EBS

INFORMATION TECHNOLOGY POLICY

Document Version	3.1
Status	Revised
Document_Type	IT Policy
Date	January 2024

Table Of Content	**Page**

General

1.1 Introduction

EBS Information Technology Policy (IT Policy) defines a set of policies that all internal and external individuals in EBS must adhere to when utilizing information technology resources. It includes clients, employees, contractors, vendors, etc. The IT Policy governs the use and operations of information technology throughout EBS. Specific references to IT titles, roles or the IT department should be interpreted to include any personnel that manage the function.

These policies are to be applied based on the level of risk posed to EBS operations. Levels of control are dependent on a risk assessment of the business environment, and appropriate controls must be implemented to adequately mitigate identified risk. EBS's assets must be protected in a manner commensurate with its confidentiality, integrity, and availability.

1.2 Goals

- ✓ Develop a standard IT Policy focusing on areas of high IT business risk.
- ✓ Align policy against key control objectives related to IT risk.
- ✓ Implement sustainable governance model around IT Policy.
- ✓ Introduce new/updated policy into key IT risk areas.
- ✓ Ensure IT management ownership of policy.

1.3 Responsibilities

All EBS's individuals (internal and external) shall abide by the new IT Policy and in accordance with this policy; any violations of these policies must be immediately escalated to the senior management of IT Division and the respective staff's immediate manager so that the issue may be appropriately addressed. There shall be zero tolerance on any of the statements of this policy. The goal of zero tolerance is to ensure that everyone fully understands and abides by the policy to minimize risk, protecting all individuals as well as EBS.

1.4 Definition of Non-Compliance

Non-compliance means the conduct of any individual (including employees, clients, contractors, vendors, etc.) that is not supportive of IT policies.

Examples of non-compliance include, but are not limited to, the following:

- Individuals are negligent in applying appropriate securities and controls within the organization
- An individual's action or inaction contributes to the violation of the operational policies and procedures
- An individual does not immediately resolve or escalate issues
- Individuals fail to take appropriate action in response to a complaint or incident

1.5 Violations of this Policy

All individuals (including clients, employees, contractors, vendors) are responsible and will be held accountable for implementing IT Policies and Procedures as outlined in the IT Policy. Individuals who are involved in incidents of non-compliance may be subject to discipline up to and including termination of access to information technology resources.

1.6 Some Definitions

Policy: Policies are high-level management statements, instructions or business rules that provide guidance to enable individuals to make present and future decisions. Policies are mandatory. Special approval is required when anyone wishes to take a course of action that is not in compliance with policy.
For example: (Policy)You must use a UserID and Password when accountability is required.

Standards: Standards are typically collections of system-specific or procedural-specific requirements and are mandatory.
For example: (Standard) Passwords must be a minimum of 6 characters long.

Procedure: Procedures are specific operational steps or manual methods that support a policy or a standard.
For example: The procedure will define how a 6-character password is created

1.7 IT Governance

EBS Information Technology (IT) will be governed through IT Management Council involving the senior executives in IT Department and their deputies. This council will be chaired by the Head of IT and meet once quarterly. Regular input to IT strategy determination for the group will be sought at this meeting.

Policy Statements

Policy 1: Data Protection, Privacy & Confidentiality

Objective

To ensure that personal data collected and processed by EBS is managed in accordance with Data Privacy, Confidentiality and Security rules

Policy

EBS will ensure the security, privacy and confidentiality of any sensitive personal data or information that it collects, receives, possess, stores or deals with

1.1 Personal Information

Personal Information means personally identifiable information with or with combination of other information such as information provided via forms, surveys, applications or other online fields including names, postal or email addresses, telephone, fax or mobile numbers, account numbers, credit/debit card information and biometric information

Sensitive Personal Information includes information collected that is related to the password, financial Information, records and history of the bank's customers, employees of super-agent, sub-agents, EBS employees and third parties

Note: Any information that is freely available or accessible in public domain is not regarded as Sensitive personal information

1.2 Mode of Collecting Personal Information

- EBS Service Delivery Platform (ESDP) captures information, for example, when:
  - Customer submits KYC details for account opening
  - Customer performs banking transactions
  - Customer applies for a loans
  - Customer pays for Value-added services
  - Customer pays for tax and other government utility services such as water, electricity, etc.

- EBS Service Delivery Platform (ESDP) also receives and stores personal information when:
  - any online transaction is done by the agent on behalf of the bank customer
  - via cookies when the super-agent or sub-agent visits ESDP Online Portal

EBS shall not keep any sensitive personal data of information in its Agent Management Platform for longer than required for the purposes for which the information may lawfully be used or is otherwise required by any other law for the time being in force. EBS ensures that sensitive personal information is used only for the purpose for which it is collected.

1.3 Disclosure of Information

EBS never publishes any sensitive personal information obtained from the provider of the information

1.4 Data Security

1.4.1 Physical, Technical and Organizational Security Measures:

EBS takes customer confidentiality and security very seriously. Appropriate technical and organizational security measures to protect personal information, including internal security procedures that restrict access to disclosure of personal data are implemented. EBS uses encryption, firewalls and other technology and security procedures to help protect the accuracy and security of sensitive personal information and prevent unauthorized access or improper use.

EBS adopts best practices like ISO 27001 for physical, technical and organization measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorized processing or access

EBS ensures that unauthorized persons are not allowed to gain access to data processing systems in which sensitive personal data or information are processed. Personal Data in the course of electronic transmission during transport or during storage on a data carrier cannot be read, copied, modified or removed without authorization, and providing a mechanism for checking toe establish who is authorized to receive and who has received the information.

1.4.1 Employee Confidentiality Agreements:

All persons involved in any stage of processing personal data and information explicitly are made subject to a requirement of secrecy which continues after the end of the employment relationship

Policy 2: Information Ownership/Disclosure/Loss

Objective
To ensure the establishment of roles and responsibilities to properly manage and protect information assets

Policy
This policy defines the information security roles and responsibilities of Owners, Custodians, and users of information assets

2.1 Roles and Responsibilities

2.1.1 Responsibility Assignment:

Management shall specifically assign responsibility for the control measures protecting every major production type of information

2.1.2 Roles and Responsibilities of Owners:

Information Owners are senior business unit managers with the authority for acquiring, creating, and maintaining information and information systems within their assigned area of control. Owners are responsible for categorizing the information for which they have been designated an Owner using classifications.

To assist with contingency planning efforts, Owners also are responsible for categorizing information, or specific application systems, according to a criticality scale defined by the IT department. Owners are responsible for authorizing user access to information based on the need to know.

Designated information Owners are responsible for establishing and updating specific written policies regarding the categories of people who will be granted permission to access information. As needed, these policies shall specify limitations on the use of this information by those to whom access has been granted.

2.1.3 Information Owner Training:

The IT department will provide Owners with training, reference material, and consulting assistance so that they may appropriately make these and related decisions and distinctions. Owners also must make decisions about the permissible uses of information including relevant business rules.

Owners are responsible for choosing appropriate information systems, and relevant controls for information handled by these systems, consistent with policies and standards issued by the IT department. For example, Owners must define the validation rules used to verify the correctness and acceptability of input data. These validation rules and other controls for protecting information must be formally approved in writing by the relevant Owner before major modifications can be made to production application systems.

Owners must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security-related control deficiencies pertaining to the information for which they are the designated Owner.

2.1.3 Roles and Responsibilities Of Custodians:

Information Custodians are staff within the IT department, in physical or logical possession of information from Owners. Custodians are charged with the provision of information systems services consistent with the instructions of Owners, including information security measures such as encryption. Using physical and logical access control systems, Custodians shall protect the information in their possession from unauthorized distribution, access, alteration, destruction, or usage.

Custodians also are responsible for providing and administering general controls such as backup and recovery systems consistent with the policies and standards issued by the IT department. Custodians are responsible for establishing, monitoring, and operating information systems in a manner consistent with policies and standards issued by the IT department

Custodians shall provide Owners with regular reports about the resources consumed on their behalf, often through a charge-back system, and reports indicating user activities. Custodians must not change the production information in their possession unless they have received explicit and temporary permission from either the Owner or an authorized user.

2.1.4 Roles and Responsibilities of Users:

Information users are individuals who have been granted explicit authorization to access, modify, delete, or utilize information by the relevant Owner. Users must use the information only for the purposes specifically approved by the Owner. Users are not permitted to make additional copies of, or otherwise reproduce or disseminate sensitive information unless the Owner has expressly agreed. Users also must comply with all security measures defined by the Owner, implemented by the Custodian, or defined by the IT department.

Users must additionally refrain from disclosing information in their possession, unless it has been designated as Public, without obtaining permission from the Owner. Users must report to the IT department all situations where they believe an information security vulnerability or violation may exist using the help desk trouble ticket system or any reporting mechanism.

IT department also must provide users with sufficient time to receive periodic information security training, and users are required to attend such training on a periodic basis. Users of personal computers have special responsibilities, for example relating to backups and virus screening

2.2 Status and Change Review

2.2.1 Changes in Status:

The individuals who play the roles of information Owners, Custodians, and Users will change on a regular basis. It is the responsibility of the local manager of all individuals to promptly report status changes to the IT department. As soon as they are known, status changes must be reflected in the identity repository immediately.

2.2.2 Privilege Transfers:

Custodians must maintain access control systems so that previously-provided user privileges are no longer provided whenever there has been a user status change.

2.2.3 Custodian Reassignment:

When a Custodian has a change in status, it is the responsibility of the Owner to promptly assign a new Custodian, and to assist the new Custodian with the assumption of tasks previously performed by the former Custodian, including necessary training.

2.2.4 Owner Status Changes

When an Owner has a change in status, it is the Chief Information Officer's responsibility to promptly designate a new Owner

2.2.5 Handling of Information Following Status Changes:

Users who change their status must leave all production information with their immediate manager. Soon after a user has a change of status, both computer-resident files and paper files must be reviewed by the user's immediate manager to determine who should be given possession of the files, or the appropriate methods to be used for file disposal or destruction.

The manager must promptly reassign the user's duties and specifically delegate responsibility for information formerly in the user's possession. It is this manager's responsibility to train the new user so that the new user is able to fully perform the tasks previously performed by the former user.

It is this manager's responsibility that the new user become acquainted with the relationships that the previous user had with both insiders and outsiders, and become acquainted with all pending transactions and incomplete projects handled by the previous user.

2.26 Periodic Privilege List Review:

Each calendar quarter, the IT department must provide Owners with a list of users who are authorized to access the information for which the Owners are responsible. Within 10 business days after the receipt of such a list, Owners must return to the IT department their approval of all current permissions given to the users of the information for which they are the designated Owner, and any corrections or deletions that may be necessary.

2.3 Other Considerations

2.3.1 Externally-Supplied Information:

In the course of normal business activities, EBS often takes possession of third-party sensitive information. Whenever a non-disclosure agreement (NDA) has been signed, an internal EBS Owner must be assigned

for information so received. The Owner must promptly report the existence of this third-party information to the IT department for inclusion in the corporate data dictionary.

2.3.2 External Data Labeling:

This third-party information must be labeled with the appropriate data classification category and treated as though it was EBS internal information with the same classification. The roles and responsibilities for Custodians and users are also relevant to externally-supplied information.

2.3.3 Corporate Data Dictionary:

To assist with the management of information, the IT department must compile and annually update a corporation-wide data dictionary and other high-level descriptions of the major EBS information assets found in production systems. It is the responsibility of the chief information officer to ensure that this data dictionary includes a current indication of the Owners for all major EBS production information assets. It is the responsibility of all Owners to know the identity of the Custodians and users for the information types that have been entrusted to their care.

2.3.4 System of Record:

Each Owner must designate a system of record that will serve as the most authoritative copy of the information under his or her care. Updates to this information must be made to the system of record before or at the same time that updates are made to other systems containing this information. It is the Owner's responsibility to ensure that all production copies of the information for which he or she is the designated Owner are maintained with appropriate controls to ensure a reasonable degree of information accuracy, timeliness, and integrity.

2.3.5 Risk Acceptance Process:

In rare circumstances, exceptions to information security policies and standards will be permitted if the information Owner and the chief information officer have all signed a properly completed risk acceptance form. In the absence of such management approval reflected on a risk acceptance form, all Owners, Custodians, and users must consistently observe relevant EBS information security policies and standards.

2.3.6 Notifications of Loss or Disclosure:

If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, its Owner, the chief information officer and the IT department must be notified immediately.

Policy 3: Backup and Restore

Objective
To ensure secure backup capability of all essential data and also ensure that all these data will be accessible in the event of a disaster or other event in which the data would be destroyed

Policy
Establish real-time replication and regular backup schedules within the centralized storage area to ensure backups of sensitive, essential and confidential data to provide ample opportunity to recover a file, folder or database.

The hardware used for EBS Service Delivery Platform (ESDP) consists of two centralized storage devices. One storage device is placed in the Production Site to serve as a primary storage and backup device while the other is placed in the Disaster Recovery (DR) Site to serve as an off-site backup and replication device.

The primary storage device holds all data and backups and serves as the primary device for file access and immediate backup. The secondary, off-site storage device replicates all data from the primary device to create a stable off-site copy of the data and backups present on the primary device.

EBS employs a double backup & restore strategy – HOT & COLD Backup & Restore

3.1 Hot Backup & Restore Strategy

- All data is replicated between storage device on Production Site and storage device on DR Site in an Active-Active mode
- In the event of a loss of data on the Production Site, all information is stored in the secondary device on DR Site and is completely up to date

3.2 Cold Backup & Restore Strategy

- HOT Backup is an excellent solution however it is always useful to perform Cold Backups that can be stored in secure locations
- All data is replicated between storage device on Production Site and storage device on DR Site in an Active-Passive mode
- A cold backup shall be scheduled to run on a set frequency for example Twice or Thrice weekly using reliable Tape drives and Tapes for long-term storage. 4. This allows for multiple copies of the full system to be stored.

- Restores are also performed at defined periodic intervals to confirm validity, correctness and restorable status of the stored data.

Policy 4: Network Security

Objective

To ensure the highest level of confidentiality, integrity, and availability when the EBS platform's network interacts with and exchanges data across public networks

Policy

EBS will ensure that measures are taken to prevent and address illicit external activities that threaten the organization's network and the data which travels on the network.

4.1 Surveillance and Incident Detection

- Where technically possible violation and security activity must be logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity, port scanning attacks, denial of service attacks, spam, etc. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.
- A computer security incident handling capability must be established to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities.
- Incident management responsibilities and procedures must be established to ensure an appropriate, effective and timely response to security incidents.

4.2. Protection of Security Assets

- All security related hardware and software shall at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, security design information must be limited on a need-to-know basis, but security should not be based on the design being secret.
- Taking into consideration the related facilities, devices, employees and validation methods used, the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information must be protected.
- Procedures and protocols shall be established and implemented for the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure. If a key is compromised, the information must be propagated to any interested party through the use of Certificate Revocation Lists or similar mechanisms and the keys changed.

4.3 Protection against External Threats

- The networks shall be protected against malicious software, such as computer viruses or Trojan horses, by a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting.
- Connection to the Internet or other public networks shall be adequately safeguarded. Firewalls and intrusion detection must be operative to protect against denial of services and any unauthorized access to the internal resources; must control any application and infrastructure management flows in both directions; and must protect against denial of service attacks.
- Use of Personal Laptops, Notebooks and other personal effects on the organization's network is prohibited without express written pre-approval from IT department

4.4 Office Automation Network Specific Policy

- Control practices must be implemented to verify the authenticity of any counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.
- Where appropriate, controls must be implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system. This requires use of cryptographic techniques or tokens for signing and verifying transactions.
- Management must ensure that, where appropriate, transactions cannot be denied by either party, and provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third-parties, with appropriate policies that take into account relevant regulatory requirements.
- Where high levels of confidentiality or integrity are required, transaction data must only be exchanged over a trusted media.

.

Policy 5: Encryption

Objective
To ensure that encryption is applied to protect the confidentiality of sensitive and critical information

Policy
EBS shall ensure that a proven standard algorithm such as Advanced Encryption Standard (AES) is used as the basis for encryption technologies. This algorithm represents the minimum actual cipher used for EBS platform and network

5.1 Data Encryption

Data classified as senstive and critical that is stored and transmitted on the EBS platform is encrypted. AES encryption with 128-bit keys provides adequate protection for classified information up to the SECRET level so this should be the minimum level utilized by the platform.

Similarly, Ephemeral Unified Model and the One-Pass Diffie Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA) using the 256-bit prime modulus elliptic curve as specified in FIPS PUB 186-3 and SHA-256 provide adequate protection for classified information up to the SECRET level.

During the transition to the use of elliptic curve cryptography in ECDH and ECDSA, DH, DSA and RSA can be used with a 2048-bit modulus to protect classified information up to the SECRET level.

5.2 Use of Encryption

- Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.
- Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.
- Procedures for the use of cryptographic controls for the protection of information must be developed and followed. Such procedures are necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.
- When developing procedures the following should be considered:
  a. the management guidelines on the use of cryptographic controls across the organization,
  b. including the general principles under which business information should be protected,

c. the approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys,

d. roles and responsibilities, e.g. who is responsible for: the implementation of the procedures; the key management,

e. how the appropriate level of cryptographic protection is to be determined, and

f. the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes)

Policy 6: Password

Objective

To ensure that properly chosen passwords are used and secured by all users of the EBS platform

Policy

EBS will establish rules to ensure users of the platform properly select and secure their password

7.1 Password Criteria

All passwords will meet the following criteria:

- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- All user-level passwords must be changed at least every 120 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must NOT be inserted into email messages or other forms of electronic communication
- Passwords should be strong with the following characteristics:
    - Contain between 8 and 32 characters
    - Contain both upper and lower case characters (e.g., a-z, A-Z)
    - Contain at least one number (e.g., 0-9)
    - Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
    - Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
    - Does not contain personal information, names of family, etc.

Policy 7: Third-Party Connection

Objective
To protect the information assets accessed by third party resources

Policy
Access by third parties to any IT asset will be strictly limited and controlled. An Assessment of third party access risks will be made and controls appropriate to producing an acceptable level of residual risk will be put in place. Third party contracts will include specification of responsibilities and consequences for unauthorized access to EBS Service Delivery Platform (ESDP).

8.1 Access Request and Approval

Access to EBS Service Delivery Platform (ESDP) will be provided to third parties having a business need for the same. All access will be provided only after approval from the relevant authority.

8.2 Privilege Allocation

Necessary privileges will be allocated by the respective Super-Agent Management Teams and and EBS Management Teams. Super-Agent Management Teams and EBS Management Teams are responsible for disabling the access after requested time

8.3 Connection on Internal Network

If access is required on the internal network, the third-party user machine will meet CBN's IT Security standards.

8.4 Remote Network Access

External network connections to the EBS Service Delivery platform (ESDP) will be separated by Firewall. Remote access to ESDP's network will be secured.

8.5 Non-disclosure Agreements

Third party vendors will sign non-disclosure/confidentiality agreement with EBS as drafted by legal department

8.6 Penalties

Non-compliance with the non-disclosure/confidentiality agreements and contracts signed with EBS can lead to penalties to Third Party Vendors

Policy 8: Incidence Response

Objective
To ensure quick, effective and orderly response to incidents

Policy
EBS shall ensure that incident management responsibilities and procedures are established

8.1 Incident Types

EBS shall establish procedures to cover all potential types of security incidents, including:

- information system failures and loss of service,
- denial of service,
- errors resulting from incomplete or inaccurate business information, and
- breaches of confidentiality.

8.2 Corrective Actions

In addition to normal contingency plans (designed to recover systems or services as quickly as possible), the procedures must also cover:

- analysis and identification of the cause of the incident,
- planning and implementation of remedies to prevent recurrence, if necessary,
- collection of audit trails and similar evidence,
- communication with those affected by or involved with recovery from the incident, and
- reporting the action to the IT department.

8.3 Audit Trail

Audit trails and similar evidence must be collected and secured as appropriate, for:

- internal problem analysis,
- use as evidence in relation to a potential breach of contracts, policies, or regulatory requirements,
- use in the event of civil or criminal proceedings, e.g. under computer misuse or information protection, and

8.4 System Control

Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures must ensure that:

- only clearly identified and authorized staff are allowed access to live systems and information,
- all emergency actions taken are documented in detail,
- emergency action is reported to management and reviewed in an orderly manner, and
- the integrity of business systems and controls is confirmed with minimal delay.

Policy 9: Physical Security

Objective
To minimize losses from theft, interference, environment hazards, damage to, or inappropriate disposal of information assets

Policy
EBS will ensure adequate physical security mechanisms are provided and are commensurate with the level of security required for that class of information assets EBS will ensure adequate safeguards are provided against environment hazards for all information assets based on their classes

Various areas within the premises comprise sensitive and valuable information and equipment. The physical layout of the premises may restrict the methods that may be used to ensure that only authorized individuals are able to gain physical access to such sections. In order to achieve adequate physical security, EBS will ensure efforts are directed towards protecting:

- secure areas; and
- equipment installed therein

10.1 Secure Areas

EBS will ensure that appropriate access control mechanisms are provided to prevent unauthorized damage, access and interference to data center and information assets

10.2 Equipment Security

IT equipment will be protected as far as possible from environment hazards and unauthorized access. Equipment security controls shall be implemented to prevent loss, damage, theft, or compromise of information systems and interruption to providing agent banking services

Policy 10: Business Continuity and Disaster Recovery

Objective

To ensure that ensure IT services are available as required and to ensure a minimum business impact in the event of a major disruption

Policy

EBS shall ensure that Integrated Disaster Recovery and Business Continuity Plans are established to reduce or eliminate the impact of unexpected events by proactively identifying and documenting the essential components and actions necessary to restore the computing infrastructure and applications which facilitates the continuance of critical agent management and banking services. These plans limit loss to the Bank by reducing uncertainty during an outage or event, and facilitate a quick, organized, efficient, and effective response

10.1 IT Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

- IT Business Continuity Plans must be in line with the overall Business Continuity Plan to ensure consistency. Furthermore, the IT continuity plan should take into account the IT long- and short-range plans to ensure consistency.
- IT Management will undertake a formal risk assessment to determine the requirements for a BCP.
- IT Management will develop a BCP that covers all essential and critical business activities.
- The BCP must meet all regulatory requirements.
- IT Management must develop a DRP and assign a Recovery Time Objective (RTO) to all applications and computing infrastructure that support critical business processes.
- DRPs must satisfy the requirements of the BCPs and meet applications RTOs.
- Executive Management is responsible for declaring an emergency and the activation of BCPs and/or DRPs.

10.2 Critical IT Resources

- The continuity plan shall identify the critical application programs, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs. Critical data and operations should be identified, documented, prioritized and approved by the business process owners, in cooperation with IT management.
- A Business Impact Analysis (BIA) must be completed for all critical processes. Disaster Recovery Plans (DRPs) must be developed that address the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all applications supporting critical business processes.

10.3 IT Business Continuity Plan and Disaster Recovery Plan Contents

Written plans (both BCP and DRP) shall be developed and contain the following at the very least:

- Guidelines on how to use the continuity plan
- Emergency procedures to ensure the safety of all affected staff members
- Response and recovery procedures that contain predetermined prioritized actions on how to respond to a disruptive event, activate the plan, recover critical business processes, and bring the business back to the state it was in before the incident or disaster.
- The identification of alternate work locations and alternate work procedures (if necessary) if the primary site is unavailable. Procedures to equip the alternate work site (including telecommunication systems, telephone, etc.), including contracts with third parties.
- Procedures to safeguard and reconstruct the home site
- Inclusion of reconstruction plans for re-recovery of all systems resources at original location
- Co-ordination procedures with public authorities
- Communication procedures with stakeholders, employees, key customers, third party Service providers and management.
- Critical information (such as current names, addresses, telephone/GSM numbers of key personnel, etc.) on continuity teams, affected staff, customers, public authorities and media.

10.4 Minimizing IT Business Continuity and Recovery Requirements

EBS Management shall establish procedures and guidelines for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.

10.5 Maintaining the IT Business Continuity and Disaster Recovery Plans

- The BCP and DRP must be reviewed and maintained, at a minimum, annually or upon major changes to the business or IT infrastructure.
- IT Management must provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires that continuity plan maintenance procedures aligned with change and management and human resources procedures.
- The plan must be updated to incorporate business and IT environment changes. Such changes include, but are not limited to, business priorities, new or decommissioned business processes, alternate work strategies, alternate site strategies, personnel changes, etc.

10.6 Testing the IT Business Continuity and Disaster Recovery Plans

- The BCP and DRP must be tested, at a minimum, annually or upon major changes to the business or IT infrastructure. This requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.
- In areas where applications and supporting infrastructure are substantially similar, DRP testing may be conducted with a sampling of priority applications that are representative of the computing environment. All other priority applications must be certified to the process. The certification must be reviewed whenever major changes are made to an application.

10.7 IT Business Continuity and Disaster Recovery Plans Training

- An awareness and training plan must be developed. The disaster continuity methodology must ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.

10.8 IT Business Continuity Plan and Disaster Recovery Plan Distribution

- Given the sensitive nature of information in the continuity plans (both BCP and DRPs), they must be distributed only to authorized personnel and should be safeguarded against unauthorized disclosure. Consequently, sections of the plan need to be distributed on a need-to-know basis.

10.9 Back-up Site and Hardware

- EBS Management shall ensure that the continuity methodology incorporates an identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these types of services should be concluded.
- Arrangements must be made for processing applications at an alternate backup site if the original location is damaged/destroyed or otherwise unavailable. Processes must be in place to ensure that essential supplies and equipment are available to support application RTOs. , store essential equipment or there must be processes in place to reorder or procure such material in a timely manner. If stored, they must be kept in a different building with sufficient distance from the original location to ensure their availability in the event that a disaster occurs in the original location. Essential supplies and equipment may include critical forms, paper stock, magnetic media, tapes, printers, etc.

10.10 Backups and Off-site Storage

- Essential data, programs, and documentation for computing infrastructure and applications must be backed up to support recovery and business continuity plans.

10.11 Wrap-up Procedures

On successful resumption of the IT function after a disaster or a test, IT management shall establish procedures for assessing the adequacy of the plan and update the plan accordingly.

Assigned IT Devices and Equipment

This policy serves as guideline to all EBS Staff (FTEs and Consultants) on how EBS assigned IT assets are:
(a) Requisitioned (b) Assigned (c) Managed (d) Returned or Incident as may apply.

1. All EBS staff are assigned IT asset upon when onboarded as EBS FTE Staff or Consultant-Such assets must be tagged and provisioned with assigned EBS ID tags.
2. Such assets remain as provisioned to the Employee/Consultant's SOLE use throughout their employment as EBS Employee/Consultant and SHOULD not be shared or transferred to any 3rd party unless authorized to do so **(This must have signed approval by EBS mgmt.)**.
3. **SECURITY** – For avoidance of spread of Malware/Viruses, assigned IT asset must not be used for downloading non-business-related materials such as movies or other prohibited materials that can introduce Malware or viruses.
4. The same applies to the use of the office Internet/WIFI services that has been open for business use to all staff for all business-related services – Any employee found connecting their phones or Laptops for downloading of non-business-related items shall be reprimanded according to the EBS related disciplinary process for abuse of company resource(s).
5. Replacement of assigned IT asset shall follow the defined process of logging a request using a Staff IT Asset(s) replacement form – In such situation the asset being replaced must be certified as working ok just as when it was assigned including all assigned peripherals especially the device power cable and other related materials. The asset replacement form can be found at https://drive.google.com/drive/folders/1lQsfQLPRDm0GYzChi-G-PbXqQPwm55B0?usp=share_link and state clearly reason(s) for the replacement.
6. **UNDER NO CIRCUMSTANCES MUST AN IT ASSET BE REPLACED WITHOUT THE STATED FORM AND APPROVAL BY THE RELEVANT LINE MANAGER OR MGMT!**
7. Faulty devices must be reported to the head of IT and escalated to the management stating the specific fault(s)
8. The IT team lead is the only authorized person permitted to have access to where such devices are kept and no other person unless authorized to do is authorized to perform this function.
9. As part of the EBS exit process the assigned IT assets must be confirmed ok and all returned as provisioned when being onboarded as EBS staff, failure to do means that individual exit will remain **PENDING AND UNAPPROVED INCLUDING DUE PAYMENTS ESPECIALLY FINAL SALARY DUES AS WELL AS OTHER ENTITLEMENTS**.
10. (9) must be (a) Confirmed by Head of IT, and (b) HR and EBS Operations Head – ONLY!!
11. In the event of theft or loss, staff members are expected to report the situation to the management within 24hrs with a police report to validate the claim.
12. Failure to comply with the above will be regarded as gross misconduct and shall be treated in line with EBS' disciplinary policy.

Asset Handling

Employees are responsible for the proper management/handling of the asset allocated to them. Each employee is responsible for its usage and should any issue arise, the cost of repair will be borne solely by the employee. The underlisted guidelines will aid usability of allocated assets:

Employees should also note that overcharging laptops can lead to various issues, including reduced battery lifespan, diminished performance, and potential safety hazards. To ensure the longevity and optimal functioning of our electronic devices, it is crucial that we all take responsibility for properly managing our laptop charging habits.

Based on this, employees are required to adhere to the following guidelines:

1. Unplug when fully charged: Once your laptop is fully charged, please disconnect it from the power source promptly. Leaving laptops plugged in for prolonged periods can lead to unnecessary stress on the battery.

2. Utilize power management settings: Ensure that your laptop's power management settings are configured appropriately. This includes setting up sleep and hibernation modes to conserve power when not in use.

3. Report issues: If you notice any issues with your laptop's battery or charging performance, promptly report them to the IT department. Do not attempt to fix or replace the battery yourself.

IT SHOULD BE NOTED THAT ALL EMPLOYEES SHALL BEAR THE COST OF REPAIR/REPLACEMENT OF ANY ALLOCATED ASSET IF THE CAUSE OF DAMAGE WAS ESTABLISHED AS A CASE OF MISHANDLING AND VIOLATION OF STATED IT POLICY.

Consent

I consent to bear the cost of repair/replacement of any asset allocated to me if the cause of damage is established to be as a result of my mishandling, negligence or violation of the details stated in this IT policy document.

NAME OF EMPLOYEE: _____

SIGNATURE: _____

DATE: _____