

POLICY

FRAMEWORK ON INFORMATION AND COMMUNICATION TECHNOLOGY



ADOPTED 2025

With funding from:



Table of Contents

FOREWORD	5
Definitions	6
Acronyms	8
Legal Framework.....	9
PART: 1.....	10
1. Acceptable Use	10
1.1 Purpose.....	10
1.2 Scope	10
1.3 Objectives	10
1.4 Application	10
1.5 Principles	11
1.6 Acceptable use	11
1.7 Personal use	11
1.8 Unacceptable use	11
1.9 User account	12
1.10 E-mail usage	12
1.11 Internet and network usage	12
1.12 Compliance.....	12
1.13 Authority and Responsibility	12
1.14 Interim Measures	12
PART :2	13
2. Security	13
2.1 Introduction.....	13
2.2 Purpose.....	13
2.3 Principles.....	13
2.4 Objectives	13
2.5 Application	14
2.6 Requirements.....	14
2.7 Protection of information assets	14
2.8 Protection of Hardware and Software Assets	14
2.9 Security Awareness Training.....	15
2.10 Security Program Methodology	15
2.11 Roles and Responsibilities.....	15
2.12 Risk management	16
2.12.1 Members of Parliament, and their staff	17
2.12.2 Secretariat.....	17
PART: 3.....	18
3. Privacy and Confidentiality	18

3.1 Introduction.....	18
3.2 Scope.....	18
3.3 Protection of Information	18
3.4 Parliament Information	18
3.5 Individual Information	19
3.6 Purposeful Use	19
3.7 Reduced Data Retention	19
3.8 Confidentiality and Authorisation.....	19
3.9 Roles and Responsibilities	19
PART :4	21
4. General Provision	21
4.1 Non-compliance	21
4.2 Review of the policy.....	21
Appendix A: Examples of acceptable and unacceptable Use of IT Resources	22

FOREWORD

Information and Communication Technology (ICT) has become an integral part of any organisation in this modern world, playing a profound role in improving communication, innovation and efficiency. Therefore, an emerging call for legislative bodies to embrace technology and the Parliament of Namibia is no exception.

Parliament can harness the benefits of information technology by applying it to core functions such as legislative drafting, parliamentary reporting, and the distribution of digital information. Additionally, IT can enhance data analysis, citizens' participation, and research, among other parliamentary functions.

To this end, the Parliament of Namibia has made tremendous progress in moving towards an Information Communication Technology (ICT) compliant institution. A comprehensive e-parliament strategy aimed at accelerating efficiency within the operations of parliament and in its interactions with stakeholders. This strategy was developed and launched in 2022 with the support of the World Bank.

Prior to that, at the height of the COVID 19 pandemic, the National Assembly had installed a digital multimedia system to continue with its operations when disruptions were encountered due to the outbreak. The digital system that can support remote working and sittings, can further give lawmakers access to a lot of digital parliamentary documents such as the Order Paper, Minutes of proceedings, Bills, the Constitution and Standing Rules and Orders among many others. The system further enables the Speaker, as the Presiding Officer, to control debate in the House as well as enabling Members to vote electronically.

We have further managed to introduce the livestream of parliamentary sessions and oversight activities on social media and have revamped the parliament website with assistance from the Konrad Adenauer Stiftung (KAS). The Parliament is also unveiling several newly created digital tools which include a Mobile Application and an Online Bill Register System, designed to provide easy access to parliamentary information and actively involve citizens in the lawmaking process.

To ensure the effective use of these ICT tools and their security and protection, there was a need to develop a framework, hence the compilation of this policy. The Policy focuses on four essential areas of: Acceptable Use, Security, Privacy and Confidentiality, and General Provisions.

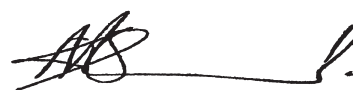
The adoption of this framework marks a critical milestone in the development of a comprehensive ICT policy for Parliament, which will guide ICT usage and protection within our institution.

I would like to acknowledge and appreciate the assistance offered by our development partners who have contributed immensely to ensuring that the Parliament of Namibia becomes a fully-fledged ICT centre. These development partners include the Enhancing Participatory Democracy in Namibia (EPDN), the Konrad Adenauer Stiftung (KAS), the National People's Congress of China, the Turkish Cooperation and Coordination Agency (TIKA), and the World Bank.

I am confident that we will rise to the challenge of creating a conducive ICT environment and ensuring that parliament fulfills its mandate of lawmaking, oversight, and representation through the usage of the necessary ICT tools to foster the socio-economic development of Namibia, in alignment with the aspirations of our people.



Prof. Peter. H. Katjavivi (MP)
SPEAKER TO THE NATIONAL ASSEMBLY



Hon. Lukas Sinimbo Muha (MP)
CHAIRPERSON TO THE NATIONAL COUNCIL

Definitions

TERM	DEFINITION
Business units	Different departments/divisions/subdivisions within the National Assembly/National Council
Cloud computing	The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer
Computing Devices	Computing resources include all The Parliament owned, licensed, or managed hardware and software, and use of the Parliament network via a physical or wireless connection, regardless of the ownership of the device connected to the network
Computing Resources	Includes, but not limited to personal computers, servers, networks, data sets, printers, internet and internet access and software.
IT Security tools	A range of solutions designed to protect a business from the threat of data breaches, malware or cybercrime
IaaS, PaaS, SaaS	Types of cloud computing delivery models
ICT Services	Refers to forms of technology that are used to transmit, process, store, create, display, share or exchange information by electronic means.
IT Asset	IT assets are the integral components of the organisation's IT infrastructure used for storage, management, control, display, data transmission, and more.
IT infrastructure	The collection of hardware, software, networks, facilities, and related services that deliver IT operations. IT infrastructure components include servers, storage systems, networking devices, operating systems, databases, and other software applications.
Malware payload	Payload in the context of malware refers to malicious code that causes harm to the targeted victim.
Members	Refers to the Members of Parliament
peer-to-peer networks	Is a network where devices or nodes share resources and services directly without centralized control
Parliament	Refer to National Assembly and National Council
Parliamentary users	Members, Member staff, secretariat, secretariat
Non-parliamentary users	External partners, service providers, government offices, ministries and agencies (OMAs).
Parliament's code of conduct or ethics	Parliament's code of conduct or ethics refers to the Public Service Staff Rules and Code of Conduct

Personal data	Any information relating to an identified or identifiable individual such as the name, address, email address
Secretariat	Staff members of National Assembly or National Council
Secretary to the National Assembly/National Council	The Accounting Officer of the National Assembly/National Council
Security posture	An organization's security posture is its readiness and ability to identify, respond to and recover from security threats and risks.
Specific legal provisions	Refers to detailed clauses, sections, or stipulations within a law, statute, regulation, or legal document that explicitly outline certain rules, obligations, rights, procedures, or restrictions.
Stakeholders	Refers to individuals, groups, or organisations that have an interest in the legislative process and make use of Parliament's IT infrastructure.
Their Staff	Refers to staff members appointed by political parties
Service providers and Visitors	Individuals/Companies visiting Parliament to render any services to Parliament and using Parliament's IT infrastructure.

Acronyms

ICT	Information and Communication Technology
IaaS	Infrastructure as a Service
IT	Information Technology
MP	Member of Parliament
NA	National Assembly
NC	National Council
NCIS	Namibia Central Intelligence Services
OMAs	Offices, Ministries and Agencies
PaaS	Platform as a service
PO	Privacy Officer
PSC	Parliamentary Service Commission
SaaS	Software as a service
VPN	Virtual Private Network

Legal Framework

The Policy is underlined by the following legal and policy prescripts:

- Constitution of the Republic of Namibia, 1990.
- Information and Communication Technology (ICT) Policy for the Republic of Namibia 2024 -2034
- E-Government Strategic Action Plan of the Public Service of Namibia (2014–2018)
- Ministry of Health and Social Services ICT Policy 2008
- Namibia e-Parliament Strategy 2022 -2027
- South Africa North West Provincial Legislature Information and Communication Technology Combined Policy 2022
- International Code of Practice for Information Security Management (ISO 27002) and
- European Union Directive on Privacy and Electronic Communications.

PART: 1

1. Acceptable Use

1.1 Purpose

The computing, digital technology, and digital information resources at the Parliament of the Republic of Namibia herein referred to as "Parliament", are essential to the organisation's mission.

Usage of these resources is a privilege that is extended to:

- Members and their staff
- the Secretariat
- Service providers and visitors

Acceptable use means, respecting the rights of other digital users, the integrity of physical and digital assets, pertinent license and contractual agreements, and where applicable, maintaining compliance with legal and regulatory requirements.

Users have access to valuable organisational resources, including sensitive and critical data, and to internal and external networks. Consequently, it is important for all users to act in a responsible and ethical manner.

This policy establishes specific requirements for the use of all computing and network resources within Parliament, and it is subject for review after a period of five years and/or when necessary.

1.2 Scope

This part applies to all users of computing resources owned and/or managed by Parliament.

Computing resources include all licensed software, hardware and networks owned and/or managed by Parliament. It also includes the use of Parliament network via a physical or wireless connection, regardless of the ownership of the device connected to the network.

1.3 Objectives

The objectives of this part are to:

- Define the responsibilities of users who are given access privileges to Parliament computing resources.
- Ensure that Parliament's computing resources are used in a professional, ethical and lawful manner;
- Ensure stable, secure, available and confidential working environment for the parliament community;
- Assist Parliament improve internal processes and performance.

1.4 Application

This part applies to:

- Members and their staff
- Secretariat
- Service providers and visitors hereafter referred to as "parliamentary users".

This part extends to include any other organisation or individual using Parliament computing resources whether they conduct business with the Parliament and access Parliament IT infrastructure, hereafter referred to as “non-parliamentary users”.

1.5 Principles

Users:

- Shall only use computers, accounts and files for which they have authorisation to access resources needed to perform their stated job functions.
- Shall adhere to Parliament password standards to protect their passwords and to secure resources against unauthorised use or access.
- Are individually responsible for appropriate use of all resources assigned to them, including computers, network resources, software and hardware.
- Shall not provide the resources or other forms of assistance to allow any unauthorised person to access Parliament computers, networks or information.
- Shall not attempt to access or provide resources to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorisation by Parliament's system administrator.
- shall comply with the policies and guidelines for any specific set of resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- Shall not store, share, process, analyse or otherwise communicate official information, data or files using unauthorised mediums, applications or infrastructure including but not limited to cloud, IaaS, PaaS, SaaS or peer-to-peer networks.

Parliament shall be bound by contractual and licensing agreements with regard to third-party resources. Users are expected to comply with all such agreements when using such resources.

1.6 Acceptable use

Acceptable use includes:

- Communicating with other parliamentary and non-parliamentary users to carry out duties, functions and activities for the purposes of parliamentary and professional development activities;
- Performing research by accessing online reports, presentations, websites etc;
- Discussing professional issues or participating in professional associations via online forums;
- Filing online job applications or participating in online interviews.

1.7 Personal use

Limited personal use is also acceptable if the use of Parliament computing resources does not:

- interfere with the parliamentary user's official duties/functions;
- generate additional cost to Parliament;
- result in damages to or disruption of Parliament computing resources.

1.8 Unacceptable use

Unacceptable use includes the use of Parliament's computing resources:

- For non-parliamentary purposes;
- Personal economic gain;
- In any way that is in violation of Parliament's code of conduct or ethics; or,
- In a way that is considered offensive, defamatory, obscene or harassing.

1.9 User account

Parliament provides user account to Parliamentary users. Users must use their accounts in accordance with the User Account and Password Standards. To retain relevant data for business continuity, User Accounts for key offices shall be in accordance with the name of the position e.g. Office of the Secretary, Office of the Chairperson of National Council, etc.

1.10 E-mail usage

Parliamentary emails and other electronic communication systems must only be used for official activities in accordance with the user account and password standards.

All official business must be conducted using the parliamentary email account.

Parliamentary users:

- Responsible for the content of any electronic messages sent using their account;
- Accept that the privacy and security of messages sent over internet cannot be guaranteed;
- Must not use their Parliament email addresses when creating accounts for purposes unrelated to their work;
- Must be vigilant with email use;
- Should be aware of and know how to avoid being the target of phishing and spear phishing attempts as these emails are a major source of cyber compromises.

1.11 Internet and network usage

Unless otherwise instructed by the appropriate authority of both houses, the Information Technology Subdivision's security tools will be used to restrict internet access to non-authorised or risky sites (i.e. pornographic and plagiarism sites, pirated material, known hacker organisations etc.).

1.12 Compliance

Individuals found to be in violation of this part, shall be subject to disciplinary action not limited to restriction, possible loss of privileges, suspension, or termination.

1.13 Authority and Responsibility

The IT Subdivision is responsible for authorising, managing, and auditing the use of computing resources by using monitoring, inspection and audit tools, to ensure compliance to this policy.

1.14 Interim Measures

With instruction from the Secretary to the National Assembly/National Council, Parliament may temporarily disable service to an individual or a computing device, when they are in an apparent non-compliance to this policy.

PART :2

2. Security

2.1 Introduction

Parliament is an institution that holds public trust in the Namibian society. Anything that compromises the confidentiality or integrity of the sensitive information and technology entrusted to it poses a serious risk to its reputation. Similarly, anything that compromises the availability of the information required by Members of Parliament (MPs) to perform their duties poses a risk to their ability to effectively carry out their constitutional and Parliamentary functions. It is therefore important that Members, their staff and the Secretariat, understand their roles in maintaining information technology (IT) security.

This part provides the overarching direction, scope and context for Parliament IT security which is to be sound, clear and enduring. This policy is supported by related internal administrative policies and standards of Parliament.

2.2 Purpose

The purpose of this part is to anticipate, mitigate, prevent or avoid possible IT threats which could be complex, pervasive and potentially infiltrate Parliament's information system. All business activities and conduct must therefore endeavour to apply secure controls and use authorised IT assets to avoid undue risks to the Parliament information systems and information.

2.3 Principles

Parliament's IT security activities are guided by the following principles reflecting its core values and objectives. These are:

- Strengthening guardianship of the institution by enhancing the availability, integrity, and confidentiality of Parliament information while optimising the use of public resources.
- Sharing, applying and managing recommended industry standards concerning IT security to protect the information assets and reputation of Parliament, where possible.
- To reflect and respond to the changing needs of the institution and Members, as well as to external threats and risks.
- To support a responsible and secure management of a comprehensive, fully adopted and implemented/administered IT security program by assessing and formulating plans to mitigate risks.

In keeping with industry standards, Secretariat, Members and their staff, must adhere to, adopt and incorporate all recommended practices, technology tools and controls.

2.4 Objectives

The objective of the IT security program is to protect the information and other assets of Members, their staff and the Secretariat from undue risks.

The objectives of this part is:

- To define the overarching IT security requirements, direction and expectations associated with the protection of accessibility, integrity and confidentiality of IT assets;
- To define the responsibilities and controls necessary for adequate IT security throughout Parliament;
- To ensure the availability of the ICT services and assets.

- To reduce the risk of failure to the operation of the Parliament.

2.5 Application

This part applies to:

- Members and their staff
- Secretariat
- Service providers and visitors, hereafter referred to as “parliamentary users”.

This part extends to include any other organisation or individual using Parliament computing resources whether they conduct business with the Parliament and access Parliament IT infrastructure, hereafter referred to as “non-parliamentary users”.

Any agreements with third parties such as contractors or visitors requesting access to Parliament services must include an acknowledgement of this policy and an agreement to comply with it as a term of contract. Any such agreements must also stipulate that failure of the third party to comply with the policy would result in the immediate termination of the agreement. In addition, contractor's or visitor's/guest's access can be terminated at any time.

2.6 Requirements

This policy should be read in conjunction with the Information Technology Acceptable Use Policy and other applicable policies. Parliamentary users must apply proactive IT security controls in accordance with this policy.

2.7 Protection of information assets

Members, with advice and support from Information Technology Sub-division, are accountable for safeguarding their information assets by applying appropriate controls and practices. Members own all information assets created by them or by their staff, regardless of where these assets are located.

Parliament owns all information assets created or received by the Secretariat from any source including Members and non-Members using Parliament hardware and/or software resources.

2.8 Protection of Hardware and Software Assets

All IT assets used within Parliament are to be identified, always recorded and maintained. The Information Technology Sub-division in collaboration with the directorate responsible for stock control is responsible for compiling and managing a comprehensive inventory of IT assets.

It is recommended that Members, their staff and the Secretariat only use hardware and software authorised by the Information Technology Sub-division for Parliamentary business. Only Information Technology Sub-division -authorised hardware or software may be purchased.

Members', their staff and the Secretariat's personal IT hardware or software shall be subjected to an assessment and the activation and/or placement of added security treatments prior to being connected to Parliament's IT infrastructure.

No hardware, software or other IT assets will be introduced onto Parliament's IT infrastructure without due approval by Information Technology Subdivision. The Secretariat shall request an assessment by Information Technology Subdivision prior to purchase or acquisition of such assets with Parliament funds. All additions to the Parliament IT infrastructure will be subject to rigorous routine testing and change management prior to installation.

2.9 Security Awareness Training

The Information Technology Subdivision shall develop training material and provide IT security awareness training to Members, their staff and the Secretariat. It is strongly recommended that all parliamentary users attend regular IT security awareness programs.

2.10 Security Program Methodology

Parliament shall protect information assets through the use of carefully managed administrative, physical, technical and service providers' controls. These controls shall include the use of formally approved operating procedures.

Pursuant to this policy and in accordance with industry standards, the Secretaries of both houses with the support of the Head of the Information Technology Subdivision shall issue appropriate directives on the delivery and governance of operating practices for the entire organisation.

These shall include the:

- Segregation of responsibilities;
- Management of elevated privileges;
- Monitoring;
- Effective password management;
- Detection of anomalies and unauthorised activities;
- Recording and regular maintenance of IT Assets
- Data storage and transmission, and incident management.

Any information asset stored or transmitted using Parliament IT infrastructure may be monitored for security purposes.

The Information Technology Subdivision shall perform inquiries for all suspected or known threat activity through established standard incident management protocols. Where possible, the Information Technology Subdivision may provide insights and recommendations in the spirit of correcting or improving the security posture.

2.11 Roles and Responsibilities

STAKEHOLDER	ROLES AND RESPONSIBILITIES
Presiding officers	<ul style="list-style-type: none"> • Approve this policy on recommendation by their respective Secretaries, who have authority over the financial and administrative matters of Parliament.
Members and their staff	<ul style="list-style-type: none"> • Safeguard their IT assets and Parliament's information assets in their custody; • Manage their information assets with the appropriate security handling requirements; • Request an assessment prior to the procurement or acceptance of donations of IT assets; • Purchase only authorised IT assets; • Report any incident to Information Technology Subdivision as soon as possible which shall include but not limited to the loss of Parliament IT assets, or potential breaches in IT security; • Ensure that third parties under their control who are performing work that may affect IT security, are competent in terms of education, training and experience, and; • Ensure that third parties under their control are aware of this policy, their responsibilities, and the implications of non-compliance.

Head of the IT Subdivision	<ul style="list-style-type: none"> • Providing IT security advice and support, where possible, to Members, their staff and the Secretariat; • Taking decisions concerning all IT assets to be used on Parliament's IT infrastructure; • Ensuring that the IT security program complies with applicable laws and other Parliament approved policies; • Implementing, operating, maintaining and monitoring IT security safeguards; • Developing and maintaining formal and approved IT security policies, standards, strategies, and procedures that are responsive to the security environment; • Developing and maintaining IT security incident handling processes and procedures; • Auditing, monitoring and performing inquiries on potential, imminent and actual IT security events or incidents and for leading the response and recovery; • Establishing and maintaining agreements with the Namibia Central Intelligence Services (NCIS) and other security organisations to request technical and operational support, as required; • Requesting funds to support IT security requirements; • Supporting continuous training and awareness for IT users with respect to threats, roles, responsibilities and obligations regarding IT security, and; • Reporting to the joint management committee on the status of IT security within Parliament.
Heads of Directorates	<ul style="list-style-type: none"> • Exercising due diligence in safeguarding the IT assets in their custody; • Acting as custodians of information assets when those assets are: <ul style="list-style-type: none"> ○ Under their control or the control of employees or third parties working under their authority; or ○ Created, stored, processed and transmitted on Parliament hardware and/or software under their control or the control of employees or third parties working under their authority; • Using only authorised IT assets for Parliament Administration business; • Reporting any incident, loss of IT assets or potential breaches in IT security to Information Technology Subdivision as soon as possible; • Ensuring that employees and contractors doing work under their control, which may affect IT security, are competent in terms of education, training or experience, and are aware of this policy, their contribution to IT security and the implication of non-compliance.
Secretariat	<ul style="list-style-type: none"> • Understanding this policy and their obligation to contribute to IT security; • Exercising due diligence when handling IT assets owned by or in the custody of Parliament; • Reporting any incident, loss of IT assets or potential breaches in IT security to Information Technology Subdivision as soon as possible. • Participate in IT Security awareness training

2.12 Risk management

The occurrence of IT security incidents, particularly those involving Parliament network and infrastructure, can have a significant impact on Parliament's operation. The ability to detect and respond to security incidents in a coordinated and consistent fashion is essential to the maintenance of Parliament operations and services, and to ensure the confidentiality, integrity and availability of Parliament information and IT assets.

If there is a suspected violation of this policy, a suspected security threat, a compromised system or performance issues with Parliament IT assets, Parliament may conduct an inquiry. Such an inquiry is based on the perceived threat level and aims to identify the threat, investigate its

severity, and take measures to resolve it, such as suspending or terminating access to the network.

2.12.1 Members of Parliament, and their staff

If a suspected security threat to Parliament IT asset is detected, the Information Technology Subdivision shall identify the threat, investigate its severity and take measures to resolve it. The Information Technology Subdivision shall seek consent prior to disclosing any information or data acquired because of an inquiry. Only information relating to the event (e.g., malware payload, method of compromise, actor) shall be disclosed to other investigative bodies as required, for the purposes of the investigation.

2.12.2 Secretariat

An inquiry into the use of Parliament's IT asset by an employee of the Parliament can be initiated by the Head of the Information Technology Subdivision or at the request of a member of Parliament's Management Committee.

PART: 3

3. Privacy and Confidentiality

3.1 Introduction

This part informs parliamentary users what personal data Parliament collects, how it is used, and the measures Parliament takes to keep it safe. The policy represents Parliament's commitment to privacy and includes provisions on processing of personal data related to Members, their staff and the Secretariat.

Parliament shall ensure that all personal data is handled in a secure way and it is only used as outlined in the sections below.

3.2 Scope

This part applies to all official and personal data processing activities under the responsibility of Parliament. All business units are accountable for ensuring that personal data is protected in all processes across its entire life cycle. All parliamentary users, service providers and stakeholders are responsible for compliance to this policy.

Collection of personal data by Parliament and the disclosure to Offices, Ministries and Agencies (OMAs) and related authorities shall only be carried out based on specific legal provisions. In all cases, this policy imposes restrictions necessary to meet requirements of relevant laws.

3.3 Protection of Information

Information can be defined in many ways such as public, private, confidential, personal, academic, etc. For the purposes of this policy, information is categorised as either Parliament information or individual information. Within Parliament information, there are specific definitions for certain types of information. The level of security required for various information categories depends on:

- Who created the information;
- Who is maintaining the information;
- The nature of the information; and,
- Whether there are specific laws or Parliament requirements, or guidelines associated with the use and distribution of such information.

3.4 Parliament Information

As an institution, the Parliament has many types of official information. In addition, directorates, and other units may have other types of internal business information specific to their areas.

Directors and unit heads are responsible for securing confidential and business information maintained on the systems under their authority as required. In addition, they are responsible for developing appropriate security practices for their internal business information.

Members, their staff and the Secretariat shall only access confidential or business information for which they are authorised and shall only use such information for the purposes for which it is intended.

Members, their staff and the Secretariat are required to comply with security practices established by Parliament to protect official and personal confidential information.

3.5 Individual Information

Individual information includes official, research, personal and business correspondence, and other records created and managed by individual Members, their staff or the Secretariat. As creators and managers of this information, individuals are responsible for securing and protecting such information.

Individual information should be protected based on the level of risk associated with its loss or misuse. The Information Technology Subdivision may assist individuals by offering services including secure storage of files with systematic copying of data and/or archiving. Nonetheless, Members, their staff and the Secretariat are ultimately responsible for securing their own information and should take action to assure their individual data is protected to the level they deem adequate.

3.6 Purposeful Use

Personal data may be collected only for specific, explicit and legitimate purposes and may not be further processed contrary to such intended purpose. Business process owners (in consultation, where necessary, with the directorate responsible for legal services) shall define and document data processing purposes. Changes of purpose are permissible only with the consent of the individual or if permitted by law. Based on the defined and documented purposes, business process owners shall motivate the personal data records/items necessarily processed to serve those purposes.

3.7 Reduced Data Retention

The longer personal data is retained, the higher the risk of accidental disclosure, loss, theft and/or information growing stale. At Parliament, personal data is retained only for the minimum amount of time necessary to support the business purpose or to meet legal requirements.

Any personal data kept by Parliament shall be managed in accordance to relevant internal retention policies. An expiry date shall be set and stored together with such personal data. Retention expiration triggers are connected to a specific phase, for example, when collecting the personal data or when closing a record. The retention periods are implemented in all systems, including backups and third-party environments.

3.8 Confidentiality and Authorisation

Only the authorised staff of the Secretariat, who are obligated to observe the requirements regarding data confidentiality, can be involved in the processing of personal data. They are prohibited from using such data for their own private purposes, to transfer personal data to unauthorised parties or to make it accessible in any other improper way to unauthorised people. Within this context, "unauthorised" also means the use of personal data by employees in so far as they are not required to have access to the respective personal data to fulfil their duties. The confidentiality obligation survives termination of the employment relationship.

3.9 Roles and Responsibilities

The responsibility for adherence to this part lies with the Management who have the following roles and responsibilities:

- Each house of Parliament shall have a staff assigned as a Privacy Officer, that revises and executes the privacy management program, and reports to the Management committee.
- The legal department safeguards compliance with relevant laws and regulations.

- The Human Resource Department shall proactively protect employees' privacy and execute the relevant sections of the privacy management program.
- The Head of Information Technology Subdivision is responsible for the application of adequate security controls and mitigating measures, as outlined in the IT Security Policy.

Every business process in which personal data is processed falls under the delegated responsibility of the relevant mandated business process owner.

PART :4

4. General Provision

4.1 Non-compliance

Members, their staff and the Secretariat are responsible for their own actions. In the event of non-compliance, the Head of the Information Technology Subdivision shall notify the relevant Member, staff or the employee of the Secretariat and shall endeavour to resolve the situation.

In the event that a Member fails to comply, the Head of the Information Technology Subdivision and or the Secretaries may discuss the issue with the Speaker or the Chairperson. In a situation involving a serious breach in security, the Head of the Information Technology Subdivision may suspend any or all access of the member to Parliament IT assets on the Parliament IT infrastructure. The matter shall also be reported to the Committee on Privileges of the National Assembly and Council, respectively.

In the event of non-compliance by an employee, the Head of the Information Technology Subdivision will notify the Member or manager of the employee.

Any employee who knowingly or unknowingly fails to comply with this policy may be subject to examination and/or appropriate disciplinary measures which may include suspension of access to Parliament IT assets. In addition, any employee whose actions compromise Parliament IT assets may be subject to criminal prosecution or civil action.

4.2 Review of the policy

The ICT revolution changes rapidly in the sense that the policy can become obsolete or outdated very quickly. It is therefore imperative that revisions and new clauses are added periodically to account for new developments in the field. This policy shall be reviewed every **three (3) years** or in case of a significant change in policies and regulation, that warrant this policy update.

The effective date of this policy will be the date of approval by the Two Houses.

Appendix A: Examples of acceptable and unacceptable Use of IT Resources

Examples of the acceptable personal use of IT resources include, but are not limited to:

- communicating with family, friends and others for personal needs.
- keeping up to date with news and current events.

Examples of the unacceptable use of IT resources include, but are not limited to:

- Wilfully or deliberately creating or sending sexually explicit, pornographic or obscene images; images, material or messages that are defamatory, discriminatory, derogatory, violent or harassing or intended to incite hatred; or images, information or material intended to annoy, harass or intimidate another person;
- Engaging in libel, defamation, harassment, intentional misrepresentation or fraud, or the publication of private information;
- Posting messages to newsgroups, blogs or chat areas that are likely to be considered by others to be abusive, offensive or inflammatory;
- Impersonating another person or forging or otherwise misrepresenting an identity;
- Intentionally altering the configuration of computing equipment or bypassing access restrictions or security features without prior authorisation from the respective Parliament IT management group;
- Intercepting electronic communications or security scanning;
- Knowingly introducing or spreading viruses or Trojans or any other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or personal information to any IT resource;
- Gaining illegal or unauthorised access to other computers or networks;
- Attempting to intercept, collect or store data about third parties without their knowledge or consent;
- Generating or forwarding chain letters or similar correspondence (which can often contain or lead to contamination);
- Knowingly causing a denial of service to or interference with any Parliament IT resource;
- Sending confidential or classified information without obtaining proper authorisation or taking appropriate security measures;
- Using Parliament's IT resources for personal gain or for commercial purposes unrelated to Parliament's business;
- Representing personal opinions as those of the Parliament;
- Wilfully violating copyright, licensing, trademarks or other intellectual property rights;
- Using Parliament's IT resources for any unlawful purpose;
- Using any or all assigned administrative privileges other than for their original business purpose;
- Lending or providing use of Parliament IT resources to unauthorised individuals.
- Allowing non- Parliament devices to connect through a personal mobile "hot spot," utilising a "proxy site," or attempting any other way of circumventing network safety measures.
- Peer-to-peer (computer-to-computer) file sharing or downloading.
- Unauthorised Virtual Private Network tunnelling.
- Gambling online;
- Playing real-time online games;
- Downloading and/or live-streaming personal movies and audio files (music)
- Using Parliament email accounts on personal sites or in forums; and
- Using personal electronic devices and computers connected to Parliament's IT infrastructure without prior authorisation from the Information Technology Subdivision.

