1.0 PUBLIC SECTOR INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY IN EKITI STATE

1.1 INTRODUCTION

The Public Sector Information and Communication Technology (ICT) Policy of Ekiti State outlines the guiding principles and strategies for the effective use and management of ICT within the state public sector. This policy aims to ensure the efficient delivery of public services, enhance transparency and accountability, promote innovation, and safeguard data and information.

1.2 OBJECTIVES

The objectives of the policy guide are to;

I. Enhance Service Delivery: ICT will be leveraged to improve the accessibility, quality, and efficiency of public services, ensuring seamless interaction between citizens and the government.

II. Foster Innovation: Encourage the adoption of emerging technologies, such as artificial intelligence, block-chain, and data analytics, to drive innovation and transform public service delivery.

III. Ensure Data Security and Privacy: Establish robust measures to safeguard public sector data, protect citizens' privacy, and comply with relevant data protection regulations.

IV. Promote Open Data: Facilitate the availability and accessibility of government data to promote transparency, accountability, and citizen engagement.

V. Build Digital Skills and Literacy: Promote digital literacy programs and provide training opportunities to equip public sector personnel and citizens with the necessary skills to effectively utilize ICT.

VI. Ensure Interoperability and Integration: Foster the integration of ICT systems and promote interoperability between different government departments to streamline processes and enhance efficiency.

1.3 GOVERNANCE AND COORDINATION

1.3.1 The Governance Framework of ICT Policy

There shall be an established ICT governing body which seats with the Ministry of Innovation, Science and Digital Economy and responsible for developing, implementing, and monitoring ICT policies, standards, and guidelines across the public sector and ministries in Ekiti State

1.3.2 Ministry of Innovation, Science and Digital Economy

The Ministry of Innovation, Science and Digital Economy will spearhead the supervision of robust ICT policies tailored to the specific needs and aspirations of Ekiti State. Implementing Cutting-Edge Technologies: As the vanguard of innovation, The Ministry will introduce and integrate cutting-edge technologies across various sectors of the public domain. This includes initiatives such as e-governance platforms, digital infrastructure enhancement, and fostering a culture of digital literacy and inclusion. Setting Standards and Guidelines: To ensure coherence and efficiency in ICT utilization, The Ministry will establish standards and guidelines governing the adoption and deployment of digital solutions within ministries and public sector entities. These standards will promote interoperability, security, and optimal utilization of resources. Monitoring and Evaluation: The Ministry will undertake rigorous monitoring and evaluation processes to track the efficacy of implemented ICT policies and initiatives. This involves assessing key performance indicators, identifying bottlenecks, and iterating strategies to enhance overall effectiveness.

Promoting Digital Economy: Recognizing the transformative potential of the digital economy, The Ministry of Innovation, Science and Digital Economy will actively promote initiatives aimed at fostering entrepreneurship, innovation, and digital skills development. By nurturing a conducive ecosystem for digital startups and SMEs.

1.3.3 BICT

The Ekiti Bureau of ICT serves as the primary governmental body responsible for overseeing the implementation, regulation, and advancement of Information and Communication Technology (ICT) initiatives within the state.

The head of the Bureau of ICT shall be (Permanent Secretary or Executive Secretary) appointed by the Governor from the Civil Service on the recommendation of the Ekiti State Head of Service. He/She must possess first degree in ICT Management or related Fields and also be a registered member of ICT professional associations in Nigeria (NCS, CPN, NITPCS). He or she must possess significant experience in Managing ICT projects and infrastructure with requisite qualification and not less than Five (5) years postgraduate cognate experience.

As regards the ICT policy, the roles of the Ekiti Bureau of ICT encompass several key functions essential for its successful implementation. These roles include:

I. **Policy Development:** The Bureau is responsible for formulating, reviewing, and updating the ICT policy in alignment with the state's strategic objectives and regulatory frameworks. This involves conducting research, gathering stakeholder input, and drafting policy documents that address current and emerging ICT challenges and opportunities.

II. **Policy Implementation**: The Bureau oversees the execution of the ICT policy by coordinating with relevant government departments, agencies, and stakeholders. It ensures that the policy directives are translated into actionable plans, projects, and initiatives that drive progress towards the defined goals and objectives.

III. **Compliance Monitoring**: The Bureau monitors compliance with the ICT policy to ensure that government entities adhere to its provisions and guidelines. This involves conducting regular audits, assessments, and evaluations to measure progress, identify areas of non-compliance, and recommend corrective actions as needed.

IV. **Capacity Building**: The Bureau facilitates capacity-building initiatives to enhance the ICT skills and capabilities of government officials, employees, and stakeholders. This includes organizing training programs, workshops, and seminars on ICT-related topics, such as cyber security, digital literacy, and emerging technologies.

V. **Stakeholder Engagement**: The Bureau engages with various stakeholders, including government agencies, industry partners, academia, and civil society organizations, to foster collaboration and synergy in ICT policy implementation. It facilitates dialogue, partnerships, and knowledge sharing to leverage collective expertise and resources for ICT development.

VI. **Strategic Planning:** The Bureau participates in strategic planning processes to align ICT initiatives with broader government priorities and development agendas. It contributes insights, analysis, and recommendations to ensure that ICT investments and interventions support the achievement of socio-economic objectives.

VII. **Innovation Promotion**: The Bureau promotes innovation and entrepreneurship in the ICT sector by supporting research, development, and commercialization activities. It identifies opportunities for innovation, facilitates technology adoption, and nurtures a conducive ecosystem for ICT startups and innovators.

VIII. **Performance Evaluation:** The Bureau conducts performance evaluations and impact assessments to measure the effectiveness and outcomes of ICT policy implementation. It collects data, analyzes trends, and generates reports to inform decision-making, policy refinement, and continuous improvement efforts.

1.3.4 ICT Cadre

The ICT Cadre of Ekiti State Public Service shall consist of specialized groups or categories of professionals in expertise and skills in areas of ICT such as ICT Infrastructure management, Software development, Network administration, Data analysis and Cyber security among others. Headed by the Permanent Secretary or Executive Secretary of the Bureau of ICT, the ICT Cadre shall ensure consistent and effective ICT management throughout the public sector and civil service in Ekiti state. Its responsibilities include; Policy developments, Policy implementation and Policy monitoring.

1.3.4.1 Policy Development

The governing body shall develop comprehensive ICT policies that address various aspects such as, security, data management, procurement, training, and access control of ICT in the state. These policies will provide a framework for the effective use and management of ICT resources.

These policies include:

I. Innovation Policies: The governing body shall develop policies on strategies to be implemented by the government on ways to foster and support innovations. These policies will include providing funding for research and development, protecting intellectual property rights, supporting startups and entrepreneurial ventures, promoting collaborations and partnerships, establishing an agile regulatory framework, investing in skills development and education, encouraging open data and open innovation, supporting innovation hubs and supporting high-growth sectors.

II. Security Policies: The governing body shall develop policies that outline security measures to protect ICT systems, networks, and data from unauthorized access, breaches, and cyber threats. These policies may include guidelines on user authentication, encryption, incident response, and security awareness training

III. Data Management Policies: Policies related to data management will cover aspects such as data privacy, data governance, data sharing, and data quality. They will define standards for data collection, storage, processing, and disposal, ensuring compliance with applicable regulations and best practices.

IV. Procurement Policies: The governing body shall establish policies for the procurement of ICT resources, equipment, software, and services. These policies will outline the procedures, criteria, and considerations for selecting vendors, ensuring value for money, and promoting fair and transparent procurement practices.

V. Training and Capacity Building Policies: Policies related to training and capacity building will focus on developing the skills and knowledge of public sector personnel in ICT. They will address training needs assessment, training program design, delivery methods, and evaluation to ensure a skilled workforce capable of effectively utilizing ICT resources.

VI. Access Control Policies: Access control policies will define guidelines for granting and managing user access to ICT systems, networks, and data. They will outline the roles and responsibilities of users, password policies, user authorization processes, and access restriction measures to protect sensitive information and ensure appropriate access levels.

VII. Policy Framework: The governing body shall establish a comprehensive policy framework that aligns with national and organizational strategies. This framework will provide a cohesive structure for all ICT policies, ensuring consistency, integration, and coherence among different policy areas.

VIII. Stakeholder Engagement: During the policy development process, the governance body shall engage relevant stakeholders, including government agencies, ICT experts, industry representatives, and civil society organizations. This engagement will help gather input, consider diverse perspectives, and ensure that policies reflect the needs and expectations of all stakeholders.

IX. Review and Updates: The g governing body shall establish a mechanism for regular review and updates of ICT policies. This will enable policies to remain current, responsive to evolving technology trends, and aligned with changing regulatory requirements.

1.3.4.2 Policy Implementation

The governing body shall oversee the implementation of ICT policies across the state public sector. It will work closely with ministries and departments of the state to ensure adherence to the policies and provide guidance on best practices. The Policy Implementation functions include:

I. Policy Communication: The governing body shall develop a communication strategy to effectively disseminate the ICT policies to all relevant stakeholders. It will ensure that ministries, departments, and personnel are aware of the policies, their objectives, and the expected outcomes. Clear and comprehensive communication channels will be established to address any queries or concerns related to policy implementation.

II. Guidance and Best Practices: The governing body shall provide guidance and support to ministries and departments on the best practices for implementing the ICT policies. It will offer expertise, resources, and tools to assist in policy implementation, ensuring that the policies are effectively translated into action.

III. Training and Capacity Building: The governing body shall identify training and capacity building needs related to policy implementation. It will develop training programs and initiatives to enhance the knowledge and skills of public sector personnel, enabling them to effectively implement the ICT policies. This may include training on specific tools, processes, or procedures required for policy compliance.

IV. Monitoring and Evaluation: The governing body shall establish mechanisms to monitor and evaluate the implementation of ICT policies. Regular assessments will be conducted to gauge the level of compliance, identify challenges, and measure the impact of the policies on improving ICT management and service delivery. The feedback obtained through monitoring and evaluation will be used to refine and improve policy implementation.

V. Oversight and Coordination: The governing body shall provide oversight and coordination to ensure consistent and uniform implementation of ICT policies across ministries and departments in the state. The governance body shall work closely with relevant stakeholders to promote understanding, compliance, and alignment with the established policies.

VI. Collaboration and Support: The governing body shall foster collaboration and cooperation among ministries, departments, and relevant stakeholders to facilitate policy implementation. It will establish forums for sharing experiences, challenges, and best practices, enabling cross-departmental learning and support. The governance body may also provide support in the form of technical assistance, guidance, or resources to overcome implementation barriers.

VII. Performance Management: The governing body shall establish performance indicators and metrics to assess the effectiveness of policy implementation. These indicators will help track progress, identify areas of improvement, and measure the impact of policy implementation on achieving desired outcomes. Regular reporting on policy implementation will be conducted to provide transparency and accountability.

1.3.4.3 Policy Monitoring

The governing body shall monitor the implementation and effectiveness of ICT policies in the state. It will establish mechanisms to assess compliance, identify areas for improvement, and address any issues or concerns related to policy implementation. The following are some of the policy monitoring.

I. Compliance Assessment: The governing body shall establish mechanisms to assess compliance with ICT policies across ministries, departments, and relevant stakeholders. It will develop criteria, benchmarks, and indicators to measure the extent to which the policies are being followed and implemented.

II. Monitoring Mechanisms: The governing body shall establish monitoring mechanisms to gather data and information related to policy implementation. This may include regular audits, reviews, surveys, or self-assessment processes to assess the level of compliance, identify gaps, and evaluate the effectiveness of policy implementation.

III. Performance Evaluation: The governing body shall evaluate the performance and outcomes of policy implementation. It will measure the impact of ICT policies on improving service delivery, enhancing efficiency, promoting innovation, and achieving the desired objectives. This evaluation may involve data analysis, performance indicators, and feedback from stakeholders.

IV. Identification of Areas for Improvement: Through monitoring activities, the governing body will identify areas where policy implementation can be improved. It will identify gaps, bottlenecks, or challenges in compliance and address them through targeted interventions, guidance, or capacity building initiatives.

V. Feedback and Communication: The governing body shall establish feedback mechanisms to gather inputs, concerns, and suggestions from stakeholders regarding policy implementation. It will ensure open channels of communication to address issues, clarify guidelines, and provide support to ministries, departments, and personnel.

VI. Reporting: The governing body shall prepare regular reports on the monitoring findings, compliance status, and outcomes of policy implementation. These reports will provide transparency and accountability to stakeholders, enabling them to track progress, understand challenges, and make informed decisions related to policy improvement and adjustment.

VII. Continuous Improvement: The governing body shall use the monitoring results to drive continuous improvement of ICT policies and their implementation. It will analyze the monitoring data, identify lessons learned, and incorporate feedback to refine policies, guidelines, and processes for better governance and outcomes.

VIII. Remedial Actions: If non-compliance or issues are identified during monitoring, the

governing body will take appropriate remedial actions. This may involve providing guidance, additional training, or support to enhance compliance, addressing identified gaps, or revising policies and procedures as necessary.

1.3.5 Standards and Guidelines

The governing body shall develop and maintain ICT standards and guidelines to ensure consistency, interoperability, and security across the public sector in the state. These standards will cover areas such as infrastructure, data management, cyber-security, and procurement etc.

I. Infrastructure Standards: The governing body shall establish standards for ICT infrastructure, including hardware, software, networks, and systems. These standards will define the specifications, configurations, and requirements for infrastructure components to ensure compatibility, reliability, and scalability.

II. Data Management Standards: Standards related to data management will address various aspects such as data classification, storage, sharing, quality, and retention. These standards will outline best practices for managing and protecting data, ensuring consistency, accuracy, and availability across the public sector.

III. Cyber-security Standards: The governing body shall develop cyber-security standards to protect ICT systems and data from unauthorized access, breaches, and cyber threats. These standards will cover areas such as network security, access controls, encryption, incident response, and security awareness training.

IV. Interoperability Standards: Interoperability standards will focus on promoting seamless integration and data exchange among different ICT systems and applications used across the public sector. These standards will enable information sharing, collaboration, and interoperability between ministries, departments, and agencies.

V. Procurement Guidelines: The governing body shall develop guidelines for ICT procurement to ensure fair, transparent, and efficient procurement processes. These guidelines will outline the procurement procedures, evaluation criteria, vendor selection processes, and contract management practices for acquiring ICT products and services.

VI. Accessibility Standards: The governing body shall establish accessibility standards to ensure that ICT services and resources are accessible to all citizens, including those with disabilities. These standards will promote inclusive design, usability, and accessibility features in ICT systems, websites, and digital content.

VII. Compliance and Auditing: The governing body shall monitor compliance with ICT standards and guidelines across the public sector. It may conduct audits, assessments, or reviews to ensure adherence to the established standards and identify areas for improvement or corrective actions.

VIII. Updates and Maintenance: The governing body shall regularly review and update the ICT standards and guidelines to keep pace with evolving technology trends, regulatory requirements, and emerging cyber-security threats. It will ensure that the standards remain relevant, effective, and aligned with the strategic objectives of the public sector.

1.3.6 Capacity Building

The governing body shall play a key role in developing and implementing training programs to enhance the digital skills and ICT literacy of public sector personnel of the state. The Bureau of ICT shall oversee the capacity building of personnel. The bureau will identify training needs, provide guidance on training resources, and promote a culture of continuous learning.

1 Training Needs Assessment: The governing body through its bureau shall conduct a thorough assessment of the training needs of public sector personnel in relation to ICT.

This assessment will identify the existing skills gaps, areas for improvement, and emerging ICT trends that require attention. The findings of the assessment will inform the development of targeted training programs.

I. Training Program Development: Based on the training needs assessment, the governing body through its subcommittee shall develop comprehensive training programs that address the identified gaps and objectives. These programs may cover a range of topics, including basic ICT literacy, specialized software training, cybersecurity awareness, data management, and emerging technologies. The programs will be designed to cater to personnel at different levels of ICT proficiency.

II. Training Resources and Materials: The subcommittee shall provide guidance and access to training resources and materials that support the training programs. This may include online courses, training modules, videos, reference materials, and best practice guides. The resources will be curated to ensure they are up-to-date, relevant, and aligned with the training objectives.

III. Training Delivery: The subcommittee shall oversee the delivery of training programs, which may include a combination of in-person workshops, online courses, webinars, and mentoring. It will collaborate with relevant training providers, both internal and external, to ensure that the training delivery methods are effective and accessible to all personnel.

IV. Continuous Learning Culture: The subcommittee shall promote a culture of continuous learning and professional development within the public sector. It will encourage personnel to actively participate in training programs, pursue self-directed learning opportunities, and stay updated with evolving ICT trends. The governance body may also organize knowledge-sharing sessions, communities of practice, or learning forums to facilitate peer-to-peer learning and knowledge exchange.

V. Performance Evaluation: The subcommittee shall evaluate the effectiveness of the training programs and assess their impact on improving the digital skills and ICT literacy of public sector personnel. Feedback from participants, assessments, and performance indicators will be used to measure the outcomes and make necessary adjustments to the training programs.

VI. Collaboration with Stakeholders: The subcommittee shall collaborate with relevant stakeholders, including training institutions, industry experts, and professional associations, to leverage their expertise and resources in capacity building efforts. This collaboration will ensure that the training programs are comprehensive, relevant, and aligned with industry standards and best practices.

VII. Monitoring and Evaluation: The subcommittee shall monitor the implementation of the training programs and evaluate their effectiveness in enhancing the digital skills and ICT literacy of public sector personnel. It will track participation rates, gather feedback from participants, and measure the impact of the training on job performance and service delivery.

1.3.7 Evaluation and Reporting

The Ministry of Innovation, Science and Digital Economy through The Bureau of ICT shall establish mechanisms for evaluating the effectiveness of ICT policies and initiatives. It will collect and analyze data, monitor key performance indicators, and prepare regular reports on the progress and impact of ICT implementation in the public sector. This include;

I. Evaluation Framework: The committee shall develop an evaluation framework that outlines the key areas to be assessed and the criteria for evaluating the effectiveness of ICT policies and initiatives. This framework will serve as a guide for conducting evaluations and measuring the desired outcomes and impacts.

II. Data Collection and Analysis: The committee shall establish mechanisms to collect relevant data on ICT implementation and its impact within the public sector. This may include data on service delivery, efficiency gains, cost savings, user satisfaction, and other relevant metrics. The collected data will be analyzed to assess the effectiveness of ICT policies and initiatives and identify areas for improvement.

III. Key Performance Indicators (KPIs): The committee shall define and monitor key performance indicators that align with the objectives of ICT policies and initiatives. These KPIs will provide measurable targets and benchmarks for evaluating progress and success. Examples of KPIs may include the percentage of services delivered digitally, reduction in response times, cost savings through ICT implementation, or user satisfaction ratings.

IV. Impact Assessment The committee shall assess the impact of ICT implementation on the public sector and its stakeholders. This assessment will evaluate the extent to which ICT initiatives have achieved their intended outcomes, such as improved service delivery, enhanced transparency, increased efficiency, or better access to information. It may involve surveys, case studies, user feedback, and other evaluation methods.

V. Reporting: The committee shall prepare regular reports on the progress and impact of ICT implementation within the public sector. These reports will provide an overview of the achievements, challenges, and future plans related to ICT policies and initiatives. The reports will be shared with relevant stakeholders, including government officials, policymakers, and the public, to ensure transparency and accountability.

1.4 GUIDELINES/USE OF ICT ASSETS IN PUBLIC SECTOR

The use of Information and Communication Technology (ICT) equipment is an integral part of operations within the public sector in Ekiti State. ICT equipment, such as computers, laptops, mobile devices, and networking devices, plays a crucial role in facilitating the delivery of public services, enhancing efficiency, and promoting effective communication and collaboration. To ensure the responsible and optimal use of ICT equipment, guidelines are put in place to outline the expectations, best practices, and security measures that public sector personnel must follow. These guidelines are designed to promote the efficient utilization of ICT resources, protect sensitive data and information, and maintain the integrity of the public sector's ICT infrastructure. They provide a framework for personnel to understand their roles and responsibilities when using ICT equipment, emphasizing the importance of compliance with organizational policies and legal regulations.

By adhering to these guidelines, public sector personnel contribute to the overall effectiveness of ICT operations and help create a secure and productive digital environment. The guidelines cover various aspects, including authorized use, proper handling, security measures, software compliance, data protection, assets management/inventory, and reporting security incidents.

1.4.1 Authorized Use

I. All ICT equipment provided by the Ekiti state government to the public sector shall be used solely for official purposes.

II. personnel are expected to utilize the equipment in a manner that aligns with their job responsibilities and contributes to the effective delivery of public services.

III. personnel should refrain from using the ICT equipment for personal activities, unless explicitly permitted by organizational policies or relevant guidelines. Personal use of ICT equipment can lead to a misuse of resources, compromise network security, and adversely affect productivity and has a penalty.

IV. To support authorized use, personnel shall be required to sign an acknowledgment or agreement that they understand and will abide by the policies and guidelines governing the use of ICT equipment in the state.

1.4.2 Equipment Use Guidelines:

I. ICT equipment should be handled with care to ensure its longevity and functionality.

II. personnel should follow manufacturer guidelines for setup, usage, and maintenance. Any damage or malfunction should be reported promptly to the designated IT support or technical personnel.

III. When setting up ICT equipment, personnel should carefully follow the provided instructions to ensure proper installation and configuration. This includes correctly connecting cables, plugging in power sources, and configuring software settings as per the manufacturer's recommendations.

IV. During regular usage, personnel should handle ICT equipment with care, avoiding rough or careless handling that could lead to physical damage. They should be mindful of their surroundings and keep the equipment in a secure and stable location to minimize the risk of accidental falls, spills, or other incidents that may cause harm.

V. personnel should perform routine tasks, such as cleaning keyboards and screens, removing dust from ventilation areas, and periodically checking for loose cables or connections. Any signs of damage, malfunction, or abnormal behavior should be reported promptly to the designated IT support or technical personnel for further assessment and resolution.

1.4.3 Security Measures

personnel/User must strictly adhere to established security measures to protect sensitive data and information from unauthorized access, loss, or misuse. By following these security measures, personnel contribute to maintaining the confidentiality, integrity, and availability of valuable resources within the public sector.

I. Strong Passwords: Users/personnel should create strong and unique passwords for accessing ICT equipment and related accounts. Passwords should be a combination of uppercase and lowercase letters, numbers, and special characters. It is essential to avoid using easily guessable or commonly used passwords and to change them periodically.

II. Device Locking: When not actively using ICT equipment, users/personnel should lock their devices or enable password-protected screensavers to prevent unauthorized access. This practice is particularly important when leaving devices unattended in shared work spaces or public areas.

III. Unauthorized Software Installations: Users must refrain from installing unauthorized software or applications on ICT equipment. Only approved and licensed software should be installed, as unauthorized installations can introduce security vulnerabilities and compromise the integrity of the system.

IV. Access Control: Users should only access and share confidential or sensitive information based on the principle of least privilege. This means that access should be granted only to authorized individuals who require it to perform their job duties.

V. Data Encryption: Confidential or sensitive data stored on ICT equipment, such as laptops or portable storage devices, should be encrypted to prevent unauthorized access in the event of loss or theft. Encryption helps protect the confidentiality of the data, even if the physical device is compromised.

VI. Phishing Awareness: Users should exercise caution when handling emails, attachments, or links from unknown or suspicious sources. They should be vigilant in identifying and reporting phishing attempts or suspicious activities to the designated IT support or security personnel.

VII. Data Backup: Regular backup of data stored on ICT equipment is crucial to ensure its availability and to protect against data loss in case of hardware failure or other unforeseen events. Users should follow the organization's data backup procedures to ensure important information is adequately preserved.

VIII. Physical Security: ICT equipment should be stored in secure locations, and access to sensitive areas should be restricted to authorized personnel only. Personnel should report any suspicious or unauthorized individuals attempting to access ICT equipment or sensitive areas to the appropriate security personnel.

Note: Any access to confidential information should follow the established authorization processes and be in compliance with relevant laws and regulations.

1.4.3.1 Breach/ Incident Reporting

This section outlines the procedures and guidelines for reporting and addressing incidents and breaches within the organization. It aims to promote a culture of security awareness, timely reporting, and effective response to safeguard sensitive information and mitigate potential risks. The policy emphasizes confidentiality, non-retaliation, and adherence to legal and regulatory requirements.

1.4.3.2 Reporting Channels and Procedures

Personnel members are to report any suspected or confirmed incidents or breaches promptly through designated reporting channels, such as the IT department, security team, incident response team, or a dedicated reporting hotline or email. Personnel members should follow these step-by-step procedures to report incidents:

I. Identify the Incident: personnel should recognize any suspicious or unauthorized activity, data breach, security vulnerability, or any other incident that may pose a risk to the organization's information or systems.

II. Gather Information: personnel should collect as much relevant information as possible about the incident, including the date, time, location, individuals involved (if known), and any supporting evidence or documentation.

III. Contact the Designated Reporting Channel: personnel should report the incident promptly using the designated reporting channels established by the organization. This may include contacting the IT department, security team, incident response team, or using a dedicated reporting hotline or email.

IV. Provide Detailed Information: When reporting the incident, personnel should provide a detailed description of the event, including what occurred, how it was discovered, and any potential impact or risk to the organization.

V. Follow Reporting Instructions: personnel should follow any specific instructions provided by the designated reporting channel regarding the format or method of reporting. This may include using a specific incident reporting form, providing additional supporting documents, or following a specific reporting protocol.

VI. Maintain Confidentiality: personnel should keep the incident and any related information confidential, disclosing it only to authorized personnel involved in the investigation and response process.

1.4.3.3 Designated Reporting Channels

I. IT Department: personnel members should report incidents related to ICT systems, hardware, or software to the IT department.

II. Security Team: Incidents involving physical security, unauthorized access, or suspicious activities should be reported to the security team.

III. Reporting Hotline or Email: A dedicated reporting hotline or email address should be facilitated to report incidents.

1.4.3.4 Incident Report

When reporting an incident, personnel members should include the following information, if available:

I. Date and time of the incident.

II. Description of the incident, including what occurred and how it was discovered.

III. Any individuals involved or witnesses, if known.

IV. Supporting evidence or documentation, such as screenshots, logs, or other relevant materials.

V. Potential impact or risk to the organization's information, systems, or operations.

1.4.3.5 Confidentiality and Non-Retaliation

The Ministry of Innovation, Science and Digital Economy shall ensure the confidentiality of the identity of personnel members who report incidents, except where disclosure is required by law or regulation

I. Personnel members shall be assured that their report and the details provided will be handled with utmost confidentiality and used solely for the purpose of investigation and response.

II. Non-retaliation against personnel members who report incidents in good faith is strictly prohibited. The organization will take appropriate measures to prevent and address any form of retaliation, and individuals found to engage in retaliation will be subject to disciplinary action.

1.4.3.6 Compliance

Non-compliance with this policy, including retaliation against whistle blowers or failure to report incidents, may result in disciplinary action, up to and including termination of employment.

1.5 DATA MANAGEMENT AND SECURITY POLICY

This section aims to ensure the proper handling, storage, and protection of data within the Ekiti State public sector. This section establishes guidelines and procedures for data management, access control, data privacy, and security measures to safeguard sensitive information and promote responsible data practices.

1.5.1 Data Handling and Storage

Personnel members must adhere to proper data handling procedures, including collecting, storing, transmitting, and disposing of data. This includes ensuring data accuracy, maintaining data integrity, and avoiding unauthorized disclosure or modification.

1.5.1.1 Data Collection:

I. Personnel members are only allowed to collect data only for legitimate and authorized purposes, ensuring compliance with applicable laws and regulations.

II. Data collected should be accurately and completely stored, using reliable and approved sources.

III. Unnecessary or excessive data collection should be avoided.

1.5.1.2 Data Storage:

I. Data should be stored securely in designated systems or databases with appropriate access controls.

II. Proper categorization and classification of data should be implemented based on sensitivity and confidentiality levels.

III. Regular backups of data should be performed to prevent loss or corruption.

1.5.1.3 Data Transmission:

I. When transmitting data, personnel members should use secure channels and encryption methods to protect data integrity and confidentiality.

II. Data transmission should be limited to authorized recipients or systems.

III. Personnel members should exercise caution when sharing data through email, file transfers, or other electronic means, ensuring proper security measures are in place.

1.5.1.4 Data Accuracy and Integrity:

I. Personnel members are responsible for ensuring the accuracy and integrity of the data they handle.

II. Any errors, discrepancies, or inconsistencies in the data should be promptly reported to the designated personnel or data custodians.

III. Proper validation and verification processes should be followed to maintain data accuracy.

1.5.1.5 Data Access and Authorization:

1. Access to data should be granted on a need-to-know basis, following the principle of least privilege.
II. Personnel members should not access or retrieve data that is beyond their authorized scope or job responsibilities.

III. Any unauthorized attempts to access or modify data should be reported immediately.

1.5.1.6 Data Disposal:

I. When data is no longer needed or reaches the end of its retention period, proper disposal methods should be followed.

II. Confidential or sensitive data should be securely deleted or destroyed using approved methods to prevent unauthorized access or recovery.

1.5.1.7 Data Privacy:

I. Personnel members should respect and uphold data privacy principles, including obtaining appropriate consent when required.

II. Personal and sensitive data should be handled with utmost care, ensuring compliance with applicable data protection laws and regulations.

1.5.1.8 Reporting Data Incidents:

I. Any incidents or breaches related to data handling should be promptly reported through the designated reporting channels or incident response procedures.

II. Personnel members should cooperate with the incident response team and provide necessary information for investigation and resolution.

1.5.2 Data Storage and Retention

Data should be stored in secure and designated storage systems. Appropriate retention periods will be defined for different types of data, and regular data backups will be performed to prevent data loss.

1.5.2.1 Secure Storage Systems:

I. Data shall be stored in secure and designated storage systems that provide appropriate levels of physical and logical security.

II. Access controls shall be implemented to restrict unauthorized access to stored data.

III. Security measures such as encryption, firewalls, and intrusion detection systems should be in place to protect data from unauthorized access or breaches.

1.5.2.2 Data Classification and Categorization

I. Data shall be categorized based on its sensitivity and criticality.

II. Different levels of security controls and access privileges shall be applied to each category of data.

III. Data classification shall align with the organization's data classification framework or standards.

1.5.2.3 Retention Periods

I. Appropriate retention periods shall be defined for different types of data, considering legal and regulatory requirements, business needs, and best practices.

II. Retention periods shall be regularly reviewed and updated to ensure compliance with changing regulations and organizational requirements.

III. Retention schedules shall clearly specify the duration for which data should be retained and the criteria for its disposal.

1.5.2.4 Data Backup and Recovery:

I. Regular data backups should be performed to ensure data integrity and availability.

II. Backup procedures should be established, including frequency, methods, and locations of backups.

III. Backup data should be securely stored and tested periodically to verify its integrity and effectiveness in restoring data.

1.5.2.5 Data Archiving

The sub-committee on archiving and digitization shall be in charge of both hardcopy and softcopy of data/ information archiving. All data from every ministry/MDAs shall be due for storage every 6 months. The archived data/information shall be stored on the universal portal for the state government.

I. Archiving mechanisms should be implemented to store data that is no longer actively used but may be required for legal, historical, or reference purposes.

II. Archived data should be securely stored and protected against unauthorized access or tampering.

III. Archiving procedures should define the criteria for moving data to the archive and the process for retrieving archived data when needed.

1.5.2.6 Data Disposal

Data due for disposal shall be determined by the ICT Professionals. The sub-committee on archiving and digitization shall give the ICT Professionals recommendations on data/information due for disposal.

I. When data reaches the end of its retention period or is no longer required, proper data disposal procedures should be followed.

II. Data disposal methods should ensure permanent and secure erasure or destruction of data to prevent unauthorized access or recovery.

III. Disposal processes should comply with relevant laws, regulations, and environmental considerations.

1.5.2.7 Data Privacy and Confidentiality

I. Compliance with Data Protection Laws: The public sector personnel shall comply with relevant data protection laws and regulations made by the governing body, ensuring the privacy and confidentiality of personal and sensitive information.

II. Data Sharing and Disclosure: Data sharing and disclosure shall be limited to authorized individuals or entities based on defined criteria, legal requirements, or consent.

III. Non-Disclosure Agreements: personnel members with access to sensitive data shall be required to sign non-disclosure agreements to ensure the confidentiality and protection of such information.

IV. Breach: any breach from the agreement in part (c) shall be taken up to the authority and shall be penalized.

1.6 TRAINING AND PERSONNEL DEVELOPMENT

The section states the process and procedures in which public servants/ civil servants should be trained in the use of ICT to enhance their skills and competencies in the use of ICT tools. The ICT Professionals shall be in charge of the training and personnel development. This policy aims to ensure that all personnel members have the necessary knowledge and proficiency to effectively and securely utilize ICT tools for their job responsibilities. The ICT Professionals shall be responsible for (and coordination of) the following functions,

1.6.1 Training Needs Assessment:

I. The Bureau of ICT shall conduct regular training needs assessments to identify the specific ICT training requirements of personnel members.

II. The assessments will consider the personnel members' roles, responsibilities, skill levels, and the evolving ICT landscape.

III. The identified training needs will serve as a basis for designing and delivering relevant ICT training programs.

1.6.2 Training Program Design and Delivery:

I. The Bureau of ICT with stakeholders of the civil service shall develop a comprehensive training program that covers various aspects of ICT tools and their application in the workplace.

II. Training programs will be designed to be interactive, engaging, and tailored to the diverse learning needs of personnel members.

III. Different delivery methods will be employed, including instructor-led sessions, online courses, workshops, and self-paced learning modules.

IV. Training materials, resources, and support systems will be provided to facilitate effective learning and skill development.

1.6.3 Training Evaluation:

The effectiveness of the ICT training programs will be evaluated through participant feedback, assessments, and performance indicators. Evaluation results will be used to continuously improve the training programs and address any identified gaps or areas for enhancement.

1.7 DISPOSAL OF EQUIPMENTS

This section outlines the guidelines for the proper disposal of ICT equipment in the public sector. It ensures that the disposal process is conducted in an environmentally responsible and secure manner while protecting sensitive data and complying with applicable laws and regulations. Before equipment could be rendered useless or irrelevant, The Ministry of Innovation, Science and Digital Economy must verify that such equipment is irrelevant and non-repairable. No ministry or department shall dispose equipment without the approval of The Ministry.

1.7.1 Disposal Procedures

1.7.1.1 Inventory and Assessment

I. Maintain an up-to-date inventory of all ICT equipment.

II. Regularly assess equipment for disposal based on its age, functionality, and technological obsolescence.

1.7.1.2 Data Erasure

I. Prior to disposal, ensure that all data stored on the equipment is securely and irreversibly erased.

II. Use approved data wiping or destruction methods to prevent unauthorized access to sensitive information.

1.7.1.3 Environmentally Responsible Disposal

I. Dispose of equipment in an environmentally responsible manner, following applicable waste management and recycling regulations.

II. Collaborate with certified e-waste recycling vendors or organizations to handle the disposal of electronic equipment.

1.7.1.4 Secure Disposal:

I. Maintain the physical security of equipment during the disposal process to prevent theft or unauthorized access to data.

II. Ensure that equipment is securely transported to disposal or recycling facilities to mitigate the risk of data breaches.

1.7.1.5 Documentation: Maintain records of all disposed equipment, including serial numbers, disposal dates, and disposal methods.

I. Retain relevant disposal documentation for auditing and compliance purposes.

1.7.2 Equipment Disposal Team

1.7.2.1 ICT Department:

I. Coordinate and oversee the disposal process, including data erasure and coordination with recycling vendors.

II. Ensure compliance with data protection and privacy regulations during the disposal of equipment.

1.7.2.2 Asset Management Team:

I. Maintain accurate records of ICT equipment inventory and manage the disposal process.

II. Collaborate with the ICT department to identify equipment for disposal.

1.7.2.3 Security Team:

I. Ensure the physical security of equipment during the disposal process.

II. Monitor and report any breaches or incidents related to equipment disposal.

1.7.2.4 Procurement Department:

Coordinate with the ICT department to ensure proper disposal procedures are followed when acquiring new equipment. (SEE SECTION 1; 7.0)

Note: Compliance

All personnel members are required to comply with this policy and adhere to the established procedures for the disposal of ICT equipment. Non-compliance may result in disciplinary actions as per organizational policies.

1.8 PROCUREMENTS OF ASSETS

This section highlights the guidelines for the procurement of assets, specifically ICT equipment, in the public sector. It ensures a transparent, efficient, and cost-effective procurement process that meets the needs of the organization while promoting fairness, competition, and compliance with applicable laws and regulations.

1.8.1 Objective

The procurement process outlined within this ICT Policy aims to ensure the transparent, efficient, and accountable acquisition of ICT goods and services for Ekiti State. This process is guided by the Ministry of Innovation, Science, and Digital Economy in collaboration with the Bureau of Procurement, with the overarching goal of optimizing resource utilization and fostering innovation and technological advancement.

1.8.2 Principles

The procurement process shall adhere to the following principles:

I. ***Transparency***: All procurement activities shall be conducted openly and transparently, allowing for fair competition and equitable access to opportunities.

II. ***Efficiency***: Procurement procedures shall be streamlined to minimize delays and ensure timely delivery of ICT goods and services.

III. ***Compliance***: All procurement activities shall comply with relevant laws, regulations, and ethical standards to uphold integrity and accountability.

IV. ***Value for Money***: The procurement process shall prioritize value for money, seeking to maximize the quality and benefits obtained from ICT investments.

1.8.3 Procedures:

I. ***Needs Assessment***: The ICT requirements of Ekiti State shall be assessed to identify the specific goods and services needed to support government operations and initiatives.

II. ***Budget Allocation***: The Bureau of Procurement, in consultation with The Ministry of Innovation, Science and Digital Economy, shall allocate budgets for ICT procurement activities based on identified needs and available resources.

III. ***Tendering Process***: ICT goods and services shall be procured through competitive bidding processes, including open tendering, request for proposals (RFPs), or request for quotations (RFQs), as appropriate.

IV. ***Evaluation and Selection***: Bids received shall be evaluated based on predetermined criteria, such as technical specifications, price, quality, and compliance with requirements. The selection of suppliers or service providers shall be conducted impartially and in accordance with established evaluation procedures.

V. ***Contract Award***: Contracts shall be awarded to successful bidders, detailing the terms, conditions, and deliverables of the procurement agreement.

VI. ***Monitoring***: The Ministry of Innovation, Science and Digital Economy and the Bureau of Procurement shall monitor the implementation of procurement contracts to ensure compliance with agreed-upon terms and performance standards.

VII. ***Review and Improvement***: The procurement process shall be periodically reviewed and evaluated to identify areas for improvement and enhance effectiveness and efficiency.

1.9 Collaboration and Oversight:

The Ministry of Innovation, Science and Digital Economy and the Bureau of Procurement shall collaborate closely to oversee the implementation of the procurement process, ensuring alignment with the objectives and principles of this ICT Policy. Oversight mechanisms shall be established to monitor compliance, address challenges, and promote continuous improvement in procurement practices.

2.0 ICT AND ENTREPRENEURSHIP

2.1 Introduction

The Government of Ekiti State recognizes the vital role of Information Communications and Technology (ICT) in fostering entrepreneurship and marketing. This policy framework aims to provide guidance and support for the development of a vibrant entrepreneurial ecosystem that leverages ICT for economic growth, job creation, and innovation. An entrepreneur is an individual who identifies opportunities in the marketplace, allocates resources, and creates value. Entrepreneurship is the act of being an entrepreneur which implies the capacity and willingness to undertake conception, organization, and management of a productive new venture, accepting all attendant risks and seeking profit as a reward. In economics, entrepreneurship is sometimes considered a factor of production, at par with land, labor, natural resources, and capital.

2.2 Objectives:

I. Foster a culture of entrepreneurship: Encourage individuals to embrace an entrepreneurial mindset, leveraging ICT as a catalyst for business innovation and growth.

II. Promote digital literacy and skills development: Ensure that individuals have the necessary ICT skills to succeed in entrepreneurial endeavors and adapt to the digital economy.

III. Facilitate access to resources and support: Provide entrepreneurs with access to funding, mentorship, networking, and business development services, enabled by ICT platforms.

IV. Foster innovation and technology adoption: Encourage the use of emerging technologies and digital solutions to drive innovation in entrepreneurship and enhance competitiveness.

V. Enhance regulatory and policy frameworks: Develop supportive policies, regulations, and incentives that create an enabling environment for ICT- driven entrepreneurship.

2.2.1 Strategies

I. Entrepreneurship Education:

a. Integrate entrepreneurship education at all levels of the educational system, emphasizing the use of ICT tools, business planning, and digital marketing.

b. Collaborate with educational institutions and industry experts to develop entrepreneurship curricula and provide training to teachers.

II. Access to Finance:

a. Establish a dedicated fund for ICT-driven startups and entrepreneurs, providing access to capital, seed funding, and venture capital investment.
b. Facilitate partnerships between financial institutions, angel investors, and startups to enhance access to financing options.

III. Incubation and Acceleration Programs:

i. Establish incubation centers and innovation hubs equipped with ICT infrastructure, mentorship programs, and business development support.
ii. Provide mentorship, coaching, and networking opportunities to entrepreneurs through specialized accelerator programs.

IV. Digital Skills Development:

a. Offer training programs, workshops, and online courses to enhance digital literacy and ICT skills for entrepreneurs and aspiring business owners.
b. Collaborate with industry experts and organizations to provide specialized training in areas such as digital marketing, e-commerce, and data analytics.

V. Technology Adoption and Innovation:

a. Encourage the adoption of emerging technologies, such as artificial intelligence, blockchain, and Internet of Things (IoT), in entrepreneurial ventures.
b. Facilitate technology exchange platforms, innovation challenges, and hackathons to spur collaboration, idea generation, and prototyping.

VI. Policy and Regulatory Support:

a. Review and update existing policies and regulations to create an enabling environment for ICT driven entrepreneurship, including simplified business registration processes and tax incentives.
b. Establish mechanisms for regular consultation with stakeholders to identify and address policy barriers and challenges.

VII. Networking and Collaboration:

a. Organize entrepreneurship conferences, networking events, and knowledge-sharing platforms to foster collaboration and idea exchange among entrepreneurs.
b. Promote public-private partnerships to leverage industry expertise, resources, and networks to support entrepreneurs.

VIII. Digital Marketing and E-commerce:

a. Provide training and support in digital marketing strategies, social media management, and e-commerce platforms to enhance online visibility and market reach for entrepreneurs.
b. Foster collaborations with e-commerce platforms and online marketplaces to facilitate the expansion of entrepreneurial ventures into the digital marketplace.

2.2.2 Action Plan

I. Establish an Implementation Committee: Form a dedicated committee comprising representatives from relevant government agencies, educational institutions, industry associations, and entrepreneurship support organizations to oversee the implementation of the policy framework.
II. Develop a Detailed Roadmap: Create a comprehensive roadmap that outlines specific activities, timelines, responsible entities, and key milestones for each objective and strategy identified in the policy framework.
III. Allocate Resources: Ensure adequate financial resources are allocated to support the implementation of the action plan, including funding for training programs, infrastructure development, mentorship initiatives, and support services.
IV. Stakeholder Engagement: Engage and collaborate with stakeholders, including entrepreneurs, educational institutions, industry experts, and support organizations, to gather input, build partnerships, and facilitate the implementation process.
V. Monitor Progress: Regularly track and monitor the progress of each activity and initiative outlined in the action plan to ensure timely execution and identify any bottlenecks or challenges.
VI. Review and Adjust: Conduct periodic reviews of the action plan to assess its effectiveness and make necessary adjustments based on emerging trends, feedback from stakeholders, and evaluation results.

2.2.3 Resource Allocation

I. Financial Resources: Allocate a dedicated budget to support the implementation of the policy framework, ensuring sufficient funding for training programs, infrastructure development, incubation centers, mentorship programs, and other support services.
II. Human Resources: Assign qualified personnel within relevant government agencies to oversee and coordinate the implementation of the policy framework. Provide training and capacity building opportunities to enhance their knowledge and skills in ICT and entrepreneurship.
III. Infrastructure Development: Allocate resources to establish and maintain ICT infrastructure, such as high-speed internet connectivity, technology hubs, incubation centers, and digital training facilities, to support entrepreneurs and facilitate their access to digital tools and resources.

2.2.4 Monitoring Mechanisms

I. Key Performance Indicators (KPIs): Define a set of measurable KPIs that align with the objectives of the policy framework, such as the number of startups supported, jobs created, digital skills training participants, and funding allocated.
II. Data Collection and Reporting: Establish a data collection and reporting system to gather relevant information on the progress and impact of initiatives implemented under the policy framework. Regularly analyze and report the data to monitor the effectiveness and identify areas for improvement.
III. Stakeholder Feedback: Solicit feedback from stakeholders, including entrepreneurs, mentors, and support organizations, through surveys, focus groups, and consultations. Use this feedback to evaluate the effectiveness of the implemented initiatives and make necessary adjustments.

2.2.5 Periodic Evaluation

I. Conduct Periodic Reviews: Conduct periodic evaluations to assess the overall effectiveness, impact, and alignment of the policy framework with the vision and objectives. Evaluate the progress made, identify successes, challenges, and areas for improvement.
II. Stakeholder Consultations: Engage stakeholders in the evaluation process to gather their perspectives, suggestions, and feedback on the implemented initiatives.
III. Policy Refinement: Based on the evaluation results and stakeholder feedback, refine and update the policy framework as needed to ensure its continuous relevance and effectiveness in supporting ICT integration and entrepreneurship.

2.2.6 Training and Capacity Building

The objective of the Training and Capacity Building Framework is to equip entrepreneurs and marketers in Ekiti State with the necessary knowledge, skills, and tools to effectively leverage ICT for marketing and entrepreneurship, thereby driving business growth, contributing to the state economy, and promoting market expansion.

2.2.6.1 Training Needs Assessment:

I. Conduct a comprehensive assessment of the training needs of entrepreneurs and marketers in Ekiti State, considering their existing knowledge, skills, and proficiency in utilizing ICT for marketing and entrepreneurship.
II. Identify specific areas where training and capacity building are required, such as digital marketing strategies, social media marketing, e-commerce platforms, data analytics, and emerging technologies.

2.2.6.2 Training Programs and Workshops:

I. Develop a curriculum and training modules that cover various aspects of ICT in marketing and entrepreneurship.
II. Offer both theoretical and practical training sessions that provide hands-on experience and case studies.
III. Collaborate with industry experts, digital marketing professionals, and ICT specialists to deliver high-quality training programs.
IV. Customize training programs to cater to the specific needs of different sectors, industries, and business sizes.

2.2.6.3 Training Delivery Methods

I. Conduct in-person training sessions at designated training centers or educational institutions in Ekiti State.
II. Utilize online platforms and e-learning modules to provide flexible and accessible training opportunities.
III. Organize webinars, workshops, and conferences to facilitate knowledge sharing, networking, and interactive learning experiences.
IV. Encourage participation in industry-specific forums, conferences, and events to expose entrepreneurs and marketers to the latest trends and best practices.

2.2.6.4 Training Content and Topics

I. Digital Marketing Fundamentals: Provide training on the core principles of digital marketing, including SEO, social media marketing, content marketing, email marketing, and online advertising.
II. E-commerce Strategies: Offer training on setting up and managing e-commerce platforms, optimizing product listings, implementing secure payment systems, and effective supply chain management.
III. Data Analytics and Insights: Provide training on data analytics tools, data interpretation, customer behavior analysis, and leveraging data to make informed business decisions.
IV. Emerging Technologies: Include training on emerging technologies such as AI, VR/AR, blockchain, and their applications in marketing and entrepreneurship.

2.2.6.5 Certification and Recognition

I. Introduce certification programs to recognize the achievement and competence of entrepreneurs and marketers who successfully complete the training programs.
II. Collaborate with relevant institutions and industry associations to establish accreditation standards and ensure the certifications are widely recognized.

2.2.6.6 Continuous Learning and Support

I. Encourage participants to engage in continuous learning through online resources, industry publications, and professional networks.
II. Establish a support system where entrepreneurs and marketers can seek guidance, mentorship, and technical assistance in utilizing ICT tools and strategies for their businesses.
III. Organize periodic refresher courses, advanced training sessions, and update training modules to keep entrepreneurs and marketers abreast of the latest ICT trends and advancements.

2.2.6.7 Monitoring and Evaluation

I. Regularly assess the effectiveness and impact of the training programs through participant feedback, performance evaluations, and case studies.
II. Gather insights from participants on the practical application of the acquired knowledge and skills in their businesses.
III. Use the feedback to make necessary improvements, update training content, and enhance the overall quality of the training programs.

2.3 INTERNET OF THINGS

2.3.1 Objective

This subsection aims to establish guidelines and regulations for the secure and effective utilization of Internet of Things (IoT) technologies within Ekiti State. The objective is to leverage IoT to enhance service delivery, improve efficiency, and promote innovation while ensuring the protection of privacy, data security, and infrastructure integrity.

2.3.2 Scope

This subsection applies to all government agencies, departments, and entities within Ekiti State that utilize or plan to implement IoT technologies. It encompasses the deployment, management, and monitoring of IoT devices and systems across various sectors and applications.

2.3.2.1 Regulatory Framework:

Standards Compliance: IoT implementations shall adhere to relevant international and national standards to ensure interoperability, reliability, and compatibility.

2.3.2.2 Data Privacy

Measures shall be implemented to safeguard the privacy of individuals' data collected and processed by IOT devices, adhering to data protection laws and regulations.

I. **Security Protocols**: Strong encryption, authentication, and access control mechanisms shall be implemented to protect IoT devices and networks from unauthorized access, manipulation, and cyber attacks.

II. **Environmental Considerations**: Sustainable practices shall be incorporated into IoT deployments to minimize energy consumption, waste generation, and environmental impact.

III. **Accessibility:** IoT solutions shall be designed to ensure accessibility and inclusivity for all users, including persons with disabilities, by adhering to accessibility standards and guidelines.

2.3.2.3 Implementation Guidelines:

I. **Risk Assessment:** Prior to deployment, a thorough risk assessment shall be conducted to identify potential security vulnerabilities, privacy risks, and compliance requirements associated with IoT projects.

II. **Vendor Evaluation:** Vendors and suppliers of IoT devices and services shall be vetted based on their adherence to security standards, data protection practices, and commitment to sustainability.

III. **Data Management:** Clear policies and procedures shall be established for the collection, storage, processing, and sharing of data generated by IoT devices, ensuring compliance with legal and regulatory requirements.

IV. **Life cycle Management:** IoT devices shall be managed throughout their lifecycle, including provisioning, monitoring, maintenance, and decommissioning, to ensure ongoing security and performance.

V **User Awareness:** Training and awareness programs shall be provided to stakeholders involved in IoT initiatives to educate them about security best practices, privacy considerations, and ethical use of IoT technologies.

2.3.3 Monitoring and Compliance:

Ongoing Monitoring: Regular monitoring and auditing of IoT systems and networks shall be conducted to detect and respond to security incidents, anomalies, and performance issues.

Compliance Audits: Periodic audits shall be conducted to assess compliance with IoT policies, standards, and regulations, with corrective actions taken as necessary to address identified gaps or non-compliance.

2.3.4 Conclusion

This IoT subsection of the ICT Policy for Ekiti State outlines the principles, guidelines, and procedures for the responsible and secure implementation of IoT technologies. By adhering to these provisions, Ekiti State aims to harness the potential of IoT to drive innovation, improve service delivery, and enhance the quality of life for its citizens, while safeguarding privacy, security, and sustainability considerations.

3.0 LAND AND SURVEY ICT POLICY

3.1 Introduction

The use of Information and Communication Technology (ICT) in land and survey management has become increasingly important in recent years. The integration of ICT in the land and survey sector has the potential to improve efficiency, accuracy, and transparency in land administration. The purpose of this policy is to provide guidelines for the use of ICT in land and survey management to ensure that these benefits are realized.

3.2 Objectives

The objectives of the policy guide are to:

I. **Improve the efficiency and effectiveness of land administration**: ICT will be leveraged to efficiently and effectively improve processes by integrating ICT tools into land and survey management activities.

II. **Time management**: Integrating ICT will enhance the accuracy and timeliness of land surveying activities using ICT tools such as GIS(Geographical Information System), GNSS(Global Navigation Satellite System), and 3D laser scanning.

III. **Tracking of progress:** Will ensure that land and survey data is accurate, up-to-date, and easily accessible to all stakeholders through the development of an integrated land and survey information system. Provide better accessibility to surveyed lands' records via centralized databases that can be accessed remotely from multiple locations while ensuring proper authorization protocols are put in place to protect privacy

IV. **Security of land data:** Enhance the security and privacy of land and survey data through appropriate security measures such as data encryption, access controls, and regular

backups to prevent unauthorized access or tampering with information obtained through digital means.

V. **Facilitate management and communication:** To improve stakeholder engagement in land and survey management activities by using ICT systems to facilitate communication between landowners, surveyors, legal professionals, and other stakeholders.

VI. **Consistency of data:** Ensure consistency across all aspects of a survey, including measurements, calculations, mapping, etc., by using standardized digital tools.

VII. **Transparency and accountability:** To promote transparency and accountability in land administration by using ICT systems to provide easy access to land records and other relevant information to stakeholders.

VIII. **Cost reduction:** By increasing the accuracy and precision of data collected during land surveys and by reducing the time and cost associated with traditional paper-based land administration processes by utilizing modern technology and software.

3.3 Governance and Coordination

3.3.1 Governance Structure

The Ministry of Innovation, Science, and Digital Economy shall serve as the governing body responsible for overseeing ICT initiatives within the land and survey management sector. A committee comprising representatives from the Ministry, Bureau of Lands and Survey, and other relevant stakeholders shall be established to provide guidance and oversight.

3.3.2 Stakeholder Engagement

Collaboration with stakeholders from the Bureau of Lands and Survey, including land administrators, surveyors, and mapping professionals, shall be integral to the development and implementation of ICT policies and initiatives.

3.3.3 Policy Monitoring and Review

I. **Regular Assessment:** The Ministry of Innovation, Science, and Digital Economy shall conduct periodic assessments to evaluate the effectiveness and efficiency of ICT implementation within the land and survey management sector.

II. **Feedback Mechanisms**: Feedback mechanisms shall be established to gather input from stakeholders regarding the usability, functionality, and impact of ICT systems and tools.

3.3.4 Guidelines and Standards

I. **ICT Infrastructure:** Guidelines shall be established for the procurement, deployment, and maintenance of ICT infrastructure to support land and survey management activities.

II. **Data Management:** Standards for data collection, storage, and sharing shall be developed to ensure the integrity, accuracy, and accessibility of land-related information.

3.4 Data Security

Measures shall be implemented to safeguard land and survey data against unauthorized access, manipulation, or loss, including encryption, access controls, and regular backups.

3.4.1 Cybersecurity: Protocols shall be established to protect ICT systems and networks from cyber threats, including malware, phishing, and hacking attempts.

3.4.2 Incident Reporting

a. **Reporting Procedures**: Protocols shall be established for reporting and responding to ICT-related incidents, including data breaches, system failures, or security breaches.

b. **Incident Response Team**: An incident response team comprising representatives from the Ministry of Innovation, Science, and Digital Economy and the Bureau of Lands and Survey shall be designated to address and mitigate ICT incidents promptly.

3.4.2.1 Conclusion

This subsection of the ICT Policy for Land and Survey Management reflects Ekiti State’s commitment to leveraging technology for efficient and transparent land administration and surveying processes. Through collaboration between the Ministry of Innovation, Science, and Digital Economy and the Bureau of Lands and Survey, the state aims to enhance service delivery, promote good governance, and support sustainable land management practices in Ekiti State.

3.5. Disposal of Equipments

This section outlines the guidelines for the proper disposal ofland and survey ICT equipment. It ensures that the disposal process is conducted in an environmentally responsible and secure manner while protecting sensitive data and complying with applicable laws and regulations. Before an equipment could be rendered useless or irrelevant, the data management team must verify that such equipment is irrelevant and non-reparable. No ministry or department shall dispose equipment without the approval of the data management team

3.5.1 Disposal Procedures

3.5.1.1 Inventory and Assessment

I. The audit team shall maintain an up-to-date inventory of all land and survey ICT equipment.
II. The audit team shall regularly assess equipment for disposal based on its age, functionality, and technological obsolescence.

3.5.1.2Data Erasure

I. Prior to disposal, the data management team shall ensure that all data stored on the equipment is securely and irreversibly erased.
II. Use approved data wiping or destruction methods to prevent unauthorized access to sensitive information.

3.5.1.3 Environmentally Responsible Disposal:

I. Dispose of equipment in an environmentally responsible manner, following applicable waste management and recycling regulations.
II. Collaborate with certified e-waste recycling vendors or organizations to handle the disposal of electronic equipment.

3.5.1.4 Secure Disposal:

I. Maintain the physical security of equipment during the disposal process to prevent theft or unauthorized access to data.
II. Ensure that equipment is securely transported to disposal or recycling facilities to mitigate the risk of data breaches.

3.5.1.5 Documentation: The data management team shall maintain records of all disposed equipment, including serial numbers, disposal dates, and disposal methods. ii.Retain relevant disposal documentation for auditing and compliance purposes.

4.0 DIGITAL SKILLS AND TALENT ACQUISITION POLICY

4.1 Introduction

This policy outlines the guidelines and procedures for the digitalization of skills and talent acquisition within Ekiti State. It establishes the framework for utilizing digital technologies to streamline the acquisition of skills and talent in a transparent, efficient, and inclusive manner. The vision of Ekiti State Government through the Ministry of Innovation, Science and Digital Economy is to create a robust digital ecosystem that facilitates the acquisition of digital skills and connects talent with employment opportunities. The objectives of this policy are to:

4.2 Objective

I. Streamline the skills acquisition process by digitizing application, assessment, and selection procedures.

II. Foster a diverse and inclusive workforce by providing equal access to skills acquisition programs and employment opportunities.

III. Enhance efficiency and effectiveness in talent acquisition by leveraging digital tools for candidate sourcing, assessment, and matching.

IV. Ensure data privacy, security, and compliance with relevant regulations in all digital skills and talent acquisition initiatives.

4.3 Guidelines / Acceptable Use

All MDAs involved in digital skills and talent acquisition initiatives must adhere to the following guidelines:

I. Use digital platforms and technologies in a responsible, ethical, and lawful manner.

Explanation:

MDAs must utilize digital platforms and technologies responsibly, ensuring that they are used for their intended purposes. This includes:

a. Following the terms of service and usage policies set by the digital platforms and technologies.
b. Avoiding the use of digital platforms for any illegal activities, including fraud, harassment, or the dissemination of harmful or inappropriate content.
c. Respecting intellectual property rights and refraining from unauthorized use or distribution of copyrighted materials.

Respect the privacy and confidentiality of candidate information and ensure compliance with data protection regulations

Explanation:
MDAs must prioritize privacy and confidentiality of candidate information collected and processed during the digital skills and talent acquisition process. This includes:

a. Implementing appropriate security measures to protect candidate data from unauthorized access, disclosure, or alteration.
b. Complying with data protection regulations and laws such as obtaining necessary consents, properly storing and securing data, and establish proper data retention and disposal procedures/policies.

I. Provide accurate and up-to-date information on skills acquisition programs, job vacancies, and eligibility criteria.

Explanation:
MDAs involved in digital skills and talent acquisition initiatives must ensure the accuracy and currency of information provided to candidates. This includes:

a. Regular updating of skills acquisition programs, job vacancies, and eligibility criteria to accurately reflect the current status and requirements. This entails ensuring timely adjustments to align with emerging trends and industry demands. The requirements may encompass various technical skills, including proficiency in programming languages, data analysis, cyber-security, and specific software expertise.
b. Verifying the accuracy of information provided to candidates, such as the qualifications, job descriptions, and application processes, to avoid misleading or false representation.
c. Communicating any changes or updates to candidates promptly and transparently.

Promote fair and unbiased selection processes, free from discrimination based on gender, ethnicity, religion, or any other protected characteristic.

Explanation:
MDAs involved in digital skills and talent acquisition must ensure that the selection processes are fair, transparent, and free from discrimination. This includes:

I. Ensuring that the candidate evaluation and selection criteria are based on merit, qualifications, and skills relevant to the respective positions or programs.

II. Prohibiting any form of discrimination or bias based on gender, ethnicity, religion, disability, or any other protected characteristic during the skills and talent acquisition processes.

III. Providing equal opportunities for all individuals, regardless of their background or personal attributes, and promoting diversity and inclusion in digital skills acquisition and employment.

4.3 Training and Awareness

Regular training and awareness programs will be conducted to educate personnel involved in digital skills and talent acquisition about incident reporting procedures, incident response protocols, and their roles and responsibilities in handling incidents. This will ensure that the personnel members are prepared to respond effectively in case of an incident and are aware of their obligations to report any suspicious activities.

4.4 Continuous Improvement

Incident response procedures and protocols should be periodically reviewed and updated to incorporate lessons learned from previous incidents and changes in technology, regulations, or best practices. This continuous improvement process will help enhance the effectiveness of incident management and minimize the risk of future incidents.

Breach

Non-compliance with the digital skills and talent acquisition policy may result in penalties or disciplinary actions. The severity of penalties will depend on the nature and extent of the violation. Possible penalties may include but are not limited to:

I. **Written Warning:** In cases of minor non-compliance by MDAs or service providers, an official written warning will be issued to the responsible entities. This written warning serves as a formal notice, emphasizing the need to rectify the non-compliant behavior promptly and ensure adherence to the policy's requirements.

II. **Suspension of Privileges:** If MDAs or service providers continue to violate this policy despite receiving a warning, temporary suspension of access or privileges will be enforced until the non-compliance issues are resolved. During the suspension period, the affected entities will be unable to avail themselves of certain privileges or access certain resources until they demonstrate compliance with the policy.

III. **Termination of Contracts or Agreements:** Failure to comply with this policy by MDAs or service providers will result in the termination of contracts or agreements. The termination of these contracts or agreements will be enforced, ensuring that the consequences of non-compliance are realized.

IV. **Legal Consequences:** In the case of significant or deliberate policy violations committed by MDAs or service providers, legal consequences will be enforced in accordance with relevant laws and regulations. Furthermore, individuals, MDAs, or service providers charged with penalty will be subjected to legal consequences if they refuse to comply with the penalty and fail to cease all activities associated with digital skills and talent acquisition. The penalties for non-compliance will be applied consistently and in a fair manner, considering the specific circumstances of each case. The responsible individuals, MDAs,

or service providers will be given an opportunity to respond to any allegations or findings before penalties are imposed.

4.4.1 Monitoring & Auditing

I. **Regular Monitoring**: Regular monitoring and auditing of the digital skills and talent acquisition processes will be conducted to ensure compliance with this policy. The monitoring activities aim to assess the effectiveness, efficiency, and fairness of the digital platforms, as well as identify areas for improvement. This includes but is not limited to:

II. **Effectiveness Assessment:**The effectiveness of digital platforms and tools used for skills acquisition and talent acquisition will be evaluated to determine their ability to achieve the desired outcomes. This assessment will focus on factors such as user satisfaction, successful matches between skills and job opportunities, and overall success rates of the digital processes.

III. **Efficiency Evaluation:** The efficiency and timeliness of the digital skills acquisition and talent acquisition processes will be assessed to identify bottlenecks or inefficiencies that may hinder timely acquisition of skills and talent. This evaluation will aim to streamline the process, reduce unnecessary steps, and enhance the overall efficiency of the system.

IV. **Fairness and Equal Opportunities:**The monitoring activities will ensure that the digital processes and platforms provide equal opportunities to all individuals seeking skills acquisition or employment opportunities. It will examine the selection criteria, assessment methods, and decision-making processes to identify any biases or discriminatory practices. Any identified issues will be promptly addressed to ensure fairness and equal opportunities for all participants.

V. **Compliance with policies and regulations:** The monitoring activities will verify that all aspects of the digital skills and talent acquisition processes adhere to the policies, guidelines and applicable laws and regulations.

4.4.1.1 Training

Training programs must be implemented to familiarize relevant personnel with the digital skills and talent acquisition processes, platforms, and tools. This will ensure the effective implementation of the policy and enhance the digital literacy of stakeholders involved. The training will aim to accomplish the following:

I. **Familiarize personnel with digital platforms:** Training sessions must be conducted to familiarize personnel with the digital platforms used for skills acquisition and talent management. This will include instruction on how to navigate the platforms, utilize their features, and effectively engage with candidates and stakeholders.

II. **Enhance digital literacy:** Training programs must focus on enhancing the digital literacy of personnel, ensuring they possess the necessary skills to effectively utilize digital technologies and tools in the context of skills acquisition and talent management.

III. **Explain policy guidelines and procedures:** Training sessions must provide a comprehensive understanding of the digital skills and talent acquisition policy, including the guidelines, acceptable use, and compliance requirements. This will help personnel understand their roles and responsibilities in adhering to the policy.

IV. **Promote awareness of best practices:** Training programs must highlight best practices for ensuring fairness, inclusivity, and data security throughout the digital skills and talent acquisition processes. This will include promoting unbiased selection practices, protecting candidate privacy, and maintaining data accuracy.

4.4.2 Access Controls

To protect against unauthorized access or use of candidate data and maintain confidentiality and integrity of the digital skills and talent acquisition systems, MDAs implement in place the following access controls:

I. **User Authentication:** Strong user authentication mechanisms will be employed to verify the identity of individuals accessing the digital platforms. This will include the use of unique usernames and passwords, multi-factor authentication, or other secure authentication methods.
II. **Role-Based Access Control (RBAC):** Access permissions will be assigned based on predefined roles and responsibilities. Each role will have specific access rights and privileges that align with the duties and responsibilities of the individuals assigned to those roles. Access permissions will be regularly reviewed and updated as needed.
III. **Access Request and Approval Process:** MDAs must establish a formal process for individuals to request access to the digital skills and talent acquisition systems. Access requests will be reviewed and approved by authorized personnel based on the individual's job responsibilities and the principle of least privilege.
IV. **User Account Management:** User accounts will be created, modified, and deactivated in accordance with the MDAs user account management procedures. This includes timely removal of access rights for personnel or contractors who no longer require access to the systems.
V. **Monitoring and Logging:** Access to the digital platforms at MDAs will be logged and monitored to detect any unauthorized access attempts or suspicious activities. System logs and audit trials will be regularly reviewed to identify and investigate any security incidents or potential breaches.
VI. **Confidentiality Agreements:** Authorized personnel at MDAs who have access to candidate data and other sensitive information will be required to sign confidentiality agreements to ensure the protection of that information and to emphasize their responsibility to maintain its confidentiality.

4.4.3 Training and Awareness

Training programs and awareness initiatives will be conducted at MDAs to educate authorized personnel about their responsibilities regarding access and authorization. This includes training on proper use of access credentials, understanding the importance of maintaining confidentiality, and recognizing potential security risks associated with unauthorized access.

4.4.4 Periodic Review

Access controls and authorization mechanisms will be periodically reviewed to ensure their effectiveness and relevance. Reviews will be conducted to assess the appropriateness of access privileges, evaluate the necessity of user accounts, and identify any vulnerabilities or areas for improvement in the access control system.

4.5 Roles & Responsibilities

4.5.1 Data Custodians

MDAs must have data custodians who are responsible for the management, security, and integrity of candidate data collected during the digital skills and talent acquisition process. Their responsibilities include:

I. **Safeguarding candidate information:** Data custodians ensure that candidate data is protected against unauthorized access, loss, or alteration. They implement appropriate security measures, including access controls and regular backups, to maintain data confidentiality and integrity.

II. **Compliance with data protection regulations:** Data custodians at MDAs must ensure that all data handling practices comply with relevant data protection laws and regulations.

They oversee the implementation of privacy policies, consent management, and data retention and deletion procedures.

III. **Collaboration with stakeholders:** Data custodians must work closely with system administrators, privacy officers, and other relevant stakeholders to ensure that data management practices align with the overall objectives of the digital skills and talent acquisition process.

4.5.2 System Administrators

MDAs must have System administrators who are responsible for the configuration, maintenance, and monitoring of the digital platforms and systems used for digital skills and talent acquisition management. Their responsibilities include:

I. **Platform administration:** System administrators must manage the setup, configuration, and ongoing administration of the digital platforms, ensuring their stability, performance, and availability.

II. **User management:** System administrators must oversee user accounts, access controls, and permissions within the digital platforms. They ensure that appropriate access levels are granted based on roles and responsibilities.

III. **Technical support:** System administrators must provide technical support to users, troubleshoot issues, and address any platform-related concerns raised by stakeholders.

IV. **Platform enhancements and upgrades:** System administrators must collaborate with relevant stakeholders to identify opportunities for improving the functionality, security, and user experience of the digital platforms. They oversee the implementation of upgrades and enhancements as necessary.

4.5.3 Privacy Officers

MDAs must have Privacy officers who are responsible for ensuring compliance with privacy laws and regulations in the digital skills and talent acquisition process. Their responsibilities include:

I. **Policy development and implementation:** MDA Privacy officers must develop and implement privacy policies and procedures that govern the collection, use, retention, and disclosure of candidate information. They ensure that privacy practices align with applicable laws and regulations.

II. **Privacy impact assessments:** Privacy officers must conduct privacy impact assessments to identify and mitigate privacy risks associated with the digital skills and talent acquisition process. They recommend and implement measures to enhance privacy and data protection.

III. **Training and awareness:** Privacy officers must provide training and awareness programs to stakeholders involved in the digital skills and talent acquisition process. They educate personnel at their respective MDAs on privacy best practices, data handling procedures, and their obligations under privacy laws.

IV. **Incident response and breach management:** It's the responsibility of Privacy officers to lead the response to privacy incidents and breaches, coordinating with relevant authorities and stakeholders to minimize the impact and ensure compliance with breach notification requirements.

4.5.4 Other Relevant Positions

In addition to the above roles, other relevant positions at MDAs relevant to digital skills and acquisition may include:

I. **Skills Acquisition Coordinators:** MDAs must have these individuals who oversee the planning, coordination, and implementation of digital skills and talent acquisition programs, ensuring alignment with the digital skills and talent acquisition policy.

II. **Talent Acquisition Managers:** These professionals are responsible for sourcing, screening, and selecting candidates for employment opportunities, utilizing the digital platforms and tools in accordance with the policy.

III. **Compliance Officers:** MDAs must have these individuals to monitor and ensure compliance with the digital skills and talent acquisition policy, conducting regular audits and assessments to identify areas of non-compliance and recommending corrective actions.

The specific roles and responsibilities assigned to individuals and departments at MDAs must be documented in job descriptions, organizational charts, and associated guidelines and procedures.

5.0 ICT POLICY ON DRONE DEPLOYMENT

5.1 Introduction

The purpose of this ICT policy is to provide guidelines and responsibilities for the deployment of drones within Ekiti State. It is intended to ensure safe and responsible use of drones while safeguarding privacy and confidentiality. This policy applies to all personnel who operate, maintain, or have access to drones inside our organization.

5.2 Guidelines

I. All drone operations should comply with national and local regulations.

II. Drones should be used safely and only for legitimate business purposes.

III. Drones should not be flown over populated areas, critical infrastructure, or restricted or sensitive areas, unless authorized.

IV. Operators should maintain a clear line of sight when operating drones.

V. The organization reserves the right to regulate the time and location of drone operations.

5.3 Roles and Responsibilities

I. The Head of Operations will be responsible for the implementation and monitoring of the policy.
II. The departmental manager will be responsible for ensuring that all drone operators receive adequate training on the safe and reliable use of drones.
III. Drone operators are responsible for reporting any incidents or malfunctions promptly to their departmental supervisors.
IV. All personnel whose work involves drone deployment should be aware of the guidelines and reporting procedures under this policy.

5.4 Procurement

I. All drone purchases should be approved by The Ministry of Innovation, Science and Digital Economy (SEE SECTION 1; 7.0)
II. Acquisition should follow established procurement procedures.
III. All purchases should comply with the current regulations governing drone use.

5.5 Incidence Reporting

I. All drone-related incidents or accidents should be reported to the Head of Operations within 24 hours.
II. All drone operators should complete an incident reporting form within 24 hours of any incident.
III. The Head of Operations will conduct an investigation of the incident and recommend appropriate action.

5.6 Access

I. Access to drones should be strictly controlled.
II. All drone operators should be authorized, trained, and registered.
III. Access should only be granted to personnel with a valid, business-related reason for operating the drone.
IV. Access should be immediately terminated for those who violate the rules and regulations governing drone usage.

5.7 Data management

I. Data captured by drones should be stored securely in accordance with security and privacy regulations.
II. Only authorized personnel should have access to drone-captured data.
III. Drone-captured data should be destroyed or deleted when no longer required.
IV. The State shall comply with existing regulations governing data protection, privacy, and confidentiality.

5.8 Conclusion

This ICT policy provides guidelines and responsibilities for safe, reliable, and responsible drone deployment within our organization. It aims to safeguard privacy and confidentiality and ensure compliance with regulatory requirements. All personnel whose work involves the deployment of drones should adhere to this policy, and non-compliance will result in appropriate disciplinary action.

6.0 SOCIAL MEDIA ENGAGEMENT POLICY

6.1 Objective

This subsection of the ICT Policy outlines guidelines and procedures for social media engagement by government agencies within Ekiti State. It is implemented as a policy to ensure responsible, effective, and transparent use of social media platforms to engage with citizens, disseminate information, and promote government initiatives.

6.1.1 Applicability

This policy applies to all government agencies, departments, and employees within Ekiti State who utilize social media platforms for official purposes.

6.1.2 Platforms Covered

The document encompasses all social media platforms used for official government communication, including but not limited to, Facebook, Twitter, Instagram, LinkedIn, YouTube, and any emerging platforms adopted by government agencies.

6.2 Guidelines and Standards

6.2.1 Content Guidelines:

Government agencies shall adhere to ethical standards and principles of accuracy, transparency, and integrity when creating and sharing content on social media platforms.

6.2.2 Engagement Practices

Agencies shall engage with citizens on social media platforms in a respectful, courteous, and professional manner, responding promptly to inquiries, feedback, and comments.

6.3 Security and Privacy

6.3.1 Data Protection:

Government agencies shall protect sensitive information and respect the privacy rights of citizens when engaging on social media platforms, adhering to data protection laws and regulations.

6.3.2 Account Security:

Agencies shall implement measures to secure social media accounts, including strong passwords, multi-factor authentication, and regular monitoring for unauthorized access or malicious activities.

6.4 Monitoring and Reporting

Government agencies shall monitor social media channels regularly to track engagement metrics, identify trends, and assess the effectiveness of social media outreach efforts.

6.4.1 Reporting:

Agencies shall report on social media engagement activities periodically, providing insights and analysis to inform decision-making and strategy development.

6.5 Training and Awareness

Government employees responsible for managing official social media accounts shall receive training on best practices, policies, and procedures for social media engagement.

6.5.1 Awareness:

Agencies shall promote awareness among employees about the responsible use of social media for official purposes, highlighting the importance of maintaining professionalism and upholding the reputation of the government.

6.6 Compliance and Enforcement

Government agencies shall comply with this policy and any related guidelines or directives issued by the Ministry

6.6.1 Enforcement:

The Ministry of Innovation, Science, and Digital Economy shall oversee compliance with the social media engagement policy, providing guidance, support, and enforcement measures as necessary.

6.7 Conclusion

This subsection of the ICT Policy underscores the government's commitment to harnessing the power of social media for effective communication, citizen engagement, and transparency. By implementing clear guidelines and standards, we aim to foster trust, enhance transparency, and promote meaningful dialogue between government agencies and citizens across Ekiti State.

7.0 RESEARCH AND DEVELOPMENT ICT POLICY

7.1 Introduction

The objective of this Act is to establish a framework for conducting research and documentation activities to inform evidence-based decision-making and support the effective implementation of ICT initiatives.

7.2 Objectives

I. To stimulate and encourage Research and Development in ICT
II. To harness and utilize the results of Research and Development in ICT
III. To ensure that adequate resources are provided for ICT-related research
IV. To enhance collaboration among stakeholders in the design, execution documentation and exchange of research ideas and results

7.3 Roles and Responsibilities

The Ministry of Innovation, Science, and Digital Economy shall oversee research and documentation activities within the ICT policy framework.

Relevant stakeholders, including government agencies, research institutions, and industry partners, shall collaborate in conducting research and documentation activities as appropriate.

7.4 Research Activities

I. Conduct regular needs assessments to identify ICT requirements and priorities across government sectors.

Monitor technology trends and conduct impact evaluations to inform policy development and strategic planning.

II. Benchmark against global best practices to identify opportunities for innovation and improvement

7.5 Documentation Guidelines

Document research findings, policy recommendations, and stakeholder inputs to ensure transparency and accountability in policy development processes.

I. Develop implementation guidelines, standards, and procedures to facilitate the effective execution of ICT initiatives.

II. Maintain a repository of knowledge resources, including training materials, manuals, and case studies, to support capacity building and knowledge sharing among stakeholders.

7.6 Implementation and Enforcement

The provisions of this Act shall be implemented and enforced by the appropriate authorities designated by the Government of Ekiti State.

8 .0 ARTIFICIAL INTELLIGENCE POLICY FRAMEWORK

8.1 Introduction:

Recognizing the transformative potential of Artificial Intelligence (AI) and its impact on various sectors, Ekiti State aims to foster the development and adoption of AI technologies. This policy outlines a comprehensive program to promote AI innovation, research, skills development, and deployment across the state. The program will support the growth of AI-driven solutions, drive economic development, and enhance public services in Ekiti State.

8.2 Objectives:

I. **Promote Innovation:** Foster a culture of innovation and entrepreneurship in AI, encouraging the development of cutting-edge AI technologies and solutions in Ekiti State.

II. **Research and Development:** Support research initiatives in AI, enabling collaboration between academia, research institutions, and industry to advance AI knowledge and develop state-of-the art AI systems.

III. **Skill Development**: Establish programs to enhance AI skills and expertise in Ekiti State, including training, workshops, and educational initiatives at all levels, from primary education to tertiary institutions and professional development.

IV. **Industry Engagement:** Encourage collaboration between AI startups, established businesses, and government agencies to drive AI adoption across sectors such as healthcare, agriculture, finance, transportation, and governance.

V. **Ethical and Responsible AI**: Promote the development and use of AI systems that adhere to ethical principles, ensuring transparency, fairness, accountability, privacy, and inclusivity.

8.3 Initiatives and Implementation:

I. **AI Research Centers:** Establish AI research centers in collaboration with academic institutions and research organizations. These centers will facilitate cutting-edge research, knowledge sharing, and collaboration between researchers, industry experts, and government agencies.

II. **Funding and Grants:** Allocate funding and grants to support AI research, innovation, and startups.

III. Encourage public-private partnerships to attract investment and funding for AI initiatives.

8.3.1 Skills Development Programs: Implement training programs and initiatives to develop a skilled AI workforce. Collaborate with educational institutions to integrate AI courses and curricula, and provide scholarships or fellowships for AI studies.

8.3.2 AI Innovation Hubs: Create AI innovation hubs or incubators to support startups and entrepreneurs in developing AI-driven solutions. Provide access to resources, mentorship, and networking opportunities to foster growth and commercialization of AI technologies.

8.3.3 **Data Infrastructure:** Invest in robust data infrastructure and platforms to support AI applications. Ensure data availability, quality, and security for AI development and deployment, while adhering to privacy and ethical standards.

8.3.4 **Government AI Adoption:** Encourage government agencies to adopt AI technologies to enhance public services, streamline processes, and improve governance. Develop use cases and pilot projects to demonstrate the benefits of AI in areas such as healthcare, transportation, public safety, and administrative efficiency.

8.3.5 **Collaboration and Partnerships:** Foster collaboration between academia, industry, and government agencies through partnerships, joint projects, and knowledge exchange programs. Engage with international organizations and institutions to access global expertise and best practices in AI.

8.4 Monitoring and Evaluation:

8.4.1 **Performance Metrics:** Define key performance indicators (KPIs) to measure the success and impact of the AI program. Monitor the progress of AI initiatives, research outcomes, startup growth, and skills development.

8.4.2 **Evaluation and Feedback:** Conduct regular evaluations to assess the effectiveness of the program and identify areas for improvement. Gather feedback from stakeholders, including researchers, industry representatives, and the public, to shape program strategies and priorities.

8.4.3 **Policy Iteration**: Review and update the AI program periodically to align with emerging technologies, ethical considerations, and societal needs. Adapt policies and initiatives to ensure they remain relevant and supportive of the evolving AI landscape.

8.5 Governance and Regulation:

8.5.1 **AI Regulatory Body:** The established regulatory body for the ICT POLICY (The Ministry of Innovation, Science and Digital Economy), as outlined in the previous sections, shall oversee policy implementation, compliance, and ethical considerations in AI development and deployment.

8.5.2 **Policy Coordination:** Ensure coordination among government agencies, research institutions, industry, and the AI regulatory body to align efforts, streamline processes, and foster collaboration in AI governance.

8.5.3 **Public Engagement:** Promote transparency and inclusivity by engaging the public in AI policy discussions, seeking feedback, and addressing concerns. Foster awareness and understanding of AI benefits, risks, and ethical considerations through public education initiatives.

8.6 Enhancing Public Services:

Goal: Improve the efficiency, accessibility, and quality of public services through AIimplementation.

I. **Measure:** Optimize resource allocation and service delivery by deploying AI-powered systems in healthcare, transportation, governance, and public safety sectors.

II. **Measure:** Monitor and improve citizen satisfaction rates with AI-enhanced public services through regular surveys and feedback mechanisms.

III. **Measure**: Increase the availability and usage of AI-based platforms for citizen engagement and participation in decision-making processes.

8.7 Promoting Economic Growth:

Goal**:** Foster an AI-driven economy that attracts investments, creates job opportunities, and supports local businesses.

I. **Measure:** Attract AI-related investments by tracking the number and value of AI-focused funding and venture capital initiatives in Ekiti State.

II. **Measure**: Increase the number of AI-driven businesses, startups, and technology incubators/accelerators in Ekiti State.

III. **Measure:** Track the growth of AI-related employment opportunities and the percentage of the workforce with AI-related skills through periodic assessments and reports.

8.8 Ensuring Public Safety:

Goal: Utilize AI technologies to enhance public safety measures and emergency response capabilities.

I. **Measure:** Improve response times and effectiveness of emergency services through the implementation of AI-powered analytics and predictive modeling.

II. **Measure:** Enhance surveillance and monitoring systems using AI for crime prevention, disaster management, and public safety.

III. **Measure:** Reduce accidents and incidents through the implementation of AI-based traffic management and intelligent transportation systems.

8.9 Ethical Principles

Establish ethical principles to guide the development and use of AI systems in Ekiti State.

These ethical principles provide a foundation for the responsible and ethical development and use of AI systems in Ekiti State. By adopting and adhering to these principles, Ekiti State can ensure that AI technologies are developed and deployed in a manner that upholds values such as transparency, fairness, privacy, accountability, and social well-being.

Establish principles of transparency, fairness, accountability, privacy, and inclusivity is crucial for responsible AI development and use in Ekiti State. These principles would ensure the ethical deployment of AI systems, fostering public trust, and minimizing the potential for harm or discrimination.

By incorporating penalties for non-compliance, Ekiti State can enforce adherence to these principles and promote a culture of responsible AI implementation.

8.10 Principles

8.10.1 Transparency

AI systems should be designed and operated in a transparent manner, providing clear explanations for their decisions and actions. Users and stakeholders should have access to information about how AI systems are developed, trained, and deployed.

8.10.2 Fairness and Equity

AI systems must be designed to treat all individuals fairly and without bias, regardless of their race, gender, ethnicity, religion, or socioeconomic background. Developers should actively identify and mitigate biases in training data and algorithms to ensure equitable outcomes.

8.10.3 Privacy and Data: Protection

Respect user privacy by implementing robust data protection measures. Minimize the collection of personal data to what is necessary for the intended purpose. Obtain informed consent for data collection, storage, and usage, and ensure secure handling of sensitive information.

8.10.4 Accountability and Responsibility

Ekiti State has established mechanisms to hold developers, providers, and users of AI systems accountable for their actions. Clear lines of responsibility and liability should be defined, and there should be mechanisms to address any unintended consequences, biases, or harm caused by AI systems.

8.10.5 Human Autonomy and Oversight:

Ensure that AI systems are designed to respect and enhance human autonomy. Human oversight should be maintained in decision-making processes involving AI, and there should be mechanisms for individuals to challenge or appeal automated decisions in the state.

8.10.6 Safety and Reliability:

Prioritize the safety and reliability of AI systems to avoid harm to users and the broader society. Implement rigorous testing, validation, and monitoring procedures to ensure that AI systems perform as intended and minimize the risk of errors or failures.

8.11 Guide to Safety Measurement of AI in Ekiti State

8.12 Introduction

Ensuring the safety of Artificial Intelligence (AI) systems is crucial to protect individuals, organizations, and society at large. In Ekiti State, it is essential to have a robust framework for measuring the safety of AI systems. This guide provides an overview of the stakeholders involved in measuring AI safety, their roles and responsibilities, and the key steps to effectively assess and monitor AI safety in Ekiti State.

8.13 Roles and Responsibilities:

The Ministry of Innovation, Science and Digital Economy along with The Bureau of ICT Ekiti State shall Develop and enforce safety regulations, standards, and guidelines for AI systems.

a. Monitor compliance with safety requirements and take appropriate enforcement actions.

b. Provide guidance and support to AI developers and operators in implementing safety measures.

c. Collaborate with independent evaluators to validate AI safety.

I **AI Developers and Operators:**

a. Conduct thorough safety assessments of AI systems before and during deployment.
b. Implement safety measures, including algorithmic robustness, data security, and system reliability.
c. Regularly monitor and evaluate the safety performance of AI systems.
d. Address identified safety concerns promptly and take necessary remedial actions.
e. Keep abreast of safety best practices and incorporate them into AI development processes.

I. **Public and End-Users:**

a. Report safety concerns or incidents related to AI systems to the appropriate authorities.
b. Provide feedback on the safety performance of AI systems.
c. Stay informed about AI safety considerations and educate themselves on potential risks.

8.14 Key Steps for AI Safety Measurement:

I. Risk Assessment: Conduct comprehensive risk assessments to identify potential safety hazards and risks associated with AI systems.

II. Safety Testing: Implement rigorous testing methodologies to assess the robustness, reliability, and security of AI systems. This may include testing for algorithmic biases, data quality, and system vulnerabilities.

III. Documentation and Transparency: Maintain clear and transparent documentation of safety measures, testing procedures, and mitigation strategies. This documentation facilitates accountability and helps stakeholders understand the safety considerations implemented.

IV. Ongoing Monitoring: Continuously monitor the safety performance of AI systems in realworld scenarios. Implement mechanisms for detecting and responding to safety incidents or emerging risks promptly.

V. Incident Response and Remediation: Establish protocols and procedures to address safety incidents or breaches. Develop a framework for incident response, investigation, and remediation, ensuring timely and effective actions.

VI. Collaboration and Knowledge Sharing: Foster collaboration between stakeholders, including government agencies, AI developers, independent evaluators, and end-users, to share insights, best practices, and lessons learned in AI safety.

8.15 Reporting and Compliance

I. Reporting Mechanisms: Implement reporting mechanisms for AI developers and operators to report on safety assessments, testing results, and incident occurrences to the AI regulatory body.

II. Compliance Monitoring: The AI regulatory body and government agencies should conduct periodic compliance checks and audits to ensure adherence to safety regulations and standards.

III Penalties and Enforcement: Establish penalties and enforcement mechanisms for noncompliance with safety requirements. These may include fines, suspensions, or revocations of AI system certifications or licenses.

Social and Environmental Impact:

Consider the broader social and environmental impacts of AI systems throughout their life cycle. Strive to develop and use AI technologies that contribute positively to society, promote sustainability, and address global challenges, such as climate change and inequality.

8.16 Continuous Learning and Improvement:

Foster a culture of continuous learning, improvement, and ethical awareness in AI development and use. Stay informed about evolving ethical considerations and best practices in AI, and actively engage in research, knowledge sharing, and collaboration to address emerging challenges.

Promoting Ethical AI in Ekiti State; Principles of Transparency, Fairness, Accountability, Privacy, and Inclusivity

8.18.1Introduction

Artificial Intelligence (AI) has the potential to transform Ekiti State, bringing numerous benefits to its residents. However, to ensure responsible and ethical development and use of AI, it is crucial to establish principles that guide AI systems' deployment. This article focuses on five key principles: transparency, fairness, accountability, privacy, and inclusivity. We will explore the significance of each principle in the context of AI in Ekiti State and propose penalties for those who violate these principles, promoting a culture of responsible AI implementation.

8.18.2 Penalties for Defaulters:

Failure to adhere to transparency principles can result in penalties such as fines, public disclosure of non-compliance, or suspension of AI system deployment until transparency requirements are met.

8.18.3 Fairness:

Ensuring fairness in AI systems is crucial to avoid discrimination and bias. In Ekiti State, it is essential to promote fair AI systems that treat individuals equitably and do not perpetuate existing biases. Key considerations include: measure and address algorithmic bias.

8.18.4Accountability

Accountability is a crucial aspect of responsible AI implementation. It establishes responsibility for the actions and outcomes of AI systems. In Ekiti State, accountability should be emphasized through:

I. **Clear Responsibility Allocation:**

Assign clear responsibilities to developers, providers, and users of AI systems. Establish guidelines that outline who is accountable for the system's behavior, decisions, and potential consequences.

II. **Error Reporting and Remediation**

Encourage the reporting of AI system errors or unintended consequences. Developers should be accountable for promptly addressing identified issues, rectifying errors, and providing remedies for any resulting harm.

8.19 Privacy

Protecting individuals' privacy is of utmost importance in the age of AI. In Ekiti State, privacy principles must be adhered to throughout the development and use of AI systems. Key considerations include:

I. **Data Minimization:** Minimize the collection and storage of personal data to what is necessary for the intended purpose. Avoid unnecessary intrusion into individuals'/ organization/ institution privacy and ensure the secure handling of data.

II. **Informed Consent:** Obtain informed consent from individuals for data collection, usage, and sharing. Ensure transparency about how their data will be utilized by AI systems.

8.20.1.1 AI for Transformative Healthcare

In the delivery of healthcare as a public good to the Ekiti people, the sectoral transformative potential of Artificial Intelligence, in terms of improving healthcare service delivery, management, and governance at various levels of interaction between government, citizens, businesses, and the health workforce, is as follows:

I. **Government-to-Citizen (G2C) Interactions:**

a. Service Delivery: AI-driven telemedicine platforms and virtual healthcare assistants will provide citizens with remote access to healthcare services, enabling consultations, diagnosis, and treatment from the comfort of their homes.

b. Health Information Systems: AI-powered health information systems will facilitate the seamless exchange of health data between citizens and healthcare providers, ensuring efficient management of medical records and personalised (client-centred) healthcare delivery.

II. **Government-to-Business (G2B) Interactions:**

a. Health Financing: AI will assist in delivering on the mandate of Universal Health Coverage, through optimizing healthcare financing strategies by analyzing healthcare utilization patterns, predicting future healthcare costs, and identifying fraud in insurance claims.

b. Essential Medical Products and Technologies: AI-driven supply chain management systems will ensure the timely procurement, distribution, and quality control of essential medical products and technologies, thereby benefiting both healthcare providers and medical product manufacturers.

III. **Government-to-Employee (G2E) interface:**

a. Human Resources for Health: In terms of Healthcare workforce management, government healthcare agencies will utilize AI in recruitment, capacity building, task allocation, operational collaboration and performance evaluation of healthcare professionals.

b. Leadership and Governance: AI will provide decision support to government healthcare leaders by analyzing healthcare data, predicting healthcare trends, and recommending evidence-based policies and interventions for improving healthcare outcomes.

IV. **Government-to-Government (G2G) Interelationship:**

a. Health Information Systems: AI-powered interoperable health information systems will enable seamless data exchange between government healthcare agencies, as well as on a subnational (intergovernmental) collaborative scale, thereby facilitating collaborative decision-making, resource allocation, and policy planning.

b. Leadership and Governance: AI will enhance governance in healthcare by automating administrative tasks, monitoring compliance with healthcare regulations, and providing real-time insights to government leaders for effective policy formulation and implementation.

8.21 AI and the Ekiti Kete’s Workforce.

8.21.1Policy Statement:

The civil service in Ekiti State recognizes the transformative potential of Artificial Intelligence (AI) for startups and the wider entrepreneurial ecosystem. This policy aims to facilitate the adoption of the AI policy framework established by the state government, promoting the responsible and effective integration of AI technologies among startups in Ekiti State. By providing support, guidance, and resources, the civil service seeks to empower startups to leverage AI for innovation, growth, and economic development.

8.21.1Objectives:

I. Facilitate Adoption: Support startups in Ekiti State to embrace AI technologies and integrate them into their operations and offerings.

II. Promote Responsible AI: Ensure that startups adhere to ethical and responsible AI practices, including transparency, fairness, accountability, privacy, and inclusivity.

III. Enhance Competitiveness: Empower startups to leverage AI to gain a competitive advantage, drive innovation, and create sustainable business models.

IV. Foster Collaboration: Facilitate collaboration between startups, AI experts, research institutions, and industry players to exchange knowledge, share best practices, and foster a supportive ecosystem for AI-driven startups.

8.22.1Support Mechanisms:

I. **Awareness and Education:**
   a. Conduct workshops, seminars, and training programs to educate startups about the benefits, risks, and ethical considerations of AI adoption.
   b. Provide resources, case studies, and best practice guidelines to help startups understand the practical implementation of AI technologies.

II. **Technical Assistance:**
   a. Offer technical guidance and expertise to startups regarding AI system development, implementation, and integration.
   b. Establish partnerships with AI experts, consultants, and research institutions to provide mentorship and advisory services to startups.

III. **Access to Funding:**
   a. Identify funding opportunities, grants, and financial support specifically dedicated to AIdriven startups.
   b. Assist startups in navigating funding options, connecting them with relevant funding agencies, investors, and venture capitalists.

9.0 E-GOVERNANCE POLICY

9.1 Introduction:

This policy aims to guide the state's digital transformation efforts and promote effective eGovernance practices to enhance public service delivery, transparency, and citizen participation. Recognizing the transformative power of information and communication technologies (ICTs) and the significance of a robust digital economy for the growth and development of the state, this policy aims to establish a comprehensive framework for eGovernance and digital transformation in Ekiti State. The policy focuses on promoting entrepreneurship, innovation, and inclusivity while ensuring effective governance, security, and data privacy. The policy outlines the principles, goals, and strategies to be followed, along with the roles and responsibilities of key stakeholders involved in the implementation of eGovernance initiatives.

9.2 Principles:

I. **Citizen-Centric Approach**: All eGovernance initiatives shall prioritize the needs and preferences of citizens, ensuring accessibility, convenience, and inclusivity.

II. **Transparency and Accountability:** Digital systems and processes shall be designed to enhance transparency, enable real-time monitoring, and foster accountability in government operations.

III. **Collaboration and Partnership:** Collaboration with relevant stakeholders, including government departments, private sector entities, civil society organizations, and citizens, shall be encouraged to drive innovation and ensure sustainable development.

IV. **Data Security and Privacy**: Stringent measures shall be implemented to protect citizen data, maintain privacy, and safeguard against cyber threats.

9.3 Capacity Building

Continuous capacity building initiatives shall be undertaken to equip government officials and citizens with the necessary skills and knowledge to effectively utilize eGovernance services and technologies.

9.4 Goals

I. **Enhance Service Delivery:** Digitize government services to provide efficient, transparent, and citizen-centric services accessible through multiple channels, including online portals and mobile applications.

II. **Improve Governance Efficiency:** Streamline government processes, eliminate redundancy, and reduce paperwork through automation, digitization, and process reengineering.

III. **Foster Citizen Engagement:** Promote active citizen participation in decision-making processes through digital platforms, consultation mechanisms, and open data initiatives.

IV. **Ensure Data Security and Privacy:** Implement robust cybersecurity measures, data protection frameworks, and secure digital identity systems to safeguard citizen data and privacy.

V. **Promote Digital Literacy and Inclusion**: Bridge the digital divide by providing digital literacy programs, improving access to digital infrastructure, and catering to the needs of diverse user groups.

9.5 Strategies:

The Ministry of Innovation, Science and Digital Economy shall ensure

9.5.1 Infrastructure Development:

I. A reliable and high-speed broadband network shall be established across the state to ensure widespread access to digital services.

II. Invest in the development of data centers, cloud infrastructure, and cybersecurity systems to support eGovernance initiatives.

9.5.2 Service Digitization and Integration:

I. The ICT Professionals/ Governing Council shall identify key government services for digitization, prioritizing high-demand services with significant impact on citizens' lives.

II. Develop standardized and interoperable digital platforms to integrate government services and facilitate seamless information exchange between departments.

9.5.3 Open Data and Transparency:

The ICT Cadre shall;

I. Promote the release of government data in open formats through a centralized open data portal, enabling public access and utilization.

II. Establish mechanisms for public feedback, data-driven decision-making, and real-time monitoring of government processes. iii.Citizen Engagement and Participation:

III. Develop digital platforms and mobile applications for citizen engagement, feedback collection, and participation in policy formulation and implementation.

IV. Organize online consultations, surveys, and public hearings to gather public opinions and incorporate citizen feedback into decision-making processes.

9.6 Capacity Building and Training:

I. Conduct regular training programs to enhance the digital skills of government officials, enabling them to effectively utilize eGovernance tools and platforms.

II. Implement digital literacy programs for citizens, focusing on underserved communities and marginalized groups, to enhance their digital participation.

9.7 Cybersecurity and Data Protection

I. Establish a comprehensive cybersecurity framework, including incident response mechanisms, security audits, and awareness campaigns.

II. Develop robust data protection policies and ensure compliance with relevant data protection regulations.

9.8 Implementation and Monitoring:

An eGovernance implementation committee shall be established to oversee the execution of the policy and monitor the progress of eGovernance initiatives. These committee shall;

I. Develop a detailed action plan with specific timelines, responsibilities, and resource allocation for the implementation of the policy.

II. Conduct periodic reviews and evaluations to assess the effectiveness and impact of eGovernance initiatives and make necessary improvements.

10.0 ICT POLICY ON CYBER SECURITY

10.1 INTRODUCTION

This policy outlines the cyber security measures that shall be implemented to protect key information assets, including data, hardware, software, and networks. The policy applies to all personnel, contractors, and third-party service providers who have access to these key information assets.

10.2 Objectives of the Cyber Security Policy

The objective of this subsection is to establish a comprehensive framework for ensuring the security and resilience of Ekiti State's digital infrastructure and information assets against cyber threats. This framework aims to safeguard sensitive data, protect critical systems, and promote trust and confidence in the use of Information and Communication Technology (ICT) within the state.

10.2.1 Scope:

This subsection applies to all government agencies, departments, and entities within Ekiti State that utilize ICT resources or manage digital information. It encompasses measures to prevent, detect, respond to, and recover from cyber incidents, regardless of the nature or origin of the threat.

10.3 Governing Body:

The Bureau of ICT shall serve as the governing body responsible for overseeing the implementation of cyber security measures, with monitoring and support from the Ministry of Innovation, Science, and Digital Economy. The Bureau of ICT shall collaborate with relevant stakeholders to ensure the effective enforcement of cyber security policies and procedures.

10.4 Ethical Hacking

Authorized ethical hacking activities may be conducted under the following provisions:

Authorization: Ethical hacking activities shall only be performed by authorized personnel with appropriate training and credentials.

I. **Scope:** Ethical hacking activities shall be limited to predefined targets and objectives, with clear rules of engagement and scope of testing.

II. **Reporting:** Findings from ethical hacking activities shall be promptly reported to the designated authorities for assessment and remediation.

III. **Remediation:** Vulnerabilities identified through ethical hacking shall be addressed through timely remediation measures to mitigate potential risks.

IV. **Confidentiality:** Ethical hackers shall adhere to strict confidentiality agreements and safeguard sensitive information obtained during testing.

10.5 Enforcement of the Cyber Security Policy:

The enforcement of the cyber security policy shall involve the following components:

Monitoring and Auditing: Regular monitoring and auditing of ICT systems and networks shall be conducted to identify and mitigate security risks.

I. **Incident Response Plan:** A comprehensive incident response plan shall be developed and maintained to guide the response to cyber security incidents, including procedures for containment, eradication, and recovery.

II. **Training and Awareness:** Ongoing training and awareness programs shall be provided to stakeholders to enhance their understanding of cyber security risks and best practices.

III. **Disciplinary Action:** Violations of the cyber security policy shall be subject to disciplinary action in accordance with established procedures and guidelines.

IV. **Regular Review and Updating:** The cyber security policy shall be periodically reviewed and updated to address emerging threats, technological advancements, and changes in regulatory requirements.

10.6 Conclusion:

This cyber security subsection of the ICT Policy for Ekiti State underscores our commitment to safeguarding digital assets, protecting critical infrastructure, and fostering a secure and resilient cyber environment. Through proactive measures, collaboration, and continuous improvement, we aim to mitigate cyber threats and enhance the trust and confidence of stakeholders in Ekiti State's digital ecosystem.

11.0 FINAL CONCLUSIONS

11.1 Concluding Remarks on the ICT Policy

As we conclude the formulation of the ICT Policy for Ekiti State, it is imperative to emphasize the importance of ongoing review, adaptation, and compliance to ensure its effectiveness and relevance in an ever-evolving digital landscape. Here are key considerations for closing and ending the ICT Policy:

11.1.1 Regular Reviews and Amendments:

I. The ICT Policy shall undergo periodic reviews to assess its alignment with technological advancements, emerging threats, and evolving regulatory frameworks.

II. Amendments shall be made as necessary to address gaps, accommodate new technologies, or revise strategies in response to changing circumstances.

11.1.2 Failure to Abide and Enforcement:

I. It shall be ensured that mechanisms for monitoring and enforcing compliance with the ICT Policy are in place to mitigate risks associated with non-compliance.

II. Consequences for failure to abide by the policy shall be clearly defined, including disciplinary actions or penalties for violations.

Continuous Improvement and Adaptation:

I. Stakeholders shall be encouraged to share feedback, suggest improvements, and propose innovative solutions to foster a culture of continuous improvement.

II. Flexibility and adaptability shall be maintained to ensure that the policy remains effective and responsive to emerging challenges and opportunities.

11.1.3 Education and Awareness:

I. Ongoing education and awareness initiatives shall be provided to stakeholders to ensure their understanding of the policy requirements, implications, and best practices.

II. Training programs, workshops, and communication campaigns shall be implemented to foster a culture of cyber security awareness and digital literacy.

11.1.4 Transparency and Accountability:

I. Transparency in the policymaking process, as well as accountability for implementation and outcomes, shall be upheld throughout the lifecycle of the ICT Policy.

II. Regular reporting on progress, achievements, challenges, and lessons learned shall enhance transparency and accountability.

11.1.5 Closure and Succession Planning:

I. A structured process shall be followed to ensure a smooth transition when closing or replacing the ICT Policy.

II. Succession planning shall be considered to transfer knowledge, responsibilities, and ownership of ICT initiatives to future stakeholders.

In closing, the ICT Policy serves as a strategic roadmap for leveraging technology to drive innovation, efficiency, and socio-economic development in Ekiti State. By embracing a culture of continuous improvement, transparency, and accountability, we shall navigate the complexities of the digital age while maximizing the benefits of ICT for the betterment of our society.