Information Technology Security Policy

National Film Board of Canada

Person responsible: Marco Girouard - 2013-11-28

Approved by: Luisa Frate, General Director
Finances, Operations & Technologies - 2011-09-23

NFB EMPLOYEE AND PARTNER COMMITMENT

I, the undersigned, _____confirm that I have read the NFB INFORMATION TECHNOLOGY SECURITY POLICY and agree to comply with it.

In _____on _____

Name in block letters: _____

Signature: _____

1 TABLE OF CONTENTS

2 REVISIONS

Date	Person responsible	Description
October 1, 2006	Fouzi Ben	Creation of IT Security Policy
October 1, 2010	Gilles Beauchamp	Document restructured Policy updated based on Treasury Board Secretariat recommendations
September 8, 2011	Gilles Beauchamp	Corrections and updates
Novembre 25, 2013	Marco Girouard	Change to contact names

3 DEFINITIONS

3.1.1.1 INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATION ASSETS

Information technology and telecommunication equipment, information systems, software, software packages, databases and information (text, sound, symbols or images) placed on equipment or on computer media, smartphones or mobile devices, e-mail or voice-mail systems, or any other information processing equipment.

3.1.1.2 COPYRIGHT

The exclusive right to produce or reproduce a work or significant portions thereof, in any material form, to present in public, publish or to allow any of the preceding acts as well as any rights accessory thereto or arising therefrom, all as defined by the Copyright Act.

3.1.1.3 RIGHT TO USE

Authorization granted to a person defining the use that can be made of information technology and telecommunication assets.

3.1.1.4 INFORMATION TECHNOLOGY (IT) EQUIPMENT

Computers, minicomputers, microcomputers, computerized workstations and their peripheral units or accessories for data playback, storage, reproduction, printing, transmission, reception or processing, as well as any telecommunication equipment (e.g. Blackberry, iPhone, iPad).

3.1.1.5 OUTPUT

Any object allowing storage of information or programs from a computer or its peripheral units or from telecommunications equipment.

3.1.1.6 SYSTEM MANAGER

Any personnel whose role is to manage assets, databases or information, equipment, systems or networks as defined in this policy, and any person to whom this responsibility is delegated by virtue of an agreement with the NFB.

3.1.1.7 INFORMATION TECHNOLOGY FACILITIES AND SERVICES

Information technology equipment under the responsibility of the NFB, and telecommunication and all other services provided by said equipment to the NFB.

3.1.1.8 DIGITIZED OBJECT

Textual, symbolic, sonic or visual (animated or not) information that is transformed so that it can be transmitted or viewed on telecommunication networks, processed by a computer or one of its peripherals, or stored on a computer or electronic medium.

3.1.1.9 COMPUTER WORKSTATION

Any device that can be used to access, enter, process or store data either independently or when linked with other computers.

3.1.1.10 SOFTWARE PACKAGES

A computer program designed to process an application.

3.1.1.11 COMPUTER NETWORK

An array of information technology components and equipment connected by means of telecommunication in order to access IT resources or services, or to share this access.

3.1.1.12 INFORMATION SYSTEMS

All practices and means for collecting, processing, updating, reproducing and distributing all types of information required for the NFB or one of its departments to operate.

3.1.1.13 DEPARTMENT

Any component of the NFB.

4 OBJECTIVES

The objective of the information technology and telecommunication security policy is to support the strategic objectives of the NFB[1] by ensuring the integrity of information in our possession, to ensure the security of our information technology equipment and to establish the regulatory framework governing the use of all NFB information technology or telecommunication assets.

These rules also aim to ensure compliance with all legislation regarding the use and processing of information and the use of information technologies.

[1] STRATEGIC OBJECTIVES

To exercise the NFB's leadership as a world reference point for innovation and creation of social issue documentary, community-engaged media, alternative drama and auteur animation, for and across all platforms.

To maintain and strengthen the NFB's ability to identify, develop and mentor the talent and creative skills of emerging filmmakers and Aboriginal, regional, linguistic and ethnocultural communities.

5 SCOPE

This policy applies:

- To permanent and temporary personnel of less than three months, or on contract for more than three months (artists, freelancers or companies) of the NFB and to users of the institutional services it provides. It also encompasses all individuals or outside firms called on to use information technology or telephone equipment installed at the NFB or that processes information belonging to the NFB.

- Any information technology or telecommunication asset belonging to the NFB, regardless of its location, or not belonging to the NFB but used on its premises, or located outside its premises and used to process information belonging to the NFB.

- All data entered, processed or stored using equipment, systems or other means that exploit information or telecommunication technologies that the NFB uses for its activities.

6 CODE OF CONDUCT

All users and managers of information technology or telecommunication assets, equipment, systems or networks shall comply with the NFB Employee Code of Conduct produced by Human Resources and available for consultation on the NFB intranet (http://photo-images.nfb.ca/uploads/gps/8725.pdf), particularly the sections on the use and management of information and telecommunication technologies.

Each new employee hired shall agree to comply with these rules at the time they join the NFB.

Any outside person or firm called on to use information technology or telecommunication equipment installed at the NFB or to process information belonging to the NFB is bound by the terms of their contract to comply with this policy.

7 RESPONSIBILITIES

The implementation of and compliance with this policy and rules or directives arising therefrom are the responsibility of all NFB personnel, managers and outside users of NFB facilities.

Managers of each unit are responsible for ensuring their personnel and users of the information and telecommunication technologies they offer are aware of the security principles pertaining to the use of said technologies.

8 AUTHORITY

Application of the information technology and telecommunication security policy is the responsibility of:

- NFB senior management
- The Departmental Security Officer (DSO) — Luisa Frate (Director General, Finance, Operations and Technology)
- The Chief Information Officer (CIO) — Marina Darveau (Head, Information Management)
- The IT Security Coordinator (ITSC) – Marco Girouard (Systems Administrator)
- The Head of IT (HoIT) – Pierre Métras (Head, Information Technologies)
- IT personnel
- Human Resources
- Business Affairs and Legal Services
- Supervisors and managers
- NFB personnel

No exception from this policy or the regulations arising therefrom is permitted without the written authorization of NFB senior management or its agent.

9 GUIDING PRINCIPLES

9.1 RESPONSIBILITY AND PROTECTION

The protection of institutional information technology and telecommunication facilities and their content is the responsibility of the IT department. To this end, IT must implement appropriate control and security measures to adequately protect the facilities under its responsibility.

Protecting local information technology and telecommunication equipment and its content is the responsibility of the departments that use them. These departments must implement appropriate control and security measures with the assistance of IT.

Activities	Senior Management	DSO	CIO	HoIT	ITSC	Managers & supervisors	IT personnel	Employees
Definition and updating of IT policy	I	C	C	A	R	I	C	
Application of IT policy	R	R	R	R	A	R	R	R
Incident management	I	C	C	C	A	I	R	I
Control and verification	I	A	R	R	R			

R – Responsible	= Correct execution of process and activities. There is at least one R per line.
A – Accountable	= Ownership of quality and end result of process. Exactly one A must be accountable for each activity.
C – Consulted	= Involvement through input of knowledge and information.
I – Iinformed	= Receiving information about process execution and quality.

DSO	Departmental Security Officer.
CIO	Chief Information Officer.
HoIT	Head of IT.
ITSC	IT Security Coordinator.

9.2 INFORMATION TECHNOLOGY AND TELECOMMUNICATION ASSETS AND EQUIPMENT

9.2.1 ACCESS

Only duly authorized individuals can use NFB information technology and telecommunication equipment.

Any unauthorized access or attempt to access NFB information technology or telecommunication assets constitutes a violation of this policy. IT operations personnel is responsible for ensuring that only authorized individuals have access to the NFB information technology system.

9.2.2 USE

All information technology and telecommunications assets shall be dedicated and reserved for the performance of NFB activities. However, the NFB acknowledges that, occasionally, members of its personnel may make use of some of its assets for personal purposes, for example, to process their own information, be it telephone messages or IT data.

The use of NFB information technology and telecommunication assets is a privilege, not a right. This privilege can be revoked at any time from any user who does not comply with the Information Technology Security Policy or the Code of Conduct for the Use and Management of Information Technologies.

No person shall install unauthorized software or equipment on information technology or telecommunication systems without the authorization of the Head of IT.

9.2.3 EQUIPMENT LOAN

NFB equipment may be lent to employees for short or long periods. In all cases, use of said equipment is subject to the equipment usage policy for personal purposes.

9.2.3.1 SHORT-TERM LOAN

Equipment may be loaned on a short-term basis — i.e. overnight, for a weekend or a number of days — to enable an employee to complete a project at home. In such cases, the supervisor is responsible for giving prior authorization for the equipment loan. The employee shall be responsible for the equipment borrowed (and the information contained therein) and shall take the measures necessary to return it in the same state and to ensure its security.

9.2.3.2 LONG-TERM LOAN

Long-term equipment loan, i.e. for a number of months or an indeterminate period, may be granted to employees when it is determined that this equipment will enable them to regularly perform a portion of their work. This type of arrangement should essentially be limited to management and supervisory personnel, or employees whose work demands that they regularly use this equipment outside their usual worksite (e.g. employee responsible for the smooth operation of the computer network). The employee shall be responsible for the equipment borrowed (and the information contained therein) and shall take the measures necessary to return it in the same state and to ensure its security.

9.2.4 REMOTE ACCESS TO THE NFB NETWORK (VPN)

Access to the network via VPN gives authorized users remote access to the NFB internal network. Be it from a personal computer at home (provided or not by the NFB) or a notebook computer when on the road, the personnel concerned have access, via the Internet, to the NFB's internal information systems (Intranet) as well as various servers (personal files) and institutional databases.

Access to the VPN remote network is granted, following approval by their supervisor, to NFB employees who need continuous remote access for their work, to NFB managers, supervisors and employees who must access the network for their work.

Users shall not divulge personal-access information (usernames, passwords, etc.) required for said remote access.

If employees use a personal computer to remotely access the NFB network, they must ensure that antivirus software is installed on their system and kept up to date, and that their firewall is activated. The IT department can confirm this if need be (see Human Resources Guide). During VPN access, access to other networks (Internet, 3G, 4G, etc.) should be deactivated.

Use of public computers for VPN access to the NFB network is prohibited. Web mail is accepted.

Such use, loans and VPN network access is not an employee right, and the employer reserves the right to prohibit or limit use and/or to impose disciplinary measures on employees should it determine that these privileges are abused.

9.2.5 E-MAIL

The e-mail system (Microsoft Exchange) made available to employees is the property of the NFB

Every user is responsible for the use made of information technology tools placed at their disposal by the NFB.

Since all of these services are the property of the NFB and are to be used only for work purposes, the NFB can, in case of justifiable suspicion of abuse, verify the content of e-mail and Internet usage profiles (e.g. sites visited). Only the Director General, Human Resources, can authorize the Head of IT to perform such verification. Furthermore, if an irregularity or use that contravenes this policy is discovered by chance by an IT department employee, said employee shall bring it to the attention of the Director General, Human Resources.

No inappropriate use, as described below, is acceptable or will be tolerated by the NFB:

- Sending, receiving or storing communications of a discriminatory or troublesome nature, obscene or pornographic material, or visiting of such sites. However, an exception may be granted for film research purposes if the project has been formally authorized and security measures identified in keeping with the IT (example: *Give Me Your Soul*)
- Harassment of any type and in any form whatsoever
- Messages of a defamatory or derogatory nature with regard to a person's race, age, disability, religion, nationality of origin, physical characteristics or sexual orientation; abusive, blasphemous or injurious comments; and hate propaganda
- Use for illegal purposes
- Use contrary to NFB policies or interests
- The disclosure of confidential or personal information covered by the Privacy Act
- Unauthorized use of documents protected by copyright
- Unauthorized use of passwords and encryption keys
- Business solicitation or advertising

Such prohibited usage can result in prosecution and severe disciplinary measures including dismissal.

9.2.6 USE OF THE INTERNET AND WORLDWIDE WEB

To fulfill its mandate and strategic objectives, the NFB makes an array of IT software and applications available to its employees for their activities. These tools shall be used in compliance with the information technology security standards of the Government of Canada as well as in compliance with the Privacy Act. Other software tools and IT applications are available and used by NFB personnel, although they may not fall within the responsibility of the institution. The NFB has established guidelines for the use of such applications (http://photo-images.nfb.ca/uploads/gps/9025.pdf).

Use of Internet applications or Web systems is permitted:

- For work purposes and when the tools offered by the NFB do not meet user needs.
- When Web applications are used, no personal information, as defined by the Canadian Privacy Act, shall be stored or recorded.
- The user shall also ensure that the NFB content used by these Web applications or stored on their servers remains NFB property at all times. The application usage policy must be validated by NFB Legal Services.
- A copy of the components of the work, regardless of the stage of development or phase of production shall be stored on NFB servers if these components are used or stored by external Web applications.
- Users of external Web applications are responsible for ensuring that the service provider implements the means necessary to protect and preserve the information they store (e.g. backups, information access control).
- Use of peer-to-peer sharing for exchange of forbidden files is prohibited.

9.2.7 MODIFICATION

No person shall modify or destroy NFB data, software, software packages, documentation, information systems, information technology or telecommunication equipment without the authorization of the Head of IT or Information Management.

9.3 INFORMATION SYSTEMS

9.3.1 RESPONSIBILITIES

Any section that assumes the management or update of an institutional information system shall designate a person to be responsible for said system. This person shall be responsible for system security.

The administrative authority for each section shall designate a manager to be responsible for any computer network that it manages and/or uses locally.

9.3.2 ACCESS

All institutional information systems shall be protected by an access process requiring a user identification and authentication mechanism. It shall, in addition, limit this access to authorized people only, according to the nature of the information and applications used.

People to be contacted to gain access to the following systems:

- PeopleSoft human resources and pay system: Céline Bernard (Administration, Pay Systems and Services)
- Assignment or delegation of signing authority: Louise LaBrie (Executive Assistant)
- Synchrone: Louise LaBrie (Executive Assistant)
- Oracle Financials systems: Louise LaBrie (Executive Assistant)
- FileMaker databases: Gilles Beauchamp (Analyst, Systems)
- Network access, user accounts and messaging: employee supervisors or consultants shall submit a request to Management using the form available on the Intranet (http://intranet2.nfb.ca/6help/FormulairesInformatiques/en/compteUser.php).

9.3.2.1 GOOD PRACTICE: PASSWORD ACCESS CONTROL

Measures are in place to control and protect user passwords:

- User passwords are private and shall not be divulged.
- Following a predetermined period of inactivity (maximum 15 minutes), the system shall automatically request the user's password again or end the work session. A screensaver that displays a logon screen on resume is recommended.
- Automatic locking of equipment shall be installed on office workstations, notebook computers, smartphones, cell phones and tablets (iPad, Android, etc.).
- The password shall be made up of letters, digits and special characters. It shall be at least eight characters long and be changed every three months. A password history system shall prevent use of the same password. After several unsuccessful access attempts, access shall be blocked.
- The system shall protect the confidentiality of data used to authenticate users and block display and printing of this information.

All network or system managers shall implement adequate control and security measures to ensure the protection and smooth operation of the network.

9.4 INFORMATION

9.4.1 CONFIDENTIALITY

The information stored on NFB information technology and telecommunication assets is confidential if it is of a personal nature (for example employee personal or contact information) or

if it is information the NFB is obliged protect by law, regulation, contract or confidentiality agreement.

No person shall divulge information deemed confidential by the NFB. Examples: a personal telephone number or Social Insurance Number.

9.4.2 RESPONSIBILITIES

Users of information technology and telecommunication assets shall assume responsibility for the accuracy, security, completeness of information and processes performed on the equipment they use. They shall protect the confidentiality of any information they may hold in the course of their duties as a member of NFB personnel, within the framework of a formal agreement with the NFB as a customer or supplier, or as personnel, and, if applicable, shall protect access by all means appropriate (see: 9.3.2.1 Good practice: password access control).

9.4.3 OUTPUT

All output from information technology or telecommunication systems and containing confidential information shall be stored in a secure manner and destroyed in compliance with security, confidentiality and, possibly, archiving standards, when its retention or use is no longer necessary.

9.5 COPYRIGHT

Reproduction of software, software packages, or digitized objects is permitted for backup purposes and shall be governed by the terms of the licensing agreement. Any other reproduction requires the authorization of the right-holder(s).

No person shall use illegal copies of software, software packages or digitized objects on NFB information technology or equipment, on the NFB telecommunication network or on any other IT or telecommunication that does not belong to the NFB but that is used on its premises.

9.6 ELECTRONIC COMMERCE SERVICES

The NFB shall take into account the security implications of creating or using electronic commerce services such as online transactions. The NFB uses recognized security controls in compliance with PCI DSS standards. The above points summarize the above high-level objectives and the intentions of each step for each of the 12 requirements of PCI DSS and their sub-requirements.

9.6.1.1 GOOD PRACTICES: PCI DSS REQUIREMENTS

- Install and maintain a firewall configuration to protect bank cardholder data.
- Do not use supplier default security parameters for passwords.

- Protect stored cardholder data.
- Encrypt transmission of cardholder data via open public networks.
- Use and regularly update antivirus software.
- Develop and maintain secured systems and applications.
- Restrict access to cardholder data.
- Assign a unique identifier to each person having access to a computer or network.
- Restrict physical access to cardholder data.
- Follow and monitor all accesses to network resources and bank cardholder data.
- Regularly test security systems and processes.
- Maintain an IT security policy for employees and contractors.

Each NFB employee as well as consultants, suppliers and subcontractors working for the NFB shall ensure the security of assets and information when using or operating electronic commerce service systems.

Any failure to comply, whether intentional or not, could result in penalties or disciplinary measures including dismissal, depending on the gravity of the situation and/or its consequences.

9.7 EMERGENCY AND SECURITY MEASURES

9.7.1 ACTION COMMITTEE

In the event of an emergency declared by the Departmental Security Officer (DSO), the Action Committee shall intervene. The Committee is made up of the Departmental Security Officer (DSO); Chief Information Officer (CIO); IT Security Coordinator (ITSC) and the Head of IT (HoIT). The Committee shall report its evaluation to the Commissioner, who shall consult with the manager(s) concerned as needed. The Committee shall implement the approved verification procedures. Exceptionally, should the situation require immediate action, the Committee shall take the required measures, which it shall approve as quickly as possible.

During the verification operation, the Committee shall report to the authorities concerned and, if applicable, recommend follow-up.

9.7.2 VERIFICATIONS

Verification of a user's personal information or use of assets can be conducted without the consent of said user should the NFB have serious and sufficient reason to believe that the user is employing

assets, equipment systems or networks in contravention of this policy, the Code of Conduct, the law or NFB regulations. The verification shall be conducted by the Departmental Security Officer (DSO).

Verifications shall be performed on the initiative of the Departmental Security Officer (DSO) when the DSO has good reason to believe that the rules of the policy have been breached or upon request.

Except in the case of a clear emergency, a verification of information technology and telecommunication asset systems for technical reasons, which requires the reading of a user's personal and private information, shall be conducted only by authorized personnel in the course of their duties.

Such verifications shall strictly comply with the standards of the Manager and Action-Committee Member Code of Conduct, as well as with the criteria stated in this policy.

9.7.3 OPERATIONAL CONTINUITY PLAN

The NFB has put in place documented and proven emergency measures to ensure the restoration of operation of institutional information technology and telecommunication facilities considered essential in the event of a major outage (e.g. file, extended electrical blackout, flood, terrorist attack, etc.).

Each division, sector or unit responsible for managing or updating an institutional information system shall put in place backup procedures in order to ensure essential services are maintained in the event of a major local outage.

10 PENALTIES

Any breach of the Code of Conduct, this policy or the resulting regulations shall be subject, in addition to the penalties provided by law, to the following measures:

- Cancellation of rights to access equipment and services covered by this policy
- Reimbursement of all damages the NFB is required to pay following the unauthorized, fraudulent or illicit use of its information technology or telecommunication services or assets
- Disciplinary measures or other penalties indicated in the HR guide, or applicable under the collective labour agreements and protocols in force.

11 SECURITY INVESTIGATION

All employees who have access to information systems containing protected or classified information shall be subject to a security investigation and shall obtain the appropriate clearance (Analyst, DBA, IT Technician, etc.).

12 MODIFICATION

This policy shall be evaluated annually in order to adjust to new practices and technologies used at the NFB.

Any change to this policy must be approved by the Commissioner of the NFB upon recommendation by the Departmental Security Officer (DSO).