



Northumberland

Community Futures Development Corporation
Société d'aide au développement des collectivités

Information Security Policy

1.0 General	1
2.0 Definitions.....	2
3.0 Information Security Requirements.....	4
3.1. Privacy & Confidentiality	4
3.2. Northumberland Business Development Assistance Corp. Property	4
3.3. Identification & Authentication	5
3.4. Use of Northumberland Business Development Assistance Corp. Computers	5
3.5. Access to Northumberland Business Development Assistance Corp. Information or Computers.....	6
3.6. Software	7
3.7. Internet Communications.....	8
3.8. Physical Security	9
3.9. System Risk Management	9
3.10. Monitoring.....	10
4.0 Exceptions to Policy.....	11
5.0 Non-compliance With Policy	12
Annex A - Password Standards.....	13

1.0 General

The Northumberland Business Development Assistance Corp. has adopted this Information Security Policy to ensure that adequate protection measures are taken to assure the confidentiality and integrity of the information held by Northumberland Business Development Assistance Corp. and the security of the computer system to include hardware, software, and storage devices such as disks, CDs and backup systems.

This Policy applies to Users with respect to their access to, and use of, Northumberland Business Development Assistance Corp.-held information as well as access to hardware, software or network facilities owned or controlled by Northumberland Business Development Assistance Corp. With respect to employees, this Policy is also to be read in conjunction with and form a part of Northumberland Business Development Assistance Corp.'s *Employee Handbook*. All new employees and contractors shall receive a copy of this Policy upon employment or engagement.

In the event of questions about this Policy, please contact:

Chief Privacy Officer
Northumberland Business Development
Assistance Corp.
1005 Elgin St., Suite 206
Cobourg, Ontario
Fax: (905) 372-2238

K9A 5J4
E-mail: cpo@northcfdc.ca
Telephone number: (905) 372-8315

2.0 Definitions

“Availability” means information being accessible as required.

“Confidential Information” means Personal Information; Northumberland Business Development Assistance Corp. business, tax or accounting information; employee information and disciplinary files, and archived information pertaining to former members or employees.

“Confidentiality” means the restriction of access to information only to those having a business reason to have such access as authorized by the appropriate manager within Northumberland Business Development Assistance Corp. or the client concerned. Exceptions should be forwarded to the Chief Privacy Officer.

“Disruption of network communication” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

“Integrity” means the information in question has not been modified in an unauthorized manner.

“Internet communications” means existing and future communication protocols and services including but not limited to the World Wide Web; electronic mail (“e-mail”); Instant Messaging; Internet Relay Chat; any intranet that Northumberland Business Development Assistance Corp. establishes or participates in; any proprietary data transfer protocols utilized by Northumberland Business Development Assistance Corp. in communications with others; File Transfer Protocol, TELNET and Usenet news groups.

“Members” mean an employee, officer, director or other type of member of Northumberland Business Development Assistance Corp.

“Personal Information” means any information, recorded in any form, about an identified individual, or an individual whose identity may be inferred or determined from the information.

“Security breaches” means accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these activities are within the scope of regular duties.

“User” means an individual, whether an employee, officer, director or other type of member of Northumberland Business Development Assistance Corp. who creates or accesses information on Northumberland Business Development Assistance Corp.-owned or controlled Computer System; or a computer program or application operating pursuant to an individual or organization (e.g. electronic agent).

3.0 Information Security Requirements

3.1. Privacy & Confidentiality

Users with access to Personal Information shall respect the confidentiality of that information and adhere to the requirements of Northumberland Business Development Assistance Corp.'s *Privacy Policy* and Northumberland Business Development Assistance Corp.'s *Employee Information Privacy Policy*.

Users with access to other types of Confidential Information shall respect the confidentiality of that information and not disclose such information unless specifically authorized to do so.

Each User that accesses information held by Northumberland Business Development Assistance Corp., whether owned by the Northumberland Business Development Assistance Corp. or not, regardless of form (e.g. paper or electronic) or format, shall protect that information against accidental or deliberate disclosure or destruction. Modification to the information shall be completed as per established and accepted Northumberland Business Development Assistance Corp. policies and procedures.

Confidential Information shall be:

- Physically protected through the use of locked cabinets or offices and/or technologically protected using Computer System access controls;
- Accessible for review by employees as authorized by Northumberland Business Development Assistance Corp. management;
- Corrected or marked with appropriate notation in the event inaccuracies in the information are identified; and
- Retained for such retention periods as required by law or as identified by Northumberland Business Development Assistance Corp. management.

3.2. Northumberland Business Development Assistance Corp. Property

All information and/or messages composed, sent or received using Northumberland Business Development Assistance Corp.'s computers are the property of Northumberland Business Development Assistance Corp. and may be reviewed, audited, accessed and disclosed for any purpose considered appropriate by Northumberland Business Development Assistance Corp. management. **USERS SHOULD NOT HAVE ANY EXPECTATION OF PRIVACY WITH RESPECT TO SUCH MESSAGES.** See also Section 3.10 Monitoring.

Unless contractual or licensing arrangements govern, any data or software downloaded using Internet communications into Northumberland Business Development Assistance Corp. computers becomes the property of Northumberland Business Development Assistance Corp. and may be retained, removed or destroyed at the sole discretion of Northumberland Business Development Assistance Corp. management.

3.3. Identification & Authentication

Each User shall be assigned a unique identifier ("User ID") and will be required to authenticate themselves prior to gaining access to Northumberland Business Development Assistance Corp. computers or networks. Users shall not log on to Northumberland Business Development Assistance Corp. computers using another User's User ID. **EACH USER SHALL BE RESPONSIBLE FOR ALL ACTIVITY CONDUCTED UNDER THEIR ASSIGNED USER ID.**

Associated with each User ID will be a password generated to authenticate a User prior to accessing any application, system, network or remote connection. A User shall adhere to the requirements of Annex A Password Standard. All default passwords and access codes on vendor-supplied hardware and software shall be changed prior to use by Users.

The System Administrator shall have a separate Administrator User ID and password. Administrator User IDs shall only be used for system administration purposes.

The Administrator's User ID and password shall be changed immediately upon (a) the installation of any system; and (b) immediately after use by service personnel. The administrator's password shall be documented and stored in a secure location.

Where non-specific User accounts are required, they shall be assigned to a specific User for accountability purposes. The purpose of the account shall be documented and the password associated with the account changed when a User who knows the password is no longer an employee or a contractor of Northumberland Business Development Assistance Corp.

User IDs shall be deleted from an Northumberland Business Development Assistance Corp. computer upon the termination of a User's employment or, in the case of contractors, contract. User IDs that are inactive for thirty days shall be disabled and removed.

3.4. Use of Northumberland Business Development Assistance Corp. Computers

The Northumberland Business Development Assistance Corp. shall provide employees and managers, and may (but is not required to) provide other Users, with workstations for the purposes of their activities with the Northumberland Business Development Assistance Corp. **USERS SHALL BE RESPONSIBLE AND ACCOUNTABLE FOR THEIR ACTIONS while using Northumberland Business Development Assistance Corp. hardware, software or networks, or components thereof, including desktop or laptop computers or personal digital assistants (PDAs) owned, leased or controlled by Northumberland Business Development Assistance Corp..**

Users shall use Northumberland Business Development Assistance Corp. computers primarily for business purposes. Limited and reasonable personal use of the Northumberland Business Development Assistance Corp. computers is permitted provided such use:

- a. Is not for non-Northumberland Business Development Assistance Corp. commercial purposes or personal gain;

- b. Does not:
 - i) Adversely affect the primary business use of the computer or Northumberland Business Development Assistance Corp. network;
 - ii) Conflict with a Northumberland Business Development Assistance Corp. business objective or policy;
 - iii) Consume a large amount of Northumberland Business Development Assistance Corp. computer resources;
- c. Complies with applicable law.

Northumberland Business Development Assistance Corp. management shall be solely responsible for any determination as to what constitutes limited and reasonable personal use.

Under no circumstances is a User authorized to engage in any activity that is illegal under the laws of Ontario and Canada while utilizing the Northumberland Business Development Assistance Corp. computers.

Users shall not harm or destroy, or attempt to harm or destroy, hardware, software or data on any Northumberland Business Development Assistance Corp. computer, other than their own data in the course of editing such material.

Users shall not load, install or activate, or attempt to load, install or activate onto Northumberland Business Development Assistance Corp. computers any unauthorized hardware, including, but not limited to, modems, data scopes, line monitors, nodes, gateways or bridges of any kind.

Users of Northumberland Business Development Assistance Corp.-owned or controlled portable devices (e.g. laptops, PDAs), if supplied with such equipment, shall not leave such equipment unattended when outside Northumberland Business Development Assistance Corp. offices. Information contained on such devices must be protected from unauthorized access using power-on passwords or passphrases and password or passphrase-enabled time-out or lock-out features.

3.5. Access to Northumberland Business Development Assistance Corp. Information or Computers

User access to Northumberland Business Development Assistance Corp. information or to Northumberland Business Development Assistance Corp. computers shall be on an "as authorized" basis in order to accomplish Northumberland Business Development Assistance Corp. business objectives. Networks shall have routing controls to ensure connections and information flows do not have unauthorized access to Northumberland Business Development Assistance Corp. information.

Any computer or portable device with a modem operating in "inbound mode active" (permitting external callers to connect to the device using that modem) shall not be simultaneously connected to both a Northumberland Business Development Assistance Corp. network and any external network.

3.6. Software

Only software approved for deployment by Northumberland Business Development Assistance Corp. management is permitted on any Northumberland Business Development Assistance Corp. computer or network. Downloading software programs (e.g. screen savers, audio software and messaging software) from the Internet is not permitted. All other file types downloaded from the Internet must be scanned with anti-virus software before being stored on Northumberland Business Development Assistance Corp. computers. If a User has a business requirement to download software from the Internet or to otherwise load non-Northumberland Business Development Assistance Corp. standard software, Section 4.0 Exceptions to Policy will govern.

Virus detection software shall be installed and regularly updated on Northumberland Business Development Assistance Corp. computers and networks. Users are required to report any known or suspected virus incidents to the System Administrator.

Opening e-mail attachments with “.exe” or “.com” extensions (including trial versions of software) is not permitted.

Any application to be purchased, whether custom-developed or commercially available, shall have authentication and access controls. The application should ensure that, with respect to the information it stores, the application shall maintain the integrity of the data.

Users shall report any observed or suspected software malfunctions but shall not attempt to remove the software in question unless authorized to do so.

3.7 Internet Communications

Northumberland Business Development Assistance Corp. may provide all Users with Internet access for business and limited personal purposes. Northumberland Business Development Assistance Corp. may also provide e-mail addresses with "@northcfdc.ca" to employees. Accordingly, the use of Northumberland Business Development Assistance Corp. resources that identify a user with Northumberland Business Development Assistance Corp. must be done in a manner that reflects well on the organization. All access to the Internet shall be done via approved Northumberland Business Development Assistance Corp. gateways and in a manner consistent with this Policy. Managers and employees must understand that Internet access is to be treated as a privilege that may be revoked at any time in the event of a failure to comply with this Policy. Withdrawal of access to the Northumberland Business Development Assistance Corp. network or the Internet may occur whether or not disciplinary action is taken.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use of Northumberland Business Development Assistance Corp.'s computers. In the absence of applicable Northumberland Business Development Assistance Corp. policies or if there is any uncertainty, Users should consult their General Manager or the Chief Privacy Officer.

The following system and network activities are expressly prohibited:

1. Installing or distributing "pirated" or other software products that are not appropriately licensed for use by Northumberland Business Development Assistance Corp.;
2. Copying and/or distributing material not authorized by Northumberland Business Development Assistance Corp. management including, but not limited to, music, text or photographs from magazines, books or other copyrighted sources;
3. Providing information about, or lists of, Northumberland Business Development Assistance Corp. employees to parties outside Northumberland Business Development Assistance Corp.;
4. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
5. Using an Northumberland Business Development Assistance Corp. computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws under the laws of Ontario and Canada;
6. Making fraudulent offers of products, items, or services;
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties;
8. Causing security breaches or disruptions of network communication;
9. Intercepting data not intended for the User's host computer, unless this activity is a part of the employee's normal job/duty;
10. Circumventing User authentication or security of any computer or network account;
11. Interfering with or denying service to any user other than the User's host (for example, denial of service attack);
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's use of a computer;

13. Exporting or importing software, technical information, encryption software or technology, in violation of applicable Canadian import and export control laws; and
14. Using an unassigned "User ID" and/or password.

The following communication activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material;
2. Harassing Northumberland Business Development Assistance Corp. employees or employees of members or third parties via email, telephone or paging, whether through language, frequency, or size of messages;
3. Forging email header information;
4. Soliciting email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type; and
6. Posting the same or similar non-business-related messages to large numbers of newsgroups or web sites.

Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

3.8 Physical Security

Computers located within Northumberland Business Development Assistance Corp. are to be located in areas that have appropriate physical security controls, including but not limited to, keys or combination locks, access logs and alarms. Users whose employment or contract is terminated shall return all keys assigned to them. A log of office keys shall be maintained by the Chief Privacy Officer who shall also have responsibility for the issuance and retrieval of keys.

Storage media shall be protected from environmental threats such as temperature, humidity and magnetism. All media containing Confidential Information shall be sanitized or destroyed before release for disposal to ensure that data recovery from such media is not possible.

Equipment shall not be removed from the Northumberland Business Development Assistance Corp. offices or facilities without permission.

3.9 System Risk Management

Any new computer system or modification to existing Northumberland Business Development Assistance Corp. computers or network shall be assessed for risk prior to deployment. Such a risk assessment shall examine any potential consequences of a loss of confidentiality, integrity or availability of Northumberland Business Development Assistance Corp. information or other assets, and the realistic likelihood of a loss occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented. This risk assessment may be completed by the System Administrator or

such person(s) as the General Manager believes is appropriate to conduct such an assessment.

3.10 Monitoring

The Northumberland Business Development Assistance Corp. reserves the right to monitor computers or networks to ensure compliance with this Policy. For security and network maintenance purposes, authorized individuals within Northumberland Business Development Assistance Corp. may monitor and access equipment, systems and network traffic at any time.

Such access may include:

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Northumberland Business Development Assistance Corp. computers or property;
- Access to work areas (offices, cubicles, storage areas, etc.).

For Northumberland Business Development Assistance Corp. computers important to the activities of Northumberland Business Development Assistance Corp., at a minimum, the following information shall be recorded either electronically or manually:

- Login and logout attempts;
- Unauthorized attempts to access system files;
- Attempts to create, remove, set passwords or change the system privileges of system administrators;
- System alerts or failures; and
- System configuration changes and maintenance information.

All logs, whether electronic or manual, must contain the date and time of the event and the User ID which caused the event and are to be reviewed, at a minimum, on a monthly basis.

Where a computer records information that is required to be logged and operates a clock, that computer's clock should be set, as required, to Standard Time or Daylight Savings Time in Ontario. Computer system clocks shall be checked every 60 days as to their accuracy.

Logs are to be protected against unauthorized changes or operational failures (e.g. logging media exhausted; failing to record events or overwriting itself).

Monitoring tools and systems audit processes are to be configured so as to only allow designated personnel to change such tools and processes.

Audit logs shall be archived monthly and retained according to Northumberland Business Development Assistance Corp.'s *Records Retention Policy*.

Security processes and controls are to be audited annually.

4.0 Exceptions to Policy

Exceptions to any policy requirement stated in Section 3 may be permitted if:

- An appropriate business reason is provided;
- The request is approved by the General Manager or Chief Privacy Officer; and
- The User making the request accepts all responsibility for any additional risk created by the exception.

5.0 Non-compliance With Policy

While records of communications can be created for monitoring and review purposes, Northumberland Business Development Assistance Corp. will not actively monitor the communications of Users. However, the Northumberland Business Development Assistance Corp. may do so upon suspicion or evidence of a breach of any law or the Northumberland Business Development Assistance Corp. policy and any past communication may be examined in the course of an investigation of a security breach or in the course of disciplinary action. See Section 3.2.

Any User who disregards, disobeys, disables or circumvents any element of this Policy or any security mechanism, or who attempts to do so, shall be subject to disciplinary action, up to and including termination of employment or, in the case of contractors, termination of contracts. Users should also note that, if circumstances warrant, an incident may be referred to the appropriate authorities for prosecution.

Northumberland Business Development Assistance Corp. reserves the right to restrict any User's access to Northumberland Business Development Assistance Corp. information or computers.

Agreements with external vendors or suppliers shall require compliance with this Policy in the event of use of Northumberland Business Development Assistance Corp. computers or networks by such vendors or suppliers, or employees or agents, thereof.

Annex A - Password Standards

- 1) Passwords should never be written down or stored on-line. ***
- 2) Do not use the same password for Northumberland Business Development Assistance Corp. accounts as for other non-Northumberland Business Development Assistance Corp. accounts (e.g., personal ISP account).
- 3) Where possible, don't use the same password for different access needs within the Northumberland Business Development Assistance Corp. systems. For example, select a separate password to be used to access the TEA network as is used for access to Windows.
- 4) All passwords are to be treated as sensitive, Board Confidential Information.
- 5) Do not hint at the format of a password in any conversation or communication (e.g., "my family name").
- 6) Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).
- 7) Do not reveal a password:
 - a) Over the phone to ANYONE;
 - b) In an email message;
 - c) In front of others;
 - d) To family members or co-workers; or
 - e) On questionnaires or forms.

*** Alternative solution

- 1) Individuals could write down their passwords, place them in a sealed envelope with their name and the date and provide these to the Chief Privacy Officer for storage in a locked fire-proof cabinet. The process is then undertaken each and every time an individual changes any of their passwords.