DCSR POLICY: ACCEPTABLE COMPUTER USE PASSWORD POLICY

DOCUMENT INFORMATION AND LOG

Document name	**Acceptable Computer Use and Password Policy**
Version	**1.0**
Approval Date	**March 2025**
Review date	**2027/2028**

TABLE OF CONTENTS

RELATED DOCUMENTS

Culture, Sport and Recreation Information Security Policy;

Culture, Sport and Recreation User-Id and Password Policy;

Circular: Internet and Electronic Mail Abuse in Government;

SSA's Minimum Information Security Standards (MISS).

Web Content Filtering Procedure

MPG Email Standards

POPIA Policy

Corporate Governance of ICT Policy Framework version 2

ACCEPTABLE COMPUTER USE POLICY

1. Policy Purpose

This policy defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the Culture, Sport and Recreation Information Technology resources and proprietary information, which is necessary to ensure Confidentiality, Availability and Integrity of the systems, applications, assets and information.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, persons holding learnerships with the Culture, Sport and Recreation and other workers at The Culture, Sport and Recreation, including all personnel affiliated with third parties. This policy applies to all computer equipment that is owned, rented or leased by the Culture, Sport and Recreation.

3. Definitions

A breach of security – is where an organisational policy or legal requirement regarding information security has been contravened.

Encryption – the process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission or other security purposes.

News Group – are a group of like-minded users who ask questions and swap information amongst themselves.

PC Equipment/ Computer Equipment – includes desktop computers, laptops, printers, fax machines and any other item that is connected to the Mpumalanga Provincial Government (Culture, Sport and Recreation)'s systems and/or networks.

Portable Computer / Laptop / Notebook/ Netbook – has become a generic expression for all movable computers.

User-ID / Account – is a name, number, set of initials, etc., which, combined with a password, uniquely identifies, a person authorised to use a system.

Spam – Computer Spam is the electronic equivalent of Junk mail.

Virus / Trojan Horse/ Worm or email bomb – is a form of potentially disruptive, dangerous computer program.

H-Drive – an external drive created on the user's PC for backup critical documents. This drive is only available when the official is connected to the Culture, Sport and Recreation Local network and PC is joined to the domain.

4. Responsibility

The Head: Culture, Sport and Recreation will be responsible for the Culture, Sport and Recreation's overall Acceptable Computer Use Policy. The Mpumalanga Provincial Treasury's IT Bureau will assist the Culture, Sport and Recreation to make affected users aware of this policy.

The Information Technology's infrastructure and policies will be managed and controlled by ITB.

5. Inputs and Outputs Policy Amendments

Any policy changes will be discussed between the Culture, Sport and Recreation and Mpumalanga Provincial Treasury's IT Bureau. The policy outputs and changes will be added to the policy document for review. The policy outputs will be signed-off between the Culture, Sport and Recreation and Mpumalanga Provincial Treasury's IT Bureau through the exisitng MOU.

6. Publishing the Policy

The policy shall be made available and accessible to all employees through awareness sessions, intranet, website, and manuals/hard copies.

7. Monitoring

All messages distributed via the Culture, Sport and Recreation IT infrastructure are the property of the Culture, Sport and Recreation and The Culture, Sport and Recreation maintains the right to monitor and review e-mail and Internet activity to ensure compliance with this policy.

No Culture, Sport and Recreation employees shall have the expectation of privacy in anything they store, send or receive on the Culture, Sport and Recreation email system or on the IT Infrastructure. The Culture, Sport and Recreation may monitor messages without prior notice or approval. On termination or separation from the Culture, Sport and Recreation, access will be denied to e-mail and Internet, the email address will be terminated.

8. Policy Violations

Any transgression of this policy shall be handled in accordance with Public Service Disciplinary procedures and or other relevant Labor Legislation.

9. Policy Statements

9.1 General Use and Ownership

9.1.1 While the Culture, Sport and Recreation's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on Provincial networks, systems and Applications remains the property of the Culture, Sport and Recreation. Because of the need to protect the Culture, Sport and Recreation's network, management cannot guarantee the confidentiality of information stored on any network or stand-alone device belonging to the Culture, Sport and Recreation.

9.1.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual sections are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet. In the absence of such policies, employees should be guided by The Culture, Sport and Recreation policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

9.1.3 All sensitive or vulnerable Information/ data shall be encrypted.

9.1.4 JFor security and network maintenance purposes, authorised individuals within the Culture, Sport and Recreation may monitor equipment, systems and network traffic at any time. The Culture, Sport and Recreation reserves the right to audit networks and systems on a periodic basis to comply with this policy.

9.2 Security and Proprietary Information

All computers issued by the Culture, Sport and Recreation should be joined to the ITB.local domain this enables the computer to be monitored and enabling password expiration, creation of the H-Drive for the user and regular update of security patches.

9.2.1 It is the employee's responsibility to protect all of the passwords and pass phrases assigned to them. They should not share these with any other person.

9.2.2 An excuse of unawareness of a security policy will not be acceptable.

9.2.3 A password should be changed as per the Culture, Sport and Recreation password policy.

9.2.4 All desktop computers and laptops shall be secured with a password protected screensaver which should activate after a period of no longer than 10 minutes or less, or by logging-off (Control > Alt > Delete for Windows users) when the host desktop/laptop/device will be unattended.

9.2.5 Postings by employees from the Culture, Sport and Recreation-mail address to newsgroups, chatrooms, opinion columns, comments on news sites, ALL social media etc., should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Culture, Sport and Recreation, unless posting is in the course of the performance of official functions or duties.

9.2.6 All computers used by the employee that are connected to the Culture, Sport and Recreation internet/ Intranet/ Extranet, whether owned by the employee or the Culture, Sport and Recreation, shall be continually executing approved virus-scanning software.

9.2.7 Employees shall use extreme caution when opening e-mail attachments received from unknown senders as these may contain viruses.

9.2.8 No user is allowed to change the standard configuration on their allocated desktops/laptops as per departmental desktop/laptop standard.

9.2.9 Employees shall properly monitor and manage their local and network storage space assigned to them.

9.2.10 In an effort to protect the Culture, Sport and Recreation Information Technology systems and minimize security risks, all files stored on external/ removable storage devices (e.g. Flash drives, CD's, DVD's, stiffy drives, external hard drives, etc.) shall be scanned by the approved anti-virus software once the user attempts to access any of those files. The Culture, Sport and Recreation reserves the right to automate and enforce this rule.

9.2.11 Though IT systems will be set to run Anti-virus automatically on all storage drives, users are still responsible for scanning all storage devices such as hard drive, memory sticks, etc.

9.2.12 Users must ensure that information under their control is backed up on the OneDrive in line with the criticality of the information to the Culture, Sport and Recreation. All user must ensure that the OneDrive is activayed to enable the auto backup.

9.3 Unacceptable Use

The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibility (e.g. systems administrations staff may have a need to disable the network access of a host if that host is disrupting production services). The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use:

9.3.1 Under no circumstances is an employee of the Culture, Sport and Recreation authorised to engage in any activity that is illegal under local, government or international law while utilizing the Culture, Sport and Recreation owned IT resources.

9.4 System and Network Activities

9.4.1 The following activities are strictly prohibited, with no exceptions: Violations of the rights of any person or company protected by copyright, trade secrets, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Culture, Sport and Recreation.

9.4.2 Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Culture, Sport and Recreation or the end user does not have an active license, is strictly prohibited.

9.4.3 Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

9.4.4 Security breaches or disruptions of network communication - Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties fall within the scope of regular duties.

9.3.2 Under no circumstances is an employee of the Culture, Sport and Recreation authorised to engage in any activity that is illegal under local, government or international law while utilizing the Culture, Sport and Recreation owned IT resources.

9.5. System and Network Activities

9.5.1 The following activities are strictly prohibited, with no exceptions: Violations of the rights of any person or company protected by copyright, trade secrets, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Culture, Sport and Recreation.

9.5.2 Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Culture, Sport and Recreation or the end user does not have an active license, is strictly prohibited.

9.4.4 Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

9.5.4 Security breaches or disruptions of network communication - Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties fall within the scope of regular duties.

9.5.5 Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal duty.

9.5.6 Circumventing user authentication or security of any host, network, or account.

9.5.7 Using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

9.5.8 Providing information about, or lists of, the Culture, Sport and Recreation employees to parties outside the Culture, Sport and Recreation.

9.6. E-mail and Communications Activities

9.5.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail Spam).

9.5.2 Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

9.5.3 Creating or forwarding 'chain letters or other 'pyramid' schemes of any type.

9.5.4 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup Spam).

9.5.5 All new mailboxes are created with a 250MB space limit. All users are required to manage their emails and delete emails that are no longer required. If this mailbox quota is not sufficient, users have the following options:

a. Move items to the mailbox archive.

b. Users must first clean up their mailboxes before requesting their current online mailbox size quota to be increased.

9.5.6 Culture, Sport and Recreation reserves the right to retain on backup storage users' mailbox items.

9.6 Internet

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

9.6.1 Acceptable Uses of the Internet include:

9.6.1.1 Accessing web-based business applications and tools.

9.6.1.2 Communication between Officials and non-Officials for business purposes.

9.6.1.3 Review of possible vendor web sites for product information.

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

9.6.1.5 Accessing of Government web sites and portals.

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

9.6.2 Unacceptable Uses of Internet

9.6.2.1 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.

9.6.2.2 The Culture, Sport and Recreation also prohibits engaging in fraudulent activities, or knowingly disseminating defamatory materials.

9.6.2.1. 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 Culture, Sport and Recreation 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 Culture, Sport and Recreation's Web sites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the Culture, Sport and Recreation.

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.

e. Officials must accept that all materials on the Internet are copyrighted and/or patented unless specific notices expressly state otherwise.

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

g. Any form of on-line gambling and gaming.

h. Using the internet for any purpose or in any manner that may prejudice the rights or interests of the Culture, Sport and Recreation or government in any other sphere.

10 Policy Review

This Policy shall be reviewed every three (3) years or whenever the need for a policy review arises.

11 Policy Approval Sign-Off (DG)

The Head of the Culture, Sport and Recreation takes overall accountability of the Acceptable Computer Use Policy.

12. Document Approval

This document has been endorsed and approved for use by:

MR EM MAHLANGU
(A) HEAD: CULTURE, SPORT AND RECREATION
DATE : 07/11/2025