NEXTBEWE NIGERIA LTD.

Information Security Policies

Version No.: 1.0

Date: 27th Feb 2023

1. Mobile device policy

Procedure:

NextBewe has provided a mobile device to the team that requires it for mobile device related tasks, this device will be securely connected to NextBewe's secured access points .

2. Teleworking policy

Procedure:

Teleworking requests are handled in accordance with the organization policy. Approval has to be obtained from line managers for teleworking. Adequate teleworking security measures are implemented as given below:

- A secure communication channel is established between the teleworkers and the networks of NextBewe using VPN (either NextBewe's or client provided) through which connect to the client's machine remotely

- Use of a secured VPN authentication mechanism is employed which is in line with access control policy for authenticating those users who are working remotely

- Mobile devices provided by NextBewe are protected against damage and unauthorized use. Employees to designate a workspace at home that is maintained in a safe condition, free from hazards. All the employees are to store the business related data into their respective (clients / NextBewe's) cloud storage to safeguard against loss of data

3. Acceptable use Policy (of assets)

Procedure:

Employees and external users using organization's Information or information processing facility are governed by rules for acceptable use of assets such as

- For local and remote systems require username, passwords and authentication

- For corporate email, Internet browsing, use of portable computers etc. are covered by a suite of guidelines developed and maintained by the NextBewe management

- Employees and external party users using or having access to the NextBewe assets shall be aware on the information security requirements of the organization assets associated with information and information processing facilities

- Employees responsible for their use of any information processing resources and of any such use carried out under their responsibility.

4. Information classification and handling policy

Procedure:

All information assets are classified according to this procedure. All information is handled according to the classification levels to ensure security of the information assets. The information is classified into the following categories:

- Public
- Internal
- Restricted
- Confidential

Public	Disclosure inside or outside organization would not cause any damage or inconvenience.
Internal	Disclosure inside the organization for effective implementation of procedures and processes would not cause any damage or inconvenience
Restricted	Disclosure inside or outside organization would be inappropriate and inconvenient.
Confidential	Disclosure inside or outside would cause significant harm to the interest of the organization.

Risk assessment enables NextBewe to focus on asset protection mechanisms for those assets that are most susceptible to specific risks. Information assets are assigned based on their susceptibility to risk.

The information asset classification guidelines consider the following:

- The type of asset (data or information systems process)
- The criticality of the asset
- The Information asset value
- The impact of a security breach
- The possibility of using inference and aggregation techniques to obtain information at a higher classification level from information at a lower classification level
- Criteria for giving access to information assets
- The extent of access (read, modify, delete, etc.) is given to different users

This information classification is applicable to all information, whether stored or transmitted, which is in the possession or under the control of NextBewe. For example, confidential information entrusted to the company by its customers, suppliers, business partners and others is protected with the information classification. Similarly, the employees are expected to protect third party information with the same care that they protect information belonging to NextBewe. For the purpose of this information classification, no distinctions between the words data, information and knowledge are made.

The information of NextBewe is consistently protected throughout its life cycle, from its origination to its destruction. Information is protected in a manner commensurate with its sensitivity; no matter where it resides, what form it takes, what technology was used to handle it, and what purpose it serves. Although this information classification provides overall guidance, to achieve consistent information protection, employees have to apply and extend these concepts to fit the needs of day-to-day operations.

5. Access Control Policy

Procedure:

- Manager – Facilities is responsible for creating and implementing physical access control to employees
- Manager – IT is responsible for giving access to network and system and to create user id
- HR approval is required to authorize issuance of user & network IDs and resources privileges.
- Only authorized users are allowed access to the information systems of NextBewe
- Access rights for users are granted based on the following aspects:
    - Sensitivity level of information
    - Information dissemination and entitlement policies e.g. “need-to-know” and “need-to-do” principles, segregation of duties, etc.
- Access privileges are individually defined for the different information systems (e.g. operating systems, databases, application systems, MIS portals etc.) used in NextBewe. The access privileges are based on needs and the security requirements specific to that information system.
- The IT and facilities teams review the physical & network access control system once in six months. Upon intimation from HR, both the departments are responsible for removing access based on exit information and notifying of redundant user IDs and accounts back to HR team.
- Configuration plan defines the access requirements for individual departments to perform the business functions.
- Terminals are identified through unique IP addresses.

Access controls are implemented based on policy and business requirements.

6. Policy on the use of cryptographic control

Procedure

This policy applies to information involved in the development or modification of enterprise level, centrally-managed mission critical applications that support NextBewe.

Cryptographic controls are used to achieve different information security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted

b) integrity / authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information

c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action

d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources

This policy covers encryption for Desktop, laptop, hard disks, external drives, removable media and e-mail. Full disk encryption is rolled out to all computers across the organization. The encryption software employed for use at NextBewe is **AES 128-bit/AES 256-bit** (Advanced Encryption Standard) which is a symmetric-key encryption with a 128-bit key. Any confidential data that is transmitted through the web will be encrypted using SSL/TLS.

The IT team carryout encryption as part of systems (desktops, laptops) upgrade via the build process. Organization data is not stored on computers or portable media devices unless access is required when network connectivity is not available. When it is necessary, restricted and controlled data only is stored on encrypted devices.

Where exceptions have been identified for not encrypting specific devices, computer policy settings (enforced at domain level) which enable / disable encryption can be applied individually to a specified computer and/or groups of computers.

When a portable data storage device is used, the instructions for the correct use of encryption is followed to ensure the data is encrypted. Personal storage media and equipment are not connected to the organization's network and not used for storing organization data. Other portable USB devices include mobile phones, cameras, PDAs etc. These other devices should not be used to store organization data. The IT Service Desk will advise on the best method to encrypt individual files.

For encryption of portable storage devices, the user needs to set a password for accessing the device. The password for encrypted portable devices is in line with the organization's password policy and enforced at the domain level. Using the portable device on any other computer after being encrypted requires a password in order to access it. It is important that passwords used to encrypt devices are approved by managers, so that in the event an employee leaves, the organization can access the organization's data. Computers requiring encryption for the protection of vulnerable and sensitive data will use Windows/Antivirus Bit locker encryption.

7. Key management

Procedure:

The management of cryptographic keys is essential to the effective use of cryptographic techniques. All cryptographic keys used to protect against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system is based on an agreed set of standards, procedures, and secure methods for:

- Generating keys for different cryptographic systems and different applications
- Generating and obtaining public key certificates
- Distributing keys to intended users, including how keys should be activated when received
- Storing keys, including how authorized users obtain access to keys
- Changing or updating keys including rules on when keys are to be changed and how this will be done
- Dealing with compromised keys
- Revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived)
- Recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information
- Archiving keys, e.g. for information archived or backed up
- Destroying keys
- Logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys should be defined so that the keys can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk. In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services. In order to reduce the likelihood of improper use, activation and deactivation dates for keys are defined so that the keys can only be used for the period of time defined in the associated key management policy.

In NextBewe, the digital signatures are used for certain regulatory requirements to ensure the authenticity of data, e.g. for uploading all statutory requirements such as filing Registrar of Companies (RoC) returns, Income tax filing etc.

8. Physical and environmental policy

Policy

NextBewe shall provide adequate protection to its information, information processing facility and their supporting infrastructure against unauthorized physical access and environmental threats. The policy addresses

- appropriate procedures to administer to ensure physical protection which safeguard the necessary IT infrastructure
- issues related to physical security perimeter, physical entry controls, working conditions, securing office area, server rooms, equipment security and general controls
- protect from environmental threats by implementing environmental controls to prevent damage from environment
- regularly conduct the preventive maintenance to utility equipment to ensure trouble free uninterrupted services

9. Clear desk & clear screen policy

Procedure:

Sensitive or critical business information on paper or on electronic storage media is locked away when not required; computers and terminals are left logged off or locked when unattended.

The clear desk and clear screen policy take into account the information classifications as legal, contractual, restricted and confidential requirements, corresponding risks of the organization.

The following guidelines are considered:

- Confidential or restricted information, e.g. on paper or on electronic storage media is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.
- Computers and terminals are left logged off or protected with a screen and keyboard locking mechanism controlled by a password or similar user authentication mechanism when unattended and are to be protected by key locks, passwords or other controls when not in use.
- Incoming and outgoing mail points machines are protected.
- Unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) are prevented
- Documents containing confidential or restricted classified information is removed from printers immediately
- Staff ensures their desks are clear every evening before leaving
- Handle any piece of paper only once - act on it, file it, or put it in the bin
- All computer systems shall have password protected screen saver which will enable the system to get locked after two minutes of being idle

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion shall be analysed in Risk Assessment & management.

10. Operational security policy

a. Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities

b. Documented Operating Procedures

All the process procedures are documented by all process owners. They are responsible for developing and revising them from time to time or as per requirements, if necessary and take approvals for revising / changing process and procedure documents before implementing them.

Documented operating procedures are prepared for all functions / activities associated with information processing and facilities and ensures that:

- Segregation of duties and responsibilities; conflict of interest made available centrally to all employees
- only controlled copies (PDFs) are shared and changes are to be authorized by the IT - Manager
- respective functional / department heads are responsible to ensure that the standard operating procedures are revised from time to time and up to date

Documented procedures are prepared for the following:

- ISMS manual defining ISMS policy
- Documented information for internal audit, management review, statement of applicability, risk assessment and functional process procedures
- Control objectives and controls
- Work instructions, templates etc
- Backup, equipment maintenance wherever required
- Installation and configuration of systems, scheduling requirements

c. Protection from malware

Objective:

To ensure that information and information processing facilities are protected against malware.

- The following aspects are implemented as part of malware control within information security framework:
    - IT Team to ensure that Anti-Virus software is installed at all possible entry points (Servers, Desktops, etc.) of viruses and malicious software
    - Antivirus is installed on all workstations within the inventory of NextBewe to setup with auto-update on all workstations and admin access is required to change this configuration. Monthly review of antivirus findings is done by IT team and are reviewed and tracked for closure by IT team.
    - Antivirus system is setup on exclusive intranet servers and updates are 'pushed' to all workstations on real time basis.
- Websites that are determined as malicious by security team will be blocked through firewall device.
- Weekly scans are scheduled every Friday on the user machines.
- The update of anti-virus definitions is automatically pulled when client machine is connected to the internet.
- Updates include upgrades that are the newer versions of the anti-virus software. It is the responsibility of the IT to procure and provide newer versions/engines of Anti-virus programs in regular and timely manner and ensure a quick rollout.
- IT Team checks the logs to review whether the desktops / laptop computers / servers were infected with viruses. They report all such incidents to the IT Manager

  every month about virus incidents detected and removed during that month.
- IT Team reviews the anti-virus software activity / logs, especially to check whether the users are running the AV system regularly on their desktop computers (in case the user has the option to stop the scan).
- IT Team also checks all the servers / desktops at random to ensure that they are updated with latest version

d. Information back up

Procedure:

NextBewe's critical information, system images, device configurations and logs are backed up and tested regularly. Backup scheduling of critical files and folders are carried out manually. The IT Infrastructure team implements backup schedules on all important / critical folders of Servers.

All backups are stored in a cloud environment.

The roles and responsibilities for backup activities are as mentioned below.

Activity	Responsibility
Backup important data, software, and test regularly for restorability	IT Infrastructure
Review of the backup logs need to be performed to verify the integrity in taking the backup to external media	
Backup Methodology: Backup process is initiated on server **Backup Frequency**: ● Daily backup for firewall - automatic ● Monthly – Full – Network devices and servers **Backup Media** : Cloud	IT team
Retention period: 2 quarters for full backup (Monthly) Access Controls to other media is restricted by IT Manager	IT Manager
Deletion / Erasing / Disposal of Data: As suggested by the Management and IT Manager	Management / IT Manager

e. Management of technical vulnerabilities

Procedure:

Appropriate, timely action is taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

- NextBewe has identified a 3rd party vendor for carrying out technical vulnerability testing once in a year.
- Information resources that are used to identify relevant technical vulnerabilities and to maintain awareness about them is identified for software and other technology (based on the asset inventory list, these information resources are updated based on changes in the inventory, or when other new or useful resources are found
- A timeline is defined to react to notifications of potentially relevant technical vulnerabilities
- Once a potential technical vulnerability has been identified, NextBewe identifies the associated risks and the actions to be taken; such action involves patching of vulnerable systems and / or applying other controls

- Depending on how urgently a technical vulnerability needs to be addressed, the action taken is carried out according to the controls related to change management or by following information security incident response procedures
- If a patch is available, the risks associated with installing the patch is assessed (the risks posed by the vulnerability is compared with the risk of installing the patch)
- Patches are tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls are considered, such as
    - Turning off services or capabilities related to the vulnerability
    - Adapting or adding access controls, e.g. firewalls, at network borders
    - Increased monitoring to detect or prevent actual attacks
    - Raising awareness of the vulnerability
- An audit log is kept for all procedures undertaken
- The technical vulnerability management process is monitored once in a year and evaluated to ensure its effectiveness and efficiency
- Systems at high risk are addressed first.

The correct functioning of an organization's technical vulnerability management process is critical to NextBewe therefore, regularly monitored.

An accurate inventory is essential to ensure that potentially relevant technical vulnerabilities are identified. Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures. Vendors are often under significant pressure to release patches as soon as possible. Therefore, a patch may not address the problem adequately and may have negative side effects. Also, in some cases, uninstalling a patch may not be easily achieved once the patch has been applied. If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users.

f. Restrictions on software installations and use

Procedure:

NextBewe defines and enforce strict policy on which types of software users may install. The principle of least privilege is applied. If granted certain privileges, users may have the ability to install software. NextBewe identifies what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges are granted to IT dept. Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.

All such testing is done on standalone system and if found suitable, they are implemented at the organization level.

11. Communication security

a. Information transfer policies

Procedure:

- In cases where transfer / delivery of information to the customer are stipulated contractually, the same are documented in the contract / agreement with the customers.
- The projects / departments / procedures / plans (e.g. configuration plan) identifies the exchange / delivery mechanism and any specific security requirements during the transfer.
- The respective project / department head is responsible for compliance with the contractual requirements.

12. IS policy for supplier relationship

Procedure:

NextBewe has effective procedures for controlling and monitoring the outsourced activity, to ensure CIA of information, enabling it to receive services and conduct its operations without any interruptions. It ensures that all suppliers are adhering to above policy.

NextBewe conducted a risk assessment to identify potential risks to its Information Security as a result of outsourcing information or data processing functions or services by third party organizations. This risk assessment considered the following criteria:

- The type of information or data processing functions or services that are outsourced
- The risk classification of the information or data processed by this system
- The reasons for outsourcing the function or service
- Background information about the third party
- The availability and effectiveness of the controls that are to be implemented to regulate and monitor the confidentiality, integrity and availability of the information processed by the suppliers

A formal contract, legally validated is entered between NextBewe and all suppliers providing service to NextBewe or using the NextBewe's information systems. The services to be provided by these suppliers are covered by a strong Service Level Agreement (SLA) that takes into consideration expected levels of service, security, monitoring, contingency and other stipulations as appropriate.

Contracts include information security requirements to ensure compliance to NextBewe's security policies and procedures. All contractors are required to provide information to NextBewe about related subcontractors and obtain its permission for the subcontracting, prior to initiation of work by the subcontractor.

Non-Disclosure / Confidentiality agreements to protect the NextBewe's information assets are signed by suppliers, third parties, contractors and also by sub-contractors of the vendors. A formal process is in place to ensure that service problems are addressed and managed without affecting the quality of the service provided. All suppliers who are working in the premises, need to submit their background verification / police verification report.

All suppliers are required to sign confidentiality and / or a non-disclosure agreement with NextBewe at the time of entering into agreement of their appointment, binding them from disclosing any classified information other than public releases. Third party users or contract staff also has to sign a confidentiality agreement prior to being provided access to information processing facilities. All confidentiality and/or non-disclosure agreements include information security requirements and tenure etc.,

NextBewe ensures that all outsourced personnel are verified for their back ground verification / police verification.

13. Compliance

a. Privacy and protection of personally identifiable information

Policy:

To carefully review and provide proper guidance for protection of personally identifiable information (PII) shall be ensured as required in relevant legislation and regulation where applicable.

Procedure:

An organizational data protection and privacy policy in line with ISO 27018 is developed and implemented. This policy is communicated to all persons involved in the processing of personal information.

Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who can provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that are followed.

Responsibility for handling personal information and ensuring awareness of the data protection principles are dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information are implemented.

A number of countries have introduced legislation placing controls on the collection, processing, and transmission of personal data (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data to other countries.

14. NextBewe-Specific Data usage Policy:

- If you have access to the NextBewe's computers including email (includes client issued email) and access to the internet as part of your job, you must not abuse this by using these facilities for purposes unrelated to NextBewe business.
- Limited personal use of the internet is permitted during your formal breaks. All internet use is monitored and accessing pornographic or other unsuitable material, including auctions or certain social networking sites is strictly prohibited and would be considered a serious disciplinary offence which may result in dismissal.
- Only software packages properly authorized and installed by NextBewe or its clients may be used on NextBewe equipment, you must therefore not load any unauthorized software onto NextBewe computers.
- If you have a NextBewe email address (includes client issued email), this is provided for responsible use on NextBewe business and should not be used in any other way whatsoever.
- You must not refer to NextBewe or its clients, or represent yourself on behalf of NextBewe or its clients on social media without formal permission from NextBewe with the exception of Linkedin
- All staff must make themselves familiar with NextBewe's Internet & Email Policy available from your line manager.

15. Nextbewe General Internet, Data, Email, Computer Acceptable Use Policy:

a. Internet usage guidelines:

- Employees are only allowed to use the internet and computer resources for work-related purposes during work hours.

- The use of the company's internet and computer resources must not violate any laws, infringe on the rights of others, or compromise the security of the company's information and technology.

- Employees are prohibited from downloading copyrighted material without proper authorization

- Limited personal use of the internet is permitted during your formal breaks. All internet use is monitored and accessing pornographic or other unsuitable material, including auction or certain social networking sites is strictly prohibited and would be considered a serious disciplinary offence which may result in dismissal.

b. Email and Communication Guidelines:

- Employees must use the company's email and communication tools for business purposes only and must not use them for personal or illegal purposes.

- Sensitive information, including confidential and proprietary information, must not be disclosed through email or any other communication tools without proper authorization.

- Employees must use professional language and tone in all electronic communications

c. Data / information Security:

- Employees must keep confidential information secure by using strong passwords, encryption, and data backup.

- Employees must not share passwords, leave computers unattended without logging out, or leave confidential information accessible to unauthorised individuals.(lock your computers when stepping away from your PCs)

- Employees must not attempt to bypass web browsing firewalls and administrative access to install software.

- Employees must regularly back up data and store backup copies in secure locations

d. Remote Work Policy:

NextBewe currently does not support remote working, in future case of remote working, the below will apply:

- Remote workers must comply with all company policies, including data security and acceptable use, while working remotely.

- Employees are prohibited from using personal devices for work purposes without prior approval.

e. Mobile Device Management (Mobile phones, Tabs, Ipads):

NextBewe doest allow personal devices for work, but in future, the below will apply:

- Employees may use their personal devices for work purposes, but they must comply with the company's data security policies and authorization.

- The company may install security software on personal devices used for work purposes to protect company data.

- Employees password protect all personal devices used for work purposes

- Employees are prohibited from downloading unauthorised software or apps on personal devices used for work purposes.

f. Social Media Policy:

- Employees must not use social media to disclose confidential information, harass others, or engage in any activities that might harm the reputation of the company.

- Employees must identify themselves as employees of the company when posting on social media platforms while referencing Nextbewe

- Employees must maintain a professional demeanor and tone when using social media for work purposes.

g. Software and Hardware Management:

- Employees must not install software or hardware on company-owned computers without proper authorization.

- The company is responsible for maintaining, upgrading, and repairing software and hardware.

- Employees must not bring personal computers to the office and plug in the network cable without proper authorization.

h. Training and Support:

- The company and its clients will provide training and support to help employees perform their jobs effectively.

- Employees are required to attend mandatory training sessions by the IT department.

i. Reporting Incidents:

- Employees must report any security incidents, such as hacking and phishing attempts, to the company immediately.

- The company will investigate and respond to reported incidents in accordance with established procedures.

j. Consequences of Misuse:

Employees who violate the acceptable use policy, data security policies, or any other company policies may face disciplinary action up to and including termination.

The company reserves the right to take appropriate action to protect its information, technology, and reputation.

Signed:

Parikshith Reddy

CEO

Date:

27/02/2023