SADC
Parliamentary Forum
Forum Parlementaire
Fórum Parlamentar



SADC PARLIAMENTARY FORUM INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

Table of Contents

1. Section 1: Information and Communication Technology Framework 3
   1.1. Introduction 3
   1.2. Purpose and scope 3
   1.3. Definitions 4
   1.4. Applicability of the Policy 5
   1.5. Policy Statement 6
   1.6. Roles and Responsibilities 6
   1.7. Risk Management 7
2. Section 2: Information and Communication Technology User Management 9
   2.1. User Access Management 9
   2.2. Access Control / Authorization 9
   2.3. Authentication 10
   2.4. Your Account 11
   2.5. Password Management 11
   2.6. Screen Lock 12
3. Section 3: Information and Communication Technology Network Usage 14
   3.1. Acceptable Use 14
   3.2. Security 15
   3.3. Prohibited activities 16
   3.4. Monitoring 17
   3.5. Personal devices 18
   3.6. Reporting incidents 18
   3.7. Network Access Management 20
   3.8. E-Mail Usage 20
   3.9. Email Disclaimer 24
   3.10. Internet Usage 24
4. Section 4: Information and Communication Technology Social Network Usage 25
   4.1. Social Network Usage 25
   4.2. Basic Advice and General Guidelines 26
5. Section 5: Information and Communication Technology Video Conference Usage 27
   5.1 Video Conference Usage 27
6. Section 6: Policy Compliance 28
7. Section 7: Policy Review 28

AGREEMENT 29

1. Section 1: Information and Communication Technology Framework

1.1. Introduction

The **Southern African Development Community Parliamentary Forum** is committed to ensuring staff members have access to appropriate information and communication technology (ICT) infrastructure, tools, training, and support which assists them to undertake their work efficiently and effectively.

1.2. Purpose and scope

This policy aims to provide SADC Parliamentary Forum with guidance in managing its ICT infrastructure and tools provided to staff, and users and to ensure staff use of these resources is secure and appropriate.

This policy applies to all employees, stakeholders, volunteers, and student placements (Interns). All staff members are responsible for complying with this policy, and for reporting any breaches of this policy to their supervisor or manager.

The organization is committed to providing a safe and secure ICT environment for its staff and its stakeholders. By following the guidelines and standards outlined in this policy, staff can help to ensure the protection of the organization's assets and information, as well as safeguard the privacy and security of our stakeholders.

The SADC Parliamentary Forum (SADC PF) Information, Communication, and Technology (ICT) Policy provides guidelines for the use of computer tools within the institution. The policy is subject to updates by the SADC PF and aims to establish rules that safeguard employees and the SADC PF from the potential hazards of inappropriate use. Such risks include malware attacks, system and service compromises, and legal implications.

The objective of this policy is to outline the acceptable use of computer equipment within the SADC Parliamentary Forum (SADC PF).

The policy will cover the following:

- Roles and Responsibilities
- User Access Management
- Network Usage
- Network Access Management
- E-Mail Usage
- Internet Usage

- Social Network Usage
- Video Conference Usage

Feedback and recommendations are welcomed.

1.3. Definitions

Consent	Consent means voluntary agreement to some act, practice, or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.
ICT assets or equipment	Physical items that are used for information technology or communications purposes, including computers, tablets, printers, multi-function copiers, mobile or smartphones, cameras, and data projectors.
ICT hardware or infrastructure	Interchangeable terms to describe ICT equipment along with cabling, modems, routers, phone lines and other equipment required for the operation of ICT assets.
ICT Officer	The staff member responsible for managing ICT, including infrastructure and client and organisational systems.
ICT Systems	Sets of procedures or ways of doing things. ICT systems include protocols and policies put in place by an organisation or a third party relating to the use of or access to ICT hardware or software.
ICT System user	A person who is set up with access to the organisation's ICT systems. System users include all staff members but can also include anyone else who is explicitly authorised to use the organisation's ICT systems, including students, consultants, Board members or volunteers.

Information and communication technology (ICT)	An umbrella term describing technology systems and objects that enable users to access, store, transmit, exchange, and manipulate information, including computers, networks, telecommunications (telephone lines and wireless signals), software, data storage, and audio-visual systems.
Information management	Includes the creation, collection, storage, access, use and disposal of information assets.
Public domain	In relation to confidentiality is "common knowledge," i.e. information that can be accessed by the general public.
Records	Records refer to all information created, sent and received in the course of carrying out the organisation's business.
Social media	Online tools or websites (e.g. Facebook, Twitter, YouTube, Instagram, etc.) that engage, create and share user-generated content, data and comments.
Social media identification	Online name, ID, username or user account name of individuals when using online or social media tools and programs.
Software	Any form of computer program which provides a service to users, such as Microsoft Office Word (creates text-based reports), Internet Explorer (allows access to the internet), Outlook Express (email program), and so on.

1.4. Applicability of the Policy

The SADC Parliamentary Forum (SADC PF) ICT policy is applicable to all employees, including seconded staff and consultants, who use SADC PF ICT services and assets. Additionally, the policy applies to all equipment owned or leased by the SADC Parliamentary Forum.

1.5. Policy Statement

- ICT systems are the property of the SADC Parliamentary Forum (SADC PF).
- These systems are to be used for official business purposes in serving the interests of the SADC Parliamentary Forum (SADC PF).
- Effective security is a team effort involving the participation and support of every employee and affiliate who deals with organization information and information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.
- While ICT desires to provide a reasonable level of privacy, users should be aware that the data they create on the organization systems, network, laptops and desktops remains the property of the SADC PF.
- Employees are responsible for exercising good practice regarding the reasonable use of ICT systems.
- The ICT department monitors equipment, systems, and network traffic at any time.
- Employees must be aware that all data transmitted or received on computer equipment, are not private and are subject to viewing, downloading, inspection, release, and archiving by the SADC Parliamentary Forum at all times.
- A formal procedure shall be followed to give users access rights to ICT facilities.

1.6. Roles and Responsibilities

The Corporate Services Department through the ICT Officer shall:

- Provide, maintain, improve, and secure the computer network, equipment, and communication facilities of the SADC Parliamentary Forum (SADC PF).
- Ensure the confidentiality of trade secrets, client information, employee information and confidential information generally, contained in the ICT infrastructure.
- Inform and educate users on the access to and use of ICT infrastructure.
- Identify and address the potential risks associated with the use of ICT in the workplace.

- Endeavour to promote productivity through the use of quality ICT infrastructure

The user must:

- Not share login usernames or disclose passwords to any other party.
- Ensure the confidentiality of trade secrets, client information, employee information and confidential information generally contained on ICT equipment issued to the user.
- Not intentionally bypass the security mechanisms of the equipment or any third-party security system.
- Not use ICT resources for downloading, storage, forwarding or accessing data unrelated to official business (e.g. video clips, music files or graphics, SPAM) of the SADC Parliamentary Forum (SADC PF)
- Not intentionally or negligently burden ICT infrastructure with data not related to the official business of the SADC Parliamentary Forum (SADC PF).
- Not install or use any unauthorised configuration items (software or hardware) without approval from the ICT department.

This policy is implemented in conjunction with the following policies:

- Administrative Rules and Regulations
- Secondment Policy
- Whistleblowing policy
- Internship Policy

1.7. Risk Management

The SADC Parliamentary Forum is committed to the development and implementation of information and communication technology (ICT) systems that adhere to relevant legislation and industry best practices. The Risk Management Framework ensures these systems remain effective, secure, and regularly monitored to proactively mitigate risks and address vulnerabilities.

Key Components of the Risk Management Framework

The framework encompasses the following:

- **Risk Identification**: Continuously documenting potential risks, including cyber threats, hardware failures, data breaches, and regulatory non-compliance.
- **Risk Assessment**: Regularly evaluating the likelihood and impact of identified risks using a standardized risk assessment matrix.
- **Risk Mitigation**: Enforcing strategies to reduce or eliminate risks, such as deploying robust security measures, enhancing staff training, and implementing strict access controls.
- **Risk Monitoring and Review**: Continuously tracking identified risks and emerging threats to ensure the framework is updated to reflect evolving security challenges.

Other risk management actions include:

- All staff, seconded personnel, interns, and stakeholders of SADC PF are informed about this policy during their orientation.
- Ongoing training and support are provided to ensure staff can use ICT systems safely and effectively.
- This policy is reviewed annually as part of the organization's Policy Review Schedule or sooner if necessitated by changes in circumstances.
- Feedback and quality monitoring systems are leveraged to identify and implement improvements.
- ICT is a recurring agenda item in staff meetings, facilitating discussions on emerging risks and relevant issues.
- ICT systems and plans are diligently monitored and managed by designated staff members or contractors to ensure operational integrity.

2. Section 2: Information and Communication Technology User Management

2.1. User Access Management

User Access Management refers to the policies and procedures governing how users access and use the organization's ICT resources. This could include rules around user authentication, password management, and access control mechanisms to prevent unauthorized access to sensitive information.

Effective User Access Management is essential for ensuring the security and integrity of an organization's ICT systems and data. It helps to prevent data breaches, cyberattacks, and other security incidents that can compromise sensitive information.

Overall, the SADC Parliamentary Forum's ICT Policy User Access Management is designed to ensure that users have secure and reliable access to the organization's technology resources, while also protecting against potential threats and vulnerabilities.

2.2. Access Control / Authorization

Access Control refers to the different levels of access that users can have to SADC PF technology resources. Access levels are typically defined based on the user's role, responsibilities, and job functions.

Specific rules and guidelines are outlined to govern how access levels are assigned and managed. This includes defining the different access levels that exist within the organization, such as "administrator," "manager," "employee," and "guest."

Each access level is associated with a set of permissions that determine what actions a user with that access level can perform. For example, an administrator may have full access to all the organization's technology resources, while an employee may have limited access to certain systems or applications.

The Access Control includes guidelines on how access levels are assigned and revoked, and how to handle requests for access to specific resources. It may also include details on how access is monitored and audited to ensure compliance with the organization's security policies and regulations.

Overall, the Access Control policy is critical for ensuring that users have the appropriate level of access to technology resources based on their job

functions and responsibilities, while also maintaining the security and integrity of the organization's systems and data.

The Access Control is designed around 'least privilege' meaning the level you need to do your job, no more, no less. This is standard business.

We have to make sure ‘segregation of duties’ settings is based on job roles.

2.3. Authentication

Authentication refers to the process of gaining access to a computer system or application by providing valid credentials, such as a username and password. The Authentication process is typically the first step in accessing a computer system or application, and it helps to verify the user's identity and ensure that only authorized users can access the system.

To log on to a computer system or application, the user typically enters their username and password into a login screen or dialogue box. The system then verifies the credentials against a database of authorized users and, if the credentials are valid, grants access to the system or application.

In some cases, Authentication may also require additional security measures, such as multi-factor authentication, biometric authentication, or the use of security tokens.

Authentication is an essential security measure for computer systems and applications, as it helps to prevent unauthorized access and protect sensitive data. Users need to follow good password practices, such as using strong and unique passwords, changing them regularly, and not sharing them with others. Additionally, users should log off or lock their computers when they are finished using them to prevent unauthorized access by others.

You are only allowed to log on using the account and password you have been issued. You must never log on with anyone else's name and password.

Employees who negligently or intentionally share their passwords or accounts with anyone else for any reason will be held responsible for any resulting misuse of the system by others.

2.4. Your Account

As an employee, it is important to take responsibility for the use of your account and adherence to your organization's ICT policy. Here are some ways you can fulfil this responsibility:

- **Protect your login credentials**: Your account information should be kept confidential and secure. Avoid sharing your login credentials with anyone and use strong passwords that are difficult to guess.
- **Follow the ICT policy:** Familiarize yourself with your organization's ICT policy and adhere to it. Ensure compliance with the expected standards for using the organization's resources, accessing the internet, and handling sensitive data.
- **Keep your software up to date**: Make sure your software and operating systems are up to date with the latest security patches and updates. This will help to protect your account and the organization's resources from security threats.
- **Be aware of phishing attacks**: Be cautious of emails or messages that ask for personal or sensitive information. If you are unsure about an email's legitimacy, contact your IT department before responding.
- **Report suspicious activity**: If you notice any unusual activity on your account, report it to your IT department immediately. This includes any suspicious emails, unusual logins, or unauthorized access to your account.
- **Use organization resources responsibly**: Use the organization's resources only for work-related activities and avoid accessing inappropriate websites or using organization resources for personal activities.

By following these guidelines, you can help to maintain the security and integrity of your account and the organization's ICT resources.

2.5. Password Management

Password management is the practice of creating, storing, and securing passwords used to access various accounts and devices.

Password management is an important aspect of the SADC Parliamentary Forum ICT policy. The following guidelines are required for effective password management:

- **Password complexity**: Passwords should be complex and not easy to guess. Employees should be required to use a combination of upper and lowercase letters, numbers, and symbols.
- **Password length**: Passwords should be at least 8-10 characters long to ensure they are strong and difficult to crack.
- **Password expiration**: Passwords should expire every 90 days, and employees should be required to change their passwords regularly. This will help to prevent unauthorized access to their accounts.
- **Password reuse**: Employees should be prohibited from reusing old passwords. This ensures that if a password is compromised, it cannot be used again in the future.
- **Password storage**: Passwords should not be stored in plain text or written down on paper. Instead, they should be stored using secure password management tools or services.
- **Multi-factor authentication**: Multi-factor authentication (MFA) should be enabled whenever possible. MFA requires users to provide an additional form of identification, such as a security token or biometric data, in addition to their password.
- **Education and training**: Employees should be educated on the importance of password management and trained on how to create and manage strong passwords.

By adhering to these guidelines SADC Parliamentary Forum staff members and its stakeholders can enhance its security posture and reduce the risk of unauthorized access to systems and data.

2.6. Screen Lock

Screen lock is a security feature. It involves the automatic locking of a device's screen after a certain period of inactivity, requiring the user to enter a password to regain access to the device.

Screen lock is an essential security measure that should be implemented on all devices that contain sensitive information, such as laptops, smartphones, and tablets. SADC Parliamentary Forum ICT devices should automatically lock after 5 minutes of inactivity.

Screen lock is an important security measure that should be followed for the effective implementation of the SADC Parliamentary Forum ICT policy. The following are guidelines, that should be adhered to:

- **Automatic screen lock**: Employees are required to enable automatic screen lock on their devices. This ensures that the device is locked when it is not in use, preventing unauthorized access.
- **Screen lock time-out**: Devices must auto-lock after 5 minutes of inactivity. This ensures that the device is locked after a certain period of inactivity.
- **Password protection**: The screen lock should be password-protected, and employees will be required to use a strong password to unlock their devices.
- **Password sharing**: Employees are prohibited from sharing their screen lock passwords with anyone, including colleagues, friends, and family members.

Computers will automatically be locked if there is no activity on that computer after a period of 5 minutes or designated by the ICT Officer.

Remember to lock your screen when you move away from your desk and to log out or shut down your computer when you finish for the day.

3. Section 3: Information and Communication Technology Network Usage

Information and Communication Technology (ICT) Network Usage refers to the guidelines and policies governing the use of the SADC Parliamentary Forum network infrastructure and resources. The policy defines the rules and regulations that employees must follow when using the network to ensure its efficient and secure operation.

The following are some of the key areas covered by the ICT Network Usage policy:

- Acceptable use
- Security
- Prohibited activities
- Monitoring
- Personal devices
- Reporting incidents
- Network Access Management
- Email Usage

Overall, the ICT Network Usage policy is essential to ensure the efficient and secure operation of an organization's network infrastructure and resources. It helps to protect against security threats, reduce the risk of policy violations, and ensure compliance with legal and regulatory requirements.

3.1. Acceptable Use

This policy defines the acceptable use of the organization's ICT resources and infrastructure by employees. The policy also outlines the conditions for using ICT resources and infrastructure, including compliance with applicable laws and regulations, respect for the privacy of others, and the avoidance of activities that may compromise the security or integrity of the organization's ICT resources and infrastructure. The SADC Parliamentary Forum ICT Policy outlines the acceptable use of ICT resources and infrastructure by employees within the organization.

SADC Parliamentary Forum employees are expected to use ICT resources and infrastructure for legitimate business purposes only. This includes using email, internet access, and file-sharing services in a manner that supports their job responsibilities and the objectives of the organization. Employee's conditions for using ICT resources and infrastructure, including compliance with applicable laws and regulations, respect for the privacy of others, and

the avoidance of activities that may compromise the security or integrity of the organization's ICT resources and infrastructure.

3.2. Security

This policy defines the security measures that employees must follow to protect the organization's ICT resources and infrastructure. It outlines the need for strong passwords, regular updating of antivirus software, and adherence to other security best practices. The policy also specifies the measures that the organization will take to protect ICT resources and infrastructure, such as the installation of firewalls and other security software.

An Information and Communication Technology (ICT) Network Usage Security Policy is a set of guidelines and rules that define how individuals or organizations can use ICT networks and systems in a secure manner. The purpose of this policy is to ensure that the use of ICT networks and systems is consistent with business objectives and that security risks are minimized.

The following are some key elements that should be followed in the ICT Network Usage Security Policy:

- **Access Control**: Access to ICT networks and systems should be controlled through the use of authentication mechanisms such as passwords, biometrics, or smart cards. Access rights should be granted based on the principle of least privilege, which means that users should only have access to the resources they need to perform their job functions.
- **Acceptable Use**: The policy should define acceptable use of ICT networks and systems, including guidelines for email, social media, web browsing, and file sharing. This should also include restrictions on accessing unauthorized websites or downloading unauthorized software.
- **Data Protection**: Data should be protected through the use of encryption, backups, and access controls. Users should be informed about the confidentiality and integrity of data and the consequences of data loss or theft.
- **Monitoring**: ICT networks and systems should be monitored to detect unauthorized access, security incidents, and suspicious behaviour. The policy should define the frequency and scope of monitoring, as well as the roles and responsibilities of those involved in monitoring.
- **Incident Response**: The policy should define procedures for responding to security incidents, including incident reporting, containment, investigation, and resolution. This should also include

procedures for notifying relevant stakeholders, such as customers or regulatory authorities.

- **Training and Awareness**: All users should receive training and awareness programs to educate them on the importance of ICT security and how to comply with the policy. This should include regular training on new threats and vulnerabilities.
- **Compliance**: The policy should define compliance requirements and procedures for conducting compliance assessments. This should also include procedures for reporting and addressing non-compliance.
- **Physical Security**: The policy should define physical security measures for protecting ICT networks and systems from physical threats, such as theft or natural disasters.

Overall, an ICT Network Usage Security Policy is essential for SADC Parliamentary Forum to protect its assets, maintain customer trust, and comply with regulatory requirements. It should be regularly reviewed and updated to reflect changes in technology, threats, and business needs.

3.3. Prohibited activities

The policy outlines the activities that are prohibited on the organization's ICT resources and infrastructure. This includes accessing inappropriate content, engaging in illegal activities, downloading copyrighted material, or compromising the security or integrity of the organization's ICT resources and infrastructure.

The ICT Network Usage Security Policy outlines prohibited activities. These are actions that are not allowed on the SADC Parliamentary Forum ICT network or systems, as they pose a security risk to the organization. Some examples of prohibited activities are:

- **Unauthorized access**: Accessing systems, data, or networks without permission, or attempting to do so, is strictly prohibited.
- **Hacking and malware**: Attempting to break into or compromise systems, introduce malware or viruses, or engage in any other activity that could harm the network or systems is strictly prohibited.
- **Spamming and phishing**: Sending spam emails or engaging in phishing activities, such as attempting to obtain sensitive information from users, is not allowed.
- **Use of unapproved software**: Installing or using software on the network or systems that have not been approved by the organization is prohibited, as it may introduce security risks.

- **Sharing login credentials**: Sharing login credentials, such as passwords or usernames, is not allowed. Each user should have their own unique login information.
- **Using the network for personal activities**: Using the network for personal activities, such as downloading movies or music, is not allowed, as it may consume valuable resources and pose a security risk.
- **Unauthorized disclosure of sensitive information**: Sharing or disclosing sensitive information, such as personal or financial data, is strictly prohibited.

3.4. Monitoring

The policy specifies that the SADC Parliamentary Forum has the right to monitor employee activities on the organization's ICT resources and infrastructure. This includes monitoring web browsing, email, and file transfers to ensure compliance with the policy and to identify any security threats or policy violations.

Monitoring is a critical component of an ICT Network Usage Security Policy. It involves the continuous and systematic collection, analysis, and interpretation of data related to network and system activities to identify potential security breaches, unauthorized access attempts, and other suspicious activities.

The following key elements are included in the monitoring process:

- **Monitoring tools**: The monitoring process encompasses several crucial components, namely the utilization of various monitoring tools to keep track of network and system activities. These tools may comprise intrusion detection and prevention systems, security information and event management (SIEM) systems, as well as other network monitoring tools, which will be utilized by the SADC Parliamentary Forum.
- **Monitoring frequency**: The SADC Parliamentary Forum will be conducting monitoring activities on all incoming and outgoing traffic using one of the following approaches: continuous monitoring, periodic monitoring, or real-time monitoring.
- **Data retention**: The SADC Parliamentary Forum reserves the right to store and dispose of monitoring data following established policies.
- **Monitoring scope**: The SADC Parliamentary Forum will define the scope of monitoring, including the identification of network and system components that will undergo monitoring, as well as the types of activities that will be tracked.
- **Incident response**: The SADC Parliamentary Forum has defined procedures for responding to security incidents identified through

monitoring, which include incident reporting, containment, investigation, and resolution.

- **Roles and responsibilities**: There are roles and responsibilities of those involved in monitoring, such as the security operations centre (SOC), incident response team, and other relevant personnel.
- **Data protection**: Monitored data will be protected to prevent unauthorized access or disclosure.

Overall, monitoring is essential to detecting and preventing security breaches and other security incidents. This policy should be regularly reviewed and updated to reflect changes in technology, threats, and business

3.5. Personal devices

The SADC Parliamentary Forum's ICT policy outlines guidelines for the use of personal devices on the organization's infrastructure and resources. These guidelines may mandate employees to install antivirus software on their devices and restrict the types of data that can be accessed or stored on them.

The policy is designed to protect the SADC Parliamentary Forum ICT infrastructure and resources from potential security threats that could arise from the use of personal devices. The policy applies to all employees, stakeholders, and other individuals accessing the SADC PF network and systems and outlines the guidelines that must be followed when using personal devices for official business.

Under this policy, employees may be required to install antivirus software on their personal devices to prevent malware and other malicious software from infecting the organization's network and systems. The policy may also impose restrictions on the types of data that can be accessed or stored on personal devices to ensure that sensitive information is not compromised.

3.6. Reporting incidents

The policy outlines the procedures for reporting any security incidents or policy violations. This includes reporting suspicious activities, lost or stolen devices, or unauthorized access attempts.

The SADC Parliamentary Forum's policy mandates the reporting of security incidents by all employees, contractors, and other individuals who access the organization's ICT resources and infrastructure. The policy defines the

procedures that must be followed when reporting incidents, including the information that should be provided and the channels through which incidents should be reported. Timely and accurate reporting of security incidents is critical to enable prompt and effective responses to mitigate any potential risks to the organization's network and systems.

defined policies that must be followed when reporting incidents, as per the SADC Parliamentary Forum's policy:

- All security incidents must be reported immediately to the designated authority or the ICT team via the established reporting channels.
- The incident report must include a description of the incident, including the time and date, the location, the systems and data affected, and the potential impact on the organization.
- If the incident involves a personal device, the report must include details of the device and the type of data that was being accessed or stored.
- The incident report must also include any supporting evidence, such as screenshots, error messages, or other relevant information that could help with the investigation and resolution of the incident.
- The incident report must be kept confidential and only shared with authorized personnel as necessary to resolve the incident.
- Once the incident has been reported, the designated authority or the ICT team will initiate the incident response process, which may include containment, investigation, resolution, and recovery.
- After the incident has been resolved, a post-incident review may be conducted to identify any areas for improvement in the incident response process and the organization's overall security posture.

Following these policies for reporting incidents is critical to ensuring the security and confidentiality of the organization's sensitive data and infrastructure.

Overall, the SADC Parliamentary Forum ICT Policy is essential to ensure the efficient and secure operation of the organization's ICT resources and infrastructure. It helps to protect against security threats, reduce the risk of

policy violations, and ensure compliance with legal and regulatory requirements.

3.7. Network Access Management

The SADC Parliamentary Forum's ICT policy includes guidelines for network access management to ensure the security and integrity of the organization's network and systems. The policy outlines the procedures that must be followed when granting or revoking network access privileges to employees, contractors, and other individuals. The network access management guidelines cover areas such as user authentication, authorization, and accountability to prevent unauthorized access and misuse of the network and systems. By strictly enforcing these guidelines, the organization can minimize the risk of security breaches and protect the confidentiality of its sensitive data.

Guidelines for network access management as outlined in the SADC Parliamentary Forum's policy are:

- ICT will ensure that users are only provided with direct access to the networked resources that users have been specifically authorised to use. Users are not allowed to modify network hardware or devices. Only administrators can configure network devices.
- Users are not allowed to install software that provides or manipulates the network. Under no circumstances should users install any software on the systems unless otherwise authorised by ICT.
- Users are to use network protocols that are approved by ICT.
- ICT will provide firewalls for secured access between the department network and the worldwide network. Attempts to bypass the firewall are strictly prohibited.
- If you have a supplier or visitor with you that wants to connect to the network for internet access, a request should be made to the ICT Officer.
- No personal hardware or devices are allowed on the network unless authorised by ICT.

3.8. E-Mail Usage

The SADC Parliamentary Forum recognizes the importance of email as a means of communication in today's digital world. To ensure that email is used effectively and securely for official communication, the organization has established an email usage policy that outlines the procedures and guidelines to be followed by employees.

- **Purpose**: The purpose of the email usage policy is to provide guidelines and procedures for the appropriate use of email for official communication in the organization. This policy aims to ensure that email is used effectively, efficiently, and securely, in line with the organization's values and standards.
- **Scope**: This policy applies to all employees of the SADC Parliamentary Forum who use email for official communication.
- **Authorized Use**: Email is to be used for official communication only. Personal use of email is permitted but should be kept to a minimum and not interfere with the employee's work duties.
- **Security**: All email messages must be treated as confidential and proprietary information of the organization. Employees must take appropriate measures to protect email messages from unauthorized access, alteration, or disclosure. This may include using secure passwords, encrypting sensitive messages, and ensuring that emails are sent only to authorized recipients.
- **Monitoring and Retention**: The organization reserves the right to monitor email messages sent or received by employees to ensure compliance with this policy. Email messages may also be retained for a specified period for legal, regulatory, or business purposes.
- **Responsibilities**: All employees are responsible for complying with this policy and ensuring that their use of email does not compromise the security or effectiveness of the organization's communication processes.

By establishing this email usage policy, the SADC Parliamentary Forum can ensure that email is used effectively and securely for official communication and that employees are aware of their responsibilities and obligations when using email.

The SADC Parliamentary Forum will issue an email account to you, which will be subject to the following guidelines:

- All incoming and outgoing emails, as well as their attachments, will be filtered to prevent spam, viruses, and offensive content.
- Business emails sent or received through the SADC PF service are not private property and will be considered part of the organization's administrative records.
- Occasional and incidental personal use of the email facility is allowed, provided it does not interfere with job responsibilities, disrupt the system, or damage the organization's reputation. Such use must be

conducted outside of working hours, and SADC PF will not be held liable for any consequences arising from such use.

- Any information related to SADC PF's employees, suppliers, or stakeholders, other than email addresses, is confidential and must not be disclosed to unauthorized parties.
- Attachments sent through email will be subject to size limitations to prevent bandwidth issues. If you need to send or receive a large file, please consult with the ICT Officer.
- The use of web-based communication tools such as Skype is encouraged to reduce costs associated with conventional communication tools like telephone and fax.
-

The SADC Parliamentary Forum will:

- Protect the organisation from e-mail transmissible malicious software and viruses.
- Notify the sender, if an outgoing e-mail could not be sent; and notify the addressee(s), if an incoming e-mail was rejected.
- Ensure that all outgoing e-mails have the standard legal disclaimer at the bottom of the message.
- Educate users to ensure that they understand the messages, memos, notices, announcements, etc. about security threats in using the e-mail facility.
- Implement filtering mechanisms to ensure that mail sent to and from the organisation does not contain any potentially harmful or forbidden texts and/or attachments and restrict access to any undesirable websites.

An e-mail user must:

- Include a meaningful subject line before sending messages
- Not disguise or attempt to disguise own identity when sending an e-mail, and shall not forge or attempt to forge any e-mail messages
- Ensure sending a message to the right person(s)
- Keep all e-mail messages brief and formulated appropriately
- Email should be used for business purposes only; no chain messages should be circulated.
- Notify the sender if you were not the intended recipient.
- Not intentionally send any malicious material, such as a virus-infected file, either internally or externally which might compromise the ICT systems and/or operations of the SADC PF
- Report any suspicions which may either lead to the enhancement or compromise of the e-mail system security and/or operation of ICT.

- Not access (or try to access) a colleague's e-mail or use his/her e-mail account without the permission of the allocated user
- Ensure that the size of the e-mail message(s) and its attachment does not exceed the limit as set by ICT Officer.
- Not send a message(s) which could be regarded as unsolicited, derogatory, defamatory, or libellous and/or compromising the information security of the SADC PF.
- Not send any material of pornographic nature or any other offensive material (images depicting graphic violence, for instance) and report any received material of pornographic nature or offensive material.

Users must not:

- Use the facilities to transmit, either directly or indirectly, any unsolicited bulk e-mail or unsolicited commercial e-mail. You will not send or forward "Spam" including chain letters and jokes. SADC PF will limit the number of recipients to acceptable global standards.
- Upload, download, use, retain, distribute, or disseminate any images or text that is pornographic, obscene, indecent, or otherwise objectionable.
- Intentionally interfere, in any way whatsoever, with the normal operation of the network.
- Represent personal opinions as those of the SADC Parliamentary Forum.
- Send any material that is obscene, defamatory, racist, politically extreme or which is intended to annoy, harass, or intimidate another person. SADC PF shall have the right and responsibility to block the sending or receipt of such material.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside the organisation or to SADC PF.

3.9. Email Disclaimer

This email and any attachments are confidential and solely for the use of the intended recipient(s). They may contain material protected by legal professional or other privileges. If you are not the intended recipient(s) or the person responsible for delivering to the intended recipient(s), you are not authorised to & must not disclose, copy, distribute or retain this email or its attachments. No responsibility is accepted by SADC Parliamentary Forum for any loss or damage arising from receipt of this Email or its attachments or use thereof; it is also the responsibility of the recipient(s) to ensure that they are virus-free. If this email is not used for business purposes, the views & opinions expressed are those of the sender and no liability will attach to SADC PF.

3.10. Internet Usage

Internet Usage refers to the policies and guidelines for accessing and using the internet while using SADC Parliamentary Forum ICT resources and infrastructure.

Internet access shall conform to the following:

- Employees may not use the SADC Parliamentary Forum (SADC PF) systems to access or download material from the Internet which is inappropriate (literature inciting violence against foreign nationals, for example), offensive, illegal (for instance, pirated software), or which jeopardises security.
- The Internet is meant to be used for business purposes, this means research, procurement, authorised software updates and other legitimate business activities authorised by the SADC PF.
- The ICT Department should ensure that the network infrastructure is safeguarded from malicious external intrusion by deploying, a configured firewall and antivirus on all workstations.
- The ICT Department shall use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by employees. At all times, the following classes of web traffic shall be prohibited:

  - ✓ Illegal sites, child pornography, etc
  - ✓ Music and video downloads
  - ✓ Downloads that may compromise the security of the Department
  - ✓ Committing crime and terrorism
  - ✓ Distribution of spam
  - ✓ Participating in online gambling

- ✓ Spreading malware
- ✓ Accessing adult content (pornography)
- ✓ Advertising
- ✓ Dating and chat
- ✓ Playing online games

4. Section 4: Information and Communication Technology Social Network Usage

4.1. Social Network Usage

The purpose of this policy is to outline the guidelines for SADC Parliamentary Forum employees when using social networking sites and applications, as well as to safeguard the interests of the organization and its employees.

This policy applies to all SADC Parliamentary Forum employees who access social networking sites and applications, whether on the organization's ICT resources and infrastructure or personal devices.

For this policy, social media may refer to:

- Popular social networks such as Twitter and Facebook
- Photo-sharing websites such as Pinterest and Instagram
- Professional social networks such as LinkedIn
- Discussion forums such as the ones found on 4chan and Reddit
- Question and answer-based networks such as Quora and Yahoo Answers
- Review systems such as Yelp and Google Reviews

Guidelines:

- **Personal Use**: Employees are allowed to use social networking sites and applications for personal reasons but should do so outside of working hours and without impacting their job responsibilities or the reputation of the organization.
- **Professional Use**: Employees are permitted to use social networking sites and applications for professional purposes related to their work in SADC Parliamentary Forum only if authorized by their manager or supervisor.
- **Representing the organization**: When representing SADC Parliamentary Forum on social networking sites and applications, employees should ensure that they are acting per the organization's

values and policies. They should also clearly identify themselves as employees of the organization and avoid sharing any confidential information or sensitive data.

- **Posting Content**: Employees should ensure that any content they post on social networking sites and applications does not reflect negatively on the organization. They should also ensure that they do not post any content that is defamatory, discriminatory, offensive, or violates any laws or regulations.
- **Cybersecurity**: Employees should not click on suspicious links, download unknown files, or provide any personal or confidential information on social networking sites and applications. They should also report any suspicious activity or security incidents to the ICT department immediately.
- **Enforcement**: Violations of this policy may lead to disciplinary action up to and including termination of employment.

4.2. Basic Advice and General Guidelines

Whether SADC Parliamentary Forum (SADC PF) employees are posting from the organisation or personal accounts, we encourage them to follow basic best practice rules.

Adhere to these standards to avoid common social media mistakes:

Understand the social network. Different social media platforms have different purposes. For example, it is common to see more personal status updates on Facebook than on LinkedIn. Before posting, become familiar with the network by reading the Frequently Asked Questions (FAQs) and quickly researching what is and is not acceptable.

Correct your own mistakes. When you make a factual error in a post, create an update to correct it. Deleting or editing the original post should come at your discretion, depending on the situation.

Beware of potential security threats. Hackers can use social networks to distribute spam and malware. They can also launch phishing attempts. You should report suspicious activity, including questionable comments and friend requests.

Be careful when sharing information about yourself or others. Hackers can also use personal information to their advantage.

Do not escalate issues. Responding to other social media users, especially concerning a contentious subject, can result in a heated argument. To avoid

such arguments, it may be best to avoid commenting if you feel you may spark conflict.

Think before posting. This is the golden social media rule. Not only should you check grammar and spelling but ensure there will not be any negative effects of posting a status update. These include creating arguments and divulging sensitive information.

5. Section 5: Information and Communication Technology Video Conference Usage

5.1 Video Conference Usage

The purpose of this Video Conference Usage Policy is to ensure the efficient, secure and professional use of video conferencing facilities by members and staff of the Southern African Development Community (SADC) Parliamentary Forum. This policy outlines the rules and guidelines governing the use of video conferencing facilities for all Forum meetings and events.

This policy applies to all members, staff, and guests who use video conferencing facilities provided by the SADC Parliamentary Forum.

The SADC Parliamentary Forum will provide access to Video Conference Software facilities. Use of these facilities shall be subject to the following principles:

- **Purpose**: The video conferencing facilities provided by the Forum are for official business use only. All users must ensure that their video conferencing activities comply with this policy and are in accordance with the Forum's mission and values.
- **Access**: Access to video conferencing facilities is granted only to authorized personnel. Members and staff are required to keep their login credentials secure and should not share them with unauthorized individuals.
- **Conduct**: All participants must behave in a professional and courteous manner during video conferences. Any abusive, discriminatory, or offensive behaviour is strictly prohibited. The Forum reserves the right to terminate any video conference if it is deemed to be in violation of this policy.
- **Recording**: Video conferences may be recorded only with the express consent of all participants. The Forum reserves the right to retain and use any recordings for internal purposes.
- **Security**: Members and staff are responsible for ensuring the security of their devices and networks. The Forum is not responsible for any data breaches or security incidents that occur as a result of the use of video conferencing facilities.

- **Confidentiality**: Participants must respect the confidentiality of all discussions and information shared during video conferences. Any unauthorized disclosure of confidential information is strictly prohibited.
- **Technical Support**: Members and staff are responsible for ensuring that their devices and networks are compatible with the video conferencing facilities provided by the Forum. Technical support is available, and users are encouraged to seek assistance if they encounter any technical issues.
- **Compliance**: Failure to comply with this policy may result in disciplinary action, including revocation of access to video conferencing facilities.

This Video Conference Usage Policy aims to ensure the effective and secure use of video conferencing facilities by members and staff of the SADC Parliamentary Forum. All users are required to comply with this policy, and any violations will be subject to disciplinary action.

6. Section 6: Policy Compliance

- Violation of this policy, and referenced policies, may lead to restriction of access to (or usage of) the Information Communication Technology infrastructure and/or disciplinary action as per the Administrative Rules and Regulations Handbook.
- The SADC Parliamentary Forum may use any legislation relevant to the usage or protection of ICT infrastructure, in prosecuting the person who has violated this policy.
- Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual will be the responsibility of that individual. The penalty, thereof, will be determined by the Human Resource Management disciplinary process.

7. Section 7: Policy Review

This policy will be reviewed on an annual basis or if necessary, by the ICT Officer to:

- Determine if there have been changes in International, National, or Internal references that may impact this policy.

- Determine if there are improvements or changes in the ICT process that should be reflected in this policy

AGREEMENT

I _____ in my capacity as a User of the Internet and email

facilities provided by **SADC PF**, confirm that I have read, understood and do hereby accept the conditions of use stipulated in this Policy. I fully subscribe to and agree to be bound by the said conditions or any other amendments thereto.

Signed at _____ this _____ day of _____ 20___.

_____ _____

ICT Officer **Date**

_____ _____

Signature of User **Date**