



## **Background**

The Board of Trustees believes that computer systems are purchased for, and a Wide Area Network is established, for the educational and professional use of Northland's students, teachers and staff. The Board believes that use of the network is a privilege and that the Superintendent will regulate access to and use of the network by principles consistent with the Board's mission.

1. Network users are expected to conduct themselves on the network in the same fashion as they do elsewhere in the community, conforming to the laws, guidelines, rules and expectations in place that regulate person-to-person communication.
2. Users are expected to avoid actions that are illegal or unkind.
3. Users found to be in willful and/or persistent violation of these guidelines will have their network privileges revoked and may face further disciplinary action.
4. While the Board believes that the individual user is responsible for his/her actions, a safe electronic environment, especially for students in elementary grades, will be enhanced by the use of network management software that will be used to block and/or filter and/or monitor inappropriate content.
5. The Superintendent may designate the supervision of computers and networks to administrative staff, including principals, supervisors and technicians and require users to acknowledge acceptance of responsibility for appropriate use by signing a user agreement.

## **Procedures**

1. The Board acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control. Under the direction of the Superintendent, the obligation is shared, to varying degrees, by all administrators, teachers and students of the Division.



- 1.1 The superintendent will ensure that a long-range technology plan as part of the division's educational planning has been prepared and is kept current. The technology plan shall include the following keeping in mind the financial resources of the division:
  - 1.1.1 Provision for new hardware, hardware upgrading, and existing hardware reconditioning and upgrading.
  - 1.1.2 Attention to software copyright and licensing.
  - 1.1.3 The need for teacher resource material and in-service.
  - 1.1.4 A review of the computer hardware, software and network standards within the division.
  - 1.1.5 Standards for appropriate use by students and staff.
  - 1.1.6 Procedures for dealing with major disruptions to the system and a listing of appropriate staff members to contact for assistance.
  - 1.1.7 A disaster recovery plan which identifies the proper procedures to be followed.
  - 1.1.8 Survey Instruments to be used to gather information from staff and students relative to the use and quality of the technology system.
  - 1.1.9 Standards for appropriate use by students and staff.
  - 1.1.10 Procedures for dealing with major disruptions to the system and a listing of appropriate staff members to contact for assistance.
  - 1.1.11 A disaster recovery plan which identifies the proper procedures to be followed.
  - 1.1.12 Survey Instruments to be used to gather information from staff and students relative to the use and quality of the technology system.
  - 1.1.13 Consult with parents to ensure that an agreement is reached regarding the limits to student use of computer equipment.
  - 1.1.14 Ensure that students who are allowed to use the Internet and connected services are properly supervised and made aware of expectations for proper use.



- 1.1.15 Advise parents of their responsibilities in cases where instruction may be delivered at home.
- 1.2 The technology plan adopted at the school level should provide for the following:
  - 1.2.1 The opportunity for all students to develop computer literacy skills in the use of computer networks during their school program.
  - 1.2.2 The development of computer skills and knowledge of computer functions and applications shall be provided to students in an appropriately sequenced manner throughout all program levels.
  - 1.2.3 The provision for ensuring that all students receive training regarding procedures, ethics and security involving the use of the internet and connected services.
- 1.3 All users of the technology systems are to be made aware that:
  - 1.3.1 The Internet shall not be used for private or business use or political purposes.
  - 1.3.2 All accounts and passwords are to be kept confidential and not shared or made accessible to others, or left open on the system..
  - 1.3.3 The use of programs that harass Internet users or infiltrate a computing system and/or damage the software components is prohibited.
  - 1.3.4 The division and administration will assume no responsibility or liability if documents stored on division equipment are lost or damaged, nor will the division be responsible for security violations beyond the appropriate response to those persons involved in such violations.
- 1.4 Network cabling shall be installed subject to electrical code standards, and that this installation will not affect the cosmetic look of the school.



## Procedure 129

### Use of Technology

---

2. For the purpose of administering these Procedures, individual employees of the Division who have been designated by the Superintendent with the responsibility for the supervising computer use by students, teachers or staff are deemed to be "systems administrators".
  - 2.1 Network users are expected to avoid actions that are illegal such as libel, slander, vandalism, sexual harassment, theft, inappropriate access, or unkind actions such as personal attacks (flaming), invasion of privacy, as described under Unacceptable Use of Computers. All students and parents will be expected to sign a "Student User Agreement and Parent Permission Form" Form No. J740-09-04, for each of their children.
  - 2.2 Unacceptable Use includes:
    - 2.2.1 Slander and Libel -These terms are defined specifically in law. In short, slander is "Oral communication of false statements injurious to a person's reputation." Libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." In effect, users must remember that material distributed through the 'Net' is "public" to a degree that no other school publication or utterance is. Any such remark may be seen by millions of people and harmful and false statements will be viewed in that light.
    - 2.2.2 Vandalism - Vandalism refers to deliberate attempts to damage the hardware, software, or information residing on any school or district network or any other computer system attached through the network or Internet. Attempts to violate the integrity of private accounts, files or programs, the deliberate infecting of the network with a computer "virus," attempts at "hacking" into any of the computers using any method, or other such actions will not be tolerated.
    - 2.2.3 Invasion of Privacy - Users are entitled to a reasonable expectation of privacy for their files and e-mail. No user



may have access to another's private files. The systems administrator will access the private files of users only to purge them or in the event of a suspected or proven violation of school and Division rules or expectations.

- 2.2.4 Theft - The Internet is the repository of incredible amounts of information. Much of that information has been placed there for the free use of users. Law, ethics, and common courtesy require that proper acknowledgment of the use of the intellectual property of others must be made. Users should treat information found electronically in the same way they do information found in printed sources. Students will be made aware of commonly held rules against plagiarism and that these rules will be enforced by teachers. Many programs reside on the Internet. It is the responsibility of each user to comply with the requirements of the owners of the software regarding its acquisition and use. Northland School Division No. 61 will not tolerate the use of its systems for the illegal copying or storing of illegally acquired software and other inappropriate material including the downloading of music and video files.
- 2.2.5 Harassment - Users may not use the computers to harass others, either within the Northland community or in the broader Internet. Foul and abusive language, attempts to "fill" electronic mailboxes, the posting of obscene images or texts and "flames" will not be tolerated. Users should ask themselves if the information they are posting or sending would be acceptable if displayed or stated in public meeting or published in a local newspaper.
- 2.2.6 Inappropriate Access - Users may not use the Northland School Division Network to access inappropriate or "adult" materials found on the Internet. Users not exercising responsibility by accessing such materials will lose all computer access and have their accounts revoked.



- 2.2.7 Chain Letters and other "Spreading" Schemes - Whether in e-mail or in Usenet newsgroups, chain letters, pyramid schemes, forwarding or replying to "contests," "fast cash" schemes, mass cross-postings, and uninvited mass mailings are all highly wasteful of network resources and expressly forbidden on the Northland School Division Network. Users participating in such activities may have their e-mail addresses permanently revoked.
- 2.2.8 The right of appeal may be exercised by an employee or by the parent of guardian on behalf of a student. Appeal procedures shall be conducted in the same manner as any other disciplinary matter as per the Collective Agreement, Administrative Procedure 403 or school discipline policy.

### 3. Student Computer Use Guidelines

- 3.1 Northland's students have the opportunity to access technology to facilitate information gathering and communication skills. The following statements apply to all users when they access any Northland technology:
  - 3.1.1 The use of computer workstations is a privilege, not a right, and inappropriate use will be dealt with seriously. Violators will lose computer privileges.
  - 3.1.2 First priority for use of the workstations will be given to those users who have an educational need.
  - 3.1.3 Copyright laws protect software. No unauthorized copies of software or documents will be allowed on school computers. Users will not give, lend, or sell copies of software to others unless they have the written permission of the copyright owner or the original software is clearly identified as shareware or in the public domain.
  - 3.1.4 Users are expected to abide by the accepted rules of network etiquette. These include the following:



## Procedure 129

### Use of Technology

---

- 3.1.4.1 Students must be polite. They cannot be abusive in messages to others.
- 3.1.4.2 Students may not swear, use vulgarities or any other inappropriate language. Illegal activities, that is, actions considered to be a criminal offence, are strictly prohibited.
- 3.1.4.3 Students will not reveal personal information about themselves or others over the Internet such as name, phone number and address
- 3.1.4.4 Students may not access or alter other users' work.
- 3.1.4.5 Students are not allowed to access chat rooms at school.
  
- 3.1.5 Users may not move, repair, reconfigure, modify, or attach external devices to the system.
  
- 3.1.6 Users may not vandalize computers. Vandalism is defined as any malicious attempt to harm or destroy data of another user. This includes, but is not limited to, the creation or intentional spreading of computer viruses. Vandalism will result in cancellation of privileges.
  
- 3.1.7 Users may not use electronic mail and other network communication facilities to harass, offend or annoy other users of the network. Each user has the responsibility to report all violations of privacy. All mail received through e-mail accounts is the responsibility of the user, and only those contacts leading to appropriate educational growth on the Internet are permitted. Incoming and outgoing e-mail may be monitored and/or approved by the teacher or the system administrator.
  
- 3.1.8 The systems administrator has the right to monitor all accounts and read all e-mail messages.



## Procedure 129

### Use of Technology

---

- 3.1.9 Any attempt to circumvent system security, guess passwords or gain unauthorized access to any workstation is forbidden. Any user who can identify a security problem must notify the system administrator. Such information will be considered confidential.
- 3.1.10 Only the students under the active supervision of a teacher are allowed access to the Internet.
- 3.1.11 Students must provide bibliographic information of all materials downloaded from the Internet. Citation methods are expected to be age appropriate; this is one of the skills noted in the ICT Program of Studies.
- 3.1.12 Network users must keep all inappropriate material from entering any school workstation.
- 3.1.13 Use of the Internet for commercial gain or for personal/business use is not allowed from an educational site.
- 3.1.14 Additional rules and restrictions may be added by the local systems administrator at any time. Users are responsible for reading and following these rules.

#### 4. Staff Computer Use Guidelines

- 4.1 Northland's staff is provided access technology to facilitate student instruction, model appropriate technology use, communicate efficiently and perform their day-to-day job functions. The following statements apply to all users when they access any Northland technology:
  - 4.1.1 Copyright laws protect software; therefore, no unauthorized copies of software or documents will be used on divisional computers. Users will not give, lend, or sell copies of software to others unless they have the written



permission of the copyright owner or the original software is clearly identified as shareware or in the public domain.

- 4.1.2 Users are expected to abide by the generally acceptable rules of network etiquette. These include (but not limited to) the following:
  - 4.1.2.1 Be polite. Do not be abusive in your messages to others.
  - 4.1.2.2 Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly prohibited.
- 4.1.3 Use of electronic mail and other network communication facilities to harass, offend or annoy other users of the network is forbidden. Each user has the responsibility to report all violations of privacy. All mail received through e-mail accounts is the responsibility of the user.
- 4.1.4 The system administrator or superintendent has the right to monitor all accounts and read all e-mail messages.
- 4.1.5 Any attempt to circumvent system security is forbidden. A user, who feels he/she can identify a security problem, must notify the system administrator. Such information shall be considered confidential.
- 4.1.6 No inappropriate material may be kept on any workstation.
- 4.1.7 Use of the Northland technology for commercial gain or for personal/business use is not permitted. Employees may use Northland computer systems outside of normal working hours for furthering their education, training and developing software, teaching materials and the like.



4.1.8 Any software, manuals, teaching resources and the like that are created as part of an employee's normal work shall have the copyright held by the Division with credit to the author(s). Intellectual property created outside the normal scope of employment and outside of normal working hours should acknowledge the use of Northland's resources.

4.1.9 Users are responsible for reading and following these guidelines.

5. Desktop Computer Security Guidelines:

5.1 Definition

5.1.1 "Desktop computers" are personal workstations that, though possibly linked to other computers via a Local Area Network, can function as stand-alone units. Desktop computers include IBM-compatible PC's, Macintoshes, and Unix Workstations.

5.1.2 "Users" are persons who use a desktop computer workstation from time-to-time. A user who uses the same computer on a day-to-day basis or a teacher who has designated a supervisory role for the computers in a classroom or lab is considered the "custodian" for those systems.

5.2 General Obligations

Users and custodians of Desktop computers are subject to the Division's "Acceptable Use Policy" and must have signed "User Agreement" on file at the user's usual place of work or study.

5.3 Hardware Security

5.3.1 Keys to rooms, cabinets and equipment should be clearly marked and secured when not in the possession of the system custodian.

5.3.2 Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.



- 5.3.3 External devices such as scanners and hard disks should be secured against access, tampering, or removal.
- 5.3.4 Equipment should be marked with asset tags provided by the Division.
- 5.3.5 Computers should be located away from environmental hazards.
- 5.3.6 Critical data, backup media should be in fireproof vaults or in another building. This includes student databases such as Maplewood and financial management data.

**5.4 Access Security**

- 5.4.1 Utilize password facilities to ensure that only authorized users can access the system. Where the Desktop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures.
- 5.4.2 Password guidelines:
- 5.4.3 Passwords should be eight characters in length
  - 5.4.3.1 Use a mixture of letters and numbers.
  - 5.4.3.2 Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords should not be maiden names, or names of children, spouses, or pets.)
  - 5.4.3.3 Do not write passwords down anywhere.
  - 5.4.3.4 Never store passwords or any other confidential data or information on your laptop or home PC or associated floppy disks or CD's.
  - 5.4.3.5 Change passwords every three months.
  - 5.4.3.6 Do not include passwords in any electronic mail message.



5.5 Data and Software Integrity

5.5.1 Back up and store important records and programs weekly.

5.5.2 Check data and software integrity.

5.5.3 Fix software problems immediately.

5.6 Confidential Information

5.6.1 Encrypt sensitive and confidential information where appropriate.

5.6.2 Monitor printers used to produce sensitive and confidential information.

5.6.3 Overwrite sensitive files on fixed disks, floppy disks, or cartridges.

5.7 Software Licenses

5.7.1 Copyright law protects software. Unauthorized copying is a violation of the Acceptable Use policy. Anyone who uses software should understand and comply with the license requirements of the software. The Division may be subject to random license audits by software vendors. Check all files downloaded from the Internet. Do not download shareware files.

5.8 Viruses

5.8.1 Computer viruses are self-propagating programs that infect other programs. Viruses, Trojan horses, and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.



5.8.2 To decrease the risk of viruses and limit their spread:

5.8.2.1 Check all software before installing it.

5.8.2.2 Use software tools to detect and remove viruses.

5.8.2.3 Isolate immediately any contaminated system.

**6. Disaster Recovery Procedures**

**6.1 Definition**

6.1.1 A disaster is an event that renders a desktop computer fully unusable for its intended purpose. The event may be limited to a single system when one or more components fail or be part of a larger event affecting the site.

6.1.2 The scope of the computer system failure is such that it cannot be remedied by normal user-initiated maintenance.

**6.2 Notification**

6.2.1 Documented (e-mail/fax/letter) notification from the user to a technician should be initiated by system custodian and include the principal or department head.

**6.3 Hardware Repair/Replacement**

6.3.1 Technicians will make all reasonable effort to restore the system to full operating condition in a timely manner. The technician will advise the principal or administrator who has budget responsibility at the facility of the cost and timeline to affect repair.

**6.4 Software Restoration**

6.4.1 The technician will re-install operating system and commonly used software from originals carried by the technicians. Software specific to the site or workstation will be restored from original installation programs that have



been securely stored on site. User-created files will be restored from the latest available backup.

7. Network Security Guidelines:

7.1 Definition

7.1.1 "Desktop computers" are personal workstations that, though possibly linked to other computers via a Local Area Network, can function as stand-alone units. Desktop computers include IBM-compatible PC's, Macintoshes, and Unix Workstations.

7.1.2 "Users" are persons who use a desktop computer workstation from time-to-time. A user who uses the same computer on a day-to-day basis or a teacher who has designated a supervisory role for the computers in a classroom or lab is considered the "custodian" for those systems.

7.2 Computer Network Security

7.2.1 Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

7.2.2 While the technicians have responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment. The systems administrator shall be responsible for backing up the network server files daily.

7.2.3 Considerations and procedures for maintaining security on the network are the same as those stated for desktop computer security.



7.3 Disaster Recovery Procedures

7.3.1 Disaster recovery procedures are the same as those stated for desktop computer disaster recovery.

8. Security Guidelines for School-Based Servers

8.1 Definition

8.1.1 "School-Based Servers" are non-strategic servers (i.e. not critical to Northland School Division No. 61 as a whole) that are the responsibility of schools or remote offices.

8.2 Management of School-Based Servers

8.2.1 Responsibility for the management and operation (i.e. custodianship) of school-based servers resides with the school that owns the system.

8.3 Security Responsibilities

8.3.1 The day-to-day custodians of school-based servers must:

8.3.1.1 Be familiar with the requirements for maintaining the physical security of server systems and the methods for keeping data secure.

8.3.1.2 Ensure compliance to this practice by all of its users.

8.3.1.3 Report any serious breaches of security to the Principal and/or Superintendent.

8.4 Physical Security

8.4.1 The following standards of physical security of school-based servers must be met:

8.4.1.1 Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, or other environmental contaminants.

8.4.1.2 There must not be an inordinate amount of combustible material (e.g. paper) stored in the same room as the computer system.

8.4.1.3 Air temperature and humidity must be controlled to within acceptable limits.



8.4.1.4 Computing equipment should be electrically powered via an Uninterruptible Power Supply to provide the following:

8.4.1.4.1 Minimum of 15 minutes' operation in the event of a power blackout.

8.4.1.4.2 Adequate protection from surges and sags.

8.4.1.4.3 Trigger an orderly system shutdown when deemed necessary.

**8.5 Physical Access**

8.5.1 There must be procedures in place to assure that only authorized staff has access to the servers.

**8.6 Fire Detection and Control**

8.6.1 There should be smoke and thermal detectors on the premises and under-floor areas should have smoke and water detectors.

**8.7 User Access**

8.7.1 New user ids should be handled as follows:

8.7.1.1 A written record of users should be maintained.

8.7.1.2 An "Acceptable Use Agreement" should be signed and on file before a new user id is issued.

8.7.1.3 The new user id and password must be given orally to the applicant, unless special delivery has been authorized due to special circumstances.

8.7.1.4 If the Operating System supports a password aging facility, then it should be set to force password change on the first login.

**8.8 Data Integrity**

8.8.1 Security backups of all data should be made at least once per working day.



- 8.8.2 The backup regime should meet the following criteria:
  - 8.8.2.1 Enable recovery to at least the start of business on any weekday of a failure.
  - 8.8.2.2 Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.
  - 8.8.2.3 There should be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.
  - 8.8.2.4 There should be an audit of security backup media at least once every six months.
- 8.8.3 A backup regime utilizing online secure mass storage may be used that meets the following criteria:
  - 8.8.3.1 Enable recovery of documents and user-created data to the end of the day previous to a failure.
  - 8.8.3.2 Provide an additional level of backup of to end of the previous business week of documents and user-created data.
  - 8.8.3.3 Enable recovery or offsite operation of business-critical applications.
- 8.8.4 Password Aging
  - 8.8.4.1 If the Operating System provides the ability for automatic Password Aging, this will be enforced. The life of a password shall be three months.
  - 8.8.4.2 If there is no Automatic Password Aging the systems administrator shall notify users to change passwords every three months.
- 8.8.5 Documentation
  - 8.8.5.1 A printed copy of this document shall be provided to the person(s) charged with the responsibility for day-to-day operation (custodianship) of the school-based server.



9. Disaster Recovery Procedures

9.1 Definition

A disaster is an even that renders a school-based server fully unusable for its intended purpose. The event may be limited to the server itself when one or more components fail or it may be part of a larger event affecting the site.

9.2 Notification

Telephone notification to the Computer Technician should be made by the principal or system custodian and be followed up by documented notice (email/fax/letter). The scope of the event may include notification to the Superintendent as well.

9.3 Business Continuity

When a disaster occurs, the principal and/or system custodian will assess the ability of the school to continue operation with consideration for:

9.3.1 Determining the maximum time of not having the service(s) provided by the server that can be tolerated.

9.3.2 An identification of all of the threats to the system such as:

9.3.2.1 Hardware failure,

9.3.2.2 Electrical failure, or

9.3.2.3 Building damage.

9.3.3 Implementing a contingency plan for restoring services at an alternate location or utilizing alternate equipment.

9.4 Computer Technicians can give advice on damage assessment and contingency planning.

9.5 Hardware Repair/Replacement

The Computer Technician will be contacted to repair or replacement of a school-based.

9.5.1 The Computer Technician will advise the principal of the cost and timeline to affect repair.



9.6 Software Restoration

The Computer Technician will re-install operating system and business-critical software. Documents and user-created files will be restored from the latest available backup.

10. Guidelines For Strategic Systems: Central Office Servers

10.1 A strategic system is a server that meets more than one of the following criteria:

- 10.1.1 Is critical to the mission of the School Division
- 10.1.2 Affects large parts of the School Division
- 10.1.3 Yields Division-wide benefits
- 10.1.4 Is large
- 10.1.5 Is expensive

10.2 The following procedures apply to the management of servers:

- 10.2.1 Servers will be managed and operated by Computer Technicians.
- 10.2.2 The appropriate departments will manage critical software programs.

10.3 The following standards of physical security must be met:

- 10.3.1 Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, or other environmental contaminants.
- 10.3.2 Air temperature and humidity must be controlled to within acceptable limits.
- 10.3.3 Systems must be electrically powered via Uninterruptible Power Supplies to provide the following:
  - 10.3.3.1 Minimum of 15 minutes operation in the event of a power blackout
  - 10.3.3.2 Protection from surges, spikes and other transient anomalies,
  - 10.3.3.3 An orderly system shutdown when deemed necessary.



#### 10.4 Physical Access to Network Server

- 10.4.1 Technicians and Administrative staff will control access.
- 10.4.2 Access door will remain locked.
- 10.4.3 There will be security screens on all external windows.

#### 10.5 User Access

- 10.5.1 New *user id's* will be handled as follows:
  - 10.5.1.1 Written application must be submitted to a Computer Technician.
  - 10.5.1.2 The application form must be signed by someone in authority (e.g. Principal, Secretary-Treasurer, or Superintendent).
  - 10.5.1.3 The applicant must be a Northland School Division #61 employee or authorized contractor.
  - 10.5.1.4 The application form will be forwarded to the Records Management Clerk.
  - 10.5.1.5 The new user-id and password will be given orally to the applicant; unless special delivery has been authorized due to special circumstances.
  - 10.5.1.6 If the operating system supports a password aging facility, then it must be set to force password change on the first login.
  - 10.5.1.7 The access level will be no higher than required as approved by the supervisor.
- 10.5.2 Terminating Users  
The user-id of any person leaving the Division or no longer requiring access will be disabled. All files will be referred to the department supervisor for disposal.



10.6 Fire Detection and Control

- 10.6.1 There will be smoke and thermal detectors on the premises.
- 10.6.2 Under-floor areas will have smoke and water detectors.

10.7 Daily Backup

- 10.7.1 Security backups of all data will be made daily. The backup regime must meet the following criteria:
  - 10.7.1.1 Enable recovery to the start of business on any weekday of a failure.
  - 10.7.1.2 Provide at least one level of backup to the previous week, to cover the case of the failure of the primary backup media.

10.8 Offsite Storage

- 10.8.1 There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.

10.9 Media Validation

- 10.9.1 There must be a validation of security backup media once every six months. The security backup media should be replaced annually.

10.10 Consider Adding an Alternative Backup Strategy

- 10.10.1 An alternative procedure to 1.7.2 and 1.7.3 is implementing networked remote mass storage of business critical data and applications. This service must enable full data recovery to no earlier than one working day and access to business critical applications within one working day.

10.11 Password Aging

- 10.11.1 If the Operating System provides the ability for automatic Password Aging, this will be enforced. The life of a password shall be three months.



10.12 Documentation

- 10.12.1 Documentation relating to the operation of the hardware, operating system and applications of strategic systems will be stored in the same room as the system and summary copies stored in a secure off-site location. These documents shall be accessible to the Computer Technicians and the application custodians.

11. Software Change or Upgrading Guidelines

Definition

- 11.1 Software Change: covers the control of all aspects of the server's software including the operating system, its associated packages (DBMS etc.) and utilities, third party and locally developed applications, together with any command procedures and documentation to support and run them.

General Obligations

- 11.2 When changes are required to systems software it is essential that the changes are:
  - 11.2.1 Authorized and approved in consultation with the appropriate department
  - 11.2.2 Thoroughly tested on a separate computer
  - 11.2.3 Sufficiently documented
  - 11.2.4 Implemented at an appropriate time.
- 11.3 No changes to the server's software shall be made without approval from the Computer Technician, Department Supervisor or Superintendent.
- 11.4 All operating system software relating to server will be placed under the management of a Computer Technician. All software



applications will be placed under the management of the appropriate department administrator.

#### Required Process for Upgrading or Changing Software

- 11.5 Computer Technicians will be given the responsibility for testing changes to the server's software on another computer not connected to the server and after approval from the department supervisor, moving these changes to the application software on the server. A contingency plan to enable the software to be restored to its previous version in the event that the implementation is unsuccessful shall be in place.

#### Technical, Operations and End User Documentation

- 11.6 Appropriate documentation for each software element (operating system, utility, application) must be completed and accepted by the appropriate administrator and Computer Technician before the change is implemented on the server.

#### Testing Software

- 11.7 In developing, upgrading or changing software, two separate environments should be maintained:
- 11.7.1 Development area: should the Division choose to develop its own software.  
New software and changes to existing software should be prepared in the Development area by appropriately authorized software developers or applications support staff.
  - 11.7.2 Testing area for software before placing it on the server  
Once assessed as satisfactory, the new or modified software should be transferred to the testing area for testing by a Computer Technician and Department Supervisor, Superintendent. Changes to software are not permitted in the testing environment.



- 
- 11.8 Following successful completion of testing and approval by the appropriate application custodian, the new or modified software should be placed on the server. A contingency plan to enable the software to be restored to its previous version in the event that the implementation is unsuccessful shall be in place.

Documentation

- 11.9 Software Change Process  
Documents detailing the steps, including administrative approvals, must be filed in the Division's central filing system.
- 11.10 Software Change Approval  
No software change is to be undertaken without appropriate authorization from the department supervisor, Superintendent and the Computer Technician.
- 11.11 Disaster Recovery Procedures  
Disaster recovery procedures are the same as those stated for school-based servers.

12. Communications

- 12.1 Network access can be categorized into four major areas:
- 12.1.1 Local Area Network
  - 12.1.2 External Access via Modem link (Remote Access Service)
  - 12.1.3 Virtual Private Network link via Internet
  - 12.1.4 Wide Area Network (SuperNet)
- 12.2 The Division has varying degrees of control in affecting security management of these areas:
- 12.2.1 Total control over the LAN, Modem, and VPN links, given that Divisional Computer Technicians plan, install, manage, and maintain these systems.
  - 12.2.2 Limited control over the Wide Area Networks SuperNet VPNs, which are managed by a firm under contract to the Government of Alberta.
  - 12.2.3 No control over the Internet.



### 13. Local Area Networks

#### 13.1 Physical Security

- 13.1.1.1 The following standards of physical security for local area networks must be met:
- 13.1.1.2 Premises housing network control equipment must be physically strong and free from flooding, vibration, dust, and other environmental contaminants.
- 13.1.1.3 External building ducts must conform to provincial standards of service reticulation.
- 13.1.1.4 Internal building distribution of cables within ceiling, wall or floor cavities must be reticulated within protective conduits, cable trays or surface moldings.
- 13.1.1.5 Air temperature and humidity must be controlled to within equipment-defined limits.
- 13.1.1.6 Network electronics must be powered via Uninterruptible Power Supplies to provide the following:
  - 13.1.1.6.1.1 Minimum of 15 minutes operation in the event of a power blackout.
  - 13.1.1.6.1.2 Protection from transient electrical anomalies such as spike, surges, and sags.

#### 13.2 Physical Access

- 13.2.1 The Principal, Department supervisor and Computer Technician, will control access to areas housing network electronics.
- 13.2.2 Doors to areas housing network electronics will be locked with a unique key, the distribution of which will be determined by the onsite building administrator.

#### 13.3 Data Integrity

- 13.3.1 Eavesdrop Protection  
Users are categorized into security sub-groups (students, administrative staff, and general staff). By



utilizing eavesdrop protection at the network administration level; full network flexibility is retained at the user end.

Northland School Division Local Area Networks should all be protected by careful administration of security privileges. The Computer Technician will configure security privileges after consulting with the Principal, Department supervisor or Superintendent.

13.3.2 Intrusion Protection. Within the boundaries of the LAN, intrusion protection is required to prevent:

13.3.2.1 Unauthorized staff or students from indiscriminately plugging laptop computers into any access port of the network

13.3.2.2 Unauthorized access of staff and students to the Division's server.

Only those computers belonging to staff and students will be allowed to function when connected to the LAN. Visiting personnel wishing to access the network must have authorization from the local administrator for temporary access rights.

No student will be allowed Telnet or FTP access to the school or division's servers.

13.4 Modem Access (RAS)

13.4.1 No individual staff member will connect to a modem capable of receiving incoming calls to the network without approval of the onsite administrator who will ensure that the security of the network is not compromised.

13.4.2 The Computer Technicians will operate and managed the network modem facility using the following criteria:



- 13.4.2.1 All modem access will be password protected.
- 13.4.2.2 Passwords will be activated on request for service. Password security policy for the local area network will apply to the modem authentication system.

13.5 Virtual Private Network via Internet

- 13.5.1 An individual staff member may connect to a Local Area Network via Virtual Private Network connection when granted permission from a system administrator. A Computer Technician will configure and manage VPN connections to ensure that:
  - 13.5.1.1 Network security is maintained, and
  - 13.5.1.2 Security of the server is maintained.

14. Wide Area Network (SuperNet)

- 14.1 Operation of the Wide Area Network is vested in another corporate entity under contract to the Government of Alberta and providing this service to the Division.
- 14.2 Protection of Wide Area Network will be provided by network firewalls that include Intrusion Detection and Reporting
- 14.3 Because of the nature of Wide Area Networks (WANs), only limited security measures can be taken. Security for Strategic Systems must rely heavily on software applications and general computer controls. Server administrators must be aware of the risks of transmitting information over the WAN and must take these risks into consideration when:
  - 14.3.1 Determining the nature of information to be sent over the WAN, and
  - 14.3.2 Granting approval for new software applications that involve the transmission of information over the WAN.



Sensitive information such as personal and critical financial data must be transmitted in a secure manner that may include encapsulation and/or encryption.

15. Disaster Recovery Procedures

- 15.1 Disaster recovery procedures are the same as those stated for school-based servers.