KIRKLAND LAKE
THE RIGHT ENVIRONMENT

POLICY	
Policy Number: CORP2020-013	Date Approved: March 2009
Department: Corporate	Date Reviewed: October 2020
Information Systems Security and Usage	

1. Policy Statement

Not Applicable

2. Purpose

The Corporation of the Town of Kirkland Lake has invested considerable time, money and effort in building a comprehensive information system (IS) network. This network is an integral part of the Corporation's business activities: a means by which information can be securely stored, shared and manipulated across departmental lines and external audiences to result in more efficient and effective service to the people of Kirkland Lake.

There are certain moral and legal commitments that underlie the operation of such a network. There is the matter of public trust; people expect a public institution like the Town to operate in a professional manner and to protect their private information. There are legal requirements; provincial, federal and international laws dealing with information security, copyright issues, electronic abuse, etc. Lastly, there are expectations of the network users themselves; they have a right to a safe, comfortable work environment where things work as expected, when expected.

To ensure that these commitments are met, the Corporation has developed the following policy statement. This document explains who can access the network, how it is administered, and what constitutes acceptable use. It is premised on the argument that, as the owner-operator of this resource, the Corporation is legally responsible for anything that happens on it, in it or through it. Consequently, it has the right to exercise certain privileges to ensure that its interests are protected. End-users, by virtue of their use of these network resources, acknowledge the right of the Corporation to exercise these privileges, and accept that they have certain responsibilities to ensure that resources available to them are not abused, and that they do not expose the Corporation to legal or moral censure.

These policies were developed by the Corporate Services Division. They are drawn from a variety of public and private sector sources and reference materials, and are based on accepted industry standards and legal realities.

3. Scope

This document constitutes a Corporate-wide policy intended to allow for the proper use of all Corporate information system (IS) resources, effective protection of individual users, equitable access, and proper management of those resources. It is intended to supplement, not replace, existing Corporate policies, agreements, and contracts as well as federal and provincial laws and regulations.

Corporate divisions that operate stand alone IS services (such as public access services, contracted access and services) are encouraged to add individual guidelines that supplement, but do not lessen the intent of this policy. In such cases, the division will provide a copy of their division-level policy to the Information Systems Services (IS Services) upon implementation.

4. Definitions

The term “information systems” is defined as information in electronic or audiovisual format, and the hardware or software that makes possible the storage and use of such information. This includes, but is not limited to, local and externally accessed databases, electronic mail (e-mail), removable storage devices (including but not limited to CD and DVD disks, removable drives, recorded magnetic media) and any other form of digitalized information. These resources may be individually controlled or stand alone (for example, personal computers and laptops, digital cameras), peripheral equipment (such as printers, scanners, etc.), shared or networked (for example, servers and backup media), temporary or permanent installs. It also refers to services rendered over the network infrastructure, such as Internet access.

The term “end-users” is used to identify all users of the Corporation’s IS resources. This includes all Corporate personnel (full-time, part-time or contract employees), work-groups or divisions, elected representatives, contractors, third party vendors or service representatives that regularly or intermittently access the Corporate owned equipment, systems, services, processes, and applications.

5. Policy & Procedures

Corporation Privileges

The Corporation, by virtue of establishing and operating a comprehensive IS infrastructure, accepts responsibility to protect this environment from abuse, disruption and unauthorized access; and therefore to safeguard all data, personal information and confidential data through the exercise of specific privileges.

1. System Administration

Network administration is the sole responsibility of the IS Services Group. IS Services refers to Corporate personnel appointed by the Director of Corporate Services to be responsible for the strategic management of the Corporation's information systems. It includes contractors authorized to provide network administration services to the Corporation. The only contractors so authorized are the staff from the Information Systems Department of Kirkland District Hospital, with whom the Corporation has a service agreement. Any third party service vendors seeking to access the network for whatever reason must be pre-authorized by IS Services, and work under the supervision of IS Services.

2. Procurement Procedures

2.1 All purchase proposals pertaining to or impacting on the Corporation's information systems (hardware, software and services) must be developed in consultation with IS Services, to ensure that all proposed purchases conform to Corporate hardware/software standards; do not conflict with existing systems; and can be supported by IS Services staff. If a purchase is made without due consultation, IS Services may refuse to install, integrate or support the product in question. Price is not the sole basis for a purchase decision; quality, warranty, and the vendor's service record will be given equal consideration.

2.2 All departmental or division specific purchase proposals will be processed by the IS Services Project Manager. All proposals must be accompanied by an account number. The Project Manager will process the order and document all invoices, warranties, etc., providing a duplicate copy to the division in question. Details of each purchase will be recorded in the Corporation's Asset Management Database.

3. Allocation of Service Resources

3.1 IS Services reserves the right to allocate its resources on a differential basis, based on the direction it receives from management, its perceived importance of a specific requests on the overall functioning of the network, and the availability of equipment and human resources.

4. Asset Identification

4.1 A non-removable label identifies all Corporate network equipment. This label must not be tampered with or defaced. The information on the label is cross-referenced to the Corporation's Asset Management Database. Any changes or modifications to equipment must be recorded in this database. Any new assets must have this label affixed immediately upon receipt.

5. Media Storage and Tracking

5.1 IS Services is responsible for storing all original media for all Corporation software. End-users using custom or specialized software should ensure that original copies are given to IS Services. This is essential to ensure that licensing obligations are met and that replica machines can be quickly and correctly configured. Copies or duplicates of original software titles, as permitted by law and licensing agreements, may remain at the end-user site.

5.2 The Corporation and all end-users are legally bound to comply with international and Canadian (federal and provincial) copyright acts and statues, and all proprietary license agreements. Each end-user is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for equipment that he/she uses or seeks to use. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software or printed material, except for backup and archival purposes, may be a violation of international, federal and provincial law and Corporate policy.

6. Installation and Integration

6.1 IS Services are solely responsible for the installation, configuration and network integration of new assets. If third party contractors are engaged for any aspect of the installation or subsequent maintenance, they MUST work with and under the direction of the IS Services.

6.2 Any work done by a third party must be covered by a contract specifying what is being done, who is doing it, when it will be done, how, and provide service or support warranties. All third parties must sign a non-disclosure agreement before commencing work.

6.3 The only exception will be for “quick and easy” changes (patches, upgrades, minor alterations). In such instances, IS Services may assign TEMPORARY administrator rights to an end-user. Once the alteration has been made, these rights will be revoked. To request such rights, the end-user’s IS Services in writing, stating the purpose of the request and the time frame desired.

7. Denial of Service

7.1 IS Services will limit support and troubleshooting to Corporate owned and maintained hardware and software. No assistance will be rendered for unauthorized assets, assets that have been changed or modified without prior permission, or personal equipment. If such equipment is detected in routine or emergency maintenance operations, it will be removed. If unauthorized changes are found to be the cause of equipment failure or a network security breach, the end-user who made or allowed the change will be held accountable.

8. Data Storage Capacities

8.1 Each authorized end-user is allotted a maximum of 100 MB of e-mail space, and 100 MB of personal storage space on the network’s main file server. Requests for more server storage space must be made in writing to IS Services. If an end-user exceeds their quota, they will be unable to save files until sufficient space has been freed.

8.2 End-users must use their discretion as to what they store, where they store it, and how long they store it. Inappropriate files include non-business-related MP3s, graphic or picture files, games, executables, vbs files, etc. Such files consume valuable space and can introduce damaging viruses into the network. Material that includes sexually explicit content or content using vulgar, sexist, racist, threatening, violent, or defamatory language is absolutely prohibited, as is content relating to gambling and illegal activities.

8.3 A second directory on the main file server has been created for shared files under the path: (S\directory). Do not put private information on this directory.

9. Data Security

9.1 Users can set up file folders under the shared directory and limit access to select individuals granted (read only access or read and write access). To

do so, the user must request IS Services to set-up the folder in writing, identifying the specific users and their level of access. Once such a folder has been set-up, the originating user assumes all responsibility for what is stored in that folder, requesting access changes, etc.

9.2 All files stored on the file server must be stored in folders. File folders must be clearly and appropriately named so as to be easily understood by all other users with access rights. This is particularly important for files saved on the shared directory. Files left “loose” on the servers will be deleted without prior notice.

9.3 Network servers are backed up daily and secured. Information that is stored on personal computers is not. IS Services assumes no responsibility for information lost or stolen from a personal computer hard drive or any stand alone storage devices.

Access Management

10. Access Privileges

10.1 Corporation division supervisors determine which end-users under their authority shall have access to network resources. Additions or deletions must be transmitted in writing by the respective division supervisor to the IS Services.

10.2 Access to information should be provided within the context of an authorized user’s official capacity within the Corporation. Division supervisors are responsible for determining what information, systems and applications end-users under their authority can access. End-users have a responsibility to ensure that they exercise the appropriate level of protection over that information.

10.3 When an authorized user changes status (e.g., terminates employment, retires, changes positions or responsibilities within the Corporation, etc.), the unit responsible for initiating that change in status must coordinate with the user to ensure that access authorization to all Corporate resources is appropriate. An individual may not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized.

Access Procedures

10.4 End-users must use only Corporate assets to access the network. Network access originating from non-corporate computers (i.e. home computer, hotel business centre or internet café) will be denied. The exceptions are pre-authorized Virtual Private Network connections, and web mail access to Corporate e-mail services.

10.5 Users may access the network via the dedicated telephone services (Remote Access Service or RAS for short). Insofar as RAS is a potential backdoor entry point for viruses and other security breaches, users should be circumspect in their use of this service. Users must ensure that their PC is virus and spy-ware free, and that they disconnect from the service once finished. Online time should be limited during business hours, as the airport staff rely on this service for their network connectivity.

11. Ownership

11.1 All assets purchased by the Corporation remain the property of the Corporation. When taken out of use, they will be returned the purchasing division, or to IS Services for re-routing to other purposes or disposal.

11.2 All assets will be tracked in an Asset Management Database. Corporate personnel or work groups purchasing new assets, including hardware or software, will make the relevant information available to the IS Group. This includes service tag numbers, serial numbers, copies of contract documentation, warranty information, etc.

11.3 All information created, sent, retrieved, or stored on Corporate facilities and equipment is the property of the Corporation. Third party generated information (such as software programming, codes, reports, etc.) leased or lent to the Corporation for business purposes are treated as Corporate property while under lease or lend. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information by any end-user is prohibited.

11.4 The Corporation reserves the right to access and secure against deletion any information stored on or transmitted over its facilities, as well as to seize any equipment permanently or temporarily connected to the Corporate network or any stand alone Corporate hardware, if it believes, in its sole judgment, that it has a business or legal need to do so. This may be done without giving prior notice to end-users. All information may

be opened to the public, and/or disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

12. Confidentiality of Information

12.1 To the greatest possible extent, the Corporation seeks to preserve the confidentiality of information stored within or communicated over the network. Nevertheless, end-users must accept that personal and corporate information may be intentionally or inadvertently incorrectly filed or accessed, shared or distributed. Also, personal electronic communications could be forwarded, intercepted, printed, and stored by others. The Corporation assumes no responsibility or liability for any consequences, direct or indirect damages that may arise if private information stored or disseminated through its facilities is accidentally, inadvertently or purposefully corrupted, distributed or illegally used.

13. Monitoring of Usage, Inspection of Files

13.1 Users should also be aware that their use of Corporate IS assets is not completely private. While the Corporation does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the Corporation's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance.

13.2 The Corporation may also specifically monitor the activity and accounts of individual users of the network, including individual login sessions and communications, without prior notification to the end-user. This monitoring may occur in the following instances: (1) The user has voluntarily made them accessible to the public; (2) It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Corporation or to protect the Corporation from liability; (3) There is reasonable cause to believe that the user has violated, or is violating, this policy; (4) An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; (5) Upon receipt of a legally served directive of appropriate law enforcement agencies; (6) To run an inventory of an attached device for the purpose of updating Corporate records.

13.3 Any such individual monitoring, other than that specified in "(1) and (6)", required by law, or necessary to respond to bona fide emergency

situations, must be authorized in advance by the Chief Administrative Officer or his/her designate and the Director of Corporate Services; in all such cases, the appropriate division supervisor will be informed as time and the situation will allow. A division supervisor may also initiate the monitoring process. In all cases, all individuals' privileges and right of privacy will be preserved to the greatest extent possible.

14. Imposition of Sanctions

14.1 IS Services will act immediately to intervene or take special actions to forestall an immediate or potential threat to the security of a system or its users. These actions may include: (1) Suspending system access for users involved in a violation that is being investigated; (2) Taking necessary action to preserve the state of files and other information relevant or assumed to be relevant to an investigation; (3) Examining the content of e-mail and other private files, where the content may jeopardize the security of systems, the safety of other users or third parties, the ability of the Corporation to conduct necessary business, or any other appropriate use as directed by the Chief Administrative Officer and the Director of Corporate Services.

14.2 Real or suspected violations of this policy, third party agreements, or applicable provincial and federal laws will be reported to the responsible division head, the Director of Corporate Services and the Chief Administrative Officer. Persons found in violation of this policy are subject to a full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the Corporation, and legal action. Some violations may constitute criminal offences; the Corporation will carry out its responsibility to report such violations to the appropriate authorities.

End-User Responsibilities

End-users, by their access to and use of the Corporation's information systems, accept responsibility to use these resources in a manner that reflects the public trust placed in the Corporation of the Town of Kirkland Lake; to perform tasks with competence and integrity, demonstrate ethical, acceptable and professional conduct, to protect the IT environment and information it holds from abuse.

15. System Integrity

15.1 Corporate hardware and software assets are to be used for work related purposes. The use of such assets for personal purposes is permitted, provided such use is consistent with professional conduct and the incremental cost of such usage is negligible. Furthermore, personal use must not interfere with the safety, security and integrity of the Corporation's network or the information stored on the network; interfere with or pre-empt any business activity, or violate any Corporate policies or provincial, federal laws and regulations.

Authorized Access

15.2 Computer accounts, passwords, and other types of authorization are assigned to individual users. Do not record such authorization codes in an obvious or easily accessible location. Do not allow other people to use your username or password. You are legally responsible for any activity that occurs under the guise of that username/password.

15.3 Attempting to obtain another user's account password is strictly prohibited, as are attempts to access unauthorized information through the use of special passwords, loopholes in computer security systems, etc. Users are required to obtain a new password if they have reason to believe that their password has been compromised.

15.4 End-users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. This includes e-mail or internet access.

Use of Copyrighted Information and Materials

15.5 Each end-user is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for equipment that he or she uses or seeks to use. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software or printed material, except for backup and archival purposes, may be a violation of international, federal and provincial law and Corporate policy.

15.6 Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.), and the protocol for informing IS Services must be strictly adhered to. Users are prohibited from using, inspecting, copying,

storing, and redistributing copyrighted computer programs and other material, in violation of copyright laws.

16. Use of Unlicensed Software, Scripts or Applications

16.1 No software may be installed, copied, or used on Corporate resources except as permitted by the owner of the software without receiving prior authorization of the responsible division supervisor, and with the fore-knowledge of IS Services.

16.2 End-users will not independently download applications or other software, including screen-savers, calendars, or other personal enhancements. These seemingly innocuous applications frequently contain spy-ware or other irritants that can comprise the security and operation of the computer.

16.3 All information downloaded or received from non-Corporate sources must be screened with virus detection software prior to being opened or run.

17. Attempts to Circumvent Security

17.1 Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information. They are not to circumvent or subvert any other system security measures, such as anti-virus or anti-spy-ware mechanisms. This section does not prohibit use of security tools by personnel authorized by IS Services.

17.2 End-users will not intentionally develop or use programs, transactions, data or processes that harass other users or people/organizations external to the network, infiltrate the system or damage or alter the software or data components of a system.

17.3 End-users will not connect non-Corporate issued recording devices or media such as CD burners, memory sticks, disks etc. to Corporate systems.

17.4 Unauthorized probing of security mechanisms of either the Corporate network or other Internet sites is prohibited.

17.5 Authorized users may not use computing resources for unauthorized monitoring of electronic communications.

17.6 Harmful activities are prohibited. Examples include IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files, etc. Deliberate attempts to damage, destroy or degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Corporate computer system or network are prohibited.

17.7 End-users will not establish secondary Internet or other external network connections such as dial-up services, tapping into third party wireless networks, etc. without the prior written approval of IS Services.

18. Use of Personally Managed Systems

18.1 Some end-users will have personally managed systems such as laptops or desktops running over VPNs that they use to access Corporate from external location. Such end-users have a responsibility to ensure the security and integrity of their system(s). Appropriate precautions include performing regular backups, controlling physical and network access, using virus protection software, and keeping any software installed (especially anti-virus and operating system software) up to date with respect to security patches. Corporate information electronically stored on such systems must be protected as per the criteria set out in this policy.

19. Maintaining Information Integrity

19.1 Access to information should be provided within the context of an authorized user's official capacity with the Corporation. Authorized users have a responsibility to ensure that the appropriate level of protection over any information they create, store, access or communicate is maintained at all times. An individual may not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized.

19.2 Each individual is responsible for being aware of the potential for and possible effects of manipulating information, especially in electronic form. Each individual is responsible for understanding the changeable nature of electronically stored information, and to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct when they appear contrary to expectations. It is important to verify that information with the source.

19.3 End-users will not, without express authorization, seek to gain or gain, destroy, alter, dismantle, disfigure, prevent rightful access to, or otherwise interfere with the integrity of Corporate as well as third party computer-based information and/or information resources.

19.4 End-users will not, without express authorization, communicate, transfer or make available in any form Corporate information to third parties. Where communication of such information to third parties is a requirement of the end-user's regular responsibilities, the onus is on the end-user to understand to where that information is being sent, who will use it and why. End-users will report any unsolicited requests for information to their immediate supervisors and the IS Systems Group.

19.5 End-users will not upload Corporate information on any publicly accessible Internet site or with an anonymous file transfer protocol (FTP) or similar service without prior permission from their division supervisor.

19.6 Third party e-mail, instant messaging or web-mail services (Hotmail, Yahoo Mail, etc.) are prohibited. The Corporation cannot guarantee the security or integrity of such services. If information is stolen or compromised in any way, or dangers such as viruses introduced to the network through these services, the end-user who used the service in question is liable.

19.7 End-users will respect the financial structure of the Corporation's systems, and will not intentionally develop or use unauthorized mechanisms to alter or avoid charges levied by the Corporation in the normal course of its operations.

19.8 End-users will not intentionally seek information on, obtain copies or modify files, tapes or passwords belonging to other users or the Corporation;

20. Ethical Use

It is incumbent on all end-users to recognize that they are part of a community of users, and to consequently act in a manner that respects the diversity of people and opinions in the community, their right to privacy and their right to a safe and professional work environment. They also must respect the public's trust in the Corporation, and consequently demonstrate ethical and acceptable conduct. The Corporation characterizes as unethical, unacceptable and just cause for taking disciplinary action, the following kinds of activity.

21. Protection of Personal Privacy

21.1 End-users will not, without authorization, invade the privacy of individuals or entities that are creators, authors, users or subjects of information retained by the Corporation.

21.2 End-users are prohibited from looking at, copying, altering, or destroying anyone else's personal files, regardless of how such files are stored or transmitted, without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so.

21.3 End-users may not intercept or disclose, or assist in intercepting or disclosing, electronic communications or sensitive or private information about the Corporation and/or its employees and representatives by unauthorized persons or organizations, except as otherwise specifically provided.

21.4 End-users will not attempt to represent others, unless explicitly authorized to do so by those users.

21.5 Users are responsible for recognizing and honoring the intellectual property rights of others.

Freedom from Harassment

21.6 No end-user may, under any circumstances, use the Corporation's IS assets to harass any other person.

21.7 The following constitutes computer harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) Intentionally using the computer to disrupt or damage the professional or private pursuits of

another; and (5) Intentionally using the computer to invade the privacy, professional or otherwise, of another or the threatened invasion of the privacy of another.

22. Inappropriate or False Representation

22.1 Whenever end-users indicate their affiliation with the Town of Kirkland Lake in any online exchange, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of the Corporation of the Town of Kirkland Lake.

22.2 All external representations on behalf of the Corporation or any specific end-user must first be cleared with the relevant Director or end-user.

23. Personal Business

23.1 Corporate facilities, services, and networks may not be used in connection with compensated outside work or for promotion of unauthorized charitable endeavours, private business activities, or amusement/entertainment purposes unless expressly approved in advance by their supervisor.

24. Inappropriate Use

24.1 End-users are specifically prohibited to view, display, download, save, receive, or send material related to or including: (1) Offensive content of any kind, including pornographic material; (2) Material promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability; (3) Material promoting threatening or violent behaviour or other illegal activities.

24.2 End-users must not use the Corporation’s information systems for any other purposes that are illegal, harmful to the company, or non-productive. This includes: (1) Perpetuating chain e-mails or other multilevel marketing or pyramid-selling schemes, or creating and/or send "spam" (unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication); (2) Sending or encouraging "letter bombs” or messages intended to annoy, interfere, or deny e-mail use by one or more recipients, or practicing any other activity designed to deny the availability of electronic communications resources within the Corporation or against third parties; (3) Gambling or other activities

undertaken for personal financial gain, including conducting a personal business; (4) Exchanging material protected under copyright laws.

24.3 End-users will not use Corporate resources to participate in non-work related chat rooms, messenger services, Blogs, or other discussion forums, nor will they engage in any messaging behavior such as “flaming” or other such attacks.

25. Reporting Abuse

25.1 Any individual who becomes aware of improper or unethical use of IS assets, or of any action that could compromise the system’s operation or security, or pose a risk to another user or third party, is expected to report that fact to their division supervisor and/or the IS Services Group immediately.

6. Summary

Questions regarding the interpretation of this policy should be forwarded to

Project Manager
Information Systems Service Group
Department of Corporate Services
Tel: (705) 567 9361 ext. 243
Email: Wilfred.hass@tkl.ca