SIYATHEMBA MUNICIPALITY

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

1. INTRODUCTION

In this fast paced competitive environment, **Siyathemba Municipality** provides its employees with Information Communications Technologies (ICT) in order to serve customers efficiently and effectively. ICT tools include electronic media and services such as computers, email, internet, telephones and fax machines.

Siyathemba Municipality encourages the use of ICT and associated services because they can make communication more efficient and effective and they are also valuable sources of information about vendors, customers, technology and new products and services.

However, all employees and everyone connected to the Municipality's electronic media and services should remember that it is the property of the Municipality and that the purpose of connection to these technologies is to facilitate and support the Municipality business. All employees are expected to have the responsibility to use these resources in a professional, ethical and lawful manner.

2. SCOPE

This policy applies to all permanent and temporary employees, and contracting staff, and is issued by Director Corporate Service for the use of Information Communications Technologies.

3. OBJECTIVES

The objectives of this policy is to outline what constitutes acceptable use of **Siyathemba Municipality's** ICT Assets, including the handling of different types of information as well as the rules regarding the interception and monitoring of electronic communication.

Siyathemba Municipality makes ICT resources available to support its mission and general administration. To ensure that these resources are used appropriately, **Siyathemba Municipality** has developed this policy document.

In order to make certain that the policies in this document remain current, they are under constant review. Suggestions, questions and concerns are welcome, and should be addressed in writing to the Corporation's ICTS Manager. **Siyathemba Municipality** retains ownership of this policy for as long as **Siyathemba Municipality** management deems this policy to be in effect.

4. RESPONSIBILITY

The **Manager**, Information Communication Technologies Services has responsibility for the implementation of this policy. ICTS Management of the Corporation are responsible for the maintenance and updating thereof, and must ensure adherence to this policy.

5. NON-COMPLIANCE

Siyathemba Municipality reserves the right to audit compliance with this policy from time to time. Employees or contractors who breach the provisions of this policy will be disciplined in accordance with the disciplinary codes and procedures of **Siyathemba Municipality**. Any employees becoming aware of any breach of this policy should promptly and confidentially advise the persons to whom they report, to the managers of human resources, security or internal audit. **Siyathemba Municipality** reserves the right to suspend or permanently remove a user's access to some or all of the electronic communication facilities.

6. POLICY STATEMENT

6.1 GENERAL

a) In terms of its Code of Conduct, **Siyathemba Municipality** is committed to a policy of openness, integrity and accountability in the conduct of its business. **Siyathemba Municipality** is also committed to conduct its business honestly, fairly and legally. All employees are required to maintain the highest ethical standards in ensuring that the Municipality business practices are conducted in a manner, which, in all reasonable circumstances, is beyond reproach.

b) **Siyathemba Municipality** is obligated to adhere to all reasonable legal and regulatory requirements of South Africa, and in addition to its own ethical principles and values as defined in its Code of Business Conduct and Ethics. This includes legislation pertaining to data, information, electronic communication and privacy.

c) This policy governs the use of Information Communication Technology Resources, such as, but not limited to, computer hardware, printers, data, networks, long distance services, electronic fax services, software, applications and any other current or future ICT Resources adopted, acquired, installed, deployed or operated electronically.

d) Employees may not transmit personal opinions as those of the Corporation nor make any statement that may be construed to be a company statement unless authorised to do so.

e) **Siyathemba Municipality** ICTS Assets are intended for business purposes and personal usage is only allowed when:

i) It does not consume more than a trivial amount of system resources, in the opinion of the ICTS management.

ii) It does not interfere with the productivity of the individual. iii) It does not pre-empt a business activity.

iv) It conforms to all legal requirements.

f) Where private use is allowed, this is subject to intended users' acceptance of the right of **Siyathemba Municipality** to monitor all electronic communication, data or information in terms of this policy and any rights afforded to the Corporation by law.

g) **Siyathemba Municipality** will not accept responsibility for any personal loss or liability caused or incurred in any form when employees use their ICT assets, resources or facilities.

h) **Siyathemba Municipality** shall own all data and communication that was sent, generated and shared with the Municipality assets, networks and third party contracts.

Siyathemba Municipality reserve the right to inspect, intercept and or requests access to these data should it be deemed necessary.

i) **Siyathemba Municipality** has an obligation towards its shareholders, employees, customers and other stakeholders to ensure the confidentiality, integrity, availability and legality of its business operations, including data and information that resides or is transported in electronic form. All users must protect electronic information of the Municipality at all times and ensure that it is only made available to authorised recipients. To this end **Siyathemba Municipality** reserves the right to monitor the use of electronic communications, data and information residing or transported on its facilities to safeguard its operations, ensure compliance with company policy, legislation or contracts, to monitor the effectiveness and efficiency of its business and to investigate actual or potential information security violations or incidents.

j) The generation, storage, display or transport of the following types of information by use of the Municipality ICTS assets is considered unacceptable and is therefore strictly prohibited:

   i) Criminal activities or the support of any criminal or illegal activity including fraud, sabotage, theft, and hacking.

   ii) Obtaining or assisting anyone else in obtaining access to information they are not authorised to access.

   iii) Transmitting any material, that is in **Siyathemba Municipality** sole discretion, is unlawful, obscene, malicious, threatening, abusive, prejudicial, libellous, or hateful, or encourages conduct that would constitute a criminal act, give rise to civil liability, unrest or a constitute a breach of company policy. The following are expressly forbidden:

      (a) Material of a discriminatory nature.

      (b) Obscene or pornographic materials.

      (c) Derogatory or inflammatory remarks of any nature.

      (d) Political or religious viewpoints.

      (e) Material or language that might be deemed to constitute harassment.

k) The loss or damage of any hardware and/or software must be reported immediately to ICTS Department.

l) All **Siyathemba Municipality** authorised administrators and technicians as well as consultants will strictly adhere to Change and Incident Management Procedures.

m) **Siyathemba Municipality** employees, and specifically Users of the Municipality Systems, expressly acknowledge that this ICTS Policy forms an addendum to their general conditions of employment at **Siyathemba Municipality**. It remains the responsibility of each employee, and specifically Users of the Municipality Systems, to thoroughly familiarise themselves with these conditions of employment and the contents of this ICTS Policy.

6.2 EMAIL USAGE

a) Common courtesy and respect for the reader's dignity should always be observed in e-mail content. This is particularly necessary when expressing displeasure, dissatisfaction, or similar sentiments. Abusive or obscene language is prohibited.

b) An email must meet the Municipality requirements in terms of the corporate image and accuracy of information should be checked before sending a message to any email recipient.

c) All **Siyathemba Municipality** email communications are encrypted by default, should other mail systems be used, and then it is compulsory to ensure encryption of those communication mailing systems.

d) The same limits of authority will apply to e-mail as to all other forms of written communications.

e) The following actions and uses of the e-mail system are expressly prohibited:

I. Sending of bulk mail messages of a personal nature.
II. Propagation of chain letters.
III. Advertising of personal items.
IV. Subscription to mailing lists, discussion groups, a list-server, or other such bulk mailing services, for private purposes.
V. File downloads for private use.
VI. Unauthorised use of e-mail systems for purposes of hacking.

f) The software provided for e-mail services is pre-configured at installation time. Users should not modify this configuration on their own accord, as this could impact on the availability of the services, or licensing arrangements in place.

g) An email ID is assigned to all users of the email system. The email system authorises access to an email ID by way of a windows logon. This password must never be divulged to anyone and, to do so, exposes the email user to responsibility for actions undertaken by the other party. Generic group IDs must be kept to an absolute minimum and only allocated where the business function requires it. Notwithstanding the generic nature of a Group ID a named individual must carry responsibility for the Group ID.

h) Users are not allowed to furnish Municipality confidential information to an external email sender, without prior authorization by the relevant Business Unit Managers - e.g. emails that attempt to collect information from a user in an attempt to conduct identify theft know as phishing.

i) Users are responsible for maintaining the size of data that is contained within their Exchange mailboxes.

j) ICTS will endeavour to quarantine Emails in excess of 5MB that is sent to external email addresses during normal working hours (07h30 to 16h30).

k) All **Siyathemba Municipality** email auto signatures must conform to the

Corporation's Identity Usage application Guidelines.

l) All outgoing **Siyathemba Municipality** emails will contain this information disclosure in line with the Municipality auto signature policy, format and standards:

“Confidentiality Notice”: The information contained in this email message, including any attachment, is confidential and is intended only for the person or entity to which it is addressed. If you are neither the intended recipient nor the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that you may not review, retransmit, convert to hard copy, copy, use or distribute this email message or any attachments to it. If you have received this email in error, please contact the sender immediately and delete this message from any computer or other data bank. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of **Siyathemba Municipality** and or subsidiaries. All reasonable precautions have been taken to ensure no viruses are present in this e-mail and the sender cannot accept responsibility for loss or damage arising from the use of this e-mail, content and or attachments. This e-mail does not constitute a guarantee or proof of the facts mentioned herein. No employee or intermediary is authorized to conclude a binding agreement on behalf of **Siyathemba Municipality** by e-mail without the express written confirmation by a duly authorized representative of **Siyathemba Municipality**.

6.3 INTERNET USAGE

a) **Siyathemba Municipality** Internet connections must be via an approved route to an Internet Service Provider using the **SIYATHEMBA MUNICIPALITY** perimeter security devices.

b) Users of **Siyathemba Municipality** Internet facilities must respect and adhere to intellectual property rights of Internet information and Web content.

c) **Siyathemba Municipality** will not accept responsibility for any personal loss or liability caused in any form when users conduct personal transactions over the Internet.

d) The use of social networks like Twitter, Facebook and others are not allowed during normal working hours.

e) The same limits of authority will apply to Internet communications as to all other forms of written communications.

f) The creation of personal home pages using **Siyathemba Municipality** ICTS Assets is not permitted.

g) The use of “Real Time Chat” communication applications like MSN Messenger, Facebook Chat, Google Talk, Skype etc. in order to transfer **Siyathemba Municipality** data is strictly forbidden. No confidential **Siyathemba Municipality** data and or confidential personal data may be transferred with this means as **Siyathemba Municipality** cannot guarantee the security and or confidentiality of this data.

h) Users are not permitted to furnish confidential Municipality information across the Internet, without prior authorization by the relevant Business Unit Managers.

i) Public information obtained from the Internet should not to be acted upon unless verified by a reliable source.

j) Users are not permitted to launch or install any performance, security or information gathering tools without authorization from ICTS Department.

6.4 PERSONAL COMPUTER USAGE

a) Anyone seeking to remove desktop personal computer equipment from the premises must obtain authorization by way of a Security Gate Pass signed by the ICTS Department.

b) Desktop personal computer equipment must not be moved or relocated without prior approval of the relevant ICTS Department.

c) It is the responsibility of the desktop user to ensure that a backup copy of relevant desktop Personal Computer data is stored on a server or online where appropriate.

d) Modems and 3G devices directly attached to desktop personal computers are not permitted, unless authorised by ICTS Department. Dial-out or dial-in access directly to a desktop personal computer is only allowed in specific instances when troubleshooting and testing of **Siyathemba Municipality** Intranet and Internet facilities. When desktop personal computers are used in such a manner, they must be configured in line with standard **Siyathemba Municipality** devices including the installation of antivirus software, current service packs and patches.

6.5 LAPTOP USAGE

a) It is the responsibility of the individual to whom a laptop is issued to take reasonable and sensible precautions to safeguard it at all times.

b) Laptops are not allowed to be handed in as luggage at an airport, but must accompany the employee on the airplane.

c) When transported in a vehicle, laptops may not be kept in the front of a vehicle, but must be stored in the boot of the vehicle or other place of safe storage that is out of sight to criminals.

d) Modems and 3G devices directly attached to laptops are not permitted, unless authorised by the ICTS Department. Dial-out or dial-in access directly to a laptop is only allowed in specific instances when troubleshooting and testing of **Siyathemba Municipality** Intranet and Internet facilities. When laptops computers are used in such a manner, they must be configured in line with standard **Siyathemba Municipality** devices including the installation of antivirus software, current service packs and patches.

e) Employees to whom laptops have been allocated will have free movement on and off site with their computers, subject to regulations in force at the business unit regarding the movement of goods between the different areas of work. Employees should, however, be prepared to be challenged and produce proof of ownership for their laptop at any time.

f) It is the responsibility of the laptop user to ensure that a backup copy of relevant laptop data is stored on a server and or online where appropriate.

7 SOFTWARE USAGE

a) Only legally acquired software may be installed on the Municipality ICT Assets provided for business purposes by **Siyathemba Municipality**.

b) Software may only be installed in conjunction and with approval from the ICTS Department.

c) No user modifications or configuration changes may be made to software resident on the desktop personal computer without the prior approval of the ICTS Department.

d) Any software that is installed on a trial basis must be uninstalled within the agreed period.

e) Software downloads must be done in conjunction with the ICTS Department, to avoid infringement of intellectual property rights and copyrights, and to ensure that only legal software is used in the business.

f) Use of unauthorized software, including that which has been borrowed or purchased by the user is expressly prohibited.

g) Municipality purchased software must be used in accordance with contractual agreements and copyright laws.

h) Computer games, not provided as part of the standard operating system environment, may not be loaded or resident on any computer.

No Municipality purchased software or by a vendor agreement may be used for home usage unless permitted by the vendor license agreement and or without written approval of the ICTS Department.

8. WIRELESS COMMUNICATION USAGE

a) No wireless devices may be connected directly or indirectly to The **Siyathemba Municipality** network without the prior authorization by ICTS Department. Authorised wireless devices may only be used if they comply with the following requirements:

I. Make use of certificates to authorise connections. (PKI/VPN/Certificate solutions are the standard)
II. Communications are encrypted between devices.

b) Wireless internet connections are expressly prohibited when connected to any part of the **Siyathemba Municipality** Internal network.

c) The use of wireless internet connections is expressly prohibited unless used in conjunction with personal firewalls, certificates and VPN software.

d) The use of broadband wireless internet devices may not be installed or used on Municipality equipment without the written approval of the ICTS Department and where the broadband wireless connection is not used while the user is connected to the **Siyathemba Municipality** internal network and associated security mechanisms are in place e.g. Internal firewall and PKI encryption.

e) **Siyathemba Municipality** laptops may not be used when connecting from a private environment to the internet via broadband wireless without the written approval of the IT department and where the broadband wireless connection is not used while the user is connected to the internal network and associated security mechanisms are in place e.g. Internal firewall and PKI encryption.

9. PASSWORD & AUTHENTICATION

f) The disclosure of any identification and authentication information is strictly prohibited.

g) Any attempt to bypass user authentication or security to any system is prohibited, including but not limited to, accessing data intended for employees other than yourself, logging into a server or account that you are not authorised to access.

h) Each user must have a unique identifier to any application and is personally accountable to safeguard this information from unauthorised disclosure or access.

i) Passwords may not be shared or communicated to others inside or outside of the Municipality. To do so expose the individual to responsibility for actions the other party takes using the access account.

j) Permissions must be set within each application to allow other users access to your information without the need for you to share your password.

k) Passwords must be changed on a regular basis, and if you believe that your password has been compromised, you must change it immediately.

l) When leaving a workstation, you are required to either log off or lock the workstation, which requires your password to either unlock the workstation or to logon again.

m) Password caching technologies such as biometric devices are not allowed.

10 VIRUS PROTECTION

a) Viruses can be introduced to Municipality computer resources in a number of ways but one of the primary methods of infection is through the unauthorised installation of software. Viruses can be introduced via email, from the Internet or from portable storage devices such as CDs, DVDs, USB memory sticks and external drives.

b) The following precautions must be taken to protect the IT systems from viruses:

I. The standard anti-virus software must be enabled at all times.

II. Only use original software and images are allowed to install applications and operating systems. Under no circumstance users may install copies or images of software obtained from the internet other than directly from the vendor's site.

c) Any e-mail attachments should be treated with extreme caution. If the e-mail has come from a source you do not recognise, delete it or contact the ICTS Department. Do not open any attachments to such an e-mail, as this could infect your workstation and possibly the entire **Siyathemba Municipality** network.

d) Software may only be installed in conjunction with the ICTS Department; this includes software downloadable from the internet.

e) Never turn your computer on with a portable storage device in a drive or connection, as this action could activate a virus.

f) Clearly label portable storage devices with all relevant information that will assist you in assessing their usability, and store them securely.

g) Externally supplied portable storage devices with executable code must be checked for viruses before being used on any of the Municipality ICT Assets.

h) Never use portable and or external storage devices from an unknown source.

11 INFORMATION DISCLOSURE

During their service with **Siyathemba Municipality** employees retain proprietary information and knowledge. Present and former employees must guard against disclosing or using this information to the prejudice of the Municipality interests. **Siyathemba Municipality** reserve the right to take action, including legal action, against present and former employees who disclose or use Any **Siyathemba Municipality** proprietary information to the detriment of the company.

12 DATA SECURITY

a) If highly confidential data is stored on the Municipality ICTS Asset, it must be encrypted with technologies like Bitlocker and / or PGP.

b) If restricted data is stored on the Municipality ICT Asset, it must be password protected. It may also be encrypted as an additional precaution.

c) Any data stored on an individual's workstation or laptop is the responsibility of that individual. Any data that is regarded as a company asset must be stored on a server and or online where appropriate.

d) All highly confidential and restricted information stored on a laptop must be encrypted using the standard encryption methods of **Siyathemba Municipality** (e.g. Bitlocker & PGP).

e) The use of "Real Time Chat" communication applications like MSN Messenger, Facebook Chat, Google Talk, Skype etc. in order to Transfer **Siyathemba Municipality** data is strictly forbidden as per the internet usage policy.

f) Data on portable storage devices must be managed in accordance with the **Siyathemba Municipality** Information Classification Scheme. Under no circumstances may highly confidential or restricted information be stored, transported, or housed on portable storage unless a specific written exemption has been granted by the responsible Director and the respective IT department. An exception to this will be allowed when all the following criteria have been met:

I. Information is stored in an encrypted format using the standard encryption methods of **Siyathemba Municipality**.
II. There must be a dual factor authentication mechanism on the device.
III. The ICTS Department has configured and tested the configuration.
IV. All sensitive data stored on portable storage devices must be labelled accordingly and stored in a place of safekeeping.

g) Only company authorised PDA's and Smartphones are allowed to be connected to any **Siyathemba Municipality** ICTS assets. Users that are recipients of highly confidential or restricted information via e-mail on these devices must comply with the following criteria:

I. No e-mail data may be stored on the device, and should remain on the server at all times, unless the device is capable of remote deletion.
II. Dual factor authentication is required every time an e-mail session is established in the form of a certificate and a PIN.
III. Communications back to the network must be encrypted in accordance with the **Siyathemba Municipality** encryption standard.
IV. Inactive sessions must automatically disconnect after 10 minutes.

V. Attachments may be downloaded onto the device as long as the information contained therein is deemed not to be company confidential or public.

VI. Lost or stolen devices must be reported to the ICTS department immediately, so that certificates can be revoked.

13 MONITORING OF ELECTRONIC COMMUNICATION

a) The following monitoring or interception of electronic communication authorised by the ICTS department is allowed:

I. Daily monitoring for security incidents or privacy violations.

II. Filtering of incoming and outgoing e-mails to scan e-mail attachments for viruses, disinfect or quarantine infected files as appropriate and allow only accepted type of attachments to be transmitted.

III. Monitoring of Internet, email and voicemail facilities to ensure appropriate use, to protect Municipality resources against viruses and to ensure that these resources are used for primarily for business purposes.

IV. Monitoring for software licensing compliance to prevent infringement of intellectual property rights and copyrights to ensure that only legal software is used within BPC

V. Audit investigations for forensic or statutory requirements.

b) Complete records must be kept whenever monitoring or interception of electronic communications occurs.

c) Any other form of monitoring or interception of electronic communication must be approved by the relevant director or general manager.

d) The following monitoring or interception of electronic communication is expressly prohibited:

I. Monitoring or interception by unauthorised individuals.

II. Monitoring or interception of electronic communication to commit or assist in illegal acts such as hacking or launching of attacks against **Siyathemba Municipality** or other companies ICT facilities.

14 THIRD PARTY ACCESS

a) Third parties such as consultants or contractors often need to connect their computers or other ICT devices to the Municipality network to perform work on behalf of the Municipality. For purposes of this policy, third party access is defined as: 'External access to the **Siyathemba Municipality** networks from a location outside of **Siyathemba Municipality** wide area network by a third party’. This type of access introduces additional risks to our network e.g. viruses, inappropriate information disclosure.

b) The following precautions must be taken to protect the Municipality from this type of access:

I. Adequate advanced notice must be given to the ICT discipline about the intended third party access requirements.

II. Third party access devices must be submitted to the ICTS department for assessment, set-up, configuration and approval of their connection and use.

III. Third parties provided third party accesses to the Municipality network are required to sign this policy.

IV. Third parties devices found connected to the Municipality network without the required approval will be disconnected, access rights revoked and disciplinary action initiated against anyone found to have facilitated this access.

V. **Siyathemba Municipality** will not accept responsibility for any damage or data loss to a third party device approved for connection and used on the Corporation's network.

b) When such a connection is no longer required, it is the responsibility of the Municipality employee who facilitated this access to notify the IT department so that the connection can be terminated and the entire Municipality software removed.

15 REMOTE ACCESS SERVICES

a) For the purposes of this policy remote access is defined as 'The facility available to employees (permanent and temporary) and contractors of **Siyathemba Municipality** to access the Municipality information and systems from a remote location, across an external telecommunications service' This policy applies to all types of remote access, whether fixed or 'roving' including travelling users, home workers, and remote office workers. Remote access services enable users to work from home, viewing e-mails or appointments, browsing the internet or accessing their data files.

b) **Siyathemba Municipality** recognises that as a result of remote access services, new risks are introduced including loss or corruption of sensitive data, breach of confidentiality and non-compliance with regulatory standards, amongst others. The following precautions must be taken to protect **Siyathemba Municipality** from the risks associated with remote access services:

I. Dual factor authentication must be used for all remote connections.
II. Highly confidential or restricted information must be encrypted when transmitted utilizing remote access services.
III. VPN termination must be configured from device to device.
IV. Only devices authorised and configured by the ICTS department may be used for remote access services. These devices must, at a minimum have the following configured:

a. The current standard of operating system and service pack, including the latest patches.
b. The current version of the group approved antivirus software, including the latest update.

V. It must be noted that use of individual modems on site are prohibited.
VI. When connecting to public or un-trusted networks, a personal firewall, configured by the IT department, must be used. Users are not permitted to make changes to this configuration.
VII. A remote connection to other networks is prohibited unless conducted in conjunction with the IT department.

VIII. No remote access is allowed in a classified secure network segment. This will be controlled via ACL’s and VLAN’s.

IX. Authorisation for remote access must be removed immediately when the connection is no longer required or employment is terminated.

16 POLICY IMPLEMENTATION GUIDELINES

a) The Head of Corporate Services is the Policy Owner
b) The Head of Corporate Services will ensure implementation of this policy.
c) All employees must formally be informed of this policy.
d) The Head of Corporate Services must ensure that sufficient internal arrangements are in place to address the requirements of this policy and shall ensure that all Senior Managers are sufficiently informed to support this Policy.

17 PROCEDURAL REQUIREMENTS

This policy references the Procedures for issuing and connection of hardware to the Municipality network.

18 MONITORING AND REVIEWING

The ICTS Manager and General Manager - Internal Audit will conduct internal audits to ensure compliance with this policy. The Director-Corporate Services will monitor the effectiveness of this policy and initiate corrective actions.

19 EFFECTIVE DATE

This policy takes effect from the date of approval (signature) and shall be reviewed periodically every three years (3) or on direction from the Municipal Manager

APPEDNIX A

GLOSSARY

- **ACL's:** Access control list. A "list" of all users and their access rights and privileges used to manage and control access to the various systems, files and data.
- **BIOS Password:** Basic Input / Output System password. Password managed by the BIOS program.
- **Dual Factor Authentication:** A strong authentication scheme using two independent factors, one memorised e.g. PIN and one generated e.g. token card.
- **Encryption:** Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Encryption prevents any non-authorized party from reading or changing data.
- **Hotfix/Patch:** A program written to change or rewrite portions of an existing program to resolve incorrect function of the existing program.
- **MAC Address:** Media Access Control address is a unique hardware number assigned to computers on a network for accurate communication and data exchange amongst computers connected to a network.
- **PDA:** Personal Digital Assistant. A device used for managing your activities such as scheduling meetings or tasks, to send or receive e-mails, etc. This device could be synchronized with the e-mail software, such as Outlook, on your personal computer for exchanging appointment information and e-mails between the personal computer and the PDA.
- **PIN:** Personal Identification Number. A unique number used to verify the identity of a particular user.
- **RAS:** Remote Access Service. A service that provides a user access to the BPC networks and resources from a (remote) location outside the BPC facilities that the user normally utilizes, through a telephone dial-up connection, e.g. accessing the BPC network and resources from home for e-mails, appointments, etc.
- **Service Pack:** A group of hotfixes/patches packaged into one program to address specific problems experienced with the operation of an existing program.
- **Smartphone:** Wireless telephone with specialized computer features such as, e-mail, internet browsing, etc. currently available on the latest cellular telephones
- **Spoof:** To deceive for the purpose of gaining access to someone else's resources.
- **USB Memory Stick:** A mobile data storage device, like a Stiffy disk, Jump drive, External Hard drive, but using a specialized connection called the Universal Serial Bus (USB) to download or upload data.
- **PKI:** Public Key Encryption
- **PGP:** Pretty Good Privacy
- **Bitlocker:** Windows 7 and Vista Disk Encryption
- **VLAN:** Virtual Local Area Network. A zoning methodology whereby a network is virtually divided into different zones with different security practices and controls being applied.
- **VPN:** Virtual Private Network. The same philosophy as for a VLAN. The key differences are:

  - The zoning can be applied broader than a LAN to a Wide Area Network (WAN) and there is an element of privacy or dedication of the virtual network to a particular entity such as a business or department, etc.

- **Workstation:** This is any type of computer or laptop used by an IT user in the execution of their duties.
- **DL:** Distribution List – Outlook, when users are Group in a mailing list.
- **Wireless Communication:** A communications medium that allows devices to connect without the use of physical media, such as cabling

APPENDIX B

PRIVACY WAIVER, MONITORING AND INTERCEPTION OF ELECTRONIC COMMUNICATIONS NOTICE AND ACKNOWLEDGEMENT OF UNDERSTANDING

Privacy Waiver

Employees are given IT resources (computers, software, e-mail and Internet access) to assist them in the performance of their job functions. Employees should have no expectation of privacy in anything they create, store, send or receive using the Municipality Information and communications technologies equipment. The computer network is the property of **SIYATHEMBA MUNICIPALITY** and is used to conduct company business. Users expressly waive any right of privacy in anything they create, store, send or receive using the Municipality computer equipment, software or e-mail and Internet system. Users consent to allow company personnel access to and review of all materials created, stored, sent or received through any Municipality network or Internet connection.

Monitoring and Interception of Electronic Communications

The Municipality has the right to monitor and log any and all aspects of its Municipality network including, but not limited to, monitoring e-mail sent and received by users, monitoring chat and newsgroups, monitoring file downloads, and all communications including voicemail, sent and received by users.

Acknowledgement of Understanding

All users of **Siyathemba Municipality** IT assets, resources and infrastructures are expected to accept the terms and conditions of this policy. This appendix will be attached to and will form part of the approved policy. Users must accept the terms and conditions of the policy by signing this acknowledgement of understanding. Management within a user’s business unit must manage and keep proper record of the acknowledgement of understanding signed by users.

I have read and agree to comply with the terms of this policy governing the use of **Siyathemba Municipality** IT assets, resources and infrastructures including e-mail and internet usage, personal computer and laptop usage, software usage, wireless communication usage, passwords, viruses, information disclosure, data security, monitoring and interception of electronic communications, third party access and remote access services (RAS). I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

______________________ ______________________

Employee Name: Signed:

______________________ ______________________

Designation: Date:

APPENDIX C

INDEMNITY

I, the undersigned, in consideration for being granted permission to make use of the **Siyathemba Municipality** IT Assets, do hereby indemnify and hold BPC harmless against all claims for loss of damage of any kind whatsoever or any other legal proceedings arising from my use of the said **Siyathemba Municipality** IT Assets as a result of negligence, breach of contract or other wrongful act that I may knowingly or unknowingly commit whilst utilizing the said **Siyathemba Municipality** IT Assets.

I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Employee Name:

Signed:

Designation:

Date:

APPENDIX D

E-MAIL GUIDELINES

As e-mail communication has proliferated, the need for e-mail guidelines has also increased. It turns out that there are easy-to-follow rules of e-mail etiquette that can ensure your e-mail is read, understood, acted upon, and processed quickly, accurately, and efficiently. E-mail best practices establish standard rules to ensure consistency and predictability in e-mail communication. The overall goal is to improve productivity by helping recipients organize, prioritize, and process e-mails more quickly. Use these in conjunction with the e-mail subject line designations to ensure that your e-mails are read and acted upon appropriately.

When sending e-mail

- Send e-mail only to those involved in the discussion/decision and include them on the “To:” line (not the “cc:” line).
- If the e-mail involves assigning an action item to a recipient, make sure he or she is listed on the “To:” line.
- Use the “cc:” line for recipients from whom no action is required but awareness is important (this is equivalent to the subject line designation “FYI”).
- Don’t send large attachments
- Limit the use of or don’t use “bcc:” because it breaks Users Office Outlook rules.
- For conference call meeting requests:
- Include the phone number and PIN in the location line.
  - Attach links to reference material in the body of the request.

When replying to e-mail

- Reply only to those involved in the discussion/decision.
- Limit “reply all” responses to those who need to act upon, implement, or be informed about the discussion.

When forwarding e-mail

- Revise subject lines by using appropriate subject line designations.
- When forwarding a long thread, use the appropriate subject line designation and summarize the contents of the thread.
  - Where there has been no additional commentary, put the forwarding history at the bottom of the e-mail and note that forwards have been deleted or moved.

E-mail Subject Line Designations

E-mail subject line designations are used by the sender to give the recipient an indication about the nature of the e-mail. The intent is to provide sufficient information to allow recipients to quickly organize and prioritize e-mails, along with quickly and easily identifying commitments and requests.

In addition to using the designations, you should make certain that the subject line is as informative as possible so the recipient knows how to process the mail. For example, when appropriate, include requested actions and due dates in the subject line. The use of e-mail designations in combination with other e-mail best practices will streamline e-mail processing as well as help e-mail users quickly identify requests, agreements, and commitments.

Results Driven E-mail

In this case, “results” doesn’t just mean achieving your own objectives. It also means getting results from your audience. This means creating communications that include specific, actionable goals to which the Field can respond.

The following provides a framework of the key elements of results-driven communications:

1. **Use a subject line designation with the date and the specific action that needs to be completed by that date.**
2. **Flag the content with enough lead time to complete any required actions.**
3. **Executive summary/announcement/situation:** What is it I want to communicate (a product, program, service), and what do I want my audience to do about it?
4. **Goal:** What is the intended outcome of the call to action?
5. **Deliverables:** Are there any deliverables that need to accompany the communication?
6. **Time frame:** What are the key dates related to this communication?
7. **Call to action:** Specific action to be taken. This can be broken down by audience; that is, one group may have one call to action, while a different group may have another.
8. **Where to go for more information:** Are there online resources or key contacts that recipients should know about?
9. **Questions, comments, suggestions: How can the audience respond with feedback?**

The Communications Template was created for Siyathemba Municipality so that Communicators can easily:

1. Improve the overall quality of communications sent via email.
2. Incorporate the Communications Guidelines by using Subject Line Designations within all email.
3. Prevent recipients from forwarding or replying-to-all to your messages or meeting requests.
4. Quickly set importance for messages or meeting requests that you send.

   Assign flags for messages so that recipients take appropriate action on your communication. More and more, decisions are being made on what email to keep and what email to delete via Smartphone's. Without a clear subject and call to action, Communicators have no chance of reach their intended audiences via email. Communicators are very busy people too and often, communications are sent via email without disabling the Reply All feature and then all it takes is one person to hit Reply All, now there will be either a mass exodus from your DL or complaints sent directly to the owner of the DL, which is 9 times out of 10 is YOU. We also have this feature available in Calendar, so when you send a Meeting Request to 50 people, someone accidentally doesn't hit the Reply All button, cause major productivity loss for the Virtual Team