Western Cape
Government

IT End User Policy
Western Cape Government

Version 1.5 as of 09 October 2015

Please Visit the Blue Pages for a signed Copy
http://intrawp.pgwc.gov.za/Blue_Pages/Cel.asp

Contents

Document Version Control

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
22/04/2008	P&S	1.0	• Private use if email modified, GroupWise and instant messaging changes
12/08/2010	P&S	1.1	• Integration of information security
07/12/2010	P&S	1.2	• Modification of email retention
06/12/2012	P&S	1.3	• Change in mailbox quotas
29/10/2014	Security Team	1.4	• Adding of administrator account restriction for users under point 5. • Edited Queries section to conform to recent policy amendments. • Added contents table.
09/10/2015	Security Team	1.5	• Annual review

Approvals

JOB DESIGNATION	**NAME**	**SIGNATURE**	**DATE**
CHIEF INFORMATION OFFICER	LANCE WILLIAMS		

1. POLICY PURPOSE

The purpose of this policy is to ensure the proper use of Information Communication and Technology (ICT) assets of the Western Cape Government (WCG). The policy applies to any ICT asset the WCG has or may install in the future. Users have a responsibility to use ICT assets in an efficient, effective, ethical and lawful manner.

2. SCOPE OF APPLICATION

This policy is applicable to all WCG employees, contractors and agents who act on behalf of the WCG or are in its employment and are end users of the WCG IT Systems, equipment and Infrastructure.

3. GUIDING PRINCIPLES

The primary purpose of the Acceptable Use Policy is to protect the WCG, Officials, Contractors, other spheres of government and other parties from illegal or damaging actions by individuals, whether deliberate or unintended. The primary guiding principle is that WCG information technology assets should be used for WCG business purposes.

4. LEGAL FRAMEWORK

This policy draws its mandate from the following prescripts:

- The Electronic Communications and Transactions Act (Act No. 25 of 2002)
- The Public Service Act (Act No. 111 of 1984)
- The National Strategic Intelligence Act (Act No. 39 of 1994)
- The Protection of Personal Information (Act No. 4 of 2013)
- The Protection of Information Act (Act No. 84 of 1982)
- The National Archives and Record Service of South Africa Act (Act No. 43 of 1996)
- SABS/ISO 27k
- The Minimum Information Security Standards (MISS) and/or the Guidelines for the handling of Classified Information (SP/2/8/1)
- The Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 (Act No. 70 of 2002).

5. POLICY STATEMENT

5.1. General Provisions

a) The WCG is governed by a broad range of legislation regulating telecommunications including, but not limited to, the Electronic Communications and Transactions Act, 2002, and the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, (the Interception Act).

b) Users are bound by all relevant legislation and policies regulating telecommunications and electronic communications and undertake at all times to act in accordance with all relevant legislation and policies. Users acknowledge that they have been granted access by the organisation to telecommunications information technology and resources, including e-mail and Internet access. The sole reason for providing such access to Users is to perform duties and responsibilities in accordance with their job function or other official purposes of the WCG.

c) Users acknowledge that they have no expectation of privacy when utilizing any telecommunications equipment and resources operated under the auspices of the WCG and they grant permission to the WCG to intercept, monitor, read, filter, block or otherwise act upon any electronic telecommunication, stored file or indirect communication which is or has been under their control, received by them or transmitted by them as contemplated in the RICA Act.

5.2. Use of WCG IT Equipment

a) The end user shall be responsible for his or her workstation or portable computer.

b) If the equipment is stolen, damaged, borrowed or otherwise unavailable for normal business activities it shall immediately be reported via the *Incident Management Procedure*.

c) WCG equipment must not be removed from WCG premises without a valid removal permit.

d) Equipment must be physically secured or physically protected to guard against theft.

e) Users must ensure that equipment assigned to them has been added to the asset inventory and has received a unique identifier and classified in accordance with the Asset register.

f) Users with WCG equipment at their homes shall safeguard the equipment as required by *IT Security Policies*.

g) Users shall ensure that they keep mobile equipment in their possession at all times when they are in a public place.

5.3. Desktop Computer Use

a) The device (Computer Desktop, Laptop) may not be connected to two or more networks simultaneously.

b) No modems may be connected to any devices that are attached to the WCG's production network.

c) Users must be supplied with a username and password in order to access services on the production network of the WCG.

d) Users must keep passwords secure and not share their account credentials. Users are responsible for the security of their passwords and accounts.

e) The device must be locked or logged off when unattended.

f) The device must be kept up to date with the latest anti-virus software and virus definitions and Operating System updates.

g) Before introducing any new electronic data into the WCG network an anti-virus scan will be performed.

h) The user must not disable, and/or change the configuration of the anti-virus software.

i) Users shall not load any illegal or unapproved software onto the device.

j) Users acknowledge sole responsibility for any unauthorized or pirated software found in their possession or on the systems and equipment allocated to or used by them.

k) Users are not allowed to have a local administrator account.

5.4. Email

Electronic Mail usage is granted for the sole purpose of supporting organisational business activities. The WCG supports the installation and usage only of approved email clients.

Usernames must be assigned by the WCG (through the Centre for e-Innovation) and reflect internally mandated e-mail naming conventions.

5.4.1. Acceptable Email Use

a) Communicating in a professional manner.

b) Personal communications that are brief and do not interfere with work responsibilities.

c) Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending the message.

d) Departmental mass internal e-mails, such as bulletins and information brochures, must be approved before dissemination.

5.4.2. Unacceptable Use of Email

a) Creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.

b) Creating and exchanging information that is in violation of copyright or any other law. The WCG is not responsible for use of e-mail that contravenes the law.

c) Opening file attachments from an untrustworthy source or with a suspicious or unexpected subject line.

d) Sending confidential information to unauthorized people or violating the Minimum Information Security Standards. Otherwise using e-mail in a way that increases the WCG's legal and regulatory liability.

e) Communications that strain the WCG network or other systems unduly, such as sending large files to large distribution lists.

f) Using any e-mail system, other than the WCG e-mail system, for WCG- related communications.

g) Circulating chain letters and/or commercial offerings.

h) Circulating unprotected data and personally identifiable client/citizen data that would violate section 14 of the Constitution.

i) Promoting or publishing a User's political or religious views, operating a business or for any undertaking that offers personal gain.

j) Using the e-mail system for any purpose or in any manner that may prejudice the rights or interests of the WCG or government in any other sphere.

5.4.3. Email Quotas

a) Online Mailbox

i. All new mailboxes are created with a 1GB space limit. All users are required to manage their emails and delete emails that are no longer required.

ii. If this mailbox quota is not sufficient, users have the following options:

- Move items to the online archive
- Apply via DITCOM for an increase to your current online mailbox quota

iii. Users must first clean up mailboxes before applying for additional space.

iv. Deleted Item Retention Period: Users are able to recover deleted email using the Outlook 2010 Client. The deleted item retention period is 180 Days

b) Online Archives

i. The online archive is provided to all WCG employees, with a pre-determined set of retention policies aimed to assist the WCG in meeting their compliance and regulatory goals.

ii. The primary goal of the archive solution is to provide a reliable, stable enterprise messaging archiving system which will allow users to archive data and will facilitate a smaller primary mailbox.

iii. All new online archive mailboxes have a **5GB size limit**. The archive mailbox maximum size limits is 5GB.

iv. Deleted Item retention period for an Archive:

- Users are able to recover deleted email using the Outlook 2010 Client.
- The deleted item retention period is 14 Days.

c) Local Archives: No local archives (PST's) will be allowed on the hard drive of the workstation or laptop.

5.4.4. Email Retention

The WCG will make use of retention policies and retention tags to manage email. The default policy will move all folders in the mailbox to archive after 2 Years. Email older than 5 years will be removed from the online archive mailbox.

5.5. Internet

Internet usage is granted for the sole purpose of supporting WCG business activities necessary to carry out job functions. All Internet based transactions originating from within the WCG's production network, are logged using the IP address of the workstation, the workstation host name, as well as the site visited and the time, for auditing and compliance purposes.

5.5.1. Acceptable Uses of Internet

a) Accessing web-based business applications and tools.

b) Communication between Officials and non-Officials for business purposes.

c) Review of possible vendor web sites for product information.

d) Reference regulatory or technical information in line with the relevant the job description or official functions.

e) Accessing of Government web sites and portals.

f) Conducting research in line with relevant job description or official functions.

5.5.2. Unacceptable Uses of Internet

Acquisition, storage, and dissemination of data that are illegal, pornographic, or which negatively depict race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth is specifically prohibited.

The WCG also prohibits engaging in fraudulent activities, or knowingly disseminating defamatory materials.

Other activities that are strictly prohibited include, but are not limited to:

a) Accessing information that is not within the scope of the Official's work. This includes unauthorised accessing and / or reading of WCG information, unauthorised access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

b) Deliberate pointing or hyper-linking of the WCG's Web sites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the WCG.

c) Any conduct that would constitute or encourage a criminal offence, lead to civil liability, or otherwise violates any regulations, directives or the common law.

d) The use, transmission, duplication, or voluntary receipt of material that infringes on the copyright, trademarks, trade secrets, or patent rights of any person or organisation. [Officials must accept that all materials on the Internet are copyrighted and/or patented unless specific notices expressly state otherwise].

e) Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls and the express permission from the relevant mandated parties.

f) Any form of on-line gambling and gaming.

g) Using the internet for any purpose or in any manner that may prejudice the rights or interests of the WCG or government in any other sphere.

5.6. Remote Access

a) Users must only make use of remote access facilities in accordance with the Remote Access Policy (*Information Security – Remote Access Security Policy*).

b) Users must not remotely connect to the WCG network and another network at the same time.

5.7. Information Security

a) Users must report all security incidents in accordance with the *IT Incident Management Procedure*.

b) All users accessing WCG information shall preserve the confidentiality, integrity and availability of information.

c) Users must ensure that all media, such as floppy disks, memory sticks, drives and CDs, to be discarded is formatted and cleansed of all data. If media is damaged and cannot be formatted the media shall be destroyed in such a manner that repair of the media is impossible.

d) Users must ensure that all media used for the storage of data is stored in a secure environment and within safe distance of any electromagnetic interference, such as cell phones, that can damage the media.

e) Users must not share folders to all on the network from their computers without proper user logon authentication access security in place.

f) Users must not make any unauthorised copies of or modifications to the contents of any WCG information resources.

g) Users must handle all information resources in a secure manner.

h) Users must ensure that information under their control is backed up in line with the criticality of the information to WCG.

6. PRIVACY GUIDELINES

a) The WCG maintains the right to monitor and review e-mail and Internet activity to ensure compliance with this policy, as well as to fulfilling the WCG's responsibilities in terms of legislation. Users have no expectation of privacy.

b) On termination or separation from the WCG, access will be denied to e-mail and WCG Internet, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.

c) Officials who leave the WCG will have their mailbox disabled immediately after exiting the organisation.

d) The WCG reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received. Intercepting, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated WCG Officials.

e) The WCG reserves the right to alter, re-route or block the delivery of e-mail messages as appropriate. This includes but is not limited to:

   i. Rejecting, quarantining or removing attachments and/or malicious code from messages that may pose a threat to WCG resources.

   ii. Discarding attachments, such as music, that are considered to be of little business value and involve a significant resource cost.

iii. Rejecting or quarantining messages with suspicious content.

iv. Rejecting or quarantining messages containing offensive language.

v. Re-routing messages with suspicious content to designated WCG employees for manual review.

vi. Appending legal disclaimers to messages.

f) Electronic messages are permissible as evidence in a court of law.

g) Any content created with the e-mail system is considered the intellectual property of the WCG.

7. BREACH

Where a breach or a disregard of this policy has occurred, appropriate disciplinary action will be taken in line with the relevant WCG policies.

8. EXEMPTIONS

The Chief Information Officer within the Centre for e-Innovation has the sole right to exempt a person from this policy. The exemption will not be valid unless:

(a) It is in writing;

(b) It is signed and dated by the Chief Information Officer;

(c) The Internal Audit Department is notified of the exemption; and

(d) A record is kept of the exemption.

9. POLICY EFFECTIVE DATE

The policy will be effective on the date on which it is signed by the relevant authority.

10. QUERIES

Queries and questions on this policy should be addressed to:

- Policy and Strategy Directorate – Centre for e-Innovation email: ICTpolicy@westerncape.gov.za
- Employees not satisfied with the application of this policy must follow the Grievance Procedure and/or Dispute Resolution Procedure.
- This policy must, upon request, be made available to employees in any of the eleven (11) official languages, sign language and Braille.
- This policy must be reviewed as and when the need arises.
- Policy and Strategy Directorate must monitor the implementation and evaluate the impact of this policy.

12. Appendix – Definition of Terms

Access control: A system to restrict the activities of users and processes based on the need-to-know.

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation; generally used to refer to the process for performing encryption.

Badge reader: A device which reads badges and interconnects with a physical access control system.

Booting: The process of initialising a computer system from a turned-off state.

Bridge: A device which interconnects networks or that otherwise allows networking circuits to be connected.

Cipher lock: A device that requires the entry of passwords at doors and which provides physical access control over a room or building.

Closed Area: An area in which sensitive information is being processed and openly stored. The area is not normally occupied 24 hours a day and therefore, due to the sensitive information stored there, requires physical access controls and alarms.

Company Property: Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of WCG and are not the property of users of the electronic communications services.

Confidential information: A designation for information, the disclosure of which is expected to damage WCG or its business affiliates.

Critical information: Any information essential to WCG business activities, the destruction, modification, or unavailability of which would cause serious disruption to WCG business.

Cryptographic challenge/response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then, transformed using an encryption process and a response is returned to the connected computer system.

Data Security Classification: The reference to "sensitive" data refers to the classification of WCG data into two basic categories:

WCG Proprietary is information pertaining to business operations, new products, techniques, proposals or related information which, if compromised, would seriously impair WCG operations.

WCG Private is information pertaining to business operations or individuals, and is of such importance to the WCG, or is so personal in nature, that indiscriminate release would have adverse effects on the WCG or the employee involved. Privileged employee information such as salaries and personnel records such as change requests is typical of WCG Private.

Default file permission: Access control file privileges (read, write, execute, etc.) granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password issued when a new user-ID is issued, or an initial password provided by a computer vendor when hardware/software is first delivered.

Downloading: The transfer of data from a host computer (mainframe, minicomputer, network server, etc.) system to a connected workstation, such as a personal computer.

Dynamic password: A password which changes each time a user logs-into a computer system.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time-stamping, and other security objectives.

End-user: A user who employs computers to support business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process achieved by user-IDs and fixed passwords (see hand-held tokens and dynamic passwords).

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security check (such as providing a password).

Gateway: A computer system used to link networks which can restrict the flow of information and which employs some access control method.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the timeframes that these types of information must be kept.

Isolated computer: A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.

Log-in banner: The initial message presented to a user when he or she first makes connection with a computer.

Log-in script: A set of stored commands which can log a user into a computer automatically.

Master copies of software: Copies of software which are retained in an archive and which are not used for normal business activities.

Microcomputer: A general purpose or portable (including laptop) computer consisting of one or more microprocessors assembled in a unit that will fit on top of a desk. The unit typically consists of a central processing unit (CPU), video display, keyboard, disk drive, and a number of peripheral devices such as a printer and CD-ROM drive. The terms "microcomputer" and "personal computer" (PC) are considered synonymous and may be used interchangeably in this document.

Multi-user computer system: Any computer which can support more than one user simultaneously.

Password guessing attack: A computerised or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorised access.

Password reset: The assignment of another (temporary) password when a user forgets or loses his/her password.

Password-based access control: Software which relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorised ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user-ID: A user-ID which has been granted the ability to perform special activities, such as shut down a multi-user system.

Restricted Area: An area in which sensitive information is being processed or worked and therefore requires physical access controls.

Restricted information: Particularly sensitive information, the disclosure of which is expected to severely damage WCG or its business affiliates (see confidential information).

Router: A device that interconnects networks using different layers of the Open Systems Interconnection (OSI) Reference Model.

Screen saver: A computer program that automatically blanks the screen of a computer monitor, CRT, LCD, Plasma after a certain period of no activity.

Hand-held token: A commercial dynamic password system which employs a smart card to generate one-time passwords that is different for each session.

Security patch: A software program used to remedy a security or other problem (commonly applied to operating systems).

Sensitive information: Any information, the disclosure of which could damage WCG or its business associates. Any data labelled as WCG secret or WCG top secret.

Shared password: A password known by and/or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges allowing the involved user or process to perform activities which are not normally granted to other users.

Suspending a user-ID: The process of revoking the privileges associated with a user-ID.

Systems administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Terminal function keys: Special keys on a keyboard that can be defined to perform certain activities such as save a file.

Uploading: The transfer of data from a connected device, such as a personal computer, to a host system (mainframe, minicomputer, server, etc.).

User-IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Parliament or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus: A parasitic software program, equipped with the means of reproducing itself, that spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making copies of it.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.