Vancouver Firefighters' Credit Union

Information Systems Privacy and Security Policy

1 Corporate Information Security Policy

1.1 Purpose

The purpose of this policy is to protect from all threats, whether internal or external, deliberate or accidental, the information assets of Vancouver Firefighters' Credit Union:

1.2 Objectives

The implementation of this policy is important to maintain and demonstrate CU integrity in dealing with members and vendors.

It is the policy of **Vancouver Firefighters' Credit Union** to ensure:

- Information is protected against unauthorized access
- Confidentiality of information is maintained
- Information is not disclosed to unauthorized persons through deliberate or careless action
- Integrity of information through protection from unauthorized modification
- Availability of information to only authorized users when needed
- Regulatory and legislative requirements are met
- Business continuity plans are produced, maintained and tested as far as practicable
- Information security training is given to all Employees
- All breaches of information security and suspected weaknesses are reported and investigated

1.3 Applicability

All **Vancouver Firefighters' Credit Union** staff and vendors, employed under contract, who have any involvement with information assets covered by the scope of the Information Security Management System, are responsible for implementing this policy and shall have the support of the **Vancouver Firefighters' Credit Union** Management who have approved the policy.

1.4 Compliance

Failure to comply with this policy may result in breaches of security, leading to the exposure of data of a confidential or sensitive nature. Lack of compliance may result in disciplinary action, as circumstances dictate.

2 Asset Management

Information and information systems constitute valuable Vancouver Firefighters' Credit Union resources. The asset management policy is the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

2.1 Identification of assets

Vancouver Firefighters' Credit Union must identify assets under their control including:

- Software;
- Hardware;
- Services including computer and communications services, and general utilities;
- Information assets including: database and data files, contracts and agreements, system documentation, research information, user manuals, operational or support procedures, continuity plans, fall back arrangements, archived information.

documentation, research information, user manuals, operational or support procedures, continuity plans, fall back arrangements, archived information.

2.2 *Documenting and maintaining asset inventories*

An inventory of all important assets associated with information systems must be documented and maintained. The loss, theft or misappropriation of assets must be reported immediately to the IT Service Desk. Where the loss, theft or misappropriation involves information the Incident response plan must be initiated.

2.3 *Acceptable use of Assets*

Rules for the acceptable use of information systems must be identified, documented and implemented.

3 Human Resources Security

These are the information security requirements for employees, external consultants and contractors that have an employment relationship with Vancouver Firefighters' Credit Union.

- Reference, credit and criminal records checks must be completed prior to hire or engagement
- Responsibilities for information and systems security documented in the End User Technology Agreement must be signed off upon hire.
- Security breaches or policy violations must be reported and investigated and appropriate disciplinary action taken where warranted
- All CU assets must be returned on termination of employment
- Access rights to information systems must be terminated on termination of employment

3.1 *Security Roles and Responsibilities*

Security roles and responsibilities must be documented and communicated to all employees, consultants and contractors to ensure that they are informed of their information security roles and responsibilities. These are documented in the End User Technology Agreement.

3.2 *Screening of Employees, External Consultants and Contractors*

Employees, external consultants and contractors screening must be performed prior to entering a working relationship with Vancouver Firefighters' Credit Union.

All staff must undergo reference, credit and criminal records checks prior to entering a working relationship with Vancouver Firefighters' Credit Union.

Disciplinary Process

Security breaches or policy violations caused by employees, external consultants and contractors must be reviewed by Management.

Upon receipt of information identifying employees, external consultants and contractors responsible for a security breach or policy violation, managers are responsible for:

- Ensuring the Information Systems team has been informed of the potential security breach or policy violation;
- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining, in consultation with their Human Resource consultant, if disciplinary action is warranted for employees;
- Determining if disciplinary action is warranted for non-employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

3.3 *Termination Responsibilities*

Managers must advise employees, external consultants and contractors of on-going

3.3 *Termination Responsibilities*

Managers must advise employees, external consultants and contractors of on-going confidentiality responsibilities that continue to apply after termination of employment.

3.4 *Return of Assets*

Employees, external consultants and contractors must return Vancouver Firefighters' Credit Union assets upon termination or change of employment.

3.5 *Removal of Access Rights*

The access rights of employees, external consultants and contractors to information systems must be removed upon termination of employment and reviewed upon change of employment.

4 Physical and Environmental Security

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of Vancouver Firefighters' information and information systems.

4.1 *Physical Security*

Information processing facilities must be appropriately protected. The physical security of the information processing facilities must take into account employees, external consultants and contractor's safety, and the protection of sensitive or valuable information and assets.

4.2 *Physical Entry Controls*

Secure areas must be protected by appropriate entry controls to ensure that only authorized employees, external consultants and contractors are allowed access.

Entry controls
Access to any Vancouver Firefighters' Credit Union information processing facility or areas where sensitive information is kept must be restricted. Entry controls must identify, authenticate and monitor all access attempts as follows:

- Every person authorized to enter a facility must be issued with an alarm fob and password;
- Visitors must be accompanied by an authorized person;
- An electronic reader that logs the identity, time, date, and access privileges of each entry attempt must do such checking. Entry control may be achieved using keys, proximity card readers or other technologies;
- Employees, external consultants and contractors must challenge anyone in a secure area who is not known to them;
- Access rights to secure areas must be reviewed and updated regularly.

4.3 *Equipment Security*

Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards

Equipment sites
The design and layout of information processing facilities must provide protection from security threats and must include:

- Servers and other centralized computing equipment must be located in a secure information processing facility.
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas; and,
- Locating shared printers, scanners, copiers, and facsimile machines away from public or reception areas, or in passageways or other areas where users who do not have a need-to-know can access printed material.

Equipment protection
The design and layout of information processing facilities must provide protection from physical and environmental hazards. Safeguards must include:

- Ensuring that equipment is properly vented and that the temperatures and humidity in

The design and layout of information processing facilities must provide protection from physical and environmental hazards. Safeguards must include:

- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Providing lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Providing employees, external consultants and contractors with approved eating and drinking areas separate from work areas containing equipment;
- Briefing employees, external consultants and contractors who work with equipment about safety practices in the workplace;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems;

4.4 Planning and Design and Maintenance

Power and telecommunications cabling must be protected from interception and damage.

Power and telecommunications cabling must be protected from interception and damage. The following methods can increase protection:

- Power and telecommunications cabling must be underground and/or in a secure conduit;
- Power cables should be protected with electromagnetic shielding;
- Cables must not be accessible in public areas; and
- Inspection boxes, termination points, patch panels, control rooms and other facilities must be secured and located inside a communications room.

4.5 Security Controls

Equipment must be protected when off-site from Vancouver Firefighters' Credit Union premises.

Authorized use
Off-site use of equipment must be authorized. Equipment for off-site usage may include:

- Desktop and laptop computers;
- Portable storage devices;
- Mobile devices; and,
- Printers, scanners, copiers and facsimiles

Security controls
Vancouver Firefighters' Credit Union equipment being used off-site must be protected commensurate with the sensitivity of the information it contains and the value of the equipment.

Employees, external consultants and contractors must ensure that:

- Sensitive data is encrypted;
- Equipment is protected from unauthorized access by the use of a logical or physical access control mechanism (e.g., password, USB key or smart card);
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and,
- They are familiar with the operation of the protection technologies in use;
- Vancouver Firefighters' Credit Union equipment must not be left unattended in a public place;
- Vancouver Firefighters' Credit Union equipment must be kept under direct control at all times when travelling;
- They must use physical locking, restraint or security mechanisms whenever possible;
- Take measures to prevent the viewing of sensitive information other than by authorized persons;
- They must not permit other persons to use the equipment; and,
- They must report loss of equipment immediately to the IT service desk.

- They must not permit other persons to use the equipment; and,
- They must report loss of equipment immediately to the IT service desk.

4.6 *Reassignment of Hardware and Media Destruction*

Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed.

Destruction of hardware
Hardware media used to store information or software must be destroyed in a secure manner.

5 Communications and Operations Management

Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide services.

Controls for operations include documented processes, staff duties and formal methods to implement changes to facilities. This includes: methods to protect information, create copies for back-up and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

5.1 *Change Management*

Changes to information systems and information processing facilities must be controlled.

Change management process
A change management process must be documented and implemented to control changes by:

- Identifying and recording significant changes;
- Assessing the potential impact, including the security impact, of the change;
- Obtaining approval of changes from the product manager(s) responsible for the information system;
- Planning and testing changes including documenting fall back procedures;
- Communicating change details to relevant employees, external consultants and contractors; and,
- Evaluating that planned changes were performed as intended.

5.2 *Segregation of Duties*

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information systems.

Segregation of duty
Where feasible, the risk of disruption to information systems should be reduced by:

- Maintaining documentation for every server and network device;
- Automating functions to reduce the reliance on human intervention for information systems;
- Requiring that individuals authorized to conduct sensitive operations do not audit those operations;
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action; and,
- Implementing information systems security controls to minimize opportunities for collusion.

5.3 *Separation of Development, Test and Operational Facilities*

Development and test information systems must be separated from operational information systems.

Separation requirements
Operational information systems must be protected by:

- Separating operational environments from test, development and operating environments;
- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational

- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified employees, external consultants and contractors;
- Preventing access to compilers, editors and other tools from operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems;
- Limiting the use of operational data, when possible, in development, test or training information systems; and,
- Limiting the use of personal information, when possible, in development, test or training information systems.

5.4 *System Acceptance*

Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.

System acceptance process
System acceptance criteria must be included as part of the system development and acquisition process.

Prior to implementing new or upgraded information systems, the following must occur:

- Acceptance criteria are identified including privacy, security, systems development and user acceptance testing;
- *Security certification* is attained, indicating the system meets minimum acceptance criteria; and,
- *Security accreditation* to proceed with implementation is attained.

5.5 *Protection against Malicious and Mobile Code*

Security awareness, prevention and detection controls must be utilized to protect information systems against malicious code.

Prevention and detection controls
The following activities must be taken to protect Vancouver Firefighters' Credit Union information systems from malicious code (e.g., viruses, worms):

- Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malicious code before use; and,
- Maintaining business continuity plans to recover from malicious code incidents.

User awareness
The Information Security Officer is responsible for developing user awareness programs for malicious code countermeasures.

Information Security team members are responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

6 Network Security Controls

A range of controls must be implemented to achieve and maintain security within the Vancouver Firefighters' Credit Union network.

Control and management of networks
Network infrastructure security controls and security management systems must be implemented for networks to ensure the protection of information and attached *information systems*.

Vancouver Firefighters' Credit Union must consider network-related assets which require protection including:

Vancouver Firefighters' Credit Union must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and *cryptographic keys*;
- *Network management information*;
- *Network pathways and routes*;
- Network resources such as bandwidth;
- *Network security boundaries and perimeters*; and,
- Information system interfaces to networks.

Employees, contractors and external consultants must not store Vancouver Firefighters' Credit Union information on non Vancouver Firefighters' Credit Union owned and managed computing devices. Non Vancouver Firefighters' Credit Union owned computing devices must not be connected to the Vancouver Firefighters' Credit Union network unless inspected and approved by IT.

Configuration control
To maintain the integrity of networks, changes to network device configuration must be managed and controlled such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;
- Access controls and *multi-factor authentication*;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Firewall reviews must be performed at least annually and after significant change to ensure that configuration baselines reflect actual device configuration.

Secured path
Where required information must only be transmitted using a *secured path*.

Secured paths for information transmission must use controls such as:

- Data, message or session encryption, such as SSH, SSL or VPN tunnels; and,
- Systems to detect tampering.

Wireless Local Area Networking
Wireless Local Area Networks must utilize the controls specified by the Information Security Officer and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by Vancouver Firefighters' Credit Union authentication services;
- The use of strong, frequently changed, automatically expiring encryption keys and passwords;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

6.1 Management of Removable Media

All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media.

All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media.

Use of portable storage devices
The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.

Employees using portable storage devices must protect the information and information technology assets in their custody or control by ensuring it is encrypted and physically secure

Human factors
Employees using portable storage devices must be:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with operation of the required protection technologies and when they must be used; and,
- Familiar with security event and loss reporting procedures.

Risk assessment factors
The impact of disclosure or loss of information stored on portable media must be considered, such as:

- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media destruction;
- Improper long term storage environment;
- Exposure to malicious and mobile code; and,
- Incomplete erasure of data prior to device disposal.

Mandatory controls
Minimum information protection safeguards for the use of portable storage devices include:

- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Not storing the only version of a document on portable storage devices;
- Documented authorization processes for use of portable storage devices;
- Encryption of confidential stored data;
- Contractual requirements for third parties that transport, handle or store portable storage devices; and,
- Secure erasure and disposal.

6.2 *Secure Disposal of Media*

Media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.

6.3 *Information Handling*

Media must be handled and stored so as to prevent unauthorized information disclosure or misuse.

6.4 *Security of System Documentation*

Systems documentation must be protected from unauthorized access by access controls, passwords, and encryption or digital signatures as appropriate to the information classification;

6.5 *Physical Media in Transit*

Media being physically transported must be appropriately protected.
Minimum media transport requirements are:

Media being physically transported must be appropriately protected.
Minimum media transport requirements are:

- Inspecting identification credentials of couriers upon pickup and delivery of packages;
- Obtain and retain receipts for media shipments;
- Using packaging that will protect the media from loss or damage; and,
- Packaging so that the classification of the media is not displayed.
- Ensuring any media sent by courier is encrypted and classified

7 Business Information Systems

Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems.

Information systems utilizing on-line transactions must have security controls commensurate with the value and classification of the information.

7.1 On-line transaction security

Information systems containing on-line transactions must have security controls commensurate with the value and classification of the information.

Security controls must be implemented to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

7.2 Publicly Available Information

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

Internet site security
The publication, modification or removal of information on publicly available information systems must be approved by the appropriate business owner. Business owners are responsible for maintaining the accuracy and integrity of the published information. Security controls must be developed, documented and implemented to:

- Maintain a record of changes to published information;
- Maintain the integrity of published information;
- Prevent the inappropriate release of sensitive or personal information;
- Monitor for unauthorized changes; and,
- Prevent unauthorized access to networks and information systems.

7.3 Audit Logging

Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations.

8 Access Control Policy

Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by regulations that protects particular types of information (e.g., personal, sensitive or PCI) and business requirements. Mechanisms for access control include password management, user authentication and user permissions.

8.1 Access Control

Access to information systems and services must be consistent with business needs and be based on security requirements.

Access control should:

on security requirements.

Access control should:

- Consider both physical and logical access to assets;
- Apply the "*need to know*" and "*least privilege*" principles;
- Set default access privileges to "deny-all" prior to granting access;
- Require access by unique user identifiers or system process identifiers to ensure that all accesses are auditable;
- Have permissions assigned to roles rather than individual user identifiers.

8.2 Access Management

There must be a formal user registration and de-registration process for granting access to all information systems.

Registration

This process should:

- ensure access requests are approved by the supervisor/manager of the *user* requesting access, and,
- ensure the reasons for requesting access are consistent with job responsibilities;
- Maintain records of access right approvals;
- Ensure *employees, external consultants and contractors* understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- Ensure accesses are traceable to an identifiable individual or process;
- Ensure each user is assigned a single unique identifier for accessing information systems.
- Ensure the responsibilities for authorizing access are segregated from the responsibilities for granting access;
- Restrict access by using predefined role permissions;
- Provide secure and separate transmission of the user identifier and password to the user;

Deregistration

This process should include:

- The removal of access privileges for employees no longer with the organization;
- The prompt review of access rights whenever a user changes duties and responsibilities;
- The prompt review of access rights whenever the user's branch or department is involved in significant reorganization;
- The review of access privileges for employees on extended absence or temporary assignments;
- The immediate removal of access privileges for employees, contractors, and external consultants terminated for cause concurrent with notification to individual; and,
- The monthly check for and removal of terminated, inactive or redundant user identifiers.

8.3 Password Management

The issuance of authentication credentials must be controlled through a formal management process.

Individuals must be formally designated to have the authority to issue and reset passwords. The following applies:

- Passwords shall only be issued to users whose identity is confirmed prior to issuance;
- Individuals with the authority to reset passwords must transmit new or reset passwords to the user in a secure manner (e.g., using encryption, using a secondary channel);
- Whenever technically possible temporary passwords must be unique to each individual and must not be easily guessable;
- Passwords must never be stored in an unprotected form; and,
- Default passwords provided by technology vendors must be changed to a password compliant with Vancouver Firefighters' Credit Union standards during the installation of the technology (hardware or software).

compliant with Vancouver Firefighters' Credit Union standards during the installation of the technology (hardware or software).

8.4 *Review of Access Rights*

User access rights must be reviewed at regular intervals. A formal process must be implemented for the regular review of access rights.

8.5 *Password Use*

Users must follow good security practices in the selection and use of passwords as documented in the Electronic Services Policies and Procedures.

8.6 *Clear Desk and Clear Screen*

Users must ensure the safety of sensitive information from unauthorized access, loss or damage.

Securing the work space
Users should secure their work space whenever it is not supervised by an authorized person, including during short breaks, attendance at meetings, and at the end of the work day.

Securing the work space includes:

- Clearing desk tops and work areas;
- Securing documents and *portable storage devices* in a locked desk or file cabinet;
- Ensure outgoing and incoming mail is appropriately secured;
- Locking your computer;
- Locking doors and windows; and,
- Checking fax machines and printers to ensure that no sensitive information is waiting to be picked up.

8.7 *Network Access Control*

Users must only be provided access to the information systems they have been specifically authorized to use.

Access to network services
Only network services needed to support business requirements should be enabled (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system.

8.8 *Remote Access*

Access by remote users must be subject to authentication.

Remote access to Vancouver Firefighters' Credit Union networks or services must:

- Perform a *Security Threat and Risk Assessment* for each *remote access service* to determine the authentication methods to be implemented. Factors to be considered include classification of network services, information and information systems accessible from the remote access service;
- Require remote users to connect through Vancouver Firefighters' Credit Union designated remote access services or security gateways (e.g., Virtual Private Network, Desktop Terminal Services (DTS), Outlook Web Access); and,
- Require user identification and authorization prior to permitting each remote network connection.
- Obtain prior approval to interconnect networks from the Information Security Officer of every information system accessible from the remotely connected networks; and,
- Require remote network interconnections to connect through Vancouver Firefighters' Credit Union designated remote access services or security gateways (e.g., Virtual Private Network, Third Party Network Gateway).

- Require remote network interconnections to connect through Vancouver Firefighters' Credit Union designated remote access services or security gateways (e.g., Virtual Private Network, Third Party Network Gateway).

8.9 *Authentication for External Connections*

Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment.

8.10 *Protection of Diagnostic Ports*

Physical and logical access to diagnostic ports must be securely controlled.

Access control processes must be implemented for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities to prevent bypassing of information system access controls.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed, and kept active for the minimum time required.

Access to diagnostic ports from remote locations, or by third parties, or service providers must be authorized by agreements, contracts and conditions of use.

Use of diagnostic ports must be logged and monitored for suspicious activity.

8.11 *Network Segregation*

Groups of information services, users and information systems must be segregated on networks. Network perimeters must be established to control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

8.12 *Network Connection Control*

The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system

Logical and physical network connection control

The ability of users to physically and logically connect to networks must be restricted according to the access control policy. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

8.13 *Mobile Computing and Teleworking*

Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices.

Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices.

Information protection paramount

The use of portable storage devices must be managed and controlled to mitigate the inherent *risks* of portable storage devices.

The use of portable storage devices such as laptops, mobile devices (smart phones) to access, store, or process information increases the risk of information being compromised. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

Portable storage devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

Users of mobile computing services must be provided with security awareness training, to ensure that Users are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using portable storage devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with security event reporting procedures.

The Security Threat and Risk Assessment must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of the portable devices to remotely access Vancouver Firefighters' Credit Union operated networks and systems;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device destruction;
- Information destruction;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Minimum information protection safeguards for the use of portable storage devices include:

- Encryption of stored data to prevent information loss resulting from the theft of the mobile or
- remote device;
- Encryption of data transmitted via public network;
- Access control permissions on a portable storage device must be applied to prevent unauthorized access to information by system users, particularly for multi-user mobile systems;
- Regularly maintained data backups of information stored on portable storage devices using Vancouver Firefighters' Credit Union backup facilities to protect against information loss;
- To provide information availability portable storage devices must not be used to store the only copy of a Vancouver Firefighters' Credit Union record;
- Physical security of the device must be maintained to protect against asset and information loss;
- and,
- User authentication to the portable storage device and user authentication for remote access from the device must be implemented in accordance with authentication policies.

9 Information Security Incident Management

This policy establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that employees

9 Information Security Incident Management

This policy establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that employees, external consultants and contractors understand their roles in reporting and mitigating security events.

9.1 Reporting Information Security Events

Information security events must be immediately reported through appropriate management channels.

Employees must immediately report all suspected or actual information security events to the IT Team and requirements for reporting events must be included in contracts and service agreements.

9.2 Reporting Security Weaknesses

Employees must note and report any observed or suspected security weaknesses.

Employee must report any suspected or actual security weaknesses which include:

- The response process must:
    - ensure all reports are investigated and handled in a secure, confidential manner, and,
    - ensure the individual who reported the weakness is advised of the outcome when the Investigation is complete; and,
- The security awareness program should advise employees that:
    - they have a responsibility to report observed or suspected weaknesses to the Information Security Team,
    - suspected or observed weakness must not be tried or tested, and,
    - Weaknesses should not be discussed, or made known, except through approved reporting channels.

9.3 Responsibilities and Procedures

The types, volumes and costs of information security incidents must be quantified and monitored.