakeholders from all sectors of the Corporation (corporate functions and divisions) to work together around a common set of policies and procedures to secure and exploit corporate information. This area includes the following domains:

- Risk Management
- Awareness and Training
- Legal and Compliance

4.1 Risk Management

To better protect information assets of the Corporation, an enterprise-wide information security program is sponsored by executive management.

A holistic approach in collaboration with corporate Enterprise Risk Management shall be taken to mitigate identified risks to acceptable levels. FCC shall perform a periodic assessment exercise to identify major threats and vulnerabilities that could potentially disrupt operations in each of its divisions and thereafter apply appropriate remediation.

4.1.1 Vulnerability Management

Identification of vulnerabilities is a key ingredient in information security management as it highlights the weak links of FCC's perimeter. The Corporation thus shall implement continuous vulnerability assessment and remediation as an integral part of its information security governance.

Each assessment cycle shall clearly detect security vulnerabilities, establish response processes and determine measures to be taken to pare down risks to acceptable levels (risk tolerance).

In light of the above, executive management shall make the necessary investments to facilitate implementation of recommended measures, build the firm's threat intelligence, and improve its security posture line with this policy.

4.1.2 Hosted Services

For information assets hosted by external service providers, FCC shall ensure they provide necessary details on data hosting (e.g. private cloud), data encryption and network connectivity, business continuity mechanisms (backup/restore, disaster recovery procedures), incident management procedures as per industry best practices. FCC shall validate these key components are part of the contractual agreement prior to formal sign off.

4.2 Security Awareness and Training

Appropriate employee behaviour in combination with technology controls is essential for proper defense of information assets. To further leverage security governance and foster proper behaviours across the firm, a security awareness program shall be established. In this regards, FCC shall dispatch training sessions to all employees, ensure their understanding and underline the importance of their buy-in and commitment towards safeguarding the information assets of the firm. An awareness of potential impacts arising from their roles and responsibilities while performing their duties is essential to securing the firm's critical assets. Employees shall be made aware of this policy, its purpose, what is expected of them and the role they play in protecting the firm's assets.

Managers are accountable for ensuring that users under their supervision are trained on the company's security policies in accordance with their position or function.

4.3 Legal and Compliance

The Legal and Compliance Department shall inform the information security governance committee ("iSGC") of any regulatory changes and associated requirements pertaining to information security for which FCC needs to comply with. This shall serve as guidance towards necessary steps to take to ensure compliance with regulatory authorities.

Compliance of third parties (suppliers, consultants) with FCC Information Security Policy shall be evaluated by managers responsible for managing the relationships.

The Legal and Compliance Department shall ensure that contractual agreements and/or service level agreements clearly mention the responsibility of FCC and its third party providers, partners or clients with respect to information security.

5. PROTECTION

The objective of this area is to enable the required processes, technologies and resources to proactively protect information assets of the enterprise. It consists of the following domains:

- Information Access Management
- Information Asset Management
- Applications and Systems
- Network and Infrastructure

5.1 Information Access Management

Information access management is the discipline of managing access of authorized individuals, on a need to know basis, during a period of time to perform their duties.

5.1.1 Segregation of duties

FCC shall implement segregation of duties based on roles and responsibilities to maintain strong information control and reduce errors.

FCC shall institute a culture of checks and balances to counteract improper behaviour and enable proper governance of information assets.

5.1.2 Access Control

FCC shall ensure authorized users have access to appropriate information assets to perform their duties in line with business related requirements.

Access to information shall be granted on a need-to-know basis in accordance with appropriate procedures.

Each authorized user who has access to information assets has an obligation to protect these information assets in accordance with this policy.

5.1.3 Physical and Environmental Security

FCC shall ensure that its processing facilities (data centers, servers, and network components) are protected by defined security perimeters, with appropriate security barriers and adequate physical access control measures. FCC shall protect its premises to prevent unauthorized physical access.

5.1.4 Workforce Security

FCC shall ensure users are subject to security and reliability screening prior to being hired or retained. Users are responsible to protect FCC resources and report any situation that could compromise FCC's information assets.

5.2 Information Asset Management

Information asset management is the discipline of classifying assets from non-sensitive (little or no value) to highly sensitive (e.g. critical information that gives FCC a competitive edge). This is a key exercise that allows FCC to assign a level of sensitivity to information assets (regardless of medium: digital or non-digital) and determine thereafter the degree of control that needs to be put in place to secure the assets.

5.2.1 Classification of assets

FCC shall ensure appropriate procedures are in place to enable classification and management of assets based on their criticality. Information asset owner (responsible for ensuring assets are handled properly by appropriate resources as per classification), and custodian (responsible for ensuring necessary protection measures are implemented and monitored) shall be identified.

Information assets, regardless of their form or format, which are created or used in support of FCC's business, shall be protected in line with their respective value, sensitivity and associated risk of loss or compromise.

5.2.2 Disposal of assets

FCC shall ensure to have procedures in place to safely dispose of information technology equipment while minimizing the risk of exposure and misuse of any sensitive data stored on those equipment. All phases of IT asset disposal shall be covered. These include the collection, transportation, storage, and destruction of components containing data. Should a third party be mandated for disposal, FCC shall obtain a certificate as proof of proper handling of assets.

5.3 Applications & Systems

Applications and systems is the discipline of enabling the appropriate technologies and processes to secure data which either flows between different systems or is accessed by Users through desktops (in-house or remote) or via mobile devices.

5.3.1 Data Encryption

This practice shall set up adequate controls (data protection) to mitigate any risks associated with unauthorized access to informational assets. FCC shall use appropriate encryption mechanisms (disk, devices, emails, files, folders, etc.) to ensure appropriate level of protection is applied.

5.3.2 Change Management

FCC shall ensure any changes (using software engineering methodologies) to applications and systems shall be evaluated, by the right level of management, to ensure security practices are not jeopardized before migration to production. These changes can be either technology-based or process-based, driven by internal FCC teams or triggered by external vendor (service provider).

5.4 Network & Infrastructure

This discipline deals with the protection of IT equipment (network components, communication technologies and data transiting through those assets) from theft, damage as well as any disruption of services.

Security controls shall be implemented to reduce exposure from cybersecurity attacks. Different technological controls and best practices shall be enabled: anti-phishing solution, next generation firewall, cloud security service, vulnerability management, threat management, intrusion detection and prevention, equipment hardening.

6. DETECTION

The objective of this area is to enable the required processes, technologies and resources to detect any abnormal behaviour or event impacting the information assets of the enterprise. It consists of the following domains:

- Incident management
- Event monitoring and network analytics

6.1 Incident management

FCC shall have an incident management process in place to address security incidents. The severity of the security incidents shall be determined by the appropriate manager and shall dictate the level of escalation and necessary actions to be taken to bring incident to closure. In any case, the Chief Information Officer and the appropriate stakeholders shall be kept informed.

6.2 Event Monitoring & Network Analytics

Security information and event management ('SIEM') provide a means to have a holistic view of network traffic. SIEM platforms centralize network traffic information from different sources thus enabling network analysis and quick response to threats. FCC shall enable SIEM technology to improve its incident detection and response as well as event-correlation capabilities.

7. REACTION

The objective of this area is to enable the required processes, technologies and resources for quick response in case of any security breach. It includes the following domains:

- Cyberattack response
- Business continuity
- Cyber insurance and forensic

To better prepare for any potential attack, the stakeholders through the information security governance committee ('iSGC'), shall identify their top security threats on an annual basis. These shall be documented, and appropriate mitigation strategies should be put forward and communicated. During the year, via the iSGC instances, these threats shall be revisited and updated.

To further sharpen its response mechanisms, FCC shall perform a cyberattack simulation on a periodic basis. Corporate communication templates shall be prepared, procedures shall be documented, stakeholders shall be trained and measures shall be taken to ensure organizational readiness. Lessons learned from the exercise shall be integrated into the security program and implemented based on criticality.

7.1 Cyber Attack Response

Responding to a cyberattack, a cell crisis shall be formed. Cell crisis members shall be pre-identified and made knowledgeable of their respective role. Each cell crisis member shall be efficiently reachable, via mobile phone and email. The following stakeholders form part of the cell:

Mandatory cell members:
Corporate - Chief Information Officer
Corporate – Legal Affairs & Compliance
Corporate - Communications
Corporate - Chief Risk Officer
Infrastructure & User services (division)
IT Leader (division)

Ad hoc members:

Head of IT, application services
Any relevant business unit representative
Any 3rd service party provider

Users across the enterprise shall be made aware of the crisis by the communications lead. Users shall share any pertinent information with the incident management team and follow procedures in a timely and collaborative manner.

7.2 Business Continuity

This domain deals with additional mechanisms that could be activated, over and above the crisis cell and response plan following a cyberattack (causing disruption of service). Management shall decide as to the severity of the disruption and take appropriate actions should there be a need to trigger the Disaster Recovery Plan (DRP) and/or Business Continuity Plan (BCP).

7.3 Cyber Insurance and Forensic

FCC shall proactively identify and contractually engage with an external service provider for cyber insurance and forensic capabilities should the need arise. The iSGC shall be the forum for such recommendations in view of risk mitigation and brand protection.

8. Roles and Responsibilities

Security of information assets is the concerns of all Users and the IT department of each division is the custodian of its computerized information assets

The Chief Information Officer in collaboration with other heads of IT at Divisions' levels shall ensure alignment of information security program by all departments. In so doing, the Chief Information Officer chairs the Information Security Governance Committee (iSGC) which enables a forum of discussion around security initiatives. Adequate controls shall be set to ensure users consistently follow policies and procedures.

Compliance with this Information Security Policy shall be verified through audits and assessments in collaboration with the Internal Controls Department. This shall ensure adequate controls are in place.

The Chief Information Officer shall also report progress of security program and security posture to the Audit and Risk Management Committee (ARMC). Responsibilities of key stakeholders:

- Chief Information Officer: accountable for corporate information security.
- Division's Head of IT: ensures this policy is applied within his/her division.
- Users: conduct their business activities with due diligence and due care while adhering to this policy.

9. Policy Owner

Fiera Capital's Chief Information Officer is the owner of this policy.
Policy's effective date: December, 2016

10. Review Cycle

Fiera Capital Corporation's information security policy shall be reviewed once every three years or more frequently as required.