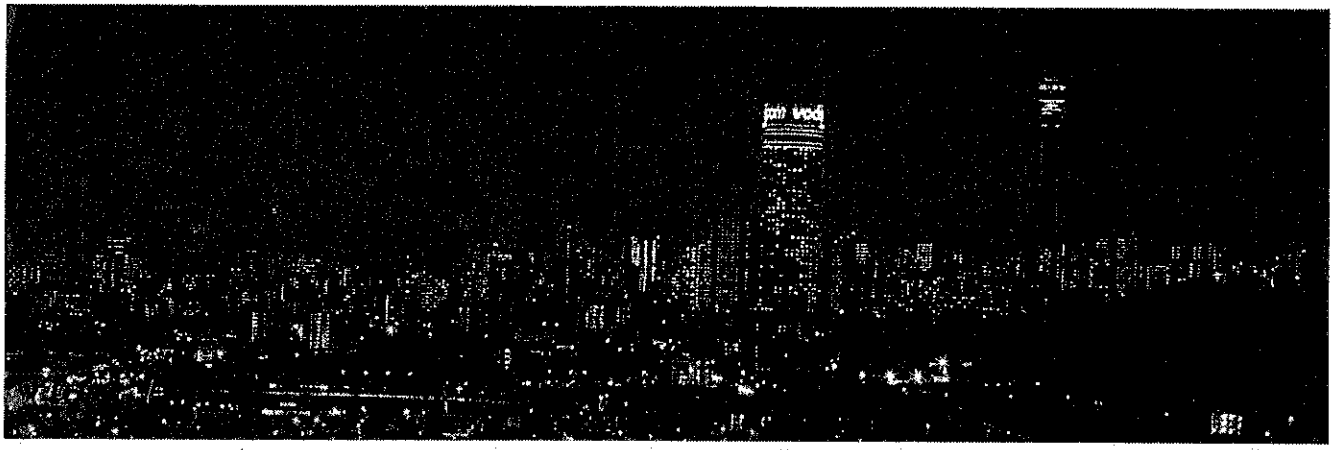


# Group Information Communication Technology and Information Management

## ICT Standards Policies and Procedures

23 May 2023

# Document Configuration Management

## Document Identification

| | |
|---|---|
| **File Name** | ICT Standards Policies and Procedures |
| **Version** | 30 |
| **Published Date** | 23 May 2023 |
| **Document Owner** | GICT&IM Governance |

## Version Change Control

| Action | Version | Name | Role / Function | Date |
|---|---|---|---|---|
| Prepare | 25 | | | April 2013 |
| Review | 26 | Ntefo Matlhage | GICT&IM Governance | 20 January 2017 |
| Review | 27 | Ntefo Matlhage | GICT&IM Governance | 30 March 2018 |
| Review | 28 | Ntefo Mathebula | GICT&IM Governance | 01 March 2019 |
| Review | 29 | Ntefo Mathebula | GICT&IM Governance | 01 March 2022 |
| Review | 30 | Ntefo Mathebula | GICT&IM Governance | 23 May 2023 |
| | | | | |

## Document Review and Reference

| **This document will be reviewed and updated every three years, when necessitated by changes in the information security landscape, and as defined below:** |
|---|
| Once in every three years |
| As and when required to update or improve content based on external factor |
| Following changes to the relevant standards |

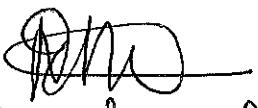
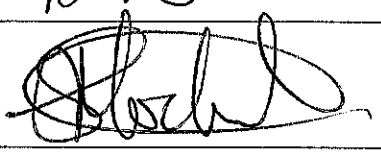
# Confidentiality

This document contains confidential and proprietary information of City of Johannesburg municipality. Policy users (COJ employees and COJ service providers) may not disclose the confidential information contained herein to any third party without the written consent of City of Johannesburg.

## Legal and Constitutional Implications

Non-compliance with the principles described in this document may result in disciplinary action, possibly including dismissal. It is therefore vital that all employees and contractors to the City of Johannesburg who utilise the City's systems are made aware of this policy.

## Document Approval

| Name | Designation | Signature | Date |
|---|---|---|---|
| Ntefo Mathebula | Acting Group Head: ICT Governance Security Risk, Audit and Compliance |  | 24/05/2023 |
| Aubrey Mochela | Group Chief Technology Officer |  | 30/05/2023 |

# Table of Contents

# 1. Introduction

## 1.1. Overview

This SPP describes the basic computer standards, policies and procedures that all of the City's employees, contractors and controllable users of the City's computer facilities are required to follow. This includes employees of utilities, contractors, vendors, and others authorised by the City's management to use the City's internal and external computer systems.

City of Joburg's information is defined as any information within its purview, including information that the City may not own but which is governed by laws and regulations to which the City is held accountable.

Technology changes at a rapid rate and it is necessary for the standards and procedures to be regularly updated. Accordingly, the Group ICT & IM Head of the City will authorise updates to the document as and when required. The latest version of the SPP document will be sent to the City Manager's Office for review and approval on a yearly basis.

The City of Joburg's information and computing assets are critical to the City's success, and must be protected from loss, modification or destruction. The City of Joburg's information is defined as any information within its purview, including information that the City may not own but which is governed by laws and regulations to which the City is held accountable. It includes data in any form, that is owned and used by the City to conduct its business, and which is captured, stored, maintained, and accessed in the City's systems and on the City's equipment. All information stored on the City's computers and equipment, or travelling over computer networks, which has not specifically been identified as the property of other parties, will be treated as though it is a City asset.

Throughout this document reference is made to the Service Desk (ICT Service Desk (The ICT Service Desk can be contacted on 0800223220)). Whenever a new service is required, or a problem is being experienced or further information is required always in the first instance contact the ICT Service Desk on 0800223220. In most cases the staff member taking your call will be able to immediately provide you with the necessary information or assistance.

## 1.2. Purpose

The ICT Standards, Policies and Procedures (SPPs) document sets out the principles and standards which determine acceptable use of the computing resources of the City of Joburg.

The primary aim of this SPP document is to balance the proper and efficient business use of the computing resources against the need for protection of the systems, services and information that makes up those resources.

## 1.3. Scope

This policy applies to all CoJ information systems, data, employees (permanent and temporary), contractors and vendors that access and use CoJ information systems and data.

This document describes the basic computer standards, policies and procedures that all of the City's employees, contractors and users of the City's computer facilities are required to follow. This includes councillors, employees of utilities, contractors, vendors, and others authorised by the City's management to use the City's internal and external computer systems.

## 1.4. Non-Compliance

Non-compliance with the principles described in this ITSPP document may result in disciplinary action, possibly including dismissal. It is therefore vital that all employees and contractors to the City of Joburg who utilise the City's systems are made aware of the SPPs. Any relevant updates or additions to the document will go through the Change Management Process. The document itself is freely available in paper (hardcopy) and electronic http://jozinet/Jozinet/jhome.nsf/homepage?openform form.

Additionally, the Human Resources department has been advised of its existence and first-time users of the City's systems are required to agree and sign electronically that they will conform to these standards and codes of practice.

Independent contractors who breach these ICT SPPs may have their contracts terminated with immediate effect and may be the subject of criminal or civil proceedings instituted against them by the City.

Users are advised to report any violation of the ICT Standard Policies and Procedures to ICT SERVICE DESK on 0800223220.

The Group ICT & IM Head will inform Group Risk and Assurance Services (GRAS) department and the user's line manager/head of the violation for disciplinary purposes. The line manager/head must report the outcome of the action to the Group ICT & IM Head and GRAS.

# 2. Policy Statements

## 2.1. RISK AND CONTROL MATRIX

This risk and control matrix provides a list of the risks intended to be address by the policy and how they are addressed by the respective set of ICT Standards, Policies and Procedures.

| No | Risk description | IT SPP Addressing the risk |
|---|---|---|
| 1 | 1. Inadvertent change or distribution of messages through error or negligence;<br>2. Unauthorised use, processing or distribution of messages;<br>3. Distortion, interruption or unwanted disclosure of messages;<br>4. Unwanted infection with, and distribution of, viruses or other harmful programs;<br>5. Unauthorised disclosure of confidential, proprietary or trade secret information;<br>6.Copyright infringement.<br>7. Phishing<br>8. Spoofing | **SPP01 – Email:**<br>Email includes both the transmission and handling of sometimes-sensitive information, care must be taken to protect the message from unauthorised access.<br><br>The purpose of SPP01 is to protect the City against threats that come with the individuals' ability to change and copy information, or to distribute information to unauthorised parties. Users can also act anonymously, or with a fake identity, and spread information under an assumed name. |
| 2 | 1. When you visit a web site, the site you are visiting can identify where your Internet connection originates. For example, if you use the Web from work, your activities can be identified as coming from the City.<br>2. Web sites can log all of your activity including any personal data you provide. The web site owner can associate you with this data on future visits. Some web sites do not respect data privacy laws and may make the information collected from you available to other organisations.<br>3. Information known as "cookies" may be placed as a file on your system by web sites. In some instances, other web sites can browse your cookie file and find personal information. Cookies may be helpful but be aware that they persist until you manually erase them.<br>4.Denial of Service<br>5.Phishing<br>6.Spoofing<br>7.Targeted attacks | **SPP02 – Internet Access & Usage:**<br>This SPP aims to protect the City against the possible dangers of loss of users' privacy or leakage of Information about either the users or the City's activities |
| 3 | 1.Risk of unauthorised user access to the City's systems and unauthorised changes to data<br>2.Lack of identification of users of the City's systems | **SPP03 – User Accounts and Passwords:**<br>The user account and password uniquely identify employees and users, and allows access to the City's information and computer services |

| | | |
|---|---|---|
| 4 | 1. Loss or theft of the workstation / laptop and Hand Held devices<br>2. Loss of business Information<br>3. Loss of productivity | **SPP04 – Usage of Computer Workstation /Latops and Handheld Devices**<br>This section describes the actions that users must take to protect these physical assets. In addition, users must follow the requirements specified in the Protecting City Information section of this document to protect the information contained on your workstation and related storage media. |
| 5 | 1. Theft of business information<br>2. Unauthorised access to computing resources and information<br>3. Reputational damage<br>4. Loss of productivity<br>5. Financial loss<br>6. Possible Litigation | **SPP05 – Protecting City Information**<br>This section identifies basic controls that must be active on all types of computer workstations and media to protect the City's information |
| 6 | 1. Theft of business information<br>2. Unauthorised access to computing resources and information<br>3. Reputational damage<br>4. Loss of productivity<br>5. Financial loss<br>6. Possible Litigation<br>7. Hacking<br>8. Denial of Service<br>9. Social Engineering | **SPP06 – Internal Networking**<br>This SPP provides guidance on how to strictly control access to the City's intranet and internal LAN systems |
| 7 | 1. Theft of business information<br>2. Unauthorised access to computing resources and information<br>3. Reputational damage<br>4. Loss of productivity<br>5. Financial loss<br>6. Possible Litigation<br>7. Hacking<br>8. Denial of Service<br>9. Social Engineering | **SPP07 – External Networking**<br>This SPP aims to control connections to the internet and other external networks |
| 8 | 1. Theft of business information<br>2. Unauthorised access to computing resources and information<br>3. Reputational damage<br>4. Loss of productivity<br>5. Financial loss<br>6. Possible Litigation<br>7. Hacking<br>8. Denial of Service | **SPP08 – Access Management to COJ Computing Resources**<br>The purpose of this SPP is to provide guidance on managing access to COJ computing resources |

| | | |
|---|---|---|
| 9 | 1. Increased downtime due to support staff being unfamiliar with the product.<br>2. Complete lack of support.<br>3. Incompatibility between systems and the base Operating System.<br>4. Virus infection<br>5.Incompatibility between products resulting in translation errors between systems or rework by City employees.<br>6. Additional procurement costs.<br>7. Additional installation and maintenance costs.<br>8. Lack of adequate security.<br>9. Severe financial penalties imposed on the City by suppliers of the software e.g., Microsoft.<br>10. Severe penalties imposed on individual employees by suppliers.<br>11. Unacceptable media exposure.<br>12. Disruption to services due to the removal or re-installation of products.<br>13. Increased unbudgeted and unnecessary training expenses.<br>14. Reduction in ability and flexibility for job sharing and transitioning;<br>15.Inability to backup or recover information. | **SPP09 – Software Usage & Licensing**<br>The purpose of this standard and policy is to address software management and usage requirements for all City of Joburg employees and contractors |

# 3. Specific ICT Standards, Polices, and Procedures

## 3.1. SPP01 – Email

### 3.1.1. Introduction

Electronic Mail (Email) functions much like ordinary mail. The sender writes an electronic letter and may add, if needed, enclosures such as text documents, graphics or spreadsheets. The sender then 'posts' the message by adding the recipient's Email address, often selected from an electronic address book. These Email addresses may be people, departments or functions and include names and some indication of location.

Email uses resources that can be distributed over several data networks. The user's conduct contributes to whether or not the availability and confidentiality of the system is ensured.

### 3.1.2. Policy statement

Email should only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment of data files to an Email is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of virus and other malicious code.

### 3.1.3. Email Naming Standards

The following naming standards have been agreed to and will apply for all City of Joburg employees:

| **Format:** | **Full first name and first character of the surname** |
|---|---|
| First Name: | Use only lowercase characters. Use the full first name, i.e., no nicknames, and do not use any middle names. |
| Initials: | Add the first initial of the surname. |
| Conflicts: | When defining a new username, if such a name already exists, then the second character of the surname will be inserted after the first character |

### 3.1.4. Size Limits of Mailboxes.

The following limits apply for all City of Joburg employees:

| **No** | **Email box size** | **Employee level description** |
|---|---|---|
| 1 | Unlimited | For Mayor, Speaker, Chief Whip & City Manager |
| 2 | 5GB | EMT, ED's, Group Heads, Directors |
| 3 | 512 MB | DD and Assistant Directors |
| 4 | 250MB | Manager and all other employees |

The request to increase mailbox to the next level should be justified by an authorised report/letter authorised by immediate Director.

Contact ICT Service Desk (The ICT Service Desk can be contacted on 0800223220) for the Email Archiving Process.

### 3.1.5. Email SPPs

1. Incidental private use is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.
2. From time to time the use of the Email system may be audited and monitored.
3. All Emails created, sent, forwarded, stored or printed are the City's property. The City reserves the right to inspect the City's Email Systems at any time without notice.
4. Through using Email you will have been deemed to have read, understood and agreed to the policies relating to Email systems contained within this document.
5. All Email users shall use the approved Email Signature Template. Contact IT SERVICE DESK for the latest template.
6. Do not as a matter of course forward confidential, trade secret or proprietary information to third parties.
7. Delete any confidential, trade secret or proprietary information from third parties you received from the Email system after having been read.

8. Only forward classified/confidential messages to other staff within the same work group and retain them on the Email system for a maximum of one month.
9. Do not send all messages as confidential as this negates the purpose and adds unnecessary overheads to the Email systems.
10. Check any Email enclosures for viruses, BEFORE opening, particularly if documents containing executable (e.g., exe, vbs, bat, pif) programs are sent. If you open a message and are prompted to "Enable or Disable macros" you should select "Disable" and scan for viruses. If any are found, then notify the IT SERVICE DESK 0800 223 220). If none are found, you may utilise the attachment.
11. If you get an attachment via email which is unsolicited or of unknown origin, detach it and scan the file using your installed Anti-Virus software. Alternatively delete it. Email ICT Service Desk (The ICT Service Desk can be contacted on 0800223220)
12. Private Email accounts (e.g., Gmail, Yahoo etc) shall not be used for COJ business communication.
13. Avoid unnecessarily large distribution lists.
14. Check your mailbox regularly for received mail.
15. Ensure that the content of your message cannot be misconstrued and that there is nothing unlawful about the transmission or content of your message.
16. From time to time, certain disclaimers may be required for messages requiring confidentiality, legal privilege etc. Request assistance from the City's legal advisor.
17. It is prohibited to display or transmit:
    - Offensive, defamatory, discriminatory or harassing material
    - Sexually explicit or other offensive images or jokes
    - Unlicensed copyright material
    - Non-business-related video and image files
    - Any message which would be deemed unlawful pursuant to the applicable law of any governing jurisdiction
    - Confidential, proprietary or trade secret information outside without authorisation
    - Advertisements
    - Chain letters.
18. Do not send or forward Email notices concerning virus or harmful code warnings to other employees.
19. Avoid sending messages with attachments larger than 8 MB. Large attachments can be compressed
20. Do not send many email messages to a single address as it may disable the destination mailbox.
21. Do not "broadcast" Email messages unnecessarily.
22. Do not create or participate in pyramid schemes.
23. When using E mail to communicate with people on the Internet:
    - Do not automatically forward internal Email to an Internet site.
    - When sending or forwarding Email to the Internet, do not include the names or user IDs of any City employees unless required.
    - Do not use autoreply to functions to respond to your Internet Email. If you use autoreply to functions such as Out of Office message option for your normal City internal Email when you are away, be sure to select the option that excludes sending the notices to Internet users.
24. Employees shall not use an E mail account assigned to another individual to either send or receive messages.
25. Employees should regularly move important information from email message files to word processing documents, databases, and other files, as Email messages may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.
26. If employees receive unwanted and unsolicited email (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should contact the IT SERVICE DESK.
27. Employees shall not employ scanned versions of hand-rendered signatures to give the impression that an E mail message or other electronic communications were signed by the sender.

28. Email is a vital communications tool for the city. Employees should therefore access their Email INBOX at least once per day. Contact the IT SERVICE DESK (IT SERVICE DESK) 0800223220 should further information relating to accessing Email be required.
29. It is the responsibility of employees to manage their own email once they have downloaded it. It is suggested that unwanted Emails are regularly deleted, and important Emails are moved to appropriate folders. Important attachments should be saved in an appropriate folder within the "My Documents" folder and saved to a network server for backup (Home Folders). Contact the IT SERVICE DESK should further information regarding the management of email be required.
30. Address books should be backed up at least once a month. Contact the IT SERVICE DESK should further information regarding the backup of the address book be required.
31. Email access is approved for CoJ employees with valid SAP numbers. All others including Temporary and Contracting/Consulting staff should log a call with the IT SERVICE DESK with the completed and signed user creation form for email access.
32. Every outgoing message should contain a disclaimer at the end e.g. *"The contents of this e-mail and any attachments are confidential. It is intended for the named recipient(s) only. If you have received this email in error, please notify the system manager or the sender immediately and do not disclose the contents to any one or make copies. Please note that the recipient must scan this e-mail and any attached files, for viruses and the like. While we do everything possible to protect information from viruses, the City of Johannesburg accepts no liability of whatever nature for any loss, liability, damage, or expense resulting directly or indirectly from the access and/or downloading of any files which are attached to this e-mail message."*
33. Email sent by City employees to Internet discussion groups, electronic bulletin boards, Social Media platform or other public forums may be removed if determined to be inconsistent with the City's business interests or policies.
34. All email attachments bigger than 8MB will be blocked and be released after 17:00.
35. CoJ has a Bulk Messaging Tool (COJ Message) whereby bulk messages to all CoJ Email users can be sent by way of the Bulk Messaging Tool. Specific SPPs relating to the usage of this facility are:
    - 35.1. Use of COJ Message is strictly for Business related mail
    - 35.2. All business-related messages should be sent to the Internal Communications Departmental Head who will review the message and where appropriate arrange for these to be distributed
    - 35.3. Bulk Email messages will be sent to all CoJ staff that have mail access and cannot be customized to be sent to a specific Region or Department.
    - 35.4. COJ Messages should not exceed 10 MB and special care should be taken where attachments are submitted for circulation. Messages exceeding the prescribed size will not be circulated and will be rejected by the administrator. Attachments should rather be submitted to the Group ICT & IM Head for publication on the City's Corporate Intranet, JoziNet. The Group ICT & IM Head will provide the Communications Department with a link to the attachment[s] for COJ Message distribution

## 3.2. SPP02 – Internet Access & Usage

### 3.2.1. Introduction

The City's information, computing assets, and corporate image on the Internet are critical to our success, and as a result, must be protected from loss, modification or destruction.

The Internet is used to connect with our customers, suppliers and other organisations. It is important to remember the following points:

- The Internet is used by millions of people worldwide.
- Unprotected information sent across the Internet may well be read by any number of unknown people.

### 3.2.2. Policy statement

Management is responsible for controlling user access and usage to the internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents.

### 3.2.3. Internet SPPs

1. Only those employees who have received department management approval may access the Internet via the City's facilities. Automatic access to the Internet is not a right, and access can be revoked if it's found that misuse of the facility is occurring.
2. Internet access on approval is granted to CoJ employees with valid SAP numbers only.
3. All others including Temporary and Contract/Consulting staff must request their City's line manager to send a completed and signed user creation to the IT SERVICE DESK; with the Contract/Consulting staff's Identity number for the Group ICT & IM Head approval and they must accept the IT SPP's. The City's IT is not liable for the support of their assets.
4. Whenever an employee posts a message to a Social Media platform, Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position of City.
5. Unless expressly authorised by the City's Management, when using City information systems, all employees are forbidden from participating in Internet discussion groups, chat rooms, Social Media platforms or other public electronic forums.
6. Participation in discussion groups, chat rooms, social media and other public Internet forums related to City business is restricted to designated employees who have been briefed about the release of confidential or sensitive information.
7. Employees shall not advertise, promote, present, or otherwise make statements about City products and services in Internet forums such as mailing lists, news groups, and social media or chat sessions without the prior approval of the City's Communication Department.
8. Although the Internet is an informal communication environment, the laws for copyrights, patents, trademarks etc. apply. Employees using City systems shall:
9. Repost material only after obtaining permission from the source
10. Quote material from other sources only if these other sources are identified
11. Reveal internal City information on the Internet only if the information has been officially approved for public release by the City's Communications Department.
12. Whenever an Internet user provides an affiliation with the City --whether implicitly or explicitly -- care shall be taken not to make any political advocacy statements or product/service endorsements unless the permission of the City's Communications Department has first been obtained.
13. When you are conducting City business while using the internet, employees shall not deliberately conceal or misrepresent their identity
14. Email sent by City employees to Internet discussion groups, electronic bulletin boards, Social Media platform or other public forums may be removed if determined to be inconsistent with the City's business interests or policies.
15. Group ICT & IM Head City information systems may routinely prevent users from connecting with certain non-business web sites. The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.
16. No employee or independent contractor to City may use the available Internet, Intranet or Email services provided by City to access newsgroups, Internet web sites and FTP sites for unauthorised and/or unacceptable purposes such as, but not limited to:
17. The viewing and/or downloading of pornographic or obscene material of any nature
18. The dissemination of material that advocates hatred and/or conflict or which causes discomfort or embarrassment to the organisation or their fellow colleagues by way of discrimination based on race, ethnicity, gender, religion, sexual orientation, age and/or material that propagates sexual harassment
19. The dissemination of any material supporting any petition, or advertising any services not specifically authorised in writing by the city

20. The transmission of any message of an abusive or defamatory nature of anyone either internally or externally.
21. The use of Internet, Intranet or Email facilities for any purpose whatsoever not connected to or forming an integral part of City's operations or business
22. Web sites that advocate any illegal activity.
23. All information taken off the Internet should be considered suspect until confirmed by City Management.
24. News feeds: email mailing lists, push data updates, Social Media platforms and other mechanisms for receiving information over the Internet shall be restricted to material which is clearly related to City business as well as the duties of the receiving employees.
25. Hot links which transfer a user's Internet session from a City web site to the web site of any outside entity are not permitted.
26. City secret, proprietary, or private information shall never be sent over the Internet unless it has first been encrypted by approved methods.
27. All software and files down-loaded from non-City sources via the Internet (or any other public network) shall be screened with approved virus detection software before being run or examined via another program such as a word processing package.
28. Users shall not up-load software which has been licensed from a third party, or software which has been developed by the City, to any computer via the Internet unless authorisation from the Group ICT &IM Head has first been obtained.
29. All users wishing to establish a connection with the City's computers via the Internet shall authenticate themselves at a firewall before gaining access to City's internal network. Contact the IT SERVICE DESK for further information.
30. No systems shall be directly connected to the Internet, and employees are prohibited from connecting any assets to the Internet.
31. Employees are prohibited from executing Java applets downloaded from the Internet unless the:
32. Applet is from a known and trusted source.
33. Digital signature has been checked and no problem has been discovered.
34. Internet access using computers in City offices is permissible only via a city firewall.
35. Other ways to access the Internet, such as direct dial-up ADSL, 3G, DSL and any other connections with an Internet Service Provider (ISP), are prohibited if City computers are employed. Non-City computers are prohibited from connection to the City's networks without written a completed and signed user creation form to the IT SERVICE DESK and the approval Group ICT & IM Head Group ICT & IM: Head.
36. Dial out or connections to any non-City systems or networks while simultaneously connected to the city internal network are prohibited.
37. Do not run security-testing tools/programs against any Internet system or server.
38. Remote connections e.g., whilst traveling or from home-based systems and laptop computers which are also utilised for City's business must only be made via authorised remote connections procedures (which employ the use of firewalls. Contact the ICT Service Desk (The ICT Service Desk can be contacted on 0800223220) for further information.
39. You should erase unwanted cookies regularly. Cookie settings may be changed in your browser preferences. Contact the Service Desk 0800 223 220 for further information about controlling cookies.

## 3.3. SPP03 – User Accounts and Passwords

### 3.3.1. Introduction

A computer access user account and password are the primary key to computer security. The importance of password maintenance and security cannot be over emphasized. All employees and users of the City's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage. The user account and password uniquely identify employees and users and allows access to the City's information and computer services. For your own protection, and for the protection of the City's resources, you must keep your password secret and not share it with anyone else.

Contact the IT SERVICE DESK if any further password information is required, or if there is any uncertainty surrounding the usage, applicability, and installation or issuing of passwords.

### 3.3.2. Policy statement

The selection of passwords, their use and management as a primary means to control access to the systems is to strictly adhere to best practice guidelines. Passwords shall not be shared with any other person for any reason.

### 3.3.3. Password SPPs

1. All user-chosen passwords for computers and networks shall be difficult to guess. Do not choose:
   - Words in a dictionary.
   - Proper nouns
   - Geographical locations
   - Common acronyms
   - Slang
   - Derivatives of user-Ids
   - Common character sequences such as "123456"
   - Spouse's name
   - Children's/boyfriend's/girlfriend's/pet's names
   - Car license plate
   - Your ID number/ birth date.
2. Do not:
   - Construct fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change.
   - Construct passwords which are identical or substantially like passwords previously employed.
   - Write down or otherwise record a readable password and store it near the access device to which it pertains.
3. Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover or use them.
4. All vendor-supplied default passwords shall be changed before any computer or communications system is used.
5. All passwords shall be changed immediately if they are suspected of being disclosed or known to have been disclosed to unauthorised parties.
6. Regardless of the circumstances, passwords shall never be shared or revealed to anyone else by the authorised user
7. Employees and users:
   - Are responsible for all activity performed with their personal user-Ids:
   - Shall not allow the user-IDs to be used by anyone else.
   - Shall not perform any activity with other users' Ids.
8. All Password must be strong and complex as below, in 9

9. Employee and user generated passwords should in general have the following characteristics and is required to meet the following standards, It should not be:
   - A Name,
   - Date of birth or a word in a dictionary.
   - Your new password must differ from your last 8 passwords used before.
   - The created Password MUST contain:
   - Upper case / capital letter
   - Lower case / small letter
   - Number/s and
   - Special characters (for an example! @, #, etc.)
   - Below is an EXAMPLE on how to create a complex Windows password, using a phrase or a sentence:
     - I drive a BMW 3 series: The password will be: !daBmw3s
     - Be not less than 8 characters in length.
     - Contain at least one alphabetic and one special character.
     - Contain a non-numeric character in the first and last position.
     - Contain no more than three identical consecutive characters in any position from the previous password.
     - Contain no more than two identical consecutive characters.
     - Not contain the user ID as part of the password.
     - Be changed at least every 60 days for systems that do not automatically force regular password changes.
     - A total of 8 passwords history has to be used before an original password can be used
10. "Screen savers" should be activated after 10 minutes of inactivity as a maximum and should be password controlled.
11. Boot passwords should be utilised.
12. Certain systems e.g., Venus have specific password requirements over and above those shown above. These systems will prompt the user for the correct information. If in any doubt, contact the IT SERVICE DESK for further information.
13. Should you forget your password contact the IT SERVICE DESK for assistance? PLEASE BE AWARE THAT THE IT SERVICE DESK PERSONNEL ARE NOT PERMITTED TO AUTOMATICALLY RESET OR REISSUE PASSWORDS. REPLACEMENT PASSWORDS WILL ONLY BE ISSUED ONCE CERTAIN PRESCRIBED SECURITY CHECKS HAVE TAKEN PLACE AND THIS PROCESS MAY TAKE SOME TIME TO COMPLETE.
14. No temporary password may be used for login.
15. All replacement passwords will be requiring to be changed on the first logon.
16. Refer to the IT SERVICE DESK for details on Password resets. Please note though that according to the agreed Security Procedures, passwords will only be issued if the person to whom the password is being issued is identifiable.

### 3.3.4. User Account SPPs

1. The User Account for all COJ System users must be a valid SAP number. Managers must send the completed and signed user creation form to the ICT Service Desk (The ICT Service Desk can be contacted on 0800223220) for creation of a new user. See Appendix A for the user creation form.
2. All others including Temporary and Contract/Consulting staff must use first 8 numbers of the valid ID number/ Passport. They should request their city's manager to send a completed and signed user creation form to the IT SERVICE DESK; with the Contract/Consulting staff's Identity number/ Passport for the Group ICT & IM Head approval and they must accept the IT SPP's.
3. Certain systems e.g., LIS have specific User Account requirements over and above those mentioned above. This account will be created as per systems requirements.
4. The COJ Systems have different User Accounts, namely:
5. Service Account, they run back-end Services (e.g., SVC_***)

6. Application Account, application installation account (e.g., APP_***). This account must be disabled after been used.
7. System Account, created automatically with system creation.
8. User Account, created for user access to COJ Systems (e.g., SAP/ ID/ Passport Number)
9. User Accounts older than 90 days of inactivity will be disabled and the 120 days of inactivity will be deleted.
10. For privileged User Account send a completed and signed user creation form to the IT SERVICE DESK, for the Group ICT & IM Head approval.
11. To grant User Account access to a specific COJ Systems, users must contact the IT SERVICE DESK.

## 3.4. SPP04 – Usage of Computer Workstation /Laptops and Handheld Devices

### 3.4.1. Introduction

The city has a large variety of assets. Many are of great value to the City's success as a business. They include the physical asset and extremely valuable proprietary and confidential information.

Protecting these assets is critical. Their loss, theft or misuse could adversely affect the city.

Every employee is responsible to help reduce the possibility and consequences of theft of all personal City computing resources and devices (e.g., desktops, laptops, Handheld Devices and similar hand-held devices), related materials such as portable hard drives, portable hard drives etc. and printed output, and the information they contain. No matter where you have these assets - in your office, in your home, at a hotel, in a plane or car, etc. you must protect them appropriately.

This section describes the actions that you must take to protect these physical assets. Based on your circumstances you may need to take additional actions to provide adequate protection. In addition, you must follow the requirements specified in the Protecting City Information section of this document to protect the information contained on your workstation and related storage media.

### 3.4.2. Policy statement

1. It is the responsibility of the user to ensure that the device is secured at all times, Should the notebook be lost, the employee will be held fully responsible for the loss, unless it can determine that the employee was not at fault.
2. Employees are responsible for the confidentiality of the information on the notebook and need to take due care about where the notebook is used and stored.
3. The Device must be secured via a Secure Cable security attachment
4. All Employees and non-employees of the City should declare their devices to security upon entry and upon exit. Exit permit may be required for the aforesaid purposes.
5. **Should the notebook be lost, the employee will be held fully responsible for the loss, unless it can be determined that employee was not at fault**
6. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices
7. Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.

### 3.4.3. Workstation/ Laptops and Hand-Held Devices Usage SPPs

1. All City Employees including Councillors will be issued with one workstation either a Laptop or a Desktop.
2. You are personally responsible for protecting any City property and information entrusted to you and for helping to protect the City's assets in general.
3. In the event of the loss, destruction, or damage to an asset, for any reason, please contact the IT SERVICE DESK for further information.
4. Always use the physical (Kensington Cable) or dock locking mechanisms provided with your laptop.
5. If you work in an office that can be locked, and where OHASA regulations allow, lock the office.

6. Activate the password protected screen lock (CTRL+ALT+DEL).
7. Lock up all materials that contain City confidential information or take them with you.
8. At the end of the workday, if your workstation is portable, secure it in a desk or filing cabinet or take it with you.
9. Keep Laptops in your possession if at all possible.
10. When traveling by air, do not put Laptops in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
11. When traveling by car, protect Laptops by locking them in the car boot when you begin your travel.
12. Laptops should not be left for an extended period of time in an unoccupied vehicle. If you must leave your Laptops in an unoccupied vehicle, then consider securing the Laptop to the body of the vehicle inside the boot.
13. If you must leave the Laptop in a hotel, lock it in the hotel safe if one is available. If a safe is not available and you have a locking cable (Kensington Cable), use that mechanism.
14. If you are traveling with City confidential material recorded on portable media such as paper, flash drive, CD, Laptop, etc., you must protect these media/devices according to the same guidelines listed above.
15. If your workstation, is stolen or lost, you must report the loss to the IT SERVICE DESK and your manager as soon as the loss is discovered.
16. NO workstation, printer, fax machine etc. may be moved to a new location or to a new user/s without following the Request for Service procedure. Please refer to section SPP09.
17. Upon delivery each workstation is specifically configured with standard tested settings, including a standard CoJ screensaver. NONE of the settings should be changed without documented reference to the IT SERVICE DESK. Workstations found to be operating incorrectly due to non-standard settings will incur extra maintenance fees.

## 3.5. SPP05 – Protecting City Information

### 3.5.1. Introduction

The City has a large variety of assets, including valuable proprietary and confidential information.

Protecting information is critical. City information is an asset of the City and needs to be protected wherever it exists. This section identifies basic controls that must be active on all types of computer workstations and media to protect the City's information. The next section discusses the additional requirements that exist when dealing with the City's confidential information. Note that several different controls are specified. They address different threats, and all the controls that are available on a workstation must be implemented.

The primary requirement for protecting the City's information is that it must be protected from all access or viewing except by people who have a business need to know the information.

### 3.5.2. Policy statement

The organization intends to fully comply with the requirements of the Constitution and related data protection legislation (e.g., ECT Act 25 of 2002, POPI Act 4 of 2013) in so far as it directly affects the organisation's activities.

### 3.5.3. Protection SPPs

1. All data and information created, stored or archived on any equipment housed within City premises or owned by the City and used by City employees and any other authorised user, is the City's property. The City reserves the right to request and inspect this data and information at any time without notice.
2. The unauthorised possession and/or usage of any equipment or software that could potentially be used to overwrite or alter any of the City's data and information, no matter where or how stored, will result in appropriate disciplinary action being taken.
3. A person who intentionally and without authority to do so interferes with data and information in a way which causes such data or information to be modified, destroyed or otherwise rendered ineffective is guilty of an offence in terms of Section 86(2) of the ECT act 25 of 2002 and may be liable to disciplinary action and/or criminal prosecution.
4. The following security controls must be activated on all computer workstations / laptops and Handheld devices:
   - Set a power-on password.

- Set a hard disk drive password (if available);
- Set a password protected keyboard/screen lock that is automatically activated by a period of inactivity - the inactivity time interval should be no more than 10 minutes (refer to SPP03 – Passwords)

5. For setting power-on and hard disk drive passwords and encryption of local databases refer to the IT SERVICE DESK.
6. Computer workstations available for shared use in any City location are not required to have hard disk drive, power-on and screen lock passwords applied. However, City employees must not place City confidential information, file sharing software, user ID files, mail files or databases on such workstations.
7. When you store City confidential information on computer systems (e.g., group web sites, SQL databases, or other shared data repositories), you must use / user accounts and designated environments to manage and limit access to the information.
8. Security controls must never be set to allow unrestricted access (e.g., World-readable, "public") to City confidential information, including your calendar. If you do not understand how to correctly set or use the security controls, you should ask for advice or assistance from the IT SERVICE DESK.
9. When you store City confidential information on removable computer media, such as portable hard drives portable hard drives, tapes, compact disks (CD/DVDs), etc., you must protect the information against theft and unauthorised access. Label the media confidential and keep them in a locked area or storage device when they are not in use. Never leave them exposed in unattended areas.
10. When printing City confidential information you must protect the information against theft and unauthorised viewing - the term "printer" includes printers, plotters, and any other device used to create hard copy output.
11. City confidential information may only be printed:
    - In a controlled access area, with access based on "need to know".
    - In an attended City printer facility, where the output is given only to its owner.
    - On a printer with capture/release facility that you control.
    - On a printer that you are personally attending.
    - If none of these options are available at your location, you may use a printer located within an open area internal office space, but you must pick up your printout material immediately.
12. Protecting City Information when working at non-City locations:
    - Ensure that City confidential information is protected so that it can only be seen or accessed by authorised people.
    - Lock up all City confidential information and material when not in use - this includes information recorded on portable media such as paper, portable hard drives, Laptops, laptops, Handheld Devices etc.
    - Use workstation passwords (power-on, disk lock, keyboard/screen lock).
    - Lock up workstations (desktops, laptops, hand-held devices, etc.) when not attended.
    - Do not transmit City confidential information on non-City networks.
    - Do not store or process City confidential information on systems which are not controlled by you or City employees.
    - Print City information only on printers where the output can be properly protected.
13. When participating in City confidential teleconferences, confirm that all participants are authorised to participate.
14. Do not store confidential City information on either Internet or Intranet servers.
15. Employees shall not forward information appearing on the Intranet to third parties without going through the appropriate internal channels (such as the City Manager or Communication Division or Group ICT & IM Head).
16. Anti-Virus is used to protect data and information across all City's assets. Employees are responsible for ensuring that they are utilizing the City's preferred Anti-Virus solution and it is up to date... Contact the ICT Service Desk (The ICT Service Desk can be contacted on 0800223220) for any further assistance. If you are traveling with City confidential material recorded on portable media such as paper, portable drives, CD/DVD, Laptop, etc., you must protect this media according to the same guidelines listed above for protecting your Laptop
17. If City Confidential Information, is stolen or lost, you must report the loss to the ICT Service Desk (The ICT Service Desk can be contacted on 0800223220) and your manager as soon as the loss is discovered.

## 3.6. SPP06 – Internal Networking

### 3.6.1. Introduction

The City's Intranet and internal LAN systems are for the exclusive use of authorised City employees and authorised users. Unlike the Internet, information on the Intranet may be disseminated only to authorised persons and is not accessible except with specific authorisation.

### 3.6.2. Policy statement

Access to the resources available from the organisation's network must be strictly controlled in accordance with agreed policy, which must be reviewed and updated regularly.

### 3.6.3. Internal Networking SPPs

1. Do not misrepresent yourself (i.e., masquerade) as someone else on the network.
2. Do not monitor network traffic (i.e., use \a "sniffer" or similar device).
3. Do not add any network device that creates an external connection (e.g. a bridge, router, gateway, hub, and modem) to your workstation.
4. NO donated or third party or non-standard equipment may be connected to any network point without the prior approval of the Group ICT & IM Head.
5. Do not install file sharing or peer-to-peer software.
6. If you must allow other users to access or store files on your network connected workstation you must select either userid access control or password access control when defining the share options for the workstation disk drives and files – contact the IT SERVICE DESK for further information.
7. You must not allow ANONYMOUS FTP, TITP, or other unauthenticated access to program or data files on your workstation. Only SFTP is allowed once approval is given. Contact the IT SERVICE DESK for further information.
8. Before any information is posted to the City's Intranet, at least two approvals shall be obtained, from the department manager in charge of the relevant Intranet page and the owner of the information (or creator of the information if the owner has not yet been designated).
9. All content posted to the City's Intranet remains the property of the City.
10. Employees shall not establish Intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of the Group ICT & IM Head.

## 3.7. SPP07 – External Networking

### 3.7.1. Introduction

Unlike internal LANs and the Intranet, connections to external public networks and the Internet has the potential to allow any person access to the City's systems. For this reason, connections to the Internet and other external networks are strictly controlled.

### 3.7.2. Policy statement

Access to the resources available from the organisation's network must be strictly controlled in accordance with agreed policy, which must be reviewed and updated regularly.

### 3.7.3. External Networking SPPs

1. If you need to connect to non-City systems or networks e.g., the Internet, to a business partner's system, etc., you must use one of the approved City firewalls. Check with the IT SERVICE DESK for further information.
2. Do not dial out or otherwise connect to any non-City systems or networks while simultaneously connected to the City's internal network. To establish such a connection, first physically and logically disconnect your workstation from the City's internal network - contact the IT SERVICE DESK for further information.
3. If you need to connect to City systems and networks from outside City premises, you must be registered to use one of the approved remote access services (VPN). Check with the IT SERVICE DESK to determine how to register to use these services.
4. NO donated or third party or non-standard equipment may be connected to any network point without the prior approval of the Group ICT & IM Head.
5. Dial line access to/from an employee's individual workstation is not allowed.
6. Employees connected via TCP/IP must not be simultaneously connected via a modem to the Internet or any other external TCP/IP network without explicit management authorisation and unless the appropriate TCP/IP commands are entered which prevents intruders from using the workstation as a pathway into the internal network. Contact the IT SERVICE DESK for further information.
7. In-house production information systems, such as a server, shall not be directly connected to the Internet. Instead, these systems shall connect with an application server, a database server, or some other intermediate computer that is dedicated to Internet business activity.
8. Other ways to access the Internet, such as dial-up connections with an Internet Service Provider (ISP), are prohibited from City owned computers, or any computer connected to any City network or system.
9. All web servers accessible via the Internet shall be protected by a router or firewall approved by the Group ICT & IM Head.
10. The establishment of a direct connection between City systems and computers at external organisation (tunnels or virtual private networks) via the Internet or any other public network is prohibited.
11. Employees and users shall not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not first obtained approval from the Group ICT & IM Head.
12. Information regarding access to the City's computer and communication systems, such as modem phone numbers, is confidential. This information shall not be posted on the Internet, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the permission of the Group ICT & IM Head.
13. Employees and users shall not leave modems connected to personal computers in auto-answer mode so that they are able to receive in-coming calls.

## 3.8. SPP08 – Access Management to COJ Computing Resources

### 3.8.1. Introduction

Access authority to City of Joburg systems should be based on current business need and controlled by verifying the identity of the user or application. The City of Joburg provides its employees ("users") with access to various computing resources. The purpose of this access is to facilitate employees' work.

# 4. ANNEXURE A: Glossary of Terms

| Term | Definition |
|---|---|
| City of Joburg Information | This is defined as any information within its purview, including information that the City may not own but which is governed by laws and regulations to which the City is held accountable. |
| Service Provider | Many of the IT services provided to the City are provided by a company named SERVICE PROVIDER. The terms SERVICE PROVIDER or SERVICE PROVIDER are used interchangeably to refer to this SERVICE PROVIDER in this document. |
| Group ICT & IM Head | For purposes of this document, Group ICT & IM Head refers to the department (Information Communication Technology and Information Management) |
| Workstation | The term workstation is defined to include any portable computing device including but not limited to Laptop computers, laptops, electronic diaries, Handheld Devices, portable scanners etc. |
| Business Information | Is defined as any information within its purview, including information that the City may not own, but which is governed by laws and regulations to which the City is held accountable. It includes data in any form, that is owned and used by the City to conduct its business, and which is captured, stored, maintained, and accessed in the City's systems and on the City's equipment. All information stored on the City's computers and equipment, or travelling over computer networks, which has not specifically been identified as the property of other parties, will be treated as though it is a City asset. |
| Local area network (LAN) | Is a computer network that interconnects computers within a limited area such as an office building and has its network equipment and interconnects locally managed. |
| Wide Area Network (WAN) | Is a telecommunications network or computer network that extends over a large geographical distance. AWAN connects different smaller networks, including local area networks (LAN) and metro area networks (MAN). |
| Computing resources | Desktops, Laptops, Handheld Devices and similar hand-held devices, related materials such as portable hard drives, portable hard drives and printed output, and the information they contain. |
| Virus | Viruses are designed at best to cause some discomfort and at worst to cause the alteration and loss of data on a computer. Viruses pose a tremendous threat and can be introduced in a number of ways, particularly from files and programs downloaded from public sources and via Email attachments. |

# 5. ANNEXURE B: Form - Request for Creation of a New User

| **Section 1: New User Information** | | | | |
|---|---|---|---|---|
| Full Name/s | | | Last Name | |
| Designation | | | Department | |
| SAP Number | | | Asset Tag | |
| ID Number (if contractor) | | | Company | |
| Contractors | Start Date | | End Date | |

| **Section 2: Access Required (Tick where applicable)** | | | |
|---|---|---|---|
| Shared Drive | Shared Drive Name | | |
| Internet | Limited Internet Access | | |
| | Basic Internet Access | | |
| | Advanced Internet Access | | |
| | Unlimited Internet Access | | |
| | EMT | | |
| Email | | | |
| VPN Access (via 3G) | Systems to be accessed | | |
| Other: please specify | | | |

| **SECTION 3: Line Manager Approval** | | | |
|---|---|---|---|
| Full Name/s | | SAP Number | |
| Designation | | | |
| Contacts (E-mail, Tel & Cell) | | | |
| Motivation (for Advanced Internet and/or VPN Access) | | | |

| | | |
|---|---|---|
| Has the user accepted/signed the COJ IT Policies and Procedures which can be found at http://jozinet | YES | NO |

| | | | |
|---|---|---|---|
| Signature | | Date | |