acsr
Department:
Arts, Culture, Sports and Recreation
North West Provincial Government
Republic of South Africa

A : 2ND Floor Gaabomotho Building
760 Dr. James Moroka Drive
P/A: Private Bag X90, Mmabatho 2735

HEAD OF DEPARTMENT

T : +27(0)18 388 2751
E: mkolojane@nwpg.gov.za

POLICY TITLE : INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY POLICY

POLICY NUMBER : 21/2017 (4TH VERSION)

DATE APPROVED : 08 MARCH 2021

REVIEW DATE : FEBRUARY 2024

TABLE OF CONTENTS

SUBJECT	PAGE
1. **ABBREVIATIONS & ACRONYMNS**	3
2. **DEFINITION OF CONCEPTS**	3-5
3. **PREAMBLE**	5
4. **SCOPE OF APPLICATION**	5-6
5. **POLICY STATEMENT**	6
6. **OBJECTIVE**	6
7. **POLICY FRAMEWORK**	6
8. **POLICY PRINCIPLES**	7
9. **POLICY CONTENT**	7
9.1 Acceptable use	7-8
9.2 ICT Risk Management	9
9.3 Physical and Environmental Security Management	9-11
9.4 Security organisation and classification	11-13
9.5 ICT Infrastructure protection	13-14
9.6 Internet and Email Security	15-18
9.7 Information Systems Acquisitions, Development & Maintenance	18
9.8 Access Control of Information Systems	18-20
9.9 ICT Service Continuity Management	20-21
10. **ROLE AND RESPONSIBILITIES**	21
10.1 Head of Department	21
10.2 Departmental Management	21
10.3 Departmental Information Technology Officer	21-22
10.4 Risk Management unit	22
10.5 MISS Manager	22
10.6 Asset Management unit	23
10.7 Provincial ICT Security Committee	23
10.8 End users	23
11. **NON-COMPLIANCE**	23
12. **FINANCIAL IMPLICATIONS**	23
13. **POLICY REVIEW**	24
13.1 Version control	24
14. **APPROVAL AND COMMENCEMENT**	24

1 ACRONYMS AND ABBREVIATIONS

ACSR: Arts, Culture, Sports & Recreation

DITO: Departmental Information Technology Officer

DPSA: The National Department of Public Service & Administration

GITO: Government Information Technology Office/r

HOD: Head of the Department

ICT: Information & Communication Technologies

IT: Information Technology

MISS: Minimum Information Security Standards

NWPG : North West Provincial Government

OTP: Office of the Premier

2 DEFINITION OF CONCEPTS

Asset: Anything that has value to the organisation, whether physical or information.

Authentication: To verify the identity of a subject requesting the use of a system and/ or access to network resources.

Authorisation: Granting access to an object after the subject has been properly identified and authenticated.

Availability: Guaranteeing that data is protected from loss and ensuring that it is available to authorised users whenever and wherever required.

Central IT: Office of the Premier: Information Technology Chief Directorate

Compromise: The unauthorised disclosure/ exposure or loss of sensitive or classified information, or exposure of sensitive operations, people or places, whether by design or through negligence

Computer: Desktop/ Laptop/ Notebook / Tablet

Computer system: Computer hardware (e.g. mainframe, minicomputer, file server, workstation, laptop; Computer software (e.g. operating system, applications); and Data processed and/ or stored (e.g. on hard disk, tape, CD-ROM)

Confidentiality: A security principle that works to ensure that information is not disclosed

Control: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal nature. NOTE: Control is also used as a synonym for safeguard or countermeasure

Data: Refers to all information that can be electronically processed, transmitted and stored. Data may be processed in internal main memories, stored on tapes or disks, and transmitted by networks.

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

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

IDs and passwords: IDs, also known as accounts are character strings that uniquely identify computer users or processes. Passwords authenticate that user or process.

Incident: An adverse event in an information system, and/or network, or the threat of the occurrence of such an event.

Information Security: The provision of organisational, technical and social measures to safeguard information assets against unauthorised access, damage and interference - both malicious and accidental.

ICT security: Entails the creation of a condition to protect computer hardware, software and data against incidental and/or deliberate unauthorised changes, destruction, disposal, removal and/or disclosure.

Information system security: is characterized in this Policy and standards as the preservation of:

- **Confidentiality**: ensuring that information and associated assets are accessible only to those authorized to have access;
- **Integrity**: safeguarding the accuracy and completeness of information and;
- **Availability**: ensuring that authorised users have access to information and associated assets when required. In securing Government's information, it is essential that the above characteristics be maintained at all times.

ICT unit: The Departmental unit responsible for rendering of ICT related services

Mobile device: Laptop/ tablet/ mobile phone

Network: Data communications system that interconnects computer systems and communication enabled devices

Peripheral: Printer/ Scanner/ Projector

Removable media: Devices which can be used to easily move data between computers. Removable media includes, but is not limited to compact disks (CDs), digital versatile disks (DVDs), flash memory cards (commonly used in digital cameras or cellular phones) and hot swappable or hot-pluggable external storage devices connected to usb or FireWire interfaces.

Risk: Combination of the probability of an event and its consequence.

Screen Saver: A computer program that automatically blanks and/ or locks the screen of a computer monitor or terminal after a certain period of inactivity.

Sensitive Information (Data): Information (Data) with classification levels of "Restricted" or "Strictly Confidential" is considered to be sensitive and should be protected accordingly.

Spam: irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

Telephone pin code : The code assigned to authenticate users when making outgoing telephone calls.

User: An employee utilizing ICT equipment

Virus, Worms and Trojan: Malicious software designed to produce itself and automatically spread to other computers or networks by attaching to or infecting other software. They can be transmitted via email attachments, by downloading infected programs from the internet sites, or can be present on a removable media. They can be real hoax, some can damage a computer as soon as their code is executed, and others can lie dormant until circumstances cause their code to be executed by the computer.

3 PREAMBLE

3.1 The Department acknowledges the importance of Information and Communication Technology (ICT) and therefore it needs to ensure that appropriate security measures are in place for all departmental ICT resources.

4 SCOPE OF APPLICATION

4.1 This Policy applies to all ACSR employees including temporary staff, interns, independent contractors and consultants.

4.2 It covers departmental servers, desktop computers, notebooks as well as any other departmental devices used to process or facilitate processing of government data.

5 POLICY STATEMENT

5.1 Information is the backbone to the achievement of business objectives and government service delivery. Government Information Technology resources are business critical assets requiring a high level of protection.

5.2 Sufficient measures, commensurate with risk, shall be taken to protect these assets against accidental or deliberate unauthorized modifications, disclosure and/ or destruction, as well as to ensure the confidentiality, integrity and availability of ACSR information resources.

6 POLICY OBJECTIVE

6.1 The broad objective is to provide the ACSR officials with ICT Security Procedures and Standards for application of effective and consistent level of security.

7 POLICY FRAMEWORK

7.1 This Policy document shall be read and applied in the context of the provisions of the following Departmental, Provincial, National and International Acts, Regulations and Guidelines:

- Constitution of the Republic of South Africa, 1996 (Act no. 106 of 1996)
- International Standard ISO/IEC 27001: 2013
- ACSR Security Policy
- ACSR procurement of IT equipment Policy
- ACSR Asset Management Policy
- ACSR Risk Management Policy
- ACSR Due Care Agreement form
- NWPG Internet and electronic-mail use Guidelines
- DPSA Corporate Governance of ICT Policy Framework, 2012
- DPSA ICT Security Policy for Public Service
- DPSA ICT Security Guideline, 2017
- State Information Technology Agency Act, 1998 (Act no. 88 of 1998)
- Minimum Information Security Standards (MISS) of 1996
- Electronic Communications and Transactions (ECT) Act No. 36 of 2005
- National Treasury Risk Management Framework

8 POLICY PRINCIPLES

8.1 Government resources are for government work – It is important for all departmental staff to remember that inappropriate conduct in the use of Information Technology and other forms of electronic communication can lead to risk for the Department. Do not utilize departmental resources for personal, commercial, fundraising, lobbying, political or other inappropriate activities.

8.2 Respect the rights of others – Do not use government systems or facilities in a way that is offensive to fellow employees or to the public, such as creating, copying or transmitting hate speech or material that is offensive in the way it addresses issues of race, creed, religion, gender, disability, age or copy materials that are sexually explicit or sexually oriented or that are related to gambling, illegal weapons, terrorist activities or for any other offensive activities.

8.3 Protect the property of Government – It is the responsibility of all ACSR staff to take all reasonable steps to protect government equipment and information and data they contain. Do not engage in any personal use of government information systems that endanger the confidentiality of government information.

8.4 Do not harm – Do not engage in non-business communications that reduce the efficiency of the network, place unapproved software on government computers, and make configuration changes that circumvent security settings or distribute information that inappropriately discloses confidential or proprietary information.

9 POLICY CONTENT

The following are the sections that cover various aspects of the Departmental ICT Security Policy:

9.1 ACCEPTABLE USE

Reference to ISO/IEC 27001:2013	Section 7, A.7 and A.8
Purpose	This Acceptable Usage Policy shall be deemed to have been accepted by the User (being the individual) on commencement of the employment relationship. This Policy is to ensure that the target audience have adequate knowledge on appropriate behaviour towards ACSR information assets.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.1.1 Disciplinary offences	9.1.1.1 Government adopts a zero tolerance stance and therefore failure to comply with this Policy or any of the supporting and complementing policies, standards and / or processes will be viewed as negligence and could result in a security violation. Appropriate disciplinary action may be

	taken thereafter. 9.1.1.2 Workstations may be regularly audited to confirm compliance to the acceptable use of the equipment. Should inappropriate content or use be identified, disciplinary action may be taken in accordance with ACSR official disciplinary procedures. 9.1.1.3 The following occurrences are strictly prohibited and will constitute a disciplinary offence: a) Unauthorised removal or tampering of peripheral equipment i.e. hard drives, CD ROM drives, RAM modules, monitors, processors, cables, keyboards, mouse units, network cards etc. from any hardware will be construed as destruction of ACSR property. b) Deliberate removal of any manufacturer, supplier or ACSR identifying Asset tags or serial number stickers located on all equipment will also be construed as destruction of government property. c) Unauthorised removal of equipment between Departments, building locations or even between workstations and people that have not been logged through the Asset formal removal process. d) Removal of equipment to any location outside of any ACSR premises in any District without the required documentation being presented to Security officers and duly authorised by the relevant officers. e) Setting up and upgrading of equipment if it has not been requested as part of a Project, or has not been logged through ICT unit for the qualified personnel to implement. f) Installation of unauthorised/ illegal software on IT equipment without the permission or authorisation from the ICT unit. This includes but is not limited to installation of games, modifying parameters of any application, operating system or any settings whatsoever, installing personal non-work related software or data, making backups or copies of any ACSR software or data whatsoever for any non-Government purpose.
Related Policies/ Procedures	ACSR Asset Management Policy, ACSR Security Policy, DPSA ICT Security Guideline

9.2 ICT Risk Management

Reference to ISO/IEC 27001:2013	Section 8.2 and 8.3
Purpose	The protection of the institution's information is risk based. Achieving secure information requires the management of risk and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the institution. This policy aims to institutionalize appropriate ICT security risk management practice within the Department.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.2.1 ICT Risk management	9.2.1.1. The Department shall ensure that the ICT risks are managed within the Departmental risk management practice in accordance with the enterprise risk management strategy and other relevant prescripts. 9.2.1.2 Risk assessments of ICT security should identify, quantify, and prioritise risks against criteria for risk acceptance and objectives relevant to the institution. The results should determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.
Related Policies/ Procedures	ACSR Risk Management Policy/ Risk Management Strategy and Implementation Plan

9.3. Physical and Environmental Security Management

Reference to ISO/IEC 27001:2013	Section A.8, A.11
Purpose	The Policy aims to ensure that only authorized individuals are allowed access to Departmental information and information processing facilities.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.3.1 IT Equipment Security	9.3.1.1 Responsibility for an IT asset starts on physical receipt of that asset by the user. 9.3.1.2 IT equipment should be used in a secure manner in order to prevent loss, damage, theft or compromise of assets and interruption to the

	Departmental operations. 9.3.1.3 IT equipment should be correctly maintained to ensure its continued availability and integrity. 9.3.1.4 Security should be applied to assets outside the Departmental premises. 9.3.1.5 Where a user wishes to temporarily remove IT equipment from any Departmental building (with exception to users who have been allocated laptop computers) procedure to remove assets from office need to be adhered to as stipulated in the ACSR Asset Management Policy. 9.3.1.6 To minimize the risk of theft, destruction, and/ or misuse, personnel must exercise sound judgement and ensure that their computers and associated peripheral devices are adequately protected. To this end: -. a) In case of a laptop computer, the user must adhere to the *Due care agreement in respect of use of computer* by ensuring that the supplied security cable is attached to the computer and secured to a desk or similar object at all times. Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises. b) In the case of a desktop, laptop computer and peripherals, where possible, the user must ensure that the office in which the desktop computer is resident is adequately secured at the close of business, or while equipment is unattended. 9.3.1.7 Areas that contain sensitive or critical information and information processing facilities should be protected by appropriate entry controls to ensure only authorised access. 9.3.1.8 Officials that have terminated their employment with ACSR, their IT equipment shall be handed over to Asset Management for allocation to the new incumbent. 9.3.1.9 Theft and Losses of IT asset should be reported to the SCM/ Asset Manager who will ensure that all relevant procedures are adhered to.
9.3.2 Clear Desk Policy	9.3.2.1 All information and storage media containing Government confidential, sensitive or non-public information must be stored in a physically secure manner when not in use. Such storage media will need to be encrypted with relevant tools by the ICT unit. 9.3.2.2 Sensitive or restricted documents must be cleared from printers immediately after been printed. 9.3.2.3 Printers used to print sensitive information must not be located in the open unless they have a security mechanism that allow the printing individual to physically provide password/ pin code before printing.

9.3.3 Disposal	9.3.3.1 Users must adhere to the disposal procedure as captured on the *Departmental Asset Management Policy* when disposing the IT equipment. 9.3.3.2 Disposal of sensitive or restricted hard copy documents must be performed by utilizing shredders in line with the relevant regulations.
Related Policies/ Procedures	ACSR Security Policy Due care agreement in respect of use of computer Departmental Asset Management Policy

9.4. Security organisation and classification

Reference to ISO/IEC 27001:2013	Section A.8.2
Purpose	The Policy aims to ensure that all intellectual property rights, privacy rights and confidentiality rights are adequately protected within ACSR by all its users.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.4.1 Intellectual Property Rights	9.4.1.1 Any computer software developed by the ACSR personnel through the use of Government computer resources within the scope of employment with ACSR whether within or outside normal working hours, remains the intellectual property of ACSR and may therefore not be sold, leased or removed without the express written consent of ACSR. 9.4.1.2 All software on ACSR computers is protected by copyright laws, commercial software purchased by the ACSR is authorised for ACSR use only and must be utilized in accordance with contractual agreements and copyright laws, unless specifically authorised within the license agreement, making copies of copyrighted software and related documentation for personal use is illegal and therefore prohibited. ICT unit will conduct regular audit and if detected, unauthorised software will be removed and the responsible person will be subject to disciplinary action. 9.4.1.3 Software used by ACSR employees must only be installed by the ICT unit. Incidental installation of software by employees will be permissible only if it is authorised legal software and makes business sense e.g. installation of software for USB modem. 9.4.1.4 Users are prohibited from granting access to ACSR software for distribution to independent contractors, clients or any third party.
9.4.2 Data Privacy and protection	9.4.2.1 ACSR users provide their consent to allow personnel designated by the ICT unit to access, monitor or process any information that the user has created, stored, sent or received on ACSR information systems. Users are

	therefore made aware that ACSR may, from time to time use human or automated means to monitor and trace the use of its computer resources. 9.4.2.2 Should it be suspected that any user has transgressed any principle contained in the ICT Security Policy, ACSR reserves the right to access all documents and/ files on any computer to establish whether a Policy has been transgressed. 9.4.2.3 With regard to data privacy and protection, the following laws are to be taken into account: a. Promotion of Access to Information Act (PROATIA) Business secrecy laws prohibit any form of disclosure to, or use of certain business information by a third party (e.g. information concerning business activities, strategic planning, etc.) b. Regulation of Interception of Communication and Provision of Communication Related Information Act (RICA) Business monitoring and interception of communication can only occur in accordance with the requirements defined in the act. c. Protection of Personal Information Bill (POPIA)/ Data Protection Principles. Data protection principles prohibit the disclosure or use of personal data of an individual without prior consent of that individual (e.g. name and address, profession, financial statements, personal profiles, etc.).
9.4.3 Data Confidentiality	9.4.3.1 Not all the information requires the same level of protection as only some information is sensitive or confidential. Information should therefore be classified and labelled by its owners according to the security protection needed and handled accordingly. 9.4.3.2 MISS Manager should assist by developing a system that will necessitate the Department to identify, categorise and classify different type of information. 9.4.3.3 The identified information owner should be held accountable for the security of the information. 9.4.3.4 All employees, contractors and consultants of ACSR who require access to classified information and critical assets in order to perform their duties must be subjected to a security screening investigation/ process.
9.4.4 Protection of Customer/ Client data	9.4.4.1 Private customer/ client data held on Government information systems must only be used for the purposes originally agreed upon with that customer. To use this information in any other manner will require approval from the customer and authorization from the line manager.

	9.4.4.2 Users are responsible for safeguarding customer data within the scope of their control. Users should not disclose any customer data to any third party without the management consent.
Related Policies/ Procedures	Departmental Security Policy Protection of Information Act, 1982 (Act no 84 of 1982) Promotion of Access to Information Act, 2000 (Act no 2 of 2000)

9.5. ICT Infrastructure protection

Reference to ISO/IEC 27001:2013	Section A.6.2, A.8.1, A.8.3, A.12.2, A.15
Purpose	This Policy aims to ensure that users are aware of their responsibility towards virus management in order to protect and preserve the integrity, availability and confidentiality of the ICT infrastructure. Additionally the Policy outlines what information security monitoring regulations for users and lastly requirements for removable computer media, for example Cell phones, removable storage, etc.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.5.1 Virus and Malware Management	9.5.1.1 The Department is reliant on the network provided by Office of the Premier: GITO. This office is responsible for securing the information systems/ internet and emails that are accessed by the departmental officials through the NWPG network. 9.5.1.2 Departmental ICT unit to ensure that detection, prevention and recovery controls to protect against viruses and malware are implemented. This will be done by installation of an authorised antivirus toolkit on all the networked computers and correct setting up of other necessary security requirements like personal firewalls and systems updates. 9.5.1.3 Departmental ICT unit will ensure that computers that are in use are running on the Operating systems that are secured and receiving regular updates. Should the Operating system (O/S) reach end of life, processes will be undertaken to either have the systems upgraded or replaced if they do not meet the minimum requirements for the later O/S. 9.5.1.4 No employee may knowingly distribute viruses or bypass any detection systems in place. 9.5.1.5 Individuals receiving data media, from any source within or outside the ACSR have the responsibility for ensuring that it is checked for viruses before

	use. Similarly, individuals intending to pass on data media within ACSR or to external third parties must ensure that it is first checked for viruses. 9.5.1.6 Through limited access rights, end users shall be prevented from disabling or changing the configuration of the antivirus software installed on their computers. 9.5.1.7 New software, portable media, and information in electronic format from external sources, shall be scanned for malicious program code, before introduction into the NWPG network.
9.5.2 Management of Removable Computer Media	9.5.2.1 Users must ensure that they keep removable computer media secure. Removal media housing ACSR data should not be left unattended and should not be shared with individuals not authorised to access the information contained thereon. 9.5.2.2 Any loss or theft of removable computer media must be treated as a security breach and reported immediately in accordance to the ACSR *Asset Management Policy*. 9.5.2.3 Removable media should only be used as a temporary data store, for a minimum possible duration and should not replace long-term storage. Business related information stored on removable media such as USB flash drives and memory cards should be cleared as soon as it is not essential to keep the information of the removable medium. 9.5.2.4 Removable computer media must always be safely removed from the computer to avoid damage. 9.5.2.5 Sensitive Government information should not be stored on removable media (i.e. CDs, DVDs, USB drives, external hard drives) unless it is adequately protected by encryption. Users must consider the risks to confidentiality of the device being stolen or read prior to putting any information on the device.
9.5.3 Third Party Access Management	9.5.3.1 The third party are all external parties that may access, process, store, communicate, or provide ICT infrastructure components for ACSR. 9.5.3.2 Information security requirements for mitigating risks associated with the third party's access to the institution's assets should be agreed with the third party and documented.
Related Policies/ Procedures	ACSR Security Policy NWPG Internet and Electronic-mail Guidelines DPSA ICT Security Guideline Memorandum of Agreement between OTP and ACSR

9.6 Internet and Email Security

Reference to ISO/IEC 27001:2013	Section 10.8
Purpose	To ensure the confidentiality and integrity of electronic mail (e-mail) messages is protected in transit, the risk of e-mail misuse is minimised and that e-mail services are available when required, making it an effective communication tool. In addition to ensure appropriate use of Internet and minimize the threat posed by the internet to Government' networks. Its main aim is to set out the guidelines, which need to be followed when making use of internet and e-mail services.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.6.1 Prohibitions	9.6.1.1 Staff members are prohibited from using the internet and emails to access or transmit prohibited material (sexually explicit, racist or discriminating information /images which may be offensive, gambling, making obscene, or harassing statements which may be illegal or downloading illegal material, if circumstances arise whereby the transition of such material is required, documented authorisation from line Management is required prior to such publication or transmission.
9.6.2 Internet Usage	9.6.2.1 Access to the internet is granted to employees based on their employment requirements, and is not to be abused. Users should be aware that tracking of sites visited occurs. Access is furthermore denied to various offensive sites. 9.6.2.2 Only Government approved versions of internet browsers are to be used with necessary cumulative updates or the applicable versions at the time. Users are prohibited from changing any configuration properties of their web browsers. 9.6.2.3 Only ICT unit officials are allowed to change web browser configurations. 9.6.2.4 Users may not browse the Internet for non-business purposes during working hours unless where it makes business sense, for example paying personal accounts via online banking, rather than taking time off from work in order to physically visit a bank or a store for the same reason. 9.6.2.5 While accessing the internet resources from Government systems, users may not deliberately visit, view, install, download, print or disseminate any prohibited material from any website. Users may also not attempt to probe other systems for security weaknesses, compromise other systems, possess or transfer data illegally or send offensive or abusive messages.

9.6.3 Email usage	9.6.3.1 The email system must be used primarily for legitimate business purposes in the course of assigned duties. Incidental and occasional limited personal use of the email system is permitted, providing at all times that such use does not: a) Interfere with the user's work or performance. b) Interfere with any other user's work or performance. c) Cause disruptions to the operations or resources of ACSR Information system resources. d) Violate any other provision of this Policy or any other applicable Policy of Government. 9.6.3.2 The ACSR regards email as a private communication between sender and recipient(s) and must make a reasonable effort to respect and protect this privacy. 9.6.3.3 Users must show good judgement when utilizing email and follow all relevant policies concerning the transmission of sensitive messages. 9.6.3.4 The use of automatic email diversion to external email addresses, unauthorised advertising and opening of attachments from unknown or non-trusted sources is prohibited. 9.6.3.5 Under no circumstances are any executable/ unknown application attachments (e.g. those with .exe or other unusual file extension) to be opened – these must be deleted immediately. 9.6.3.6 Sending of forged email messages is expressly forbidden. Individuals are not to use an email account that has been assigned to another user. All messages must clearly identify the true author. 9.6.3.7 The NWPG email system may not be used for unauthorised or illegitimate purposes. Employees may not use email to infringe the copyright or other intellectual property rights of Government or third parties, to distribute defamatory, fraudulent, harassing messages or otherwise to engage in any unauthorised or wrongful conduct. Use of both email and internet in this regard is expressly forbidden. This includes, but is not limited to: a) Spam – should the user suspect to have received spam emails, they must immediately alert the ICT unit b) Derogatory comments about a certain sex, race, religion, or sexual preference c) Private or freelance business

	d) Transmitting of pornographic, obscene or sexually exploitative material, offensive, obscene and abusive messages and images, and material that is defamatory, harassing or bullying in nature. e) Any act of discrimination contrary to the Policy of equal opportunities or offensive to the dignity of people at work. f) Any breach of the ACSR's ICT Security Policy, including the sharing of passwords. g) Defamatory remarks about products, services or other companies. f) Deliberate disclosure of confidential company information to unauthorised persons. 9.6.3.9 Business related emails should only be sent from ACSR's email system and not sent from a private email account. 9.6.3.10 Sending bulk email of a personal nature over Departmental email system is not allowed. 9.6.3.11 Chain letters should not be forwarded, created or circulated by the use of the ACSR email account. 9.6.3.12 Emails can be used as evidence in legal proceedings and can create binding contracts. Keep a file copy of significant messages sent or received by email. Users may not enter into any contractual agreement for or on behalf of ACSR using Government email facilities. 9.6.3.13 Email users are personally responsible for taking all reasonable steps to prevent unauthorised use of their email facility and consequently be held accountable for all activities under their login. 9.6.3.14 If staff will not be contactable on their email for a period greater than two days, the out of office assistant must be used to indicate the length of absence and alternative contact details. 9.6.3.15 Officials with compatible mobile phones are advised to contact ICT unit so that their phones can be configured to send and receive official emails – the Department will however not be responsible for supporting officials' mobile phones. 9.6.3.16 Should officials suspect that their emails have been infected by malware, they need to log a call to notify the ICT unit as soon as possible.
9.6.4 Termination of employment contract	9.6.4.1 Employees that have terminated their employment with the Department should have their mailboxes discontinued and will need to reapply in their new Departments if they will be in another Department the NWPG.

	9.6.4.2 For officials using the NWPG VOIP system, their pin codes should be locked upon termination of their employment.
Related Policies/ Procedures	NWPG Internet and Electronic-mail Guidelines Memorandum of Agreement between OTP and ACSR

9.7. Information Systems Acquisitions, Development and Maintenance

Reference to ISO/IEC 27001:2013	Section A.14
Purpose	The Policy aims to incorporate security measures into the life cycle of an information system particularly during the analysis and specification phase for new systems or enhancements to existing information systems.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.7.1 IS acquisitions, development and maintenance	9.7.1.1 Rules for the development of software and secure systems should be established, documented, maintained and applied to any information system implementation efforts. 9.7.1.2 When operating platforms are developed or changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on the Departmental operations or security. 9.7.1.3 Changes to systems should be controlled through formal change control procedures from the design throughout to the maintenance phase. 9.7.1.4 The Department shall ensure that the security of outsourced systems development be adequately protected during the contracting, and be supervised and monitored.

9.8. Access Control of Information Systems

Reference to ISO/IEC 27001:2013	Section A.9.4
Purpose	The Policy aims to restrict access to information or systems within ACSR computer environment to authorised users as well as to prevent unauthorised use or viewing of information and IT resources. This Policy focuses on passwords, pin codes & user ID requirements, access to all ACSR computer systems and networks, and segregation of duties related to IT to ensure that

	IT users are aware of their responsibility towards usage of information systems in order to minimize possible information security risks.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.8.1 Password and Username Management	9.8.1.1 Microsoft Active Directory shall be used to authenticate access of users to the network resources. 9.8.1.2 Users may only access the Government computer systems by means of their personal authorised usernames and passwords. 9.8.1.3 Passwords/ Telephone pin codes are never to be shared or revealed to anyone else. 9.8.1.4 Passwords/ Telephone pin codes should never be written down or stored in a computer in an unprotected form. 9.8.1.5 Users are responsible for all activities performed with their personal User IDs, users must not use any other User ID/ password/ Telephone pin code other than the User ID assigned to them and password / Telephone pin code selected by the user. 9.8.1.6 In order to ensure security and integrity of information stored on the computer, all computers must have logon passwords and set password protected screen savers for if unattended. Screen lock settings will be set to auto lock the screen after three minutes for all the computers. 9.8.1.7 New email users are advised to change the default email password immediately after their first logon. Should users struggle to do this help must be sourced from the ICT unit. 9.8.1.8 In order to prevent the unauthorised access to the computer systems, passwords shall comply with the following standards: a) Passwords are required to contain a minimum of 6 alphanumeric characters. b) Passwords must not be stored in a manner or format that is accessible to other users. c) Passwords may not be the username, full name of the employee or other information that relates to the individual (such as car registration, name of a child, etc.). d) In order to setup a strong password, it must be up to a minimum of 8 characters that must contain a combination of the following types of characters: i. Uppercase letters (A, B, C,...Z)

	ii. Lowercase letters (a, b, c,...z) iii. Numeric characters (0, 1, 2,...9) iv. Special characters ($, %, @, !,...) 9.8.1.9 A user shall be allowed a maximum of 3 attempts to Login to the Information Systems afterwards the account will be blocked. They should thereafter apply for password to be reset. 9.8.1.10 Passwords to login to Information Systems will be required to be changed after every 30 days. The system will automatically alert users when this time arrives. 9.8.1.11 Users are required to log out of all systems, including network after hours. 9.8.1.12 User passwords must be changed immediately if compromise is suspected.
Related Procedures / Guidelines to be developed	Departmental password policies for Persal, BAS and other systems ACSR Security Policy

9.9 ICT Service Continuity Management

Reference to ISO/IEC 27001:2013	Section A.17.1
Purpose	To ensure that ACSR is able to recover critical business operations that may be affected by disasters or major system disruptions within reasonable timeframes.
Details of the Policy	The requirements for complying with this Policy are set out in the following sections:
9.9.1 ICT Services continuity	9.9.1.1. The Department shall determine its requirements for business critical ICT services continuous availability should an adverse event occur. 9.9.1.2 The necessary processes, procedures and controls should be developed, implemented and maintained to ensure the required level of continuity for critical ICT services during such an adverse event. 9.9.1.3 The ICT disaster recovery plan should be embedded in the Departmental Business Continuity Plan.

Related Procedures / Guidelines to be developed	ACSR ICT-Disaster Recovery Plan DPSA ICT Security Guideline, 2017 ACSR Security Policy

10 ROLES AND RESPONSIBILITIES

10.1. Head of Department:

10.1.1 HOD in the ACSR bears responsibility of overseeing the development, approval, accountability and implementation of the ICT Security Policy

10.1.2 HOD shall rely on the Departmental Information Technology Officer (GITO) to provide with a holistic view of the Department's current ICT security posture.

10.2 Departmental Management:

10.2.1 In order to counter transgression of this Policy due to unauthorised access, management must make sure that the officials are allocated relevant IT tools that will enable them to execute their duties effectively;

10.2.2 Management of the information life cycle and the protection of electronic information, such as: the classification of information in terms of: who should have access to this information, how it should be stored, maintained and disposed of;

10.2.3 Departmental management should understand the impact of significant changes within their respective functional areas (for example, creation of new projects, changes in structures, etc.) in order to determine the impact of such changes within the larger realms of information security;

10.2.4 Making sure that Departmental ICT unit is made aware of employee/s that have terminated their employment with the Department;

10.2.5 Making sure that all newly appointed officials are aware of provisions of the IT Security Policy to ensure compliance;

10.3 Departmental Information Technology Officer (DITO):

10.3.1 DITO is responsible for the oversight of development of the ACSR ICT policies and strategies, regulations, standards, norms, guidelines, best practices and procedures;

10.3.2 Ensure the confidentiality, integrity and availability of ICT systems within the ICT environment;

10.3.3 Ensure that ICT security arrangements limits security breaches, threats, vulnerabilities and business impacts and if it does occur, to have in place the necessary mitigation arrangements;

10.3.4 Shall manage relationship with SITA and/or other suppliers of Information Technology products and services; this done by ensuring that all Business Agreements and Service Level Agreements (SLA) are adhered to;

10.3.4 Shall monitor and ensure compliance with relevant ICT regulatory framework and policies;

10.3.6 Ensure that awareness workshops in relation to this policy are conducted at least on an annual basis and for newly appointed employees;

10.3.8 Shall be responsible for escalating reported ICT security incidents to the MISS unit; and

10.3.9 In consultation with the Minimum Information Security Standards (MISS) office shall ensure that all ICT service providers undergo all security procedures before providing services to the Department;

10.3.10 Represent the department at the Provincial GITO council and ensure that the department is represented at the Provincial IT Security Committee

10.4. Risk Management unit:

10.4.1. Shall assist the ICT unit in conducting ICT risks assessments;

10.4.3. Shall ensure that ICT unit complies with the ACSR Risk Management Policy and other related procedures;

10.5. MISS Unit:

10.5.1 Shall in conjunction with the ICT unit ensure that the ACSR ICT Security Policy is implemented and complied with;

10.5.2 Shall ensure physical protection of all ICT assets of the ACSR;

10.5.3 Shall conduct/ facilitate vetting of external ICT service providers on request;

10.5.4 Shall develop a system for categorizing and classifying information according to the various levels;

10.5.5 Shall develop and implement security breach response mechanisms for the Department;

10.6. Asset Management unit:

10.6.1 Shall be responsible for tagging all ICT equipment with an asset tag;

10.6.2 Shall ensure that employees of ACSR are provided with notebook locks and sign *Due care Agreement in respect of use of computer form* when issuing them with official notebook; and

10.6.3 Shall be responsible for ensuring that equipment movement forms are readily available to be completed by all parties concerned for IT equipment that are to be relocated/ moved;

10.7 Provincial ICT Security Committee

10.7.1 Shall provide guidance to the Department with regard to the Provincial ICT Strategies and best practices.

10.8. End users

10.8.1 Shall be responsible for taking good care of IT equipment that is allocated to them;

10.8.2 Shall log calls for all their ICT security incidents that they encounter; and

10.8.3 Shall comply with all the provisions of this Policy.

11 NON COMPLIANCE

11.1 Noncompliance with this Policy shall result in re-training/ disciplinary action which may include but not limited to:

- Recouping of an amount of a lost / damaged IT asset from the official's salary in case where it is proven that loss / damage was because of an act of negligence;
- Termination of contracts in the case of contractors or consultants delivering a service to ACSR;
- Suspension;
- Dismissal.

12 FINANCIAL IMPLICATIONS

12.1 The Department will incur costs for stakeholder consultation workshops that will be conducted across the province.

13 POLICY REVIEW

13.1 An approved policy will be reviewed after a period of three years or as and when the need arises.

13.2 Any changes, edits and updates made to the ICT Security Policy will be recorded in here. Whenever there is an update, it is required that the version number be updated to indicate this.

Name of Person/ Structure making Change	Date of Change	Version Number	Notes
ICT unit	14/12/2014	01/2014	Initially approved version of ICT Security Policy
ACSR officials	14/12/2017	02/2017	Reviewed version of the ICT Security Policy
ICT unit	25/05/2018	03/2018	Reviewed as recommended by AG
		04/2020	Reviewed version of the ICT Security Policy

14 APPROVAL AND COMMENCEMENT

Signed in Mahikeng on this 8th day of MARCH 2021.

MR. T. MABE
ACTING HEAD OF DEPARTMENT