POLICY STATEMENT

District of Maple Ridge

Title: Information Security	**Policy No : 5.47**
Authority: _____ **Approval:** CMT	**Effective Date: Oct 22, 2002**

Policy Statement:

Computer information systems and networks are an integral part of business at the District of Maple Ridge. The District has made a substantial investment in human and financial resources to create and support these and other communication technologies. It is the intent of the Municipality to ensure that all District computer and information resources are safe for their intended use, and will adopt procedures and statements to ensure secure usage by all District employees.

Purpose:

Definitions:

PROCEDURES

To Information Security Policy 5.47

Title: Information Security Procedures	**Procedures to Policy No : 5.47**
Authority: _____ **Approval:** CMT	**Effective Policy Date: Oct 22, 2002** **Amended Procedures: Feb 14, 2008** **Nov 27, 2008**

1.0 Policy Statement (adopted):

Computer information systems and networks are an integral part of business at the District of Maple Ridge. The District has made a substantial investment in human and financial resources to create and support these and other communication technologies. It is the intent of the Municipality to ensure that all District computer and information resources are safe for their intended use, and will adopt procedures and statements to ensure secure usage by all District employees.

Attachment 'A'
Information Security Procedures:

1.0 Introduction

The Information Security policy and supporting procedure and statements have been adopted in order to:

- Protect the technologies and the investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the reputation of the District.
- Protect the rights of users (i.e. - Council member, employee, contractor, associate, or authorized third party).

District technologies affected by this policy and procedure include:

- Computer desktop technology including workstations, software, printers and modems;
- Network services including servers, email, internet, intranet, and remote access;
- Software, and data, including application programs, automated methodologies and operating systems;
- Voice communication including voice mail, wire and wireless communications;
- Reproduction technologies including photocopiers, fax machines, and scanners; and
- Video conferencing.

2.0 Contents

The topics covered in this procedure document include:

- Administration and Responsibilities
- Use of District Technologies
- Prohibited Use of District Technologies
- Software and Hardware
- Internet
- Email
- Access Control
- Asset and Data Control
- Computer Viruses
- Remote Access

3.0 Administration and Responsibilities

3.1 **Responsibilities** – Information security is a shared responsibility. The involvement and participation of all District staff and users is needed to ensure security controls adequately protect the organization and stakeholders.

This section identifies general responsibilities of all users of District technologies; specific sections below identify additional responsibilities.

3.1.1 **Security Policy Sponsor** – The Corporate Management Team (CMT) assumes the ultimate responsibility for the Districts security posture at the executive management level. Support from this level will give the policy and procedure legitimacy.

3.1.2 **Security Manager** – The Chief Information Officer assumes the responsibility of the IT Security Manager. Working in tandem with the Operational Security Managers, the IT Security Manager oversees and provides guidance for the overall development, implementation, and coordination of the security policy and procedures.

3.1.3 **Operational Security Manager** – For each Division, individuals are designated to manage security from an operational level. It is at the Division and Department level that risks can best be understood, and the implementation of security procedures be achieved.

Working with the IT Security Manager, or his designate, the Operational Security Managers oversee and provide guidance and leadership for the overall development, implementation, monitoring, compliance and coordination of security for their specific areas of responsibility.

On an operational basis, individual Department managers are responsible for the development, implementation and review of security controls for their respective areas. As necessary, some operational security responsibilities may be escalated to the Operational Security Managers.

The Operational Security Managers will need to ensure that all appropriate personnel are aware of and comply with this policy and procedure document, and will need to monitor the use of District technologies for compliance with this policy and procedure and investigate any reported or suspected infringements.

3.1.4 **Human Resources** – The Personnel Department has the responsibility of providing general security training and awareness for all new hires and, as needed, all users. All users will need to sign an acknowledgement attached to this policy and procedure document, when they start with the District and also upon leaving the District. Department managers have the responsibility of providing to their staff the specific security training components appropriate for their area.

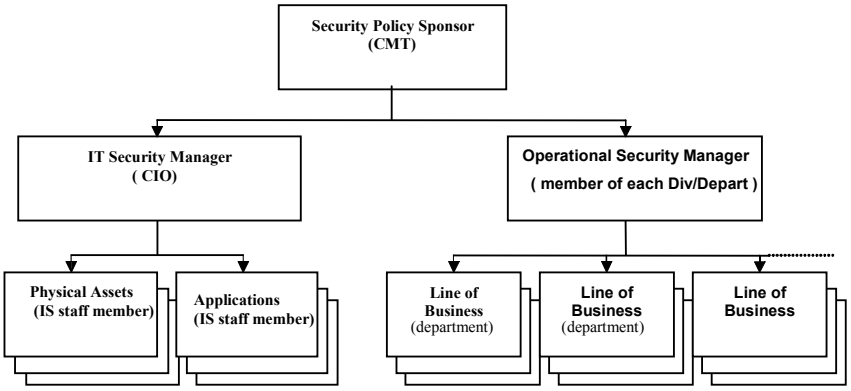
3.1.5 **Users** – Users of District technologies will review, understand and comply with this policy and procedure prior to using the technologies, and will be required to sign the attached acknowledgement.

Users will ensure that they are competent in the use of District technologies they require to perform their employment responsibilities, or will take the appropriate, approved training to achieve competency:

- in the operation of the hardware technology;
- in the use of licensed software products;
- in the use of proprietary automated methodologies; and

- to ensure that they are applying District technologies appropriate to the business requirement.

If this policy and procedure does not deal with specific circumstances at hand, then users should advise the IT or Operational Security Manager.



3.2 Compliance and Exceptions – All users must comply with both the letter and spirit of all security policies and procedures, and adopted technology standards.

The Security Policy Sponsor (CMT) assumes the ownership of the overall security policy and procedures and will direct that it be maintained, reviewed, disseminated, and complied with.

The CMT as the security sponsor must grant approval to all proposed changes or additions to the Security Policy.

The Operational Security Managers will monitor the use of District technologies for compliance with this policy and procedures and investigate any reported or suspected infringements.

3.3 Violations – Failure to observe this policy, procedures and associated guidelines may result in disciplinary action by the District depending upon the type, severity, and number of violations, and whether it causes any liability or loss to the District.

Action, in keeping with District personnel policies, for non-compliance may result in:
- suspension of service;
- user accounts and passwords may be withdrawn without notice;
- other disciplinary actions as deemed appropriate by District personnel policies or
- for cases of civil or criminal actions.

4.0 Use of District Technologies

District technologies are provided to users for business purposes and shall be returned by the user upon termination of employment or involvement with the District.

Other reasonable use is subject to Operational Security Managers' approval provided the following conditions are met:
- the use is not contrary to any provisions of this or related District policies,
- reasonable personal use is restricted to personal time and does not interfere with the user's ability to fulfill his or her employment obligations to the District,
- the user agrees to accept any expenses resulting from such use, and
- the use is restricted to the user, and does not include use by his or her family or other third parties.

Use of District technologies should be in compliance with applicable laws, contractual arrangements, professional standards and related District policies. It is recognized that where the use of a District

technology is subject to a license agreement, contract or provision of law, lack of adherence to these policies could result in individual user or District liability for monetary or other penalties.

5.0 Prohibited Use of District Technologies

Use of District technologies for any of the following purposes is strictly prohibited:

- to discriminate or harass,
- to distribute inappropriate, offensive or illicit information including sexually explicit written or graphic material,
- to promote hatred against any group,
- to distribute unauthorized advertising material whether it be with respect to District business or otherwise;
- to impersonate, distribute unsolicited non-District correspondence (chain letters, etc.), slander or otherwise defame, invade privacy, or other unacceptable, disruptive activities,
- to "hack" or otherwise attempt unauthorized access to or penetration of District, client or other third party computing and communication facilities.

6.0 Software and Hardware

6.1 Software – All software acquired for, or developed by, District employees or contract personnel is the property of the District. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

6.1.1 **Purchasing** – All purchasing of software must respect the Corporate Purchasing Policy and shall be centralized with the IS Department to ensure that all applications conform to corporate software standards, are purchased at the best possible price, are tracked as corporate assets, and so that licences are centrally managed to ensure legality and replacement.

All requests for corporate software must be submitted to the IS Department for review, to determine the standard software that best accommodates the desired request, and approval.

6.1.2 **Licensing** – Each user should make a reasonable attempt at understanding and following all applicable licenses, notices, contracts, and agreements for software used on their District computer. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of legal provisions. Upon a user leaving the District, all District data and software stored on District or personal machines will be deleted.

6.1.3 **Software Standards** – The District maintains a software standard that all users requesting use or purchase of technologies must comply with. These software standards are identified under separate cover and are supported by IS staff and user departments.

Users needing software other than those programs listed, in another document, as District standard packages must request such software from the IS Department with the approval of their supervisor. Each request will be considered on a case-by-case basis in conjunction with the adopted software standards, business need, available funding and purchasing policies.

Technologies purchased by staff for home use through the District funding plan are owned by the District until purchase has been completed by the owner, but are the responsibility of the owner and they will be required to purchase the standard District software load.

6.1.4 **Software Installation** – The IS Department is responsible for installation and support to provide software and hardware in good operating condition to District users so they can best accomplish their work tasks. It is District policy to comply with all laws regarding

intellectual property rights and licencing restrictions. Non-compliance can expose the District and the responsible user to civil and/or criminal penalties.

The IS Department responsibilities include:
- Office desktop computers;
- District laptop computers;
- District network resources;
- District databases;
- District telephone systems;
- Computer lab and public access computers;
- Home computers that are provided by the District.
- Technologies purchased through the District funding plan are the responsibility of the owner, but will be required to purchase the standard District software load.

Software may exist in any one of the following scenarios:
- An IS Department created "image" or OEM installation on the hardware.
- An IS Department installation procedure that provides for the following:
  1. Installation options.
  2. Upgrade considerations (if applicable).
  3. Data conversion (if applicable).
- a shortcut to a network application (not truly an installation).
- an automated installation through an IS Department developed solution that may be used in a rapid-deployment scenario or silent-install situation.
- a terminal application, Citrix application, or other thin-client type of application accessible via the District network.

Software cannot be present on District computers in the following scenarios:
- an installation not consistent with accepted procedures and standards.
- software purchased for a users' home computer.
- an unlicenced (e.g. – "pirated") copy of any title.

The IS Department will maintain a software inventory for management purposes. The Department will also retain original copies of all software in a central location in the office. Disks/CD's are not to be distributed to users as this software is the property of the District.

IS staff shall be responsible for the administration of access controls to all District computer systems. All requests for adds, deletions, and changes must be submitted to the IS Manager upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request The IS Manager will maintain a list of administrative access codes and passwords and keep this list in a secure area.

6.2 Hardware – All hardware acquired for, or developed by, users or contract personnel is the property of the District. All such hardware must be used in compliance with applicable licenses, notices, contracts, and agreements. The IS Department will maintain a hardware inventory for management purposes.

6.2.1 **Purchasing** – All purchasing of District computer hardware devices must respect the Corporate Purchasing Policy and shall be centralized with the IS Department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price, and is managed for asset tracking and replacement. All user requests for corporate computing hardware devices must be submitted to the IS Department along with approval of their supervisor. The IS Department will then determine the hardware standard that best accommodates the desired request.

6.2.2 **Hardware Standards** – The District maintains a hardware standard that all users requesting use or purchase of technologies must comply with. These hardware standards are identified under separate cover and are supported by IS staff and user departments.

Users requesting computer hardware beyond the corporate standard must request such hardware from the IS Department. Each request will be considered on a case-by-case basis in conjunction with the hardware standards, corporate needs and hardware purchasing practices.

6.3 Outside Equipment – No outside equipment or electronic parts (eg. – wireless cards) may be plugged into the District's network without the IS Department's review and permission.

Computers purchased through the District funding plan are the responsibility of the owner, but will be required to purchase the standard District software load to ensure compatibility with the District network.

7.0 Internet

Access to the Internet is provided to users to facilitate bonafide District business. Users are able to retrieve information, research topics, process transactions, and communicate with other organizations. Similarly, Email is an efficient means of communication whether through the Internet or through the District's network.

The Internet has risks to use. To ensure that all users are responsible and productive Internet users and to protect the District's interests, the following guidelines have been established for using this service.

7.1 Acceptable Use – Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial web sites.
- Accessing databases as required for business purposes.
- Using Email for business contacts.

7.2 Unacceptable Use – Employees must not use the Internet for purposes that are illegal, unethical, harmful to the District, or non-productive. Examples of unacceptable use are:

- Sending or forwarding chain Email (i.e. - messages containing instructions to forward the message to others).
- Conducting personal business using District resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

The organization maintains a web filtering service as an added measure of protection to prevent inappropriate access and to track how bandwidth is being used.

7.3 Downloads – File downloads from the Internet for personal or entertainment purposes are not permitted. File downloads of business related files is permitted. Installation of same may require assistance of the IS Department.

7.4 Copyrights – Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the District and/or legal action by the copyright owner.

7.5 **Monitoring** – All messages created, sent, or retrieved over the Internet are the property of the District and may be regarded as public information. The District reserves the right to access the contents of any messages sent over its facilities if the District believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Users are reminded not to put anything into an Email message that you wouldn't want to see public.

8.0 Email

Email is an efficient means of communication whether through the Internet or through the Districts network. Email also has risks. To ensure that all users are responsible and productive Email users and to protect the District's interests, the following guidelines have been established for using this service.

8.1 **Authorized Usage** – Electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

a. It does not consume more than a trivial amount of resources;
b. It does not interfere with staff productivity;
c. It does not preempt any business activity.

Users must not use communications systems for private business activities or amusement/entertainment purposes unless expressly approved by the Security Sponsor.

Users are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

8.2 **Default Privileges** – User privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a Department Director has been obtained.

8.3 **No Default Protection** – Users are reminded that District electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. See the Chief Information Officer (CIO) if this requirement is needed.

8.4 **Respecting Privacy Rights** – Except as otherwise specifically provided, users may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. The District is committed to respecting the rights of its users, including their reasonable expectation of privacy.

However, the District is also responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Users are reminded not to put anything into an Email message that you wouldn't want to see public.

8.5 **No Guaranteed Message Privacy** – The District cannot guarantee that electronic communications will be private. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy and procedure.

8.6 **Regular Message Monitoring** – It is the policy of the District not to monitor the content of electronic communications. However, it may be necessary to monitor in specific instances to support operational, maintenance, auditing, security, and investigative activities.

Users should structure their electronic communications in recognition of the fact that the District may need to examine the content of electronic communications.

8.7 **Purging Electronic Messages** – Messages no longer needed for business purposes must be periodically purged by users from their electronic message storage areas. After a certain period -- generally six months -- electronic messages should be backed up to a separate data storage media (e.g. - tape, disk, CD-ROM, etc.).

If the District is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the Security Sponsor or his designated representative has communicated that it is legal to do so.

9.0 Access Control

9.1 **Supervisor's Responsibility** – Managers and Supervisors should notify the Personnel Department and the IS Manager promptly whenever a user leaves the District or transfers to another department so that his/her access privileges can be modified or revoked.

Arrangements for system access changes for disciplinary terminations must be made ahead of time.

Access to District technologies will be reviewed and approved on a 'need-to-know' basis. A users request for access needs to be approved by the department Manager and forwarded to the IS Manager for review and implementation.

9.2 **Human Resources Responsibility** – The Human Resources Department will notify the IS Manager promptly of transfers and terminations. Disciplinary terminations must be discussed as early as possible.

Human Resources will provide new staff members with the appropriate orientation to security procedures at the District.

9.3 **Passwords** – The confidentiality and integrity of data stored on District computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each user's job duties.

Passwords will be required to be synchronized to allow users access to all appropriate District software and services for their privileges. Passwords will be required to be complex (e.g. – a minimum of 6 characters, not normal words) and will need to be changed every 90 days. Users will not be able to use the same password for at least 5 password changes.

9.4 **User Responsibilities** – The directives below apply to all users:

1. Disks and other storage media should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Disks and other storage media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment (e.g.- file servers) must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. IS staff are responsible for all computer equipment installations, modifications, and relocations. This does not apply to moves of portable computers.

6. Users with laptops shall take reasonable measures to ensure the security of the device and the data stored on it. Shared portable equipment such as laptop computers, require pre-booking using the Outlook system. Staff booking such devices are responsible for their security. No sensitive data should be stored on such shared devices.
7. Users should exercise care to safeguard the valuable electronic equipment assigned to them. Users who neglect this duty may be accountable for any loss or damage that may result.
8. USB or other mobile storage devices can contain large amounts of corporate data; users are expected to utilize encryption when transporting sensitive corporate data on such devices. IS Department personnel will provide appropriate encryption tools for the user.
9. Corporate data is not to be taken or sent off-site without prior consideration as to the criticality and sensitivity of the information contained within the file. Appropriate protections are to be utilized depending on the classification of the data. If in doubt, please consult with your Operational Security Manager or the IT Security Manager. Upon leaving the District, all users are expected to return or delete all corporate data in their possession and will be required to sign a Declaration to that effect.

9.5 Physical Security – It is District policy and procedure to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. Users are expected to ensure that resources under their control are adequately protected from theft or misuse.

9.6 Public Requests for Data – The District can release certain digital information for public use, typically for a fee as is current practice. Release of computer lists of database information that contains personal information such as names, addresses, and phone numbers will be reviewed for the protection of confidentiality.

Computer lists will only be released upon receipt of a written request and undertaking from the recipient that it will be used solely for the purpose for which it was requested.
This policy and procedure does not relate to information which is otherwise public information through other legislative authority.

The IT Security Manager will review all such requests in consultation with Operational Security Managers and the District Clerk for approval.

10.0 Asset and Data Control

10.1 Asset and Data Classification – The value and inherent risk of information or information-related assets shall be determined and classified. Controls to protect the confidentiality, integrity, and availability of the information or information-related asset are consistent with the assigned classification. A classification scheme is used to ensure the protective control implemented is proportionate to both the information asset's value to the District and its potential for loss.

10.2 Responsibility for Classification – The owner of the information or information-related asset is responsible for assigning the appropriate classification levels and applying the appropriate labeling. As the value of the information may decline over time, periodic reviews are performed by the owner and, where appropriate, the owner reclassifies the information when its value or inherent risk has changed.

10.3 Risk Assessment and Data Classification Process – The following classifications have been established:

10.3.1 **Sensitivity of Information** –The degree to which the value of the information is determined by its secrecy.

- Public – Information that is designed to be in the public domain or is readily acquired commercially or publicly.

- Internal – Information for general use by all District employees.
- Confidential – Highly sensitive or critical information. Its knowledge is restricted among District users by the Information Owner.

10.3.2 **Criticality of Information** – Criticality is comprised of two components, Integrity and Availability:

- Integrity - The degree to which the value of the information is determined by its reliability. Integrity classification is performed according to the following scale: Low; Moderate; High.
- Availability - The degree to which the value of the information is determined by its accessibility when needed. Availability classification is performed according to the following scale: Low; Moderate; High.

10.4 **Implementation of Controls** – The IT Security Manager and Operational Security Managers share responsibility with the data owners for protecting the information and will implement controls appropriate to the documented Sensitivity and Criticality classification.

11.0 Computer Viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Viruses can cause destruction of corporate resources. Computer viruses are much easier to prevent than to cure.

Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Users should not download programs from the Internet including games and screen savers. IT personnel will provide appropriate software installation and maintenance services.

Remote access users will not be able to upload files to the District network resources unless the IS Department staff can verify the integrity of the workstation or source for such upload.

The IS Department will scan incoming files and attachments for viruses, and provide appropriate notice to users when viruses are encountered. Users should notify the IS staff of any viruses they encounter.

Users should set Email filters on their workstation software to filter out junk or offensive/questionable Email.

12.0 Remote Access

Remote access is a generic term used to describe the accessing of District computer network resources by individuals not located at the District's primary offices. This may take the form of off-site offices, traveling users, or users working from home and connected to the District network.

Participation in a remote access program may not be possible for every user. Remote access is meant to be an alternative method of meeting District needs. The District may refuse to extend remote access privileges to any user or terminate a remote access arrangement at any time.

12.1 **Acceptable Use** – Hardware devices, software programs, and network systems purchased and provided by the District for remote access are to be used only for creating, researching, and processing District-related materials. By using the Districts hardware, software and network systems the user assumes personal responsibility for their appropriate use and agree to comply with the provisions of this and other appropriate District policies.

Home users using a District machine will need to ensure District standards are followed to ensure compatibility and security.

Eligibility to remotely access the District's computer network will be determined by the responsible Department Directors.

12.2 Equipment and Tools – The District may provide tools and equipment for remotely accessing the corporate computer network. This may include computer hardware, software, phone lines, email, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary.

The use of equipment and software provided by the District for remotely accessing the District's computer network is limited to authorized users and for purposes relating to District business. The District will provide for repairs to District equipment. When the user uses her/his own equipment, the user is responsible for maintenance and repair of equipment and will not be able to connect to the District network unless compatible with established standards and security settings.

12.3 Use of Personal Computers and Equipment – There are thousands of interactions between software needed by the remote user and the average mix of programs on a home computer. Troubleshooting software and hardware conflicts can take hours, and can result in a complete reinstall of operating systems and application software as the only remedy for problems. For that reason the IS Department will only provide support for equipment and software provided by the District.

Home users will need to ensure their systems are compatible with District software and network security settings.

The District will bear no responsibility if the installation or use of any necessary software causes system lockups, crashes, or complete or partial data loss. The user is solely responsible for backing up data on their home machine before beginning any District work.

Acknowledgment of Information Security Policy and Procedures

This form is used to acknowledge receipt of, and compliance with, the District of Maple Ridge Information Security Policy and associated procedures.

Acknowledgement Procedure

Complete the following steps:

1. Read the Information Security Policy and Procedure.
2. Sign and date in the space provided below.
3. Return this page only to the Personnel Department.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Information Security Policy and Procedure" and understand the same;

ii. I understand and agree that any computers, software, data and storage media provided to me by the District contains proprietary and confidential information about the District of Maple Ridge and its customers or its vendors, and that it is the property of the District at all times;

iii. I agree that I shall not copy, duplicate except for backup purposes, otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

iv. I agree that, if I leave the District of Maple Ridge for any reason, I shall immediately return to the District the original and copies of any and all software, computer materials, or computer equipment that I may have received from the District that is either in my possession or otherwise directly or indirectly under my control. Data and software on computer storage devices will be deleted.

v. I agree that if connecting from a remote site, I will ensure my computer maintains compatible settings consistent with District security policies, procedures, settings and standards.

vi. I understand and agree I must make reasonable efforts to protect all District provided software and hardware devices, and data, from theft, physical damage and inappropriate use.

_____

User Signature

_____

User Name

_____

Date

_____

Department/Location/Company

Declaration of Return or Disposal of District Information and Equipment

This form is used to acknowledge return of, or deletion of, District of Maple Ridge provided hardware and software, and data or information, that is under the control of the user. This form is used also to declare that the user no longer has any such equipment, materials, or data in his/her possession in accordance with the Information Security Policy and associated procedures.

Declaration Procedure

Complete the following steps:

1. Read the declaration and acknowledgement below.
2. Sign and date in the space provided below.
3. Return to the Human Resources Department.

Declaration and Acknowledgement

I hereby declare and acknowledge that:

1. I have returned all District provided computer hardware and peripherals, and associated materials, in my possession or otherwise directly or indirectly under my control;
2. I have returned or deleted, or otherwise destroyed, all original and copies of District supplied software in my possession;
3. I have returned or deleted all District data and information in my possession.

_____

User Signature

_____

User Name

_____

Date

_____

Department/Location/Company