BERGRIVIER MUNICIPALITY

INFORMATION COMMUNICATION TECHNOLOGY POLICY

CONTENTS

INTRODUCTION

Over the last year the Municipality has invested much time and energy in its Computer Information Systems (CIS) infrastructure. This rapid progress has improved the network greatly and opened many new possibilities to the Municipality allowing more opportunities for more efficient service delivery.

Unfortunately this rapid growth has not allowed for adequate documentation of the equipment and new procedures. Also, as computers become a more crucial part of our everyday lives, so has CIS become a critical part of the operations of the Municipality.

We have been able to provide more computers to employees enabling them to be more efficient in their daily duties. Email and other Internet based communications have allowed for more reliable and faster communications. The Internet has also opened a world of information to officials allowing them to make informed decisions and commentary. Radio based wireless communications have enabled the Municipality to link its various buildings and open vending points in a reliable and cost effective way.

Remote support options have been enabled wherever possible to improve on service response times and reduce travelling expenses.

Unfortunately this change has not always been as smooth as we would have liked and can in no way be considered complete. Certain aspects of the network have out-grown their backbone infrastructures, while other sections do not have the necessary failsafe redundancy required in the event of a disaster. The same can be said for CIS related policies. Many programs and technologies are implemented on the assumption that municipal users will be computer literate enough to adapt to the changes. If only it was always so. Failure to understand the changes often leads to frustration and while these changes are done to improve on efficiency, the converse then occurs.

By expanding the spread of computer equipment through the Municipality the risk for misuse or abuse of municipal resources has grown exponentially, as has the risk toward the security of data and other information stored by the Municipality. Threats such as error, fraud, embezzlement, terrorism, extortion, privacy violation, service interruption, viruses, spyware, data theft and sabotage are very real threats to the Municipality and without the correct policies in place it is difficult the ensure security, accountability and ownership of CIS resources and to take the correct actions against transgressions. With no formal procedures in place it is difficult for users to report problems and to ensure that these problems are addresses and resolved.

Also, with no fixed management structure in place for CIS resources there is little forward planning and the approach is reactive instead of proactive in most cases.

It is in light of the above mentioned that this document has been drafted so that the Municipality can address these issues.

PROPOSED POLICIES

1. POLICY ON THE USE OF PERSONAL COMPUTER EQUIPMENT

A. PURPOSE

The purpose of this policy is to regulate use of personal computer equipment so that the Municipality:

- controls costs with a standardized set of software and hardware that can be well supported in terms of maintenance and user training;
- uses municipal assets efficiently;
- minimizes loss of, or damage to, equipment, software and data;
- is protected from legal difficulties;
- is productive, by limiting personal use to reasonable levels;

B. SCOPE

This policy is applicable to everyone who works at the Bergrivier Municipality. This means all permanent, contract or temporary personnel including anyone supplied by a labour broker or service-provider to the Municipality. Referred to as "personnel" or “users” in this document.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose personnel use the Municipality's computers.

C. POLICY STATEMENTS

PERSONNEL MAY BE ISSUED WITH A COMPUTER

At the request of the manager a user may be issued with computer equipment and access to computer-based services. These are provided to help you do your job. Qualifying criteria are set by management. Forms will be available both off the network and from the IT Helpdesk.

Qualifying personnel will normally get a standard-issue computer from IT Department, along with standard-issue software. New equipment will be bought only if stores cannot supply. Printers are allocated in the same way but you may be expected to share a printer with other personnel.

Some personnel may need non-standard equipment or software to do their job effectively. To get this, your manager must make a recommendation in the form of a submission to management. The submission must include the details and cost of the software or equipment you need.

THE COMPUTER SYSTEMS BELONG TO THE MUNICIPALITY

The computer, the printers, software licenses, network and data that you use at the Municipality remain the property of the Municipality.

MANAGEMENT WILL SPECIFY THE STANDARD ISSUE PERSONAL COMPUTER

To make for cost-effective use of equipment and software, the Municipality will standardize on a core set of software and hardware products. The specifications will be set, and revised from time to time, by management and the Information Technology Committee (ITC). The ITC may set different standards for different parts of the organization. The standards will cover the following:

- Hardware specifications for standard issue desktop computers, notebook computers and printers. Users will be issued with a computer that meets this standard. When the standard is raised, computers below the standard will be upgraded or replaced (budget allowing), without the need for a motivation from the user.
- Specifications for new desktop computer, notebook computer or printer hardware. When the Municipality buys a new computer or printer, its specification will conform to this standard.
- Additional software set. A list of software that may be installed if needed to do the job. To control maintenance cost, no other software may be used without the written approval of both the user's Director and the Head : Corporate Services.
- Disallowed software and hardware. A list of software, hardware or categories of software or hardware that is not allowed. In setting the standard, the ITC will consider the following issues as a minimum: security, licensing, support and risk of harassment (through offensive material).

NON-STANDARD ITEMS WILL NOT BE SUPPORTED

Computer Information Systems (CIS) supports a large number of products - both hardware and software. To keep costs down, CIS limits the product range it is willing to support and provide training for. If you use software that falls outside this product range, the management cannot guarantee support for it. All reasonable requests will be considered and where many people need a non-standard product, the ITC will consider adding it to the list of items supported.

OCCASIONAL AND BRIEF PERSONAL USE IS ALLOWED

Occasional and brief personal use of your computer is allowed subject to the following restrictions:

- Personal use should not hinder the conduct of official duties.
- Only incidental amounts of employee time, time periods comparable to reasonable breaks during the day, should be used to attend to personal matters.
- Personal use should not cause the Municipality to incur a direct cost in addition to the general overhead.
- You may not install or request software that does not support official business or activities sponsored by the Municipality.
- Personal use shall comply with all other terms of this policy.

YOU HAVE A DUTY TO USE STATE RESOURCES RESPONSIBLY

Take care to use your computer responsibly, ethically and lawfully. Do not waste computer resources or unfairly monopolize resources to the exclusion of others.

You may **not** use the Municipality's computer facilities to:

- Play games or run other entertainment software.
- Save files containing images, music, sound or video onto Municipal servers, unless they are for official purposes.

- Make or store illegal copies of material protected by copyright. This includes software programs, music, and publications, in whole or in part.
- Back up your entire local hard drive onto Municipal servers.
- Print large documents if there is a viable on-screen alternative.

Any file copied from an external source must be scanned for computer viruses. This includes files from a floppy disk, USB drive, e-mail or Internet.

YOU HAVE A DUTY OF CARE OVER THE EQUIPMENT ISSUED TO YOU

You are expected to take good care of public property issued to you. This is particularly relevant to staff who use portable equipment such as notebook computers. You must take reasonable precautions against loss and damage.

If you lose or damage equipment, software or data that belongs to the Municipality you must promptly report it to your head of section and the accounting officer. In the case of theft or suspected theft, you must also report the loss to the South African Police Service.

YOU MAY HAVE TO PAY FOR LOST, DAMAGED OR STOLEN EQUIPMENT

If an item is lost, damaged or stolen while it was under your control or responsibility, the Municipality will not normally ask you to pay for it. But, you may lose this Municipality cover if you fail to follow treasury regulations or standing instructions. The main elements are summarized here. But, this summary does not replace the original prescripts, which will be used to deal with any loss.

You may lose your Municipality cover against loss if you:

- were not on official business when the loss occurred;
- were under the influence of alcohol or drugs when the loss occurred;
- had not been issued with a permit to take the item off Municipal premises;
- did not obtain a receipt for equipment you voluntarily surrendered;
- acted recklessly or negligently;
- intentionally caused the damage; or ignored any standing instructions (including Municipal Circulars);

YOU SHOULD LOG OFF YOUR COMPUTER EQUIPMENT AFTER HOURS

Unless your personal computer equipment does not need to run after hours, you should log off but leave it on at the end of your working day. This will ensure that any documents you were working on are properly closed, ready for backup. Anti-virus and other security procedures are set to run after hours in order not to interfere with computer performance during the working day.

YOU MUST BE LOGGED INTO THE NETWORK WHEN USING A COMPUTER

The Municipality provides its computer users with access to networked services. It also maintains computers remotely via the network. Computers that are not logged in cannot access networked services and cannot be maintained remotely. For this reason, you may not use your computer without first logging into the Municipal network. You must remain logged in when using the computer.

WORK SHOULD BE SAVED ON A NETWORK DRIVE

When you save work on your computer's local drive or on a USB you risk losing the work when something goes wrong. To avoid this the Municipality provides you with network-based storage, which is more reliable. If a failure does occur, work stored on the network can usually be recovered from a backup.

Consequently, you are advised to save all computer-based work you produce on a network drive. Each user has a home drive on the network. Save your work here. If you are producing work that needs to be shared, your group should ask the IT Helpdesk to set up a shared folder on the network.

You may not save, on any of the network drives, files that are unrelated to Municipal business. Any private or personal files should be saved on your local drive or on a USB drive.

YOU MUST OBTAIN A PERMIT BEFORE TAKING EQUIPMENT OFF-SITE

You may need to take portable equipment off Municipal premises, either to work at home or at another site. You must obtain written permit from your head of section *before* any equipment is removed. The permit must indicate your name as well as the description and serial numbers of equipment to be removed. The permit must also indicate an expiry or return date. Where an item is regularly removed, the permit may be issued for a maximum of 12 months.

YOU MAY NOT MOVE OR TAMPER WITH COMPUTER EQUIPMENT

Only authorized support personnel may move, upgrade or repair computer equipment. You may not remove, install or tamper with any internal component of your computer or the equipment that may be attached to it (e.g. printer). You may not move your computer equipment to another desk, room, or site - unless it is specifically designed to be carried around (e.g. notebook computer). You may not swap equipment with another user. Moving or swapping equipment will create an error in the asset register. Contact management, who will arrange for the equipment to be moved for you.

Make sure that you obtain a receipt for any computer equipment that is removed from your control. This includes equipment removed for upgrade or repair.

Users may open a printer to remove or replace paper as well as toner or print cartridge.

YOU MAY NOT USE OR STORE UNLICENSED SOFTWARE

The Copyright Act 98 of 1978 protects intellectual property against theft. If you use software without a license, you may be found guilty of a criminal offence. The author of the software may also seek civil damages. The Municipality will hold you liable for criminal or civil action that results from your infringement of copyright.

ONLY AUTHORISED SUPPORT STAFF MAY INSTALL OR COPY SOFTWARE PROGRAMS

To avoid breaking the law, the Municipality needs to control carefully the software licenses it owns. For this reason:

- Only authorized support personnel may install or upgrade software on a Municipal computer. A valid license must be allocated to each installation.
- Only authorized support staff may copy computer programs. A program may be copied only if allowed by the licensed agreement, and then only for official purposes. A user may be held personally liable for any damages, and legal costs, if he or she copies software illegally.

Maintaining central control over licenses and installations also protects you, the user, from unknowingly breaking the law.

YOU MAY PROVIDE YOUR OWN SOFTWARE, WITHIN LIMITS

There are circumstances where users will be allowed to provide their own software, or software licensed to a service provider. In this case, you must provide documentary proof that you hold a valid license before the software will be installed. The Municipality has the right to hold the license until the software is removed. The Municipality will not replace a license if it is lost, nor offer compensation.

Only authorized support staff may install the user-provided software programs.

WHAT IF THE MUNICIPALITY WROTE THE SOFTWARE?

The Municipality will normally own the copyright for software written "in-house", by the Municipality. Such software may be used within the Municipality without a license. But, users must still have these programs installed by authorized support staff.

You are still committing an offence if you copy, for non-official use, software owned by the Municipality.

IF YOU DISCOVER UNLICENSED SOFTWARE...

If you know or suspect that software on your computer is unlicensed, you must contact management who will address the problem. Make a note of the call.

YOU SHOULD AVOID STORING INAPPROPRIATE MATERIAL

Users should take care not to expose others to material that could be considered offensive. This includes words, images of any kind and recorded sounds (audio). If someone else accidentally sees material you store, you could face a charge of harassment. Regular harassment can create a hostile working environment for a co-worker.

You must not create, store, print or e-mail:

- Discriminatory, intolerant or derogatory matter based on race, religion, gender, age, ethnic or social origin, sexual orientation, disability, physical condition, HIV status, conscience, belief, political opinion, culture, language or birth.

Any form of violence, pornography, explicit nudity, sexual acts, gross depictions, satanic, militant or extremist material.

THE MUNICIPALITY IS NOT RESPONSIBLE FOR MATERIAL VIEWED

Offensive material may have been stored on your computer by another user - either accidentally or in violation of Municipal policy. You may accidentally view this material. The Municipality is not responsible for material viewed on your computer. You use your computer at your own risk. If you discover any offensive material on your computer, or on the network, you should report it to the Information Technology Officer.

MANAGERS MAY MONITOR SOFTWARE USE BY STAFF

The Municipality has a right, but not a duty, to monitor any aspect of its computer system, including use of the software on its computers. Monitoring is justified by the need to apply this policy and to measure software usage for licensing purposes. Managers may monitor a particular software program, use by certain individuals or use by their staff as a whole.

Users are also reminded that some members of management and IT personnel have unlimited access to the network and personal computers for maintenance and security reasons.

MANAGERS ARE ACCOUNTABLE FOR COMPUTER USE BY THEIR STAFF

Managers should ensure that all their computer-using staff, whether temporary, permanent or contract is made aware of the contents of this policy. You are required to apply the policy to all those who report to you. You are accountable for the use your staff makes of personal computer equipment, software and services.

D. APPLICATION OF THIS POLICY

The computer use policy will be applied in several ways:

- Where technology allows, policy will be enforced automatically. For example, Games can be prevented from running on the server.
- Management reports will highlight possible violations. These will be investigated to identify actual violations. The offender's manager will take disciplinary action in line with Municipal policy.
- Users may self-police the policy by reporting any violations via the grievance procedure.
- The Information Technology Officer may issue a specific instruction.

E. DISCIPLINARY ACTION

Some aspects of this policy are for information; others tell you what you may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Disciplinary Code and Procedures of the Municipality.

F. TERMINOLOGY

Computer virus
A computer program that interferes with, or damages the normal operation of the computer or software. Virus programs are designed to infect other computers by hiding within e-mails or runnable programs.

Copyright
Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works--as by reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the pecuniary benefits derived from it.

Municipality
The Bergrivier Municipality, under the West Coast District Municipality, Western Cape in the republic of South Africa.

Intellectual property
A broad category of intangible materials that are legally recognized as proprietary to an organization. In the computer field, hardware circuits, software and text is copyrightable. Depending on the situation, the algorithms used within hardware circuits and software may also be patentable, and most brand names can be trademarked. However, IP covers more than just copyrights, trademarks and patents; for example, customer databases, mailing lists, trade secrets and other business information are also included.

ITC Information Technology Committee.

Prescripts Regulations, instructions and directions.

USB Drive A removable disk on which data may be stored. For the purpose of this policy the term includes any removable storage device fitted to a personal computer.

H. NOTES

Certain terms in this policy should be understood expansively to include related concepts. Department includes all internal divisions.

All employees granted computer access using Municipal facilities will be provided with a written copy of this policy. This policy will also be posted on the intranet so that it is available and conspicuous to employees at all times.

2. INTERNET AND EMAIL USAGE POLICY

A. PURPOSE

The internet and email have emerged as valuable and cost-effective tools for municipal employees. However, press and court cases from around the world underscore the fact that these technologies may also pose potential problems for both employers and individual employees.

The Municipality provides selected and authorized employees with internet access and electronic communication services for the performance and fulfilment of their job responsibilities. This Internet and Email Usage Policy is designed to encourage the appropriate use of these services subject to compliance with the requirements stated therein which are necessary to minimize risks associated with such usage.

Authorized users of the internet and email services provided by the Municipality must appreciate that the access thereto is for the purpose of increased productivity and not for private activities. Authorized uses must also appreciate that any connection to the internet offers an opportunity for non-authorized users to view or access corporate information. Therefore, it is important that all connections be secure, controlled, and monitored.

These guidelines encourage all authorized employees to use common sense when they use the Municipality's internet and/or email facilities. While the Municipality has the ability to monitor internet usage, it does not do so routinely. Municipal employees are trusted colleagues and are expected to use all business tools appropriately. However, if instances of abuse of internet access become prevalent, more active monitoring might be needed. The Municipality will comply with reasonable request from law enforcement and regulatory agencies for access to logs, diaries, archives and other records regarding any employee's internet and email activities. All employees using internet and email resources are also reminded that the Municipality's internet and email files may be subject to disclosure under provisions of the law. To this end, users should have no expectation of privacy while using municipal owned or leased equipment. Information passes through or stored on equipment belonging to the Municipality can and will be monitored. Users should, further, understand that the Municipality maintains the right to monitor and review internet use and email communications sent or received by users as may be necessary or required.

Authorized internet and email users may send and receive email attachments that do not exceed 5 MB in size, provided that all attachments are scanned before they are opened by the Municipality's chosen anti-virus and content filtering software. The Municipality also acknowledges that some positions require that larger documents, logs and other files need to be sent or received by email and will consider exceptions on written requests.

To comply with international SPAM standards, employees are not permitted to send emails with more than 20 recipients. A breach of this may result in the municipality being temporarily blacklisted on the internet.

B. SCOPE

This policy applies to all employees who have been granted internet and/or email facilities. Whether this is from a computer, network enabled device (such as a multi-function printer), and mobile devices (where applicable).

C. POLICY STATEMENTS

Authorized employees should contact the Information Technology Officer if they have any questions about the following guidelines:

- The display of sexually explicit image or document on any municipal system, including related “chat-room” conversations, is prohibited and may constitute a violation of the policy on sexual harassment. In addition, such explicit material may not be archived, stored, distributed, edited or recorded using the municipal network or computing resources.
- The display of any kind of offensive image or document on any municipal system that violates any municipal policy prohibiting discriminatory or harassing activities affecting any protected group is prohibited and may constitute a violation of the municipal policy on harassment or discrimination. In addition, such material may not be archived, stored, distributed, edited or recorded using the municipal network or computing resources.
- If an authorized employee is connected unintentionally to a site that contains sexually explicit or other offensive material, he/she must disconnect from that site immediately and report the site tot IT.
- The Municipality’s internet facilities and other information technology resources may not be used knowingly to violate any applicable laws, statutes, ordinances or municipal policies. Use of municipal resources in connection with any illegal activity is grounds for immediate dismissal and it is the policy of the Municipality to co-operate with any legitimate law enforcement investigation of potential criminal activity.
- To prevent computer viruses or other potentially harmful computer codes from being transmitted to or through the Municipality’s information technology systems, the downloading or installation of any software or computer code is strictly prohibited unless explicitly authorized by the Municipal Manager or his/her nominee. All software downloaded or installed must be registered to and becomes the property of the Municipality.
- Any software or files downloaded via the internet to the Municipality’s network remains the property of the author and may be removed by the Municipality without reference to the official who downloaded such software or files. Any such files or software may be used only in a manner consistent with their licenses or copyrights. No employee may, furthermore, use the Municipality’s internet or email facilities to knowingly download or distribute pirated software or data. Violations of any software license agreements of information service contracts by the unauthorized duplication of software, files, operating instructions or reference materials is also strictly prohibited.
- No employee may use the Municipality’s internet or network to:
  - Download entertainment software or games, or to play against opponents over the internet;
  - Download images, audio or video files unless there is an explicit business related use for the material;
  - Upload any such software licensed to the Municipality or data owned or licensed by the Municipality without explicit authorization from the manager responsible for the software or data;

  - Deliberately propagating any virus, worm, Trojan horse, trap-door program code or any other code that may interfere with the operation of any information technology system;
  - Knowingly disable or overload any computer system or network or to circumvent any system intended to protect the privacy, functionality or security of another user.
- No employee may use the Municipality's internet or email facilities for personal financial gain, political activities, to express a grievance, to disseminate confidential or false information or to propagate or encourage hatred or discrimination in any manner whatsoever.
- Each authorized employee using the Municipality's internet and email facilities shall identify themselves honestly, accurately and completely (including department and job title where requested, as well as the facility disclaimer) when using these resources (for example, when participating in newsgroups or setting up accounts on outside computer systems).
- Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the Municipality may speak/write in the name of the Municipality to others, using internet or email facilities. Other employees may participate in newsgroups or forums in the course of business when relevant to their duties, but they do so as individuals speaking as themselves. Where an individual participating is identified as an employee or an agent of the Municipality, the employee must refrain from any unauthorized political advocacy and endorsement or appearances of endorsement by the Municipality. Only those managers and municipal officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the Municipality may grant such authority to newsgroup participants.
- The Municipality retains the copyright to any material created by employees in the course of their official duties, including materials posted to any forum, newsgroup or world-wide web page.
- Copyrighted materials belonging to entities other than the Municipality may not be transmitted by employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy reference only. Failure to observe copyright or license agreements may result in disciplinary action against defaulting employee including dismissal.
- Employees are reminded that newsgroups are public forums where it is inappropriate to reveal confidential information, customer data, and any other material covered by existing municipal confidentiality policies and procedures. Employees releasing protected information via the internet or email, whether or not the release is inadvertent, may be subject to disciplinary action under existing data security policies and procedures.
- The following disclaimer will be added to all emails sent out by the Municipality by any staff member:
  "This message and any attachments may be confidential and may also be privileged or otherwise protected from disclosure. It/they are sent for the attention of the named addressee(s) only. If you are not the named addressee(s) please notify the sender immediately and destroy this message. In this case, you should not copy or distribute this message or attachments, use it/them for any purpose or disclose its/their contents to any other person, opinions, conclusions and other information in this message that do not relate to the official business of the Bergrivier Municipality shall be understood as being neither given nor endorsed by it. Emails cannot be guaranteed to be secure or free of errors or viruses. The sender does not accept any liability or responsibility for any interception, corruption, destruction, loss, late arrival or incompleteness of or tampering or interference with any of the information contained in this email or for its incorrect delivery or non-delivery for whatsoever reason or for its effect on any electronic device of the recipient."

- Authorized employees may use the Municipality's internet and email facilities for non-business research or browsing during their lunchtime or designated break or outside working hours, provided that such activities do not interfere with their official duties and that all other departmental usage policies are adhered to.
- The limited use of information technology resources for personal or charitable purpose by authorized employees during non-work hours is permitted provided, that the permission of such employee's supervisor is obtained and that consumable supplies, such as paper goods, are replaced.
- The Municipality may install a variety of firewalls, proxies, internet address screening programs and other security systems to assure the safety and security of its networks. Any employee who attempts to disable, defeat or circumvent any municipal security facility will be subject to immediate disciplinary action including dismissal.
- Computers that use modems to create independent data connections may interfere with municipal network security mechanisms and can potentially be used by a third party to compromise the Municipality's network security. Any computer used for independent dial-ups or leased line connections to any computer or network, must be approved by the Municipal Manager.

ADDITIONAL PROHIBITIONS

While these guidelines define how authorized municipal employees can and cannot use the Municipality's internet and email facilities, they cannot cover every conceivable situation. For this reason, common sense and profession courtesy will still be required by any authorized user. For example, internet sites can include information or images that are acceptable to some people but others. The best practice is to err on the side of caution while using these resources. The most publicized examples of inappropriate materials including those with sexually orientated images, racism and hate speech. These sites may include "jokes" or other offensive messages that are sometimes forwarded via email to co-workers or others. It is obviously unacceptable for such material to be identified as coming from the Municipality. Material on the internet does not have to be illegal or blatantly offensive to be deemed inappropriate for the workplace. Specifically, while limited personal use of internet and email facilities is allowable, as outline above, excessive access to non-business related sites (e.g. those that feature sports, stock and other financial data, vacation and travel planning, consumer products, and entertainment) is not allowed.

D. APPLICATION OF THIS POLICY

The computer use policy will be applied in several ways:

- Where technology allows, policy will be enforced automatically. For example, Anti-Virus and Internet Proxies can filter and restrict content.
- Management reports will highlight possible violations. These will be investigated to identify actual violations. The offender's manager will take disciplinary action in line with Municipal policy.
- Users may self-police the policy by reporting any violations via the grievance procedure.
- The Information Technology Officer may issue a specific instruction.

E. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses of internet or email facilities could violate the Municipality's Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. Violations will be assessed on a case-by-case basis. If it is determined that an unauthorized user has violated one or more of the above use restrictions, that user will receive a reprimand from his or her supervisor and his or her future use will be closely monitored. If a gross violation has occurred, management will take immediate action. Such action may result in an authorized employee losing internet and/or email privileges, severe reprimand, or termination of employment at the Municipality.

Whilst this policy contains explicit guidelines for internet and email usage, the main issue is finding ways and means to use all of the Municipality's resources to promote its business goals. This means the use of the internet and email exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal internet and email facilities. This includes careful observances of copyright, software licensing and the privacy of others.

F. TERMINOLOGY

Computer virus

A computer program that interferes with, or damages the normal operation of the computer or software. Virus programs are designed to infect other computers by hiding within e-mails or runnable programs.

Copyright

Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works--as by reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the pecuniary benefits derived from it.

Municipality

The Bergrivier Municipality, under the West Coast District Municipality, Western Cape in the republic of South Africa.

Intellectual property

A broad category of intangible materials that are legally recognized as proprietary to an organization. In the computer field, hardware circuits, software and text is copyrightable. Depending on the situation, the algorithms used within hardware circuits and software may also be patentable, and most brand names can be trademarked. However, IP covers more than just copyrights, trademarks and patents; for example, customer databases, mailing lists, trade secrets and other business information are also included.

G. NOTES

Certain terms in this policy should be understood expansively to include related concepts. Department includes all internal divisions. Internet includes the Municipality's intranet and associated information technologies systems. Employee includes any person given access to the Municipality's internet, intranet and/or email facilities, including employees of the state, interns, limited term and contract employees in the service of or seconded to the Municipality. Document covers any kind of file that can be read on a computer screen as if it was a printed page, including HTML files read in an internet browser, any file meant to be accessed by a word processing or desk publishing program or its viewer. Graphics includes photographs, pictures, animations, movies, or drawings. Display includes monitors, flat panel active or passive displays, monochrome LCD’s, projectors, televisions and virtual reality tools.

All employees granted internet and/or email access using municipal facilities will be provided with a written copy of this policy.

3. IT DATA AND SYSTEM SECURITY POLICY

A. PURPOSE

This document defines the policy of Bergrivier Municipality for the application of Information Security to protect the municipality's corporate information, information systems and applications against all threats, which could endanger their confidentiality, integrity and availability.

The objective of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. The purpose of this Policy is to protect the municipality's information assets in terms of Confidentiality, Integrity and Availability.

B. SCOPE

This policy applies to all offices and users of information within Bergrivier Municipality. It applies across hardware platforms, to all departments, business units and to all partners, staff and contractors of the municipality.

C. POLICY STATEMENTS

All managers within the municipal departments are responsible for ensuring that personnel receive and understand the IT policy. Staff are required to sign a confidentiality and security undertaking.

Clients and stakeholders that access the municipality's facilities are required to sign Security Undertakings accepting the conditions as set out in this policy.

The management of the network rests with the Computer Information Systems department and can involve third party contractors as a service provider for the Bergrivier Municipality. Where this is so, the service provider must sign a Security and Confidentiality undertaking accepting the guidelines and rules as set out in this policy.

Non-Municipal employee's access to the network is subject to the security policy. Consultants employed in a permanent capacity by the municipality are classified as municipal employees for the purposes of this policy.

Part time contractors and consultants who may have access to municipal facilities, infrastructure, systems and information will be required to sign a confidentiality and security undertaking.

HIGH LEVEL INFORMATION SECURITY PRINCIPALS

Protection

Bergrivier Municipality's information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems, which process it (microcomputers, firewalls, voice mail systems, etc.), or the methods by which

it is moved (electronic mail, face-to-face conversation, etc.). Such protection includes restricting access to information based on a need-to-know basis.
Municipal management must devote sufficient time and resources to ensure that information is properly protected.

Risk Management

Municipal managers are ultimately responsible to ensure that the information is protected in a manner that is acceptable to higher management. To achieve this objective, risks should be identified by conducting regular risk analysis and, to take corrective measures where applicable.

Information Management

Decision-making within Bergrivier Municipality is also critically dependent on information and information systems. Management is expected to know the nature of information they use for decision-making (accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc.). The awareness of and fine-tuning of such information attributes is an important information management activity.

Co-Operation

Information security requires the participation of and support from all information users. All users (employees, consultants, contractors, third parties and temporaries) must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage municipal information assets. Training materials should communicate that information security is an important part of the municipality. Training and documentation with respect to information security is the responsibility of the Information Technology Department in conjunction with the Human Resources Department.

Organization

Guidance, direction, and authority for information security activities are centralized for the entire organization in the Section Head of Information Services. The office is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of the Internal/external Auditors. Investigations of system intrusions and other information security incidents are the responsibility of the Information Technology Department and the relevant department Manager.

Privacy

All messages sent over municipal computer and communications systems are the property of Bergrivier Municipality. To properly maintain and manage this property, management reserves the right to examine all data stored in or transmitted by these systems. Since Bergrivier Municipality's computer and communication systems are provided for business purposes, workers should have no expectation of privacy associated with the information they store in or send through these systems. In recognition of the privacy requirements as stated in the Constitution of South Africa, personal information will not be disclosed to any third party unless explicitly required through legal processes.

Third Parties

As a condition of gaining access to Bergrivier Municipality's computer network, every third party must secure its own connected systems in a manner consistent with the municipality's requirements. Bergrivier Municipality reserves the right to audit the security measures in effect on these connected systems without warning. The municipality also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements.

GENERALLY ACCEPTABLE POLICIES

The following policy statements constitute the core of the municipality's Information Security Policy for information and will be supported by information security procedures and standards as needed from time to time.

Classification

Information must be categorized into levels of sensitivity and protected in accordance with appropriate requirements as part of the risk management process. The sensitivity classification standard must be used throughout the municipality to ensure that the level of protection is commensurate with the controls required (security mechanisms) to protect the information against disclosure (confidentiality), modification (integrity) and / or destruction (availability and use).

Confidentiality

The confidentiality of data, depending on classification and information security directives, is recommended to be protected before transmission over networks, and where indicated during the storage of such data. Unless authorized by management, information may not be made available or disclosed to unauthorized individuals, entities or processes.

Measures should be implemented to protect information against unauthorized access, disclosure, copying, sniffing, eavesdropping and /or theft of information assets.

Availability

The continued availability and usability of services in accordance with business requirements must be ensured by implementing appropriate measures to prevent and recover from the loss of data due to acts of persons, system failures or disasters.

All information assets should be protected against:

- Destruction, damage or contamination
- Denial of authorized / legitimate access
- Delay of use or access
- Natural disasters
- Computer virus infections

Integrity

The integrity of all data, depending on classification and information security directives, is recommended to be protected at all times before transmission over networks, and where indicated, also during the storage of such data.

All information assets should be protected against threats to data integrity including unauthorized modification, destruction, and misrepresentation of data and / or computer virus infections.

Non-Repudiation

All access to the municipality's technology resources is subject to positive identification and authentication of the user before access is granted.

Measures must be implemented to ensure the non-repudiation of all financial transactions in accordance with official legislation and regulations.

Accountability

Measures must be implemented to ensure that it is possible to determine who is responsible for an action, when and from where. The measures must be in accordance with the security requirements as determined by the departmental manager.

Access Control

All data and information should be protected and safeguarded against unauthorized access. Access to technology resources will only be granted in line with the user's specific responsibilities (need-to-have principle).

Authentication

Measures must be implemented to uniquely identify or verify IT users, peripherals and / or programs and to assure individual accountability. The authentication mechanisms must be in accordance with the classification of the information that requires protection and may for example take the form of passwords, tokens, or biometric identification devices.

All users will access Bergrivier Municipality's information systems through at least the use of a unique user identification number and secret password. As a first line of defence, users should not select passwords that are easily guessable nor should personal passwords be shared with any other user.

Reporting of Security Incidents

All known vulnerabilities – in addition to all suspected or known violations – must be reported in an expeditious and confidential manner to the Manager of Computer Information Systems. Unauthorized disclosure of the municipality's information must additionally be reported to the involved information owners. Reporting security violations, problems or vulnerabilities to any party outside the municipality without prior written approval of the Information Technology Officer is strictly prohibited.

Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violations is strictly prohibited and cause for disciplinary action.

Exceptions

Exclusions based on a valid business need could be motivated for and formally authorized, in which case record would be kept of the exclusions to facilitate effective management / control processes.

MANAGEMENT POLICY

General Requirements

- Applications for remote access services will only be allowed to personnel and clients or contractors, based on a valid business need. All applications must be motivated and recommended in writing by the applicant's Director / business unit requesting the access, and handed to the Manager of Computer Information Systems. The Information Technology Manager will consider all applications for approval after consideration of the risk. Periodic access reviews will be conducted with the assistance of HR to ensure incumbents are still employed by the municipality. All accesses must be reviewed at least annually by the applicant's manager and where applicable, terminated / suspended.

- As part of the application process and before access is allowed, the user(s) applicant should sign an agreement confirming that all policies and procedures (with specific reference to anti-virus software on his / her computer) will be adhered to and that only licensed / legal software is installed on the computer.
- A central register must be maintained by the IT function or department responsible for IT of all users with dial-in / remote accesses, also indicating the access authorities to facilitate auditable processes.
- To minimize the risk of compromising security, all users of the remote access services must receive training before access is allowed. The training should include what is allowed and what is not allowed during sessions.
- In order to ensure compliance in terms of software, hardware and security requirements, the computer used for the remote access should be provided by the municipality. The use of private (home) computers may only be allowed if based on a valid business need and must be processed as a deviation from this policy. The manager/department responsible for IT security shall maintain a central register of all the deviations.
- The remote client (computer used to access the municipality's network) must have anti-virus software and the correct level of security patches as prescribed by the IT function from time to time. A process must be formulated by the IT function to ensure the regular update of the software/patches.
- Under no circumstances may the access privileges be transferred to another user without following the official normal application procedure.
- No user may be provided with access privileges that exceed those than would otherwise be afforded if working in the office (least access / authorization principle). For example if the request was to have access to the mailbox/calendar, no other access may be provided.
- To prevent an open session from being misused by unauthorized persons, all sessions must automatically be logged-off after 30 minutes of inactivity.
- The users are responsible for both logical and physical security mechanisms to the computer that is used to obtain the remote access. Due to the risk of theft, users are advised to save all data on the central server drive provided. The municipality's security requirements must be communicated to users during the training session. Comment: Logical access control refers to the measures taken to prevent an unauthorized person to get access to your computer whereas physical mechanisms relates to the physical measures taken (first and second perimeter of defence).
- Confidential information stored on remote computers must be protected against unauthorized access.
- Formal agreements with clients, partners, contractors or third parties is a requirement and must include the principle that required minimum standards compliance must be verifiable/auditable if remote access is provided.

Authentication Requirements

- Authentication servers must be configured to enforce the municipality's password standards. Strict physical and logical access control to the authentication servers and communication equipment must be enforced.
- As a minimum requirement, a unique user ID and difficult to guess password must be used for authentication.
- Users having power access privileges (e.g. to execute remote maintenance tasks and access to sensitive information and / or critical resources), may only be allowed access through the municipality's accepted authentication mechanisms. (Sensitive information is defined as information that if disclosed, will seriously and adversely affect the municipality, its business partners and / or clients and will constitute a serious compromise in the status of the municipality's operational security).

- A forced password change must be implemented on the first sign-on session (to change the initial password) and thereafter every thirty (30) days. The IT function should implement a process to ensure the secure communication of the initial password.
- No double sessions with the same authentication information may be allowed.
- To confirm the origin of the connection, dial-back features must be implemented if token-based authentication is not utilized.
- Authentication information between the users and the authentication servers must be protected with encryption.
- Users no longer requiring the access (e.g. change in job description or transfer) must be immediately removed from the system. Line management must reconsider the access privileges of users who resign as soon as possible after formal notice of the resignation. Special attention should be given to audit logs to ensure that the accounts are no longer active.
- All changes to existing and new user accounts/profiles must follow a formal change management process.
- In support of the information security strategy to protect, detect and re-act, all available audit logs and alert facilities must be enabled with monitoring and review processes in place. The reports must be reviewed by the IT support/security function and, where applicable, investigated / escalated to the manager responsible for IT security.
- The municipality reserves the right to suspend / cancel any account(s) that acted in contradiction to this policy or any other procedural requirement as formulated from time to time.

Passwords

- Passwords must NEVER be disclosed to anyone aside from a network administrator. If the user suspects that the confidentiality of the password has been compromised, the user must change it immediately and inform the Information Services Helpdesk.
- Passwords must be changed every 30 days; the authentication server must be set to automatically expire passwords after 30 days.
- Passwords should be made up of characters using:
    - Alpha (alphabetical letters), numeric (whole numbers), upper & lower case and symbols.
    - They should have a minimum length of 8 characters.
- Never use any dictionary words, acronyms, birthdays, sequential numbers, family names, football teams; dates etc., as software tools can easily crack these (must not be easily guessable).
- Passwords should not be written down unless protected in some or other form (e.g. by using a sort of encryption and locking it away).
- The authentication server/system will maintain a list of up to 5 previous passwords used per user and each new password should contain at least 3 changes. The objective of this rule is to prevent users re-using the same password over and over.

Access Control Policy

- Access to systems will only be granted where there is a clearly established business need, which is consistent with the roles and responsibilities of those granted access.
- Staff must not attempt to bypass the physical security mechanisms measures.
- The physical security steps taken are the first line of defence against unauthorized access to the municipality’s information assets.

D. APPLICATION OF THIS POLICY

Where possible, this policy will be applied automatically through means of security settings on servers, anti-virus and similar software. IT staff may also need to apply aspects of this policy manually. Employees are encouraged to familiarise themselves with this policy and adhere to it as well as report any deviations observed to the Information Technology Office.

E. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality's Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality's resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

F. TERMINOLOGY AND DEFINITIONS

Information security encompasses the management processes, technology and assurance mechanisms that will allow departments to trust their transactions, the information is usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and that confidential information is withheld from those who should not have access to it.

G. NOTES

Information and information systems are critical and vitally important to the municipality. Without reliable information the municipality could be adversely affected, both financially and reputation wise. Therefore, this policy states the minimum requirements and the responsibility that all employees, temporaries, contractors and management must comply with in order to secure the municipality's information.

This policy sets out the approach taken to manage information security to ensure that information assets are properly protected against a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental.

Bergrivier Municipality management has a duty to preserve, improve, and account for all information and information systems. They must additionally make sure that information assets are protected in a manner that is at least as secure as other organizations in the same industry handling the same type of information. To achieve this objective, annual reviews of the risks to Bergrivier Municipality's information assets will be conducted.

Similarly, whenever a security incident or audit finding indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce the municipality's exposure.

The municipality's information must be protected in a manner appropriate to its sensitivity, value, and criticality. Security measures are therefore used regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. This protection includes restricting access to information based on the need-to-know principle.
Decision-making within the municipality is also critically dependent on information, as management need to be able to rely on the integrity of information in terms of accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc. The awareness of and fine-tuning of such information is an important information management activity.

Information security requires the participation and support from all staff (including consultants, contractors, and temporaries) that will be provided with sufficient training and supporting procedures / policies to allow them to properly protect and manage the municipality's information assets.

It is the responsibility of all municipal staff to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats observed or suspected to systems or services to the manager of Computer Information Services as soon as possible to enable the volumes and costs of incidents and malfunctions to be quantified and monitored.

4. NETWORK SECURITY POLICY

A. PURPOSE

The purpose of this policy is to provide a solid foundation for the development, implementation and maintenance of secure practice within Bergrivier Municipality's networking environment.

B. SCOPE

This policy applies to all network administrators, technical and maintenance personnel, designers, users and the owner of the municipality's network. The network security policy is considered as part of the municipality's Security Policy.

C. POLICY STATEMENTS

GENERAL POLICY REQUIREMENT

It is the policy of the municipality to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information. As a minimum, authentication, access control, privacy (confidentiality), integrity, availability and audit logging must be implemented as security services on the municipality's network where possible.

AUTHENTICATION

All network devices, management stations and network users / administrators must have unique identifiers in accordance to a defined naming convention. Passwords must be implemented in accordance with the municipality's password standards.

LOGICAL ACCESS CONTROL

Access control mechanisms must be implemented on all network devices and management systems. Access may only be granted in line with the job responsibilities of network administrators (based on the "need-to-have" principle). External access to network devices and management systems must be restricted to the minimum and where applicable, strict control mechanisms must be implemented.

PRIVACY / CONFIDENTIALITY

All reasonable measures must be taken to ensure that internal and external communications between networks and network devices as well as client interfaces may not compromise security. Where applicable, encryption mechanisms must be implemented.

INTEGRITY

Mechanisms / procedures must be in place to ensure the integrity of all network devices and traffic. Real time alerts should be generated for all configuration / permission changes that can lead to a breach in security.

AUDIT LOGGING / ACCOUNTABILITY

Audit information, including alerts generated for failed logon attempts, must be available network devices and management systems where applicable.

AVAILABILITY

Network(s) and network services must be available as and when required and capable of handling the network traffic requirements.

NETWORK MANAGEMENT

- The Manager of the Information Technology Department must assign overall responsibility for network activity and act as network owner. It is the responsibility of the network owner to, among others; ensure compliance with this policy and to provide monthly feedback with regard to the state of compliance as part of the municipality's information security risk management process.
- Network strategy, standards, principles, guidelines, architectures, procedures, design, configuration, equipment, software, inventories and cabling information must be formally documented, kept up to date and reviewed annually. Only authorized personnel may be allowed access to this information/documentation in accordance with the sensitivity / security classification.
- Human resources and infrastructure that are critical to the continuity of network services should be identified and single points of failure must be minimized.
- All external connections to the municipality's network must be preceded with a risk analysis and at a minimum be protected by a firewall or similar type of device. Non IP network connections must be secured by definition characteristics and / or specific configurations to restrict access capabilities and to meet the security requirements. The connections must be reviewed periodically via a traceable process. Where applicable, internal networks (i.e. LAN's), where sensitive information is processed, must also be protected commensurate to its sensitivity.
- All external connections / third parties to the network should be assigned an owner, approved by the network owner and the head of the Department involved, individually identified and recorded. (Please refer to the detailed policy on third party connections).
- In order to provide a clear picture of the network and to minimize unwanted connections, network access control must be centrally approved by the network owner or a responsible person as appointed by him/her.
- The municipality's network should preferably be protected by creating a DMZ. No sensitive information may be stored in the DMZ.
- Services obtained from external service providers must be defined in formal agreements. The agreements must specify the requirements for security controls. Mechanisms must be in place to measure adherence to these requirements.
- Only network services required specifically for business purposes are allowed and all unnecessary network services must be disabled.
- Formal set-up standards must be agreed too and no network device may be deployed in the operational environment with default / factory password settings or any other configuration that poses a threat to security for example open FTP ports or broadcasting configuration information over the network.
- Formal processes must be implemented to ensure that all applicable security patches are kept updated.
- Methods and procedures must be implemented whereby network security issues are dealt with in a consistent manner. The results must be archived for future reference purposes.

TRAFFIC MANAGEMENT

- Network devices must be configured to prevent unauthorized access. The configuration(s) must be reviewed at least annually or after significant changes and health checked at least once every quarter. Unauthorized changes must be handled as a breach of security.
- With the exception of pre-approved operational network sniffing or monitoring devices, no other network sniffing or monitoring devices may be installed / activated without the explicit authorization of the Manager of the Information Technology Department.

- Measures must be implemented to ensure the network filtering devices cannot be bypassed and can only be accessed from designated workstations or specified IP addresses via authorized secure channels (for example SSL).
- Divulgence / broadcast of information about the network must be restricted to the absolute minimum.
- Traffic flowing over the network must be afforded the same protection / security characteristics as when stored in accordance with the classifications of the information.

NETWORK OPERATIONS

- Service levels between service providers and the municipality must be agreed too and continuously and formally monitored to ensure an acceptable level of service. All unusual entries / activities must be investigated and reported to appropriate line management for corrective action.
- Pre authorized intrusion detection mechanisms should be employed as protection against possible attacks (depending on budget and availability of technical skills).
- Effective incident response, business continuity and disaster recovery planning processes must be implemented.
- Network changes must be documented and formally accepted by the network owner and follow an accepted IT change management policy and standard.
- Physical access to network devices must be restricted to authorized personnel. Service providers and / or contractors with no service record / history, must remain under constant observation when allowed access to restricted areas.
- To reduce the risk of data in transit being intercepted, special care must be taken to protect network cables from tampering or disruption.
- Back-up versions of essential network information and software (including communications software and utilities, network control tables / settings, configuration diagrams and inventories and device configurations) must be taken at such intervals required for the continued availability of the network. The back-ups should be protected from loss, damage and unauthorized access by storage in a fireproof safe on-site and copies off-site.
- Remote maintenance must be controlled by restricting access rights and logging all activity. Diagnostic ports on network equipment must be protected by access controls.
- Access to network devices that are primarily used for security services must be approved by the Manager of Computer Information Systems. Access to any other network devices must be regulated via a formal process to request and authorize access. Record must be kept regarding the authorized access and a process implemented to ensure the timorous revocation of redundant access. The controls must be in the form of formal and traceable processes.
- Internal or external remote maintenance sessions to devices that form the security barrier (the security objects used for protection) may not be allowed unless protected / controlled through a secure channel (e.g. SSL for Telnet)
- No modems may be connected to the network without the prior approval of the Manager of the Information Technology Department. A register of all approved modems must be maintained by the Information Technology Department.
- No user may simultaneously be connected to another network by using a modem while still connected to the municipality's network.

RISK MANAGEMENT

- A formal risk analysis must be carried out at least annually for networks that support critical business applications. The results of risk analysis must include a clear indication of key risks, an assessment of their potential business impact and recommendations for the actions required to reduce risk to an acceptable level.

- The security status of the network must be subject to thorough, independent and regular security audit / review. Agreed recommendations from security audits / reviews should be implemented and reported to top management.
- With the exception of Internal Audit, no unauthorized or clandestine audit or risk analysis may be conducted without the prior approval of the network owner.
- A risk analysis must be done and the results formally considered before the implementation of technology that could negatively affect the security of the network. (The introduction of wireless networks serves as an example).
- A process must be implemented to ensure compliance with new or existing local and international statutory requirements.

D. APPLICATION OF THIS POLICY

Where possible, this policy will be applied automatically through means of security settings on servers, anti-virus and similar software. IT staff may also need to apply aspects of this policy manually. Employees are encouraged to familiarise themselves with this policy and adhere to it as well as report any deviations observed to the Information Technology Department.

SUMMARY OF MAIN RESPONSIBILITIES

Following is a summary of the main responsibilities as derived from the policy document:

- Internal Audit Formulate Network Strategy
- Implementation of policy
- Awareness
- Policy Update / Revision
- Compliance Monitoring
- Monitor Reports
- Management Information
- Reporting of Security Incidents
- Formulation of Operational Processes
- Formulation of Technical Network Standards
- Risk Analysis
- Centralized Access Control
- Network Inventory
- Network Security Device Management
- Approval of Third Party Connections
- Network Contingency Planning (including disaster recovery)
- Compliance reviews from a management perspective
- Independent ad hoc review

E. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality's Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality's resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

F. TERMINOLOGY

For the purposes of this policy the following terminologies apply:

- **Information Security**
  Information Security encompasses the management processes, technology and assurance mechanisms that will allow the municipality to trust their transactions, the information is usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and that confidential information is withheld from those who should not have access to it.
- **Network Security**
  The protection of networks and their services from unauthorized modification, destruction or disclosure and providing the assurance that the network performs its critical functions correctly.
- **Network Device**
  Any information technology and communication device used to form the infrastructure required for communication services (servers, routers, switches, bridges, firewalls, encryption devices).
- **De-Militarized Zone (DMZ)**
  The frontline when protecting valuables (i.e. information assets) from direct exposure to an entrusted environment, or; a network added between a protected network and an external network in order to provide an additional layer of security.
- **Sensitive Information**
  Any information that, if disclosed without appropriate authorization, will compromise the municipality's security or business initiatives.
- **Network Sniffing**
  The use of hardware and/or software mechanisms to analyse / monitor electronic communications (traffic) over a network.
- **Operational Environment**
  The environment responsible for the implementation and maintenance of the day-to-day security activities.
- **Communication Carrier**
  The infrastructure provided by a service provider (e.g. TELKOM) to interconnect communication devices.
- **Computer Network**
  A range of computers connected by means of communication carriers.
- **Data Traffic**
  Information in electronic format, which is communicated over a communications carrier.
- **Access**
  Physical or logical access to information or information systems through a range of network devices.

G. NOTES

Network security involves the protection of the municipality from the threats posed by authorized and unauthorized network activity. The threat(s) increases due to the interconnectivity of networks and the convergence of different network services (voice, data etc.), making it difficult to draw boundaries around the municipality and to apply controls for the protection of the internal assets.

There are obvious dangers that external connections may increase the risk of a security compromise, whilst being unaware of the risk. Network connections should therefore be protected at a level based on the risk. The assumption must be that connecting parties are to a certain degree hostile and have to be strictly controlled to ensure that the access, for which the connection was agreed, is maintained.

Certain terms in this policy should be understood expansively to include related concepts. Department includes all internal divisions.

All employees granted network access using municipal facilities will be provided with a written copy of this policy.

5. POLICY REGARDING MOBILE DATA CONNECTIONS

A. PURPOSE

To enable the necessary officials to access e-mail and internet after hours or whilst out of town; to ensure efficient and effective communication with internal and external public; and access to valuable information for business. This policy will also provide guidelines to regulate the provision of mobile data connections and applicable payments.

B. SCOPE

This policy shall be applicable to all employees, councillors and support staff that either require or already have a mobile data connections.

C. CONDITIONS

- Application must be submitted with motivation in writing to the Director.
- The facility will only be granted in exceptional cases where the nature of the work of the council or official circumstances dictates that the facility of this nature is required to benefit the municipality.
- Any overdue as a result of the usage of this facility must be approved in the normal manner prior to the work being done or shall be borne by the users.
- All rights of ownership attached to the subscriber’s number and SIM card shall at all times remain vested with the municipality.
- Provision must be made in the budget of the relevant department to cover the cost relating to the acquisition of the mobile connection including hardware, monthly contract fees, excess data, and the like.
- The Information Technology Officer is to guide to process in order to ensure that the correct packages and hardware is acquired.
- In the event of damage or loss of the mobile connection hardware, the service provider will be requested to blacklist the SIM card and the “Policy on the use of Personal Computer Equipment” will be used as a guideline in dealing with the loss.

D. DISCIPLINARY ACTION

Whilst this policy contains explicit guidelines, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of mobile connections exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when accessing the municipal network.

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis.

E. DEFINITIONS

Unless the context clearly indicates to the contrary, the following words bare the meaning ascribed thereto below:

- "**Council**" means the municipal council of Bergrivier Municipality or any duly authorised committee, political office bearer or official of the council;
- "**Full time Councillor**" means a Councillor who has been elected or appointed to an office or has been designated as full – time in terms of Section 18 (4) of the Structures Act, and as further contemplated in the Remuneration of Public Office Bearers Act, 1998 (Act No 20 of 1998) under definitions;
- "**3G card**" means a third generation or associated high speed wireless technology aimed at facilitating internal and external communication electronically.
- "**Agreement**" means application form and the terms of conditions.
- "**Application form** "means the application form completed and duly signed by the applicant for the initiation of the service.
- "**Blacklist**" means the disablement, by electronic or by means of the data card.
- "**Connection date**" means the date on which the service is activated.
- "**Data card**" means a PCMCIA card or USB device used to access the network.
- "**Electronic Communication Act**" means the Electronic Communication Act no 36 of 2005 as amended.
- "**Equipment**" means the hardware that you require to access the system and may include without limitation a data, router and such other device or devices as may be required for this purpose from time to time.
- **"Subscriber"** means the institution / person/s who entered into contract with the service provider.
- "**Hardware upgrade**" means the supply of a new data card upon the expiry of an initial period of at least 24 months against payment of any charges therefore and the simultaneous renewal of the subscription to the service for a further minimum period of 24 (twenty four) months.
- "**Initial period**" means 24 (twenty four) months from the date of activation of the service.
- "**Network**" means the:

  (i) portion of the radio frequency spectrum that has been assigned to the network operator for the purpose of wireless network coverage as envisaged in the Electronic Communication Act and wireless platform owned and managed by the network operator.
- "**Network coverage**" means the geographical area which the service can be accessed and used by the subscriber.
- "**Network operator**" means Vodacom or MTN service provider.
- "**Service**" means the Wireless 3G Broadband Internet Service provided to the subscriber.
- "**Service fees**" means the consideration due and payable by the subscriber for the service as recorded on the application form.

6. BLUETOOTH SECURITY POLICY

A. PURPOSE

This policy provides for more secure Bluetooth Device operations. It protects the municipality from loss of Personally Identifiable Information (PII) and proprietary municipal data. This policy will also protect the municipality from the risk presented by Bluetooth enabled devices (such as cellular telephones) that are on municipal premises but not owned or controlled by the municipality.

B. SCOPE

This policy is applicable to all employees bringing Bluetooth enabled devices into municipal buildings as well as authorized Bluetooth equipment. This includes, but is in no way limited to, cellular telephones, headsets, wireless memory devices, and devices such as laptops with internal or external Bluetooth antennas.

C. POLICY

VERSION LEVEL

No Bluetooth Device shall be deployed on municipality equipment that does not meet Bluetooth v2.1 specifications without written authorization from the ITC Officer. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

PINS AND PAIRING

When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area. If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, **you must refuse the pairing request and** report it to the ITC Officer immediately. Unless your Bluetooth device itself has malfunctioned and lost its pin, this is a sign of a hack attempt.

DEVICE SECURITY SETTINGS

All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.

Switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed.

Update the device's firmware when a new version is available.

SECURITY AUDITS

CIS shall perform audits to ensure compliancy with this policy. In the process of performing such audits, CIS shall not eavesdrop on any phone conversation.

UNAUTHORIZED USED

The following is a list of unauthorized uses of municipal owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.

- Using municipal owned Bluetooth equipment on non- municipal owned Bluetooth enabled devices without written approval from CIS.
- Unauthorized modification of Bluetooth devices for any purpose.

USER RESPONSIBILITIES

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth users must only access municipal information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to the ITC Officer.
- Users are to disable the Bluetooth on devices not authorized for connection (e.g.: Cellphones) when on municipal property.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

D. APPLICATION OF THIS POLICY

Where possible, this policy will be applied automatically through means of security settings on servers, anti-virus and similar software. IT staff may also need to apply aspects of this policy manually. Employees are encouraged to familiarise themselves with this policy and adhere to it as well as report any deviations observed to the Information Technology Department.

E. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

7. TECHNOLOGY EQUIPMENT DISPOSAL POLICY

A. PURPOSE

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of municipal data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

This policy has been developed to define the requirements for proper disposal of technology equipment at the municipality.

B. SCOPE

This policy applies to all technology equipment owned by the municipality.

C. POLICY

TECHNOLOGY EQUIPMENT DISPOSAL

When technology assets have reached the end of their useful life they should be sent to the local Information Technology office for proper disposal.

The ITC Officer will securely erase all storage mediums in accordance with current industry best practices.

Equipment which is working, but reached the end of its useful life to the municipality, will be disposed of by donation and/or auction as defined by law and the asset management policy.

Finance and the IT departments will determine an appropriate cost for each item.

All purchases are final. No warranty or support will be provided with any equipment sold.

Any equipment not in working order will be donated or disposed of according to current environmental guidelines.

Prior to leaving the municipality premises, all equipment must be removed from asset inventory system.

MUNICIPAL RAMIFICATIONS

Failure to properly dispose of technology equipment can have several negative ramifications to the municipality including fines, negative public perception and costs to notify constituents of data loss or inadvertent disclosure.

D. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

8. NETWORK ACCESS POLICY

A. PURPOSE

The municipal network infrastructure is provided as a central utility for all users of municipal Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet municipality demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

The purpose of the municipal Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of municipality information.

B. SCOPE

The municipal Network Access Policy applies equally to all individuals with access to any municipality Information Resource.

C. POLICY

Users are permitted to use only those network addresses issued to them by ITC Officer.

All remote access (dial in services) to municipality will be either through an approved modem pool or via an Internet Service Provider (ISP).

Remote users may connect to municipality Information Resources only through an ISP and using protocols approved by municipality.

Users inside the municipality firewall may not be connected to the municipality network at the same time a modem is being used to connect to an external network.

Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the municipality network without ITC approval.

Users must not install network hardware or software that provides network services without ITC approval.

Non municipality computer systems that require network connectivity must conform to municipal ITC Standards.

Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, municipality users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the municipality network infrastructure.

Users are not permitted to alter network hardware in any way.

D. DISCIPLANARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality's Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality's resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

E. DEFINITIONS

Information Resources (IR):
Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM):
Responsible to the municipality for management of municipal information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the municipality's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the municipality to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the municipality. If an agency does not designate an IRM, the title defaults to the Municipal Manager, and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO):
Responsible to executive management for administering the information security functions within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

9. REMOTE ACCESS POLICY

A. PURPOSE

The purpose of this policy is to protect the municipality's electronic information from being inadvertently compromised by authorized personnel using a remote access connection.

B. SCOPE

The scope of this policy is to define appropriate remote access and its use by authorized personnel.

C. POLICY

The municipality employees and authorized third parties (customers, vendors, etc.) can use remote access connections to gain access to the corporate network. Remote access should be strictly controlled, using strict password authentication. Remote access should be requested through the ITC account request process.

It is the responsibility of employees with remote access privileges to ensure a remote connection to the municipality is not used by non-employees to gain access to company information system resources. An employee who is granted remote access privileges must remain constantly aware that remote access connections between their location and the municipality are literal extensions of the municipality's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect the municipality's assets.

For additional information on wireless access to the municipal network, consult the Wireless Communications Policy.

Note: Remote access accounts are considered 'as needed' accounts. Account activity is monitored, and if a remote access account is not used for a period of six months the account will expire and no longer function. If remote access is subsequently required, the individual must request a new account as described above.

D. DISCIPLANARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

10. EXTRANET POLICY

A. PURPOSE

This document describes the policy under which third party organizations connect to the municipal networks for the purpose of transacting business related to the municipality.

B. SCOPE

Connections between third parties that require access to non-public municipal resources fall under this policy, regardless of whether a Telkom circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for the municipality or to the Public Switched Telephone Network does NOT fall under this policy.

C. POLICY

SECURITY REVIEW

All new extranet connectivity will go through a security review with the ITC Officer. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

THIRD PARTY CONNECTION AGREEMENT

All new connection requests between third parties and the municipality require that the third party and the municipality representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Municipal Manager of the municipality as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into the municipality are to be kept on file with the ITC Department.

BUSINESS CASE

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the ITC Department. Typically this function is handled as part of the Third Party Agreement.

POINT OF CONTACT

The municipality must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the municipality, and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

ESTABLISHING CONNECTIVITY

Sponsoring Organizations within the municipality that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage ITC to address security issues inherent in the project. If the proposed connection is to terminate within a lab at the municipality, the Sponsoring Organization must engage the ITC Department. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and ITC, as requested. All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will the municipality rely upon the third party to protect the municipality's network or resources.

MODIFYING OR CHANGING CONNECTIVITY AND ACCESS

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or ITC when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

TERMINATING ACCESS

When access is no longer required, the Sponsoring Organization within the municipality must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct the municipality business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct municipal business necessitate a modification of existing permissions, or termination of connectivity, ITC and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

D. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

E. DEFINITIONS

Circuit

For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.

Sponsoring Organization

The municipal organization who requested that the third party have access into the municipality.

Third Party

A business that is not a formal or subsidiary part of the municipality.

11. PROXY FILTERING AND INTERNET ACCESS POLICY

A. PURPOSE

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within municipal network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

B. SCOPE

This policy applies to all municipal employees, contractors, vendors and agents with a municipal-owned or personally-owned computer or workstation connected to the municipal network.

This policy applies to all end user initiated communications between municipality's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

C. POLICY

WEB SITE MONITORING

The ITC Officer shall monitor Internet use from all computers and devices connected to the municipal network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

ACCESS TO WEB SITE MONITORING REPORTS

General trending and activity reports will be made available to any manager as needed upon request to the ITC Officer. ITC members may access all reports and data if necessary to respond to a security incident through the ITC Officer. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to upper management upon request.

INTERNET USE FILTERING SYSTEM

The ITC shall block access to Internet websites and protocols that are deemed inappropriate for the municipality's corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services should be grey-listed in the event of abuse

- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

INTERNET USE FILTERING RULE CHANGES

The ITC shall periodically review and recommend changes to web and protocol filtering rules. Manual changes to web and protocol filtering rules will be recorded as amendments to this Policy. Changes made automatically by purchased software and subscription services will be available on request.

INTERNET USE FILTERING EXCEPTIONS

If a site is miscategorised, employees may request the site be un-blocked by written request to the ITC Department. ITC Department will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to the ITC Department after the Municipal Manager has approved it. All approved exception requests to the ITC Department must be in writing or by email. The ITC Department may unblock that site or category for that associate only. The ITC will track approved exceptions and report on them upon request.

D. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

E. DEFINITIONS

Internet Filtering

Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

User ID

User Name or other identifier used when an associate logs into the corporate network.

IP Address

Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

SMTP
Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.

Peer to Peer File Sharing
Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Social Networking Services
Internet sites such as MySpace and Facebook that allow users to post content, chat, and interact in online communities.

SPAM
Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

Phishing
Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Hacking
Sites that provide content about breaking or subverting computer security controls.

ITC
Information Technology Committee, with is usually comprised of Upper Management, the ITC Officer and other selected role players.

12. WIRELESS ACCESS POLICY

A. PURPOSE

This wireless use policy defines the use of wireless devices in the organization and specifies how wireless devices shall be configured when used.

This policy is designed to protect the organizational resources against intrusion by those who would use wireless media to penetrate the network.

B. SCOPE

This policy applies to all wireless devices in use by the organization or those who connect through a wireless device to any organizational network.

C. POLICY

RISK ASSESSMENT

The use of wireless technology has historically been a serious security risk to organizations. This is because it can be an easy access point to gain access to an organizational network. In addition data sent across it may be readable sometimes even when it is encrypted due to some of the vulnerabilities of the encryption schemes used. Therefore this policy requires a risk assessment any time a new type of wireless device is added to the network. Several items must be assessed including:

- Is this a new technology?
- Does this device use encryption and if so how well tested is the encryption protocol?
- What is the cost of implementing a secure encryption protocol?
- Has this type of device been used on our network before?
- Can this device be configured to only allow authorized users to access it or the network through it?
- How easy will it be for an attacker to fool this device into allowing unauthorized access? What methods may be used?
- What secure authentication schemes are available and what cost or overhead is associated with their implementation and maintenance?
- How practical is wireless use considering the cost, potential loss, and added convenience?

AUTHENTICATION

The authentication mechanisms of all approved wireless devices to be used must be examined closely. The authentication mechanism should be used to prevent unauthorized entry into the network. One authentication method shall be chosen. The following must be considered:

- How secure is the authentication mechanism to be used?
- How expensive is the authentication mechanism to be used?

ENCRYPTION

The encryption mechanisms of all approved wireless devices to be used must be examined closely. The encryption mechanism will be used to protect data from being disclosed as it travels through the air. The following must be considered.:

- How secure is the encryption mechanism?
- How sensitive is the data traveling through the wireless device?
- How expensive is the encryption mechanism?

CONFIGURATION

The SSID of the wireless device shall be configured in such manner so it does not contain or indicate any information about the organization, its departments, or its personnel including organization name, department name, employee name, employee phone number, email addresses, or product identifiers.

ACCESS POINTS

All wireless access points and wireless devices connected to the organizational network must be registered and approved by the designated ITC department representative. All wireless devices are subject to ITC audits and penetration tests without notice.

AUTHORITY

The ITC Officer shall have final authority over the management and security of wireless devices and wireless networking. This person may delegate these authorities as they see fit. It is strongly recommended that this person has significant experience and training in the IT field along with a substantial understanding of computer security concepts. This person should be responsible for the operation of the network.

NETWORK SEPARATION

This policy requires that parts of the network containing and supporting wireless devices directly (the wireless network) be separated from the part of the network that does not support wireless connections. The part of the network supporting wireless devices or connections shall be considered less trusted than the part of the network that does not. All file servers and internal domain controlling servers shall be separated from the wireless network using a firewall. One or more intrusion detection devices shall monitor the wireless network for signs of intrusion and log events. The type of logged events will be determined by the network administrator.

ALLOWABLE WIRELESS USE

- Only wireless devices approved by make and model shall be used.
- All wireless devices must be checked for proper configuration by the IT department prior to being placed into service.
- All wireless devices in use must be checked monthly for configuration or setup problems.

D. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

13. SERVER DOCUMENTATION POLICY

A. PURPOSE

This policy is an internal IT policy and defines the requirements for server documentation. This policy defines the level of server documentation required such as configuration information and services that are running. It defines who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers. This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

B. POLICY

For every server on a secure network, there is a list of items that must be documented and reviewed on a regular basis to keep a private network secure. This list of information about every server should be created as servers are added to the network and updated regularly.

- Server name
- Server location
- The function or purpose of the server.
- Hardware components of the system including the make and model of each part of the system.
- List of software running on the server including operating system, programs, and services running on the server.
- Configuration information about how the server is configured including:
    - Event logging settings
    - A comprehensive list of services that are running.
    - Configuration of any security lockdown tool or setting
    - Account settings
    - Configuration and settings of software running on the server.
- Types of data stored on the server.
- The owners of the data stored on the server.
- The sensitivity of data stored on the server.
- Data on the server that should be backed up along with its location.
- Users or groups with access to data stored on the server.
- Administrators on the server with a list of rights of each administrator.
- The authentication process and protocols used for authentication for users of data on the server.
- The authentication process and protocols used for authentication for administrators on the server.
- Data encryption requirements.
- Authentication encryption requirements.
- List of users accessing data from remote locations and type of media they access data through such as internet or private network.
- List of administrators administrating the server from remote locations and type of media they access the server through such as internet or private network.
- Intrusion detection and prevention method used on the server.

- Latest patch to operating system and each service running.
- Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
- Emergency recovery disk and date of last update.
- Disaster recovery plan and location of backup data.

Mail Server Documentation

- Account size limit where the person receives warnings about mailbox size
- Account size limit where the person cannot send mail anymore.
- Account size limit where the person cannot receive mail anymore.

ACCESS

The server administration staff and their management shall have full read and change access to server documentation for the server or servers they are tasked with administering. The networking staff, enterprise security staff, application development staff, and help desk staff shall have the ability to read all server documentation.

CHANGE NOTIFICATION

The help desk staff, network administration staff, application developer staff, and ITC management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

DOCUMENTATION REVIEW

The ITC Officer shall ensure that server documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any server changes were made. Also any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

STORAGE LOCATIONS

Server documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities, so that if one facility is destroyed, information from the other facility may be used to help construct the CIS infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

14. NETWORK SCANNING POLICY

A. NETWORK SCAN TYPES AND SCOPE

This network scanning policy defines network scan types, identifies reasons for scanning, identifies times when network scanning is allowed, who should approve network scanning, and specifies who should be notified when network scanning is done.

Network device location scan - This scan may use different means to determine IP addresses of active devices on the network. Methods:

- ARP Scan - An ARP broadcast can be sent to network IP addresses asking what is the MAC address of the host with IP address x.x.x.x. If a response occurs, there is an active host at that address.

Internal full port scan - Checks to determine what services are running on each host. This may be done against selected hosts or all hosts including servers and workstations. Methods:

- Socket connect scan - Tries to complete a socket connection to a port on a host computer. This scan allows the host computer to log the connection.
- SYN scan - Sends a SYN packet to the host indicating that it wants to open a socket. But when the host responds it does not finishing establishing the connection.
- FIN scan - Sends a FIN packet to a host port. If a service is not running, the port responds with a reset signal. If the port has a service running on it, the signal is ignored.

External full port scan - Checks to determine what services are running on each host. This test is done from outside the firewall and is directed toward any IP addresses owned by the organization being tested. It may use the socket connect scan method, the SYN scan method, or the FIN scan method.

Internal vulnerability scan - Tests the server to see if it is vulnerable to known flaws in the operating system, services, and applications that are running. This test may be directed toward one or more hosts including servers and workstations. This test goes beyond performing a full port scan. It attempts to get information about the operating system and services running on the host. It will attempt to determine the version of the services running on the host and may even do a penetration test.

External vulnerability scan - Same as the internal vulnerability scan except it is done from outside the organization network and is directed toward any IP addresses owned by the organization being tested.

Internal Denial of service scan - This is a scan using packets which are intentionally designed to make a system crash or tie up resources. The scan is directed against ports but the data sent is usually misconfigured in some unusual way.

External denial of service scan - Similar to the internal denial of service scan except it is directed against IP addresses owned by the organization being tested.

Password Cracking - This test may send default passwords and brute force password guessing against accounts on specified systems. This is really not like a network scan but is covered in this policy since it could potentially disrupt service depending on the password policies of the organization.

Many scanning services will offer some combinations of these types of scans. This policy covers all types of network and host scanning.

NETWORK SCANNING REASONS

Network scanning may be performed for several reasons:

- To determine whether computer systems are vulnerable to attack and fix them.
- To show companies we interact with that our servers are reasonably secure.
- To fulfill regulatory requirements.

Network scanning shall not be performed without written permission from the Municipal Manager.

NETWORK SCANNING DISRUPTIONS

Network scanning can be very disruptive to both a network and hosts that are operating on a network. No network scanning shall be allowed without close adherence to this policy and the associated procedures. Network scanning can cause systems to crash and network devices to become unreliable which can become very disruptive to the business operations.

AUTHORIZERS OF NETWORK SCANNING AND ALLOWABLE HOURS

The ITC Officer shall determine who is authorized to perform network scans. Those who perform network scans must have authorization in writing and a specified time period when they are permitted to perform network scans. This policy may limit the hours that scanning may be done so scanning is not done during business hours. Specified time periods may provide for the following constraints:

- Scanning shall be done between the hours of 13:00 - 13:45 and 21:00 – 6:00. This may be to prevent disruptions during business hours.

SCANNING NOTIFICATIONS

When scanning is to be done, the following groups of people must be notified on a daily basis:

- The ITC Officer.
- The manager responsible for system administration of the computer system to be scanned.
- The manager of applications running on the computer system to be scanned.
- The users of computer systems that will be scanned.

SCANNING PROCEDURE

A scanning procedure shall be created for all computer systems to be scanned. For each server to be scanned a list of people to be notified shall be maintained. For workstations to be scanned, users may be notified using a group email.

DENIAL OF SERVICE SCAN

Denial of service scan shall not be done without signoff of both the ITC Officer and the Municipal Manager. This is due to the fact that denial of service scans are an effort to disrupt service and will most likely disrupt one or more services. It may cause key network devices to fail. The hours during which a denial of service scan may be done shall be strictly limited and normally only after normal business hours.

B. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s). **Deliberate unauthorised Denial of Service scans will result in immediate termination of employment.**

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

15. NETWORK DOCUMENTATION POLICY

A. OVERVIEW

This network documentation policy is an internal CIS policy and defines the requirements for network documentation. This policy defines the level of network documentation required such as documentation of which switch ports connect to what rooms and computers. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

B. PURPOSE

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

C. POLICY

The network structure and configuration shall be documented and provide the following information:

- IP addresses of all devices on the network with static IP addresses.
- Server documentation on all servers as outlined in the "Server Documentation" document.
- Network drawings showing:
    - The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
    - The various security zones on the network and devices that control access between them.
    - The locations of every network drop and the associated switch and port on the switch supplying that connection.
    - The interrelationship between all network devices showing lines running between the network devices.
    - All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information.
    - All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.
- Configuration information on all network devices including:
    - Switches
    - Routers
    - Firewalls
- Configuration shall include but not be limited to:
    - IP Address
    - Netmask
    - Default gateway
    - DNS server IP addresses for primary and secondary DNS servers.
    - Any relevant WINS server information.
- Network connection information including:
    - Type of connection to the internet or other WAN/MAN.

    - Provider of internet/WAN/MAN connection and contact information for sales and support.
    - Configuration information including netmask, network ID, and gateway.
    - Physical location of where the cabling enters the building and circuit number.
- DHCP server settings showing:
    - Range of IP addresses assigned by all DHCP servers on all subnets.
    - Subnet mask, default gateway, DNS server settings, WINS server settings assigned by all DHCP servers on all subnets.
    - Lease duration time.

ACCESS

The networking and some enterprise security staff shall have full access to all network documentation. The networking staff shall have the ability to read and modify network documentation. Designated enterprise security staff shall have access to read and change network documentation but those not designated with change access cannot change it. Help desk staff shall have read access to network documentation.

CHANGE NOTIFICATION

The server administration staff, application developer staff, and ITC management shall be notified when network changes are made including:

- Reboot of a network device including switches, routers, and firewalls.
- Changes of rules or configuration of a network device including switches, routers, and firewalls.
- Upgrades to any software on any network device.
- Additions of any software on any network device.
- Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:
    - DHCP
    - DNS
    - Domain controllers
    - WINS

Notification shall be through email to designated groups of people.

DOCUMENTATION REVIEW

The network manager shall ensure that network documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings should be reviewed to determine whether there were any network changes made to support the project.

STORAGE LOCATIONS

Network documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities, so that if one facility is destroyed, information from the other facility may be used to help construct the CIS infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

16. BACKUP POLICY

A. PURPOSE

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

B. SCOPE

This policy applies to all equipment and data owned and operated by the organization.

C. POLICY

TIMING

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

STORAGE

There shall be two separate or two sets of tapes, Hard Drives, or DVD's for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate or set of tapes, Hard Drives, or DVD's for each Friday of the month such as Friday1, Friday2, etc. Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.

MONTHLY BACKUPS

Every month a monthly backup shall be made using the oldest backup set from the sets.

RESPONSIBILITY

The ITC Officer shall delegate an employee if necessary to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

TESTING

The ability to restore data from backups shall be tested at least once per month.

DATA BACKED UP

Data to be backed up include the following information:

- User data stored on the hard drive.
- System state data.
- The registry.

Systems to be backed up include but are not limited to:

- File server
- Mail server
- Internet server
- Domain controllers

ARCHIVES

Archives are made at the end of every year in December.

RESTORATION

Users that need files restored must submit a request to the ITC Officer. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

TAPE STORAGE LOCATIONS

Offline tapes used for nightly backup shall be stored in a fireproof safe, preferably off-site. Monthly tapes shall be stored across town in another facility in a fireproof safe.

This policy may contain attachments describing how various systems and types of systems are backed up such as Windows, Linux or UNIX systems.

D. DEFINITIONS

Backup

The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive

The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Restore

The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

17. INTRUSION DETECTION POLICY

A. PURPOSE

This policy provides policies to establish intrusion detection and security monitoring to protect resources and data on the organizational network. It provides guidelines about intrusion detection implementation of the organizational networks and hosts along with associated roles and responsibilities.

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

B. SCOPE

This policy covers every host on the organizational network and the entire data network including every path that organizational data may travel that is not on the internet. Paths covered by this policy even include organizational wireless networks. Other policies cover additional security needs of the organizational network and systems.

C. POLICY

OBJECTIVES

- Increase the level of security by actively searching for signs of unauthorized intrusion.
- Prevent or detect the confidentiality of organizational data on the network.
- Preserve the integrity of organizational data on the network.
- Prevent unauthorized use of organizational systems.
- Keep hosts and network resources available to authorized users.
- Increase security by detecting weaknesses in systems and network design early.

REQUIREMENTS

- All systems accessible from the internet or by the public must operate IT approved active intrusion detection software during anytime the public may be able to access the system.
- All host based and network based intrusion detection systems must be checked on a daily basis and their logs reviewed.
- All intrusion detection logs must be kept for a minimum or 30 days.

NOTIFICATION

- Any suspected intrusions, suspicious activity, or system unexplained erratic behavior discovered by administrators, users, or computer security personnel must be reported to the organizational CIS computer security office within 1 hour.

ROLES

- The intrusion detection team shall:
    - Monitor intrusion detection systems both host based and network based.
    - Check intrusion detection logs daily.
    - Determine approved intrusion detection systems and software.
    - Report suspicious activity or suspected intrusions to the incident response team.

- The incident response team shall:
    - Act on reported incidents and take action to minimize damage, remove any hostile or unapproved software, and recommend changes to prevent future incidents. Action shall be based on the approved incident response plan.

18. SERVER MONITORING POLICY

A. PURPOSE

This server monitoring policy is an internal IT policy and defines the monitoring of servers in the organization for both security and performance issues.

This policy is designed both to protect the organization against loss of service by providing minimum requirements for monitoring servers. It provides for monitoring servers for file space and performance issues to prevent system failure or loss of service.

B. SCOPE

This policy applies to all production servers and infrastructure support servers including but not limited to the following types of servers:

- File servers
- Mail servers
- Internet server
- Application servers
- Domain controllers
- DNS servers

C. POLICY

DAILY CHECKING

All servers shall be checked manually on a daily basis the following items shall be checked and recorded:

- The amount of free space on each drive shall be recorded in a server log.
- The system log shall be checked and any major errors shall be checked and recorded in the server log.
- Services shall be checked to determine whether any services have failed.
- The status of backup of files or system information for the server shall be checked daily.

EXTERNAL CHECKS

Essential servers shall be checked using either a separate computer from the ones being monitored or a server monitoring service. The external monitoring service shall have the ability to notify multiple IP personnel when a service is found to have failed. Servers to be monitored externally include:

- The mail server
- Internet server
- File
- Domain Controller

19. SYSTEM LOCKDOWN POLICY

A. PURPOSE

This system lockdown policy is an internal ITC policy and defines a general process that should be used to lock down servers and workstations.

This policy is designed to minimize risk to organizational resources and data by establishing a process for increasing the security of servers and workstations by stopping unneeded services and testing for vulnerabilities.

B. SCOPE

This policy applies to all computers and devices on the network.

C. POLICY

SERVER LOCKDOWN AND HARDENING

This section describes a general process used to lock down servers. When they are initially installed and configured. Types of servers or equipment that need hardening include but are not limited to file sharing servers, email servers, internet servers, FTP servers, DNS servers, DHCP servers, Domain controllers, Directory servers, Network devices such as firewalls, routers, and switches.

List services that will be required to run on the server. Examples include:

- DNS
- HTTP
- SMTP

List services that are running on the server and turn off any that the administrator is sure are not needed.

Do a port scan on the server - Use a security tool to test and determine any ports that the server is responding to.

Shut down any services that are not on the required list of services for the server. Especially remember to shut down services listed in Appendix A - Services Recommended for Shutdown.

Remove any unnecessary programs, services, and drivers from the server especially those not loaded by default on the server.

Patch the server with the latest patches and patch all services running on the server.

Disable or change the password of any default accounts on the server or related to any operating services.

Be sure all passwords used to access the system or used by services on the system meet minimum requirements including length and complexity parameters.
Be sure all users and services have minimum required rights and do not have rights to items not needed.

Be sure file share and file permissions are as tight as possible.

Perform a vulnerability assessment scan of the server. Patch or fix any vulnerabilities found.

Where appropriate, install and run additional security programs such as:

- Anti-virus - Install and perform latest update of software and virus definitions.
- Firewall
- Intrusion detection software - Some approved host based intrusion detection software is recommended to be run on all servers.
- Honeypot (a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems).
- Change of system and system files detection

All this software should have the latest updates installed.

Set security parameters on all software such as where anti-virus programs will scan, how often it will scan, and how often it will get virus definition updates.

Enable audit logging to log any unauthorized access.

Perform another vulnerability assessment scan of the server, and fix any discrepancies.

Take additional account management security measures including:

- Disable the guest account
- Rename default administrator accounts
- Set accounts for minimum possible access
- Be sure all accounts have passwords meeting minimum complexity and length rules.

Test the server to be sure all desired services are operating properly.

D. ENFORCEMENT

Since locking down servers is critical to the security of the organization and everyone, this policy must be enforced by management through review and auditing. Where ever possible the servers will enforce the policies through to workstations. Users are still asked to be vigilant and report any digressions.

E. APPENDIX A – SERVICES RECOMMENDED FOR SHUTDOWN

- File and Printer Sharing for Microsoft Networks - Uninstallation of this service is recommended. This service is not needed unless you want to share a printer on your local computer or share folders on your local computer with other computers.
- Messenger - Disable this service in the Services applet of Administrative Tools. This service has some serious security bugs and problems and has very little use for managing the network.
- Remote registry service - This service should be set to manual or disabled since it allows people from remote locations to modify your registry. It is a serious security risk and should only be run if required by network administrators. Set this service to manual or disabled in the Services applet of Administrative Tools.

- Secondary Logon service - If it is not necessary for lower privileged users to use the "Run As" command to run commands that only administrators or power users can run, this service should be disabled.
- Universal Plug and Play Device Host service - It broadcasts unnecessary information about the computer running the service. It may be used by MSN messenger. This service is a high security risk and should be disabled unless dependent services are required.
- Wireless Zero Configuration service - Used to support wireless connections. If you are not using wireless, this should be disabled. This service is a high security risk and should be disabled unless needed.
- Computer Browser - For home users and most organizational users, this service can be disabled. Running this service is a moderate security risk.
- NetMeeting Remote Desktop sharing - A person on a remote computer can access your desktop to help you. This service may be used by network administrators to help users with tasks. Normally this service should be disabled unless needed. Running this service is a moderate security risk.
- Remote Desktop Help Session Manager service - A person on a remote computer can access your desktop to help you. This service may be used by network administrators to help users with tasks. Normally this service should be disabled unless needed. Running this service is a moderate security risk.
- Network DDE Service - Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers. It allows two running programs to share the same data on the same computer or on different computers. Running this service is a moderate security risk. Normally this service should be disabled unless needed.
- Network DDE DSDM Service - Manages DDE network shares. Running this service is a moderate security risk. Normally this service should be disabled unless needed.
- NT LM Security support provider - Used for backward compatibility with older Microsoft operating systems. Running this service is a moderate security risk. Normally this service should be disabled unless needed or set to manual.
- SSDP Discovery service - Allows the computer to connect with networked plug and play devices on the network. This service does not support internal PnP devices. This service should be disabled unless the computer needs to connect to external networked plug and play devices.
- Telnet service - The telnet service allows a terminal connection to or from a remote computer but sends passwords in the clear. Running this service is a moderate security risk. Normally this service should be disabled unless needed or set to manual.
- Terminal services - Allows a remote connection from a remote computer usually used by network administrators to help users. Running this service is a moderate security risk. Normally this service should be disabled unless needed or set to manual. This service is commonly used by system administrators to administer servers remotely.
- Alerter service - The alerter service allows system administrators to send messages to selected users. This service should be disabled unless specifically needed.

Types of servers that need hardening (This list is not inclusive of all devices that should be hardened):

- File sharing
- Email Servers
- Internet server
- FTP servers
- DNS servers
- DHCP servers

- Domain controllers
- Directory servers
- Network devices such as firewalls, routers, and switches

20. ANTI-VIRUS, MALWARE AND OTHER THREATS POLICY

A. PURPOSE

This policy is an internal CIS policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

B. ANTI-VIRUS POLICY

The organization will use a single anti-virus product for anti-virus protection and that product is Trend Micro Security for Endpoints and Mail Servers. The following minimum requirements shall remain in force.

The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.

The anti-virus library definitions shall be updated at least once per day.

Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

C. EMAIL SERVER POLICY

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

EMAIL MALWARE SCANNING

In addition to having the standard anti-virus program, the email server or proxy server will additionally include Scanmail which will be used to scan all email for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional support call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of support calls.

BLOCKED ATTACHMENT TYPES

The email server or proxy server will block all emails with attachment types listed below. This is because these attachment types are dangerous containing active content which may be used to infect a computer with hostile software or because these attachment types are commonly successfully used by virus programs or malware to spread.

APPLICATION AND EXECUTABLES

- elf – Executable and linking format
- exe.dll.vxd - Executable
- class – Jora Applets
- lnk – Windows N7/95 shortcut
- ms – Windows Installer Package

DOCUMENTS

- Compiled HTML chm
- Mdb.accdb Microsoft Access

IMAGES

- gms – Corel Global Macro storage
- Mac – Macintosh Mcpaint Graphics
- Cpt – Cord Photopaint Image
- png – Portable Network Graphics
- wmf – Windows Metafile

VIDEO

- asf.wmv – Advance Streaming formats
- swf – Macro Media flash
- Mpg – Mpeg Moving Picture Epart Group Video
- Av – Audi Video Interleafe formats
- Mov.gt.gtm – Quick Time Movie
- Rm – Real Time
- zip - Many viruses are commonly zipping files to keep them from being scanned and providing instructions to users about how to run the attachment. Many users still do this so to secure the network, it has become necessary to block this attachment type.

The municipality cannot depend on entirely on its anti-virus software on each computer to prevent these viruses because viruses have a period of time when they spread unrecognized by anti-virus software. Blocking these file attachments will limit the possibility of virus or unauthorised intrusion.

When an email breaks the rules and contains an illegal file attachment some or all the following actions will be taken:

- Deletion of the email and notify neither the sender or the recipient. The problem with doing this is in the fact that people may be trying to send legitimate files to each other and have no way of knowing their communication attempts are failing. Training by letting users know what files are blocked can help remedy this problem
- Time the email and notify the sender - This will notify senders when their emails do not go through, but it will also notify senders who really did not send an email (when a virus spoofed them as the sender) that they sent an email with an illegal attachment. This can

cause more additional support requests and questions for the administrator on the spoofed sender's side.

- Remove the attachment and let the email go through. - This would let the receiver know that someone tried to send them an illegal attachment. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent. This policy would very likely cause your organization's support calls to increase with users calling to ask questions about why someone is trying to send them these files.

There is no ideal policy here and your system administrators must choose the best method depending on the situation being experienced by the organization. Providing training to users so they know these files are blocked and what the work around is for this situation will reduce support calls.

NETWORK EXPLOIT PROTECTION

The network is to be protected by a firewall any time it is connected to the internet. Routers connecting sub-networks of the municipality are to also have their firewalls enabled. All servers and workstations are to run a firewall as part of their anti-virus software. Where ever possible, the anti-virus software will filter unwanted or banned files and attachments and react in accordance with this policy.

D. ENFORCEMENT

Where ever possible this policy will be enforced by software on the network. Users are asked to be vigilant and ensure compliance to this policy.

E. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality’s Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality’s resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

21. STANDARD THIRD-PARTY NON-DISCLOSURE AGREEMENT

To be provided by a legal representative of the Municipality

22. DIGITAL PIRACY POLICY

A. PURPOSE

Violation of digital piracy laws carries severe financial penalties for businesses and individuals as well as possible prison time for the guilty parties.

This policy addresses how the municipality will act against digital piracy, ensure compliance with software license and deal with transgressions.

B. SCOPE

The document applies to all computer users in the municipality.

C. POLICY

- Due to the common trend of piracy the follow file types are not permitted to be saved on the servers:
  - MP3, OGG, WMA, MP4, CDA, and any other music file format.
  - AVI, MPEG, DIVX, WMV, and any other video file format.
- Where necessary, an exception can be made for official use only. Requests for an exception must be submitted in writing to the Municipal Manager for evaluation. All exceptions will be closely monitored.
- Users are not permitted to store, create or use any pirated material on any municipal equipment. Routine checks will be performed and transgressions will severely dealt with.
- Peer-to-peer protocols and file types and known websites advocating piracy will be blocked on the network.
- Users are asked to exercise caution when dealing with audio/visual media and only IT personnel should install software to ensure license compliance.

D. ENFORCEMENT

Where ever possible this policy will be applied automatically through servers, anti-virus and other monitoring software. Routine checks may be performed without warning by IT staff and/or management as well as at the request of law enforcement agencies.

E. DISCIPLINARY ACTION

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate the Municipality's Rules of Order, approved procedure manuals and other work rules, adopted by the Municipality from time to time. The Municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s). **Criminal charges may also be filed in order to protect the municipality from legal action.**

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Municipality's resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.