NEXTBEWE NIGERIA LTD.

ISMS Manual

Document ID: NXB-ISMS-Manual
Version No.: 1.0
Date: 27th February 2023

Address:

19, Lafiagi street, G.R.A,
Ilorin,
kwara - 240101
Nigeria
www.nextbewe.com

Table of Contents

Document Revision History 3
1 Scope 4
2 Normative references 4
3 Terms and definitions 4
4 Context of the organization 5
4.1 Understanding the organization and its context 5
4.2 Understanding the needs and expectations of interested parties 6
4.3 Determining the scope of the Information Security Management System(ISMS) 7
4.4 Information Security Management System 8
5 Leadership 10
5.1 Leadership and commitment 10
▪ Environment for people to flourish 10
▪ Pursuit of Excellence 10
▪ Integrity and respect above all 10
▪ Customer Delight 10
5.2 Policy 11
5.3 Organizational roles, responsibilities and authorities 12
6 Planning 13
6.1 Actions to address risks and opportunities 13
6.1.1 General 13
6.1.2 Information security risk assessment 13
6.1.3 Information security risk treatment 14
6.2 Information security objectives and planning to achieve them 14
7.0 Support 16
7.1 Resources 16
7.2 Competence 17
7.3 Awareness 17
7.4 Communication 17
7.5 Documented Information 18
7.5.1 General 18
7.5.2 Creating and updating 18
7.5.3 Control of documented information 18
8 Operation 19
8.1 Operation planning and control 19
8.2 Information security risk assessment 20
8.3 Information security risk treatment 20
9. Performance evaluation 20

9.1 Monitoring, measurement, analysis and evaluation 20
9.2 Internal Audit 22
9.3 Management review 22
10. Improvement 23
10.1 Nonconformity and corrective action 23
10.2 Continual improvement 24

Document Revision History

Version Number	Revision Date	Change Description	Effective Date
V 1.0	27-02-2023	Initial Release	27-02-2023

Document	Created by	Reviewed by	Approved by
Designation	IT Manager	Country Manager	CEO

1 Scope

The Information Security Management System**(ISMS**) manual of NextBewe (NextBewe Nigeria Limited) consists of Information Security Management System, ISMS i.e., ISO 27001:2013 for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS and to demonstrate its ability to consistently

- provide staffing services that meet customers and applicable statutory and regulatory requirements with an aim to enhance customer satisfaction through effective implementation of the system, including processes for continual improvement of the system and

- improving an information security management system safeguarding both NextBewe's and their customer's information at all times within the context of the organization

The requirements of ISO 27001:2013 are established and maintained and it provides reference to policies, processes and procedures, wherever required.

The requirements of ISMS are defined as documented information (which include organizational structure, role, responsibilities and authorities, policies, operational planning and control activities, assets, resources, risk & opportunity analysis & mitigation, business continuity plans, design and development activities, etc.) as process procedures and work instructions. NextBewe's overall Information Security Management System is based on process approach, risk based thinking and PDCA, Plan-Do-Check-Act approach, enabling the management to establish, implement, operate, monitor, review, maintain and continually improve ISMS within the organization.

The Statement of Applicability, SoA (refer NXB-ISMS-SoA) contains inclusions / exclusions of ISO 27001:2013 control objectives and controls. Accordingly, the excluded control is **A.14.2.7** i.e. outsourced development, since; the organization is not engaged in any outsourcing of development activity.

2 Normative references

While establishing the ISMS for NextBewe, the references referred are

1. ISO/IEC 27000, *Information technology — Security techniques — Information Security management systems — Overview and vocabulary*
2. ISO/IEC 27001:2013 – Information Technology – Security Techniques – Code of practice for information security management system

3 Terms and definitions

For the purposes of this ISMS, the terms and definitions given in ISO/IEC 27000 apply.

4 Context of the organization

4.1 Understanding the organization and its context

Vision Statement:

"To be Africa's largest and a globally respected IT, ITES and Business Process consulting and outsourcing firm, that provides best-of-breed business solutions, leveraging technology, delivered by best-in-class people"

Mission Statement:

"To achieve our objectives in an atmosphere of fairness, honesty, and integrity towards our clients, employees, vendors and society at large."

Values:

Customer Centricity

Leadership

Integrity

Transparency

Fairness

Pursuit of Excellence

The internal and external issues that can affect NextBewe's ability to achieve the intended outcomes of its ISMS are

Issues		Current Status	Impact on ISMS
External	Overseas clients	Understanding law of land requirements	Customer focus, legal requirements and compliance
	Competition	Many organizations work on the same model	Leadership, customer focus.
	Contractual relationship with suppliers	Agreements are in place with suppliers. Information security requirements are addressed based on applicability. Some small time suppliers are still not aware of information security / quality requirements.	Control of externally provided processes, products and services, Supplier relationships
	Market	Too much dependency on North American market	Leadership.
	Economic	Fluctuating Currency (Naira depreciating)	Opportunity
Internal	Culture	Instruction driven.	Continual improvement
	Knowledge	Low vintage employees	Competency

4.2 Understanding the needs and expectations of interested parties

NextBewe has determined

a) The interested parties that are relevant to its ISMS
b) The requirements (needs & expectations) of these interested parties that are relevant to the ISMS

The interested parties and their needs and expectations are given below. NextBewe monitor and review these needs and expectations of interested parties regularly once in a year.

Interested Parties – Their needs & expectations

Understanding the needs and expectations of interested parties			
Interested Parties	**Needs**	**Expectations**	**Relevant to ISMS**
Customers	Cost effective resources & competent teams, information security	Contractual obligations, efficient staffing and infrastructure	Customer focus
Employees	Growth & stability, Compensation, PII	Work culture, safe work environment	HR security, PII

Suppliers	On time payment	Contractual requirements	Supplier relationships
Government	legal and regulatory	fulfillment of legal and regulatory requirements	Compliance requirements
Society at large	Well being	Environmental safety	Leadership

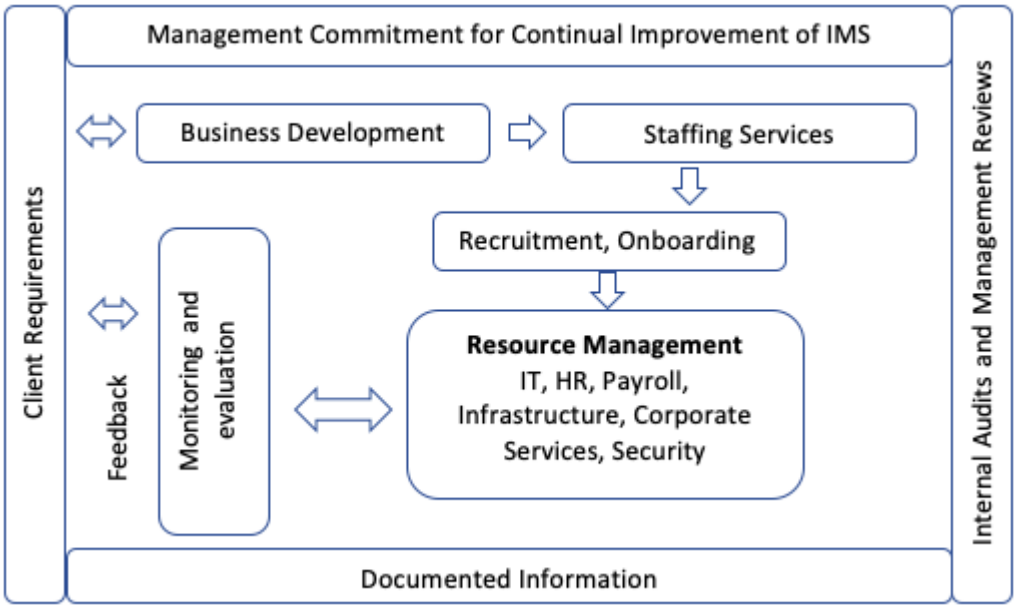
4.3 Determining the scope of the Information Security Management System(ISMS)

NextBewe while determining the boundaries and applicability for scope of ISMS has considered

a) The external and internal issues referred to in clause 4.1 and

b) The needs and expectations referred in clause 4.2

c) Interfaces, dependencies between activities performed by NextBewe and those that are performed by other organizations are given below



Interactions between Processes & ISMS

NextBewe's ISMS scope statements are:

Scope Statement

Operations, maintenance and management of Staffing services for IT & ITES companies, including support functions such as IT, Human Resources and Corporate Services.

This is in accordance with the statement of applicability, version 1.0, dated 27 Feb 2023.

The location included in the scope of ISMS is:

19, Lafiagi street, G.R.A,
Ilorin,
kwara - 240101
Nigeria
www.nextbewe.com

NextBewe's *Technology Environment* - Illustrative IT Infrastructure at the location

No	Item Name	Description
1	Servers*	AD Server, Backup and Virtual Servers
2	Networks	LAN, Wi-Fi, Internet, Applications
3	Work stations	Desktops, Laptops, mobile phones.
4	Operating systems	Windows 10 pro, Windows Server 2016 , Ubuntu,
5	Utilities	IS Devices,Non-Disclosure Agreements, Network Services.
6	Tools	Network, Helpdesk and Access Control System
7	Information systems	Network Access, Network Appliances and Application
8	Application software	JIRA, Snaggit, Anydesk,
9	Devices	Laptops , Printer, Desktop
10	Cloud services	G-suite, Microsoft Azure and anti-virus

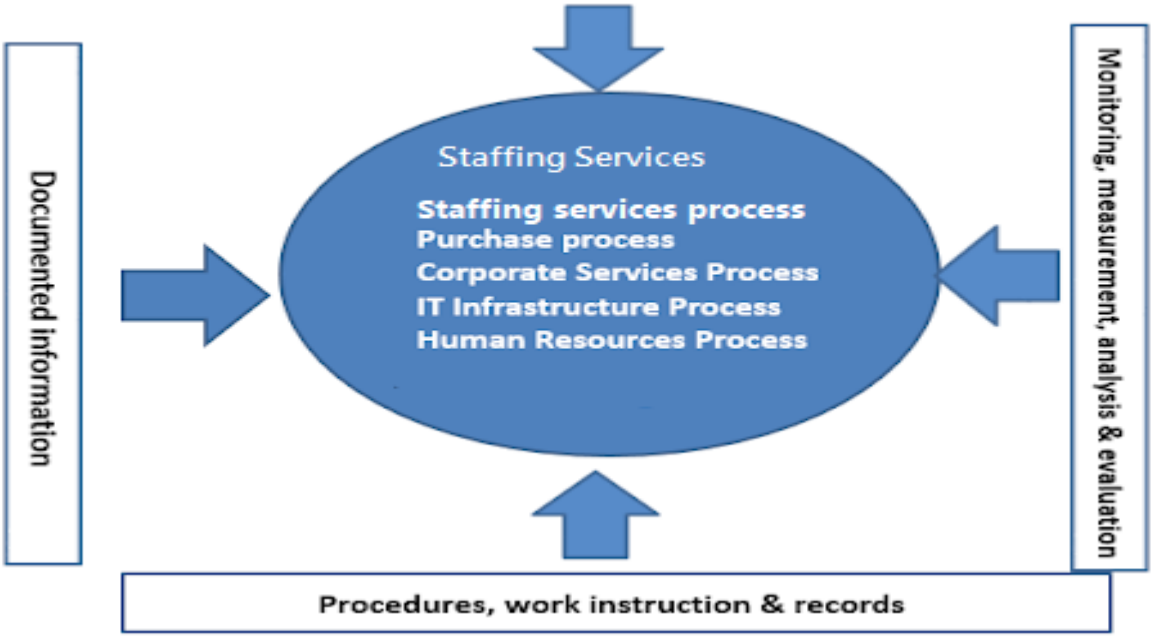
4.4 Information Security Management System

NextBewe has established, documented & implemented ISMS and to continually improve its effectiveness in accordance with requirements of ISO 27001:2013. Identification of documentation needed for the Information Security Management System and its application throughout the organization are categorized as

- Vision, Mission and Core Values
- ISMS manual & information security policy
- Statement of applicability
- Control objectives and controls
- Risk management & control of non-conformances

- Monitor, review, analyze and continual Improvement.

NextBewe has established, documented, implemented and maintains an ISMS that strives to continually improve its effectiveness in accordance with requirements of ISO 27001:2013. NextBewe has determined the processes required for the ISMS and its application throughout the organization as



The sequence of processes and their interactions are aligned in line with the business / customer needs throughout and

a) All the processes have determined their required inputs to ensure the expected output from each of these processes
b) The sequence and their interactions are determined as shown interactions between processes & ISMS
c) All processes have been defined and appropriate metrics such as productivity, efficiency, quality score, customer satisfaction, on time delivery, zero incident breaches etc. to ensure control, effectiveness through periodic monitoring for continual improvement of these processes
d) Top management has ensured that adequate resources are available as necessary
e) All personnel are assigned their roles with relevant authority, accountability and responsibilities
f) At appropriate stages the risk and opportunities are identified as per clause 6.1

g) All process performance metrics are monitored, measured and analyzed through various periodic reviews to ensure processes achieve their intended results
h) Wherever the intended results are not achieved, necessary actions are taken to aim at achieving NextBewe's objectives and for continual improvement of the processes using the process approach, PDCA as applied to the ISMS

To the extent required, NextBewe has

a) Maintained a documented information to support the operation of its processes as an Information Management System, ISMS manual NXB-ISMS-Manual and departmental process procedures as

1) Purchase & Supplier Relationships Procedure, NXB-ISMS -PSP
2) Corporate Services Procedure, NXB -ISMS -CSP
3) IT Infrastructure Procedure, NXB-ISMS - ITP
4) Staffing Services, NXB –ISMS - CEP
5) Human Resources Management Procedure, NXB – ISMS – HRP
6) Talent Acquisition procedures, NXB –ISMS- TAP

5 Leadership

5.1 Leadership and commitment

The leadership at NextBewe embraces radical transparency through ethical and exemplary leadership with a relentless focus on delivering results, promoting core values in everything that they do such as **EPIC.**

- **Environment for people to flourish**

  Cultivate a collaborative spirit and a culture of openness in which all are treated fairly and with respect, where people express themselves without fear

- **Pursuit of Excellence**

  Continuously refine our skills, deepening knowledge and leading by example

- **Integrity and respect above all**

  Adhere to rigorous ethical standards to build trust among our people, our clients, vendors and partners.

- **Customer Delight**

  To perform every assignment to the best of our abilities, always with the intention to delight and even to astonish our customers / clients

NextBewe's leadership is committed for development, implementation and continual improvement of ISMS by:

a. Establishing ISMS policies and objectives in line with strategic direction of NextBewe
b. Integrated ISMS with its process procedures seamlessly in the form of documented information
c. Ensured sufficient competent and right resources for establishing and to implement, operate, monitor, review, maintain and improve the ISMS at NextBewe
d. NextBewe has been communicating the importance of meeting information security objectives and conforming to the information security policy, its responsibilities and the need for continual improvement
e. Ensuring that the ISMS achieves its intended outcomes i.e. ISMS control objectives and information security objectives
f. Directing and supporting employees to contribute to the effectiveness of ISMS
g. Promoting continual improvement by improving the effectiveness of ISMS by reducing the security incidents, nonconformances
h. The leadership team constantly direct and engage resources to contribute to the effectiveness of ISMS
i. Promoting continual improvement throughout the organization
j. The entire staff treat ISMS as one of the functions of the organization similar to service delivery and other shared services

Refer: Management Review Procedure (NXB-ISMS-MRM) and Internal Audit Procedure (NXB-ISMS-IAP)

5.2 Policy

The top management of NextBewe has established information security policies that are

a) appropriate to the purpose of the organization and supports its strategic direction
b) identified information security objectives to support achievement of these policies, respective standard requirements are adopted as frameworks for setting up objectives
c) these policies also ensured that applicable requirements related to legal, regulatory, statutory and contractual requirements are met and some of them are

- Companies and Allied Matters Act 2020
- Finance Act 2021
- The National Information Technology Development Agency (NITDA) 2007
- Nigeria Social Insurance Trust Fund Act 1993
- The Industrial Training Fund (Amendment) Act 2011

Finance Team and Consultant CA maintains all other applicable statutory and regulatory requirements

d) provides the required commitment for continual improvement of ISMS thru periodic reviews, either once in a year or as and when required due to changes, if any,

NextBewe's Information Security Policies are as follows:

Information Security Policy

We, at NextBewe are devoted to protect the confidentiality, integrity, availability of company and client information with a persevering commitment to improve the effectiveness of the information security management system by setting up information security objectives while satisfying all applicable requirements.

For Communicating the information security policy to all interested parties, NextBewe has ensured that

e) the information security policies have been maintained as documented information
f) These policies are communicated within the organization to all employees working under the control of the organization through induction, the handbook, weekly teams connect, All Hands Meet, AHM periodic mailers etc.
g) to all interested parties, as appropriate through e-mails, contractual agreements.

5.3 Organizational roles, responsibilities and authorities

The top management of NextBewe has defined and communicated the roles, responsibilities and authorities for various position related to information security management system

a. the organization chart, roles, responsibilities and authorities as per the requirements of standard are given in annexure -1 & 2
b. reporting on the performance of the ISMS is regularly updated to management through management review meetings and various dash boards including ISMS objectives

c. IT Manager (nominated as CISO) for ensuring that the organization's ISMS conform to the requirement of ISO 27001:2013 and to report on the performance of ISMS to the top management.
d. Ensuring promotion of customer focus throughout the organization
e. Ensuring integrity of ISMS by changing it as and when the changes are taking place

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

NextBewe has considered the internal and external issues identified by the organization (4.1), the needs and expectation of interested parties (4.2) that are relevant to information management. While planning for the ISMS, to determine the risks and opportunities to address that

a. The implemented ISMS can achieve its intended outcome(s) through effective implementation and support from the leadership team
b. enhance the desirable effects by effective implementation
c. prevent or reduce undesired effects through appropriate controls
d. achieve continual improvement through monitoring, measuring, analyzing and reviews

The organization has planned for

a) Necessary actions required to address risks and opportunities

b) How to;

1. integrate and implement these actions into ISMS system / processes
2. to evaluate its effectiveness of actions taken through audits and achievement of ISMS objectives

6.1.2 Information security risk assessment

NextBewe has defined and applied risk assessment & treatment plan for all assets.

a. The process of risk assessment and treatment plan establishes and maintain risk criteria for
    1. risk acceptance
    2. criteria for performing risk assessments

b. The risk acceptance & treatment plan is so robust that, repeated risk assessments for all functions gives repeated, reliable, valid, consistent and comparable results

c. Identifies the information security risks associated with
    1. Loss of C I A
    2. Identifies the risk owners

d. Analyzes the information security risks for

    1. Potential consequences that would result if the identified risk were to materialize
    2. To assess occurrence of realistic likelihood of identified risks
    3. To determine the levels of risk

e. Evaluate the information risks

    1. Compare results of risk analysis with risk criteria that is established
    2. To prioritize analyzed risks for treatment

The risk assessment & treatment plan and risk assessment tracker are retained as documented information.

6.1.3 Information security risk treatment

NextBewe has defined and established an information security risk treatment plan, which is documented as part of Information Security Risk Assessment & Treatment Plan (NXB-ISMS-RATP) which covers the following:

a. Based on the risk assessment results, NextBewe has opted for best suitable risk treatment options
b. Determined all suitable controls that are required for risk treatment options
c. Determined that, the controls are in line with the controls given annexure A such that all applicable controls are included without omitting any relevant ones
d. NextBewe's statement of applicability describes the inclusions / exclusions of controls that are applicable or not applicable from the list annexure A. Accordingly, A.14.2.7 is excluded, since NextBewe is not outsourcing any development activity.
e. Formulated a risk treatment plan based on applicable controls
f. Risk owners are identified for various risks from their respective functions / processes and their approval is taken for the residual risks

Information security risk treatment is maintained as documented information.

Refer NXB-ISMS – RATP and Org RA.

6.2 Information security objectives and planning to achieve them

NextBewe has defined and established information security objectives for relevant functions and levels. These objectives are

a. consistent with Information Security Management System and support to achievement of same
b. these objectives are measurable
c. these objectives have been formulated taking into consideration the applicable integrated management requirements and the results of risk assessment and risk treatment plan
d. communicated to the relevant functions / people involved
e. as and when there are changes to these objectives, the same are reviewed and approved by CEO once in a year as part of strategic planning process

The Information security management objectives are retained as documented information. **Refer annexure - 4**

When planning for how to achieve these objectives for monitoring, measurement and evaluation, NextBewe has defined metrics, targets, frequency of measurement and actually achieved and tracked in the form of a dashboard. To achieve these integrated management objectives, the organization has defined the following:

f. The objectives planned to implement and monitor are promptly detecting processing errors and detect security events, to identify failed and successful security breaches and incidents, enable respective functions to assess whether security activities are performed in line with the criteria set for them, and take action to resolve any breach of security in a way that reflects the NextBewe's priorities
g. IT Manager along with functional heads determine what resources are required to carried out these activities
h. The respective functional heads assign these responsibilities to respective teams for these activities
i. Based on the issues, an action plan along with timelines / frequency are arrived by the respective functional heads
j. All actions are recorded to measure these objectives and performance of ISMS for analysis and continual improvement as per the defined frequency

As part of continuous improvement, whenever changes are required or proposed for improvement of ISMS / business processes, all such changes are implemented in a planned manner. NextBewe shall consider:

a) How the proposed changes affect or improve the ISMS and the consequences associated with these changes are reviewed? Based on these reviews a detailed action plan is prepared
b) If the proposed changes do not affect the integrity of ISMS, then the integrity of the management system is maintained by making necessary changes as and when required to various procedures
c) Ensure suitable availability of resources for the proposed changes
d) To carryout changes, allocate or re-allocate responsibilities and authorities

Control of documents procedure (NXB-ISMS-CDP) is used whenever changes are made to the ISMS.

Refer: Control of documents procedure (NXB-ISMS-CDP)

7.0 Support

7.1 Resources

NextBewe has determined and provided the required resources for establishing, implementing, maintaining and continual improvement of integrated management system. The HR department maintains a skill matrix of the personnel available in NextBewe. As and when additional resources required the same are discussed with management, for review and approval. Management team monitors the requirement and communicates the requirement to talent acquisition team.

NextBewe considers

a) The capabilities and constraints of existing resources
b) What needs to be obtained in case of external providers such as

- HR consultants for sourcing the right candidates (need based) or for BGV
- Housekeeping services
- Security services etc.,

NextBewe ensures right (competent) resources at right place and right time needed for implementing, maintaining the management system and continually improves its effectiveness to meet, exceed and enhance customer requirements to increase their satisfaction. The management is responsible for determining and making provision for resources.

Around 90% of NextBewe employees are production executives who are computer literate graduates, experienced as well as fresh from college. All the employees undergo product & process knowledge training before they start working on the actual job. For the remaining 10% employees are lateral hires or employees grown over a period, who are competent to carry out the jobs assigned to them. The basis for competency is appropriate education, skills, relevant experience as determined by the respective functional heads through job descriptions.

A need-based infrastructure is considered for (personnel, equipment, space, software / hardware, information and communication technology) various processes for realization of service delivery. The management reviews additional requirements, plan, and approves it. From the existing

resources, allocations are made to various services. If necessary, procurement / recruitment are initiated as per the NextBewe's purchasing / recruiting procedure.

Refer: Corporate Services Procedure (NXB-ISMS-CSP) and Talent Acquisition procedures (NXB –ISMS- TAP)

7.2 Competence

NextBewe considers

a. the necessary competence of persons working under its control that affects ISMS performance have been determined and maintained
b. competence requirements are determined as part of employee hiring process based on appropriate education, training and experience by the talent acquisition
c. the competence gap analysis for various individuals performing these roles are determined by HR team and the necessary training is provided by the client' training team effectiveness of training is monitored by respective stakeholders
d. Records of competency assessment are maintained by respective teams (functional heads). (Refer competency matrix)

7.3 Awareness

Employees working under NextBewe's control are aware of

a. Information security policies - The HR team as part of new hire onboarding, conducts ISMS awareness training during induction, schedule periodic training classes as per the client requirements
b. Team Leads & Managers ensure that the same is reinforced from time to time, their contribution and effectiveness of ISMS as part of service delivery
c. The HR / IT team also periodically keep communicating the implications of not conforming to ISMS through campaigns (email /desktop notifications/ posters)

7.4 Communication

NextBewe has determined requirements for internal and external communication relevant to integrated management system. Corporate communications team is responsible for internal / external communication. Communication details are given in Communication Matrix (Annexure-3) including:

a. What to communicate i.e. the importance and the benefits of strictly adhering to information security requirements and its control objectives
b. When to communicate i.e. as and when necessary due to the changes in the information security policy and its objectives

c. With whom to communicate i.e. during induction program of all new hire and in various forums / meeting in the organization internally and with all other stake holders while communicating externally
d. Who shall communicate? I.e. The top management at the organization level and while communicating externally with other stake holders, all functional heads in their routine business internally. Refer- communication matrix – Annexure -4.

7.5 Documented Information

7.5.1 General

The documented information maintained by NextBewe for the ISMS includes the following:

a. Documented information required by ISO 27001:2013
b. Other documented information determined by NextBewe as necessary for the effectiveness of the ISMS such as policies, process procedures, work instructions, legal, statutory and regulatory requirements

The need for other documentation is decided based on the complexity of processes, their interactions, and the competence of people working in various processes.

Master list of ISMS documented information is maintained by IT Manager in the word format and controlled documented information (copy) to respective functional managers in the form of PDFs. All documentation is made available to users as per the ISMS policy.

7.5.2 Creating and updating

All ISMS documents are protected and controlled by NextBewe as per control of documented information and ensure appropriate

a. Identification & description – All documented information has a title, version number, date,
b. Format & media – Soft copy format, word, excel and PPT
c. Review and approval for suitability and adequacy - document creation, review and approval details

The same is applicable for document revision also.

7.5.3 Control of documented information

The documented information required by the standard and NextBewe are documented and created. NextBewe's control of documented information is to ensure

a. The updated and latest version is shared to relevant functions / employees only on need to know basis. All pages of ISMS Manual include version number and date. The first issue

with all pages will have version no 1.0. When any particular section is revised, the version number will be incremented to 1.1, 1.2 and so on. Latest version number is indicated on the cover page with effective date. All controlled copies are shared in the form of PDF only.

b. All documents are shared as PDF only or the files are protected by using passwords.

All changes or revisions are captured in document change history or in the amendment record sheet and approved by Head-IT

c. Master Copy is maintained by IT Manager in the form of word document. Controlled copies are distributed in the form of PDF File. The access to folders etc. is role based with options of Write, Read, and Modify as appropriate.
d. All documents are shared on intranet portal. Latest version copies are only available on intranet or at point of use.
e. The latest version is mentioned on the cover page. All older versions are archived and kept for reference by IT Manager
f. As per the organization retention policy the documents are retained and after that they are destroyed (softcopies) or shredded (hard copies)

IT Manager and respective functional managers are responsible to ensure that documented information is maintained and retained as per the defined procedure.

Refer: Control of documented information procedure (NXB-ISMS-CDP)

8 Operation

8.1 Operation planning and control

NextBewe has established and maintained ISMS for ensuring actions to address the risks and opportunities and plans to achieve information security objectives

Head- IT and respective functional / process heads are responsible to ensure to keep the documented information to the extent necessary to have confidence that processes / procedures are implemented and carried out as planned.

In case of any changes planned, the same is reviewed by Head – IT and functional heads to review the consequences of unintended changes, taking actions to mitigate any adverse effects, as necessary. Document Change Management Procedure is defined, established and implemented.

Head – IT is responsible to ensure that outsourced processes are determined and controlled.

8.2 Information security risk assessment

NextBewe has formulated and implemented a risk assessment & treatment-reviewing plan. Risks are reviewed once in a year or as and when significant changes are proposed to occur by Head – IT.

Information security risk assessment and treatment plan tracker is established and implemented. IT Manager is responsible to retain the documented information related to Information security risk assessment and treatment plan. (Refer NXB-ISMS- RATP and Org RA.xlxs)

8.3 Information security risk treatment

NextBewe has formulated and implemented a risk treatment plan as part of the risk assessment methodology, to mitigate the risks identified during the risk assessment process as per the information security risk assessment procedure (NXB-ISMS-RATP). The results are tracked in a tracker.

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

NextBewe periodically evaluates the performance and effectiveness of ISMS through objectives and various other dashboards. NextBewe has determined:

a) what needs to be monitored and measured

The management team and various functional heads determine what needs to be monitored and measured to ensure that, the stipulated processes are adhered while QA team ensures service that are being delivered are meeting customer requirements. What needs to be monitored and measured are as follows:

- Management review process - Continuing suitability, adequacy and effectiveness of ISMS once in six months
- Internal audit procedure – Number of nonconformance's in each audit for measuring effectiveness of implementation of ISMS once in six months and annual external audit
- Information security procedure – downtime of equipment /systems, assessing risk and risk mitigation for business continuity, effectiveness of controls, as set out in SoA to verify that security requirements have been met or not periodically

- Various process specific parameters - respective performance measure metrics are mentioned for each processes and data is collated in dashboards

b) The methods for monitoring, measurement, analysis and evaluation needed to ensure valid results

Monitoring and measurement of all applicable controls on on daily, weekly and monthly basis as applicable are carried for monitoring effectiveness of performance of controls in the form of dashboards to ensure that, the information security requirements are meeting all NextBewe's and it's customers information security requirements. Appropriate performance metrics are identified and defined. These metrics are reviewed for adequacy & consistence.

c) When the monitoring and measuring shall be performed

For all controls, performance measures are tracked at the defined frequency as appropriate in the form of dashboards. Analysis of these measurements are carried out and reviewed in various periodic reviews and appropriate action plans for improvement are taken to ensure:

- conformity of the information security requirements meeting or exceeding customer requirements / expectations
- conformity of the management systems and
- continually improving the effectiveness of the management system and process performance metrics

When planned results are not achieved, correction and corrective action as appropriate are taken to ensure the conformity of the processes.

d) When the results from monitoring and measurements shall be analyzed and evaluated i.e. analysis of data

NextBewe has defined methods and activities for data generation, data collection, analysis, and reporting to the management using appropriate statistical techniques.

The analysis of data is carried out in the following areas

- Performance measurements of various controls
- Customer complaints / feedback
- Information security incidents
- Internal and external audit reports

Based on the output of analysis i.e. information, actionable activities are initiated for continual improvement. Appropriate statistical tools and techniques are used for analysis of data.

Refer: information security objectives

9.2 Internal Audit

NextBewe conducts internal audit once in six months to ensure that the ISMS

a. conforms to
    1. Meet NextBewe's own requirements for its integrated management systems; and
    2. Requirements of the standard ISO 27001:2013

b. is effectively implemented and maintained
c. Plan, establish, implement and maintain an audit programme(s), including the frequency methods, responsibilities, planning requirements and reporting. The audit programme(s) will take into consideration the importance of the processes concerned and the results of previous audits.
d. Define the audit criteria and scope for each audit.
e. Select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
f. ensure that the results of the audits are reported to relevant management; and
g. Retain documented information as evidence of the audit programme(s) and the audit results.

Country Manager is responsible for the areas to be audited and to ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes.

Refer: Internal audit procedure (NXB-ISMS- IAP)

9.3 Management review

NextBewe conduct management review meetings at least once in six months to review to ensure its continuing suitability, adequacy and effectiveness

The management review meeting, MRM include

a) The status of actions from previous management reviews;
b) Changes in external and internal issues that are relevant to the ISMS;
c) Feedback on the information security performance, including trends in;
    1) Non-conformities and corrective actions;
    2) Monitoring and measurement results;
    3) Audit results;
    4) Fulfillment of information security objectives;
d) Feedback from interested parties;
e) Results of risk assessment and status of risk treatment plan; and

f) Opportunities for continual improvement

The output of the Management review includes decisions related to the following:

- Minutes of meeting
- Action planning for identified issues with responsibility and timelines
- Continual improvement opportunities
- Any need for changes to the ISMS
- Resources requirements

The MRM output is retained as documented information.

Refer: Management review procedure (NXB-ISMS-MRM)

10. Improvement

NextBewe based on measurement, review and analysis, determine and select opportunities for improvement and implement any necessary actions to meet customer and own information security requirements to enhance data security. These shall include;

a) Improving effectiveness of controls to meet requirements as well as address future needs and expectations
b) Correcting, preventing or reducing undesired effects
c) Improving the performance and effectiveness of the ISMS

10.1 Nonconformity and corrective action

When a nonconformity occurs, NextBewe shall

a) react to the nonconformity by Appropriate correction and corrective actions are taken to the nonconformities encountered as applicable
    1. Take actions to control and correct it - Appropriate correction is applied to the identified nonconformity
    2. Deal with consequences of nonconformities - Appropriate corrective actions are taken across the functions to the nonconformities encountered as applicable
b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
    1) Reviewing the nonconformity;
    2) Determining the causes (root cause analysis) of the nonconformity; and
    3) Determining if similar nonconformities exist, or could potentially occur

c) implement identified action needed based on RCA

d) review the effectiveness of any corrective action taken; and

e) make changes to the integrated management system, if necessary

Ensures that the corrective actions are appropriate to the nonconformity.

NextBewe maintain a documented information for all identified non conformities consisting of

f) The nature of the nonconformities and any subsequent actions taken, and

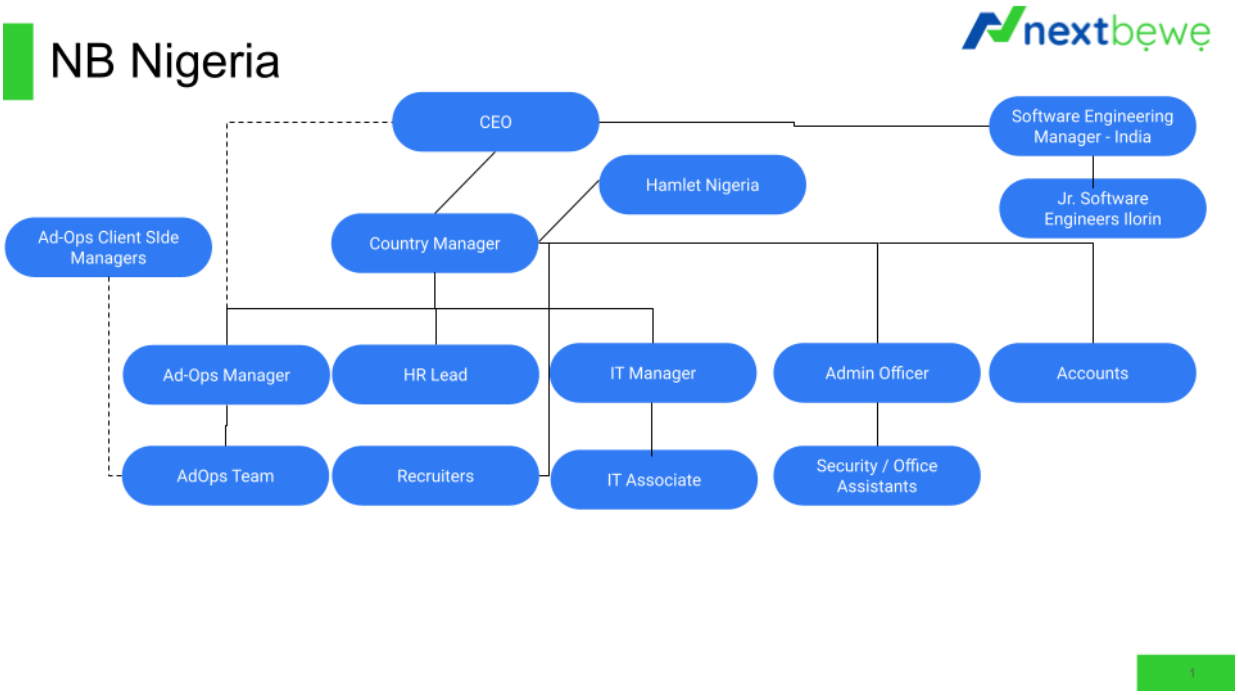
g) The results of any corrective action.

10.2 Continual improvement

NextBewe strives to improve continually the suitability, adequacy and effectiveness of the ISMS using the following

- Internal & external audit results
- incident investigation results
- feedback from interested parties
- analysis of monitored results
- management review feedback
- Information security objectives
- Industry best practices
- External audit feedbacks

Annexure -1: Organization chart



Annexure – 2: Role, Responsibilities and Authorities

CEO

- General and overall management of the organization
- Formulating security policies and short/long term strategic planning
- Overall business development in coordination with various functional heads
- Provides directives for ensuring organization-wide effective implementation of ISMS , and contributes to the functioning of the MISF
- standing in for CEO on management review committee meeting
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS
- Setting up ISMS Objectives
- Ensuring effective implementation of ISMS
- Ensuring compliance with relevant statutory, regulatory and legal requirements
-

Country Manager

- Reviewing the ISMS policy for its adequacy on a periodic basis along with the IT Manager
- Reviewing performance of the ISMS objectives and effectiveness of the controls on a regular basis
- Performing risk assessments and review residual risks on a periodic basis
- Tracking and controlling of the plans established for improving ISMS on a regular basis
- Providing internal advisory on Information Security and corporate governance relevant matters to the stakeholders, as appropriate
- Participate in Management Review meetings for reviewing the performance and improvement of the ISMS
- Support ISMS Internal Auditors to ascertain the adequacy and compliance
- Conduct training and orientation sessions on ISMS and related areas to the employees, as and when required in coordination with L&D Team
- Identify needs and request for required resources for implementing and improving ISMS
- Ensuring effective implementation of ISMS in line with ISO 27001:2013

Head – IT / Manager

- Establishing roles and responsibilities for ISMS
- Responsible for monitoring and ensuring the smooth execution of all activities related to ISMS, along with IT team initiate protective and corrective measures if a security problem is discovered and report any security breaches to the Management
- Communicating to the organization the importance of meeting Information Security objectives
- Ensuring compliance with relevant statutory, regulatory and legal requirements
- Deciding the criteria for accepting risks and the acceptable levels of risk
- Ensuring that internal ISMS audits are conducted
- Conducting management reviews of the ISMS
- Review and approval of ISMS Manual, Procedures & Policies
- Conduct risk assessment on periodic basis
- Ensuring effective implementation of ISMS
- Monitoring and reporting on the state of Information Security within the organisation
- Coordinate with the ISMS core team members to develop and enforce detailed procedures to maintain security
- Monthly review of incident reports/logs and communicate with ISMS core team members
- Monitoring for actual or potential Information Security breaches
- Preparing and implementing ISMS documentation
- Monitoring the state of Information Security of the organisation
- Creating awareness amongst employees on the responsibilities and accountability for Information Security
- Sharing and analysing security issues with ISMS Core team members
- Ensuring effective implementation of ISMS

Head -Accounts

- The Head-Accounts shall budget for finance for all information security related initiatives, also facilitates the Information Security Management System in the function
- Incorporate relevant terms and conditions as required by ISMS in the contracts given to third party by the organization
- Identify and address legal and regulatory requirements and contractual security obligations that are applicable to the organization
- Ensure BCP and compliance to the BCP from Finance perspective
- Communicate the various security processes and initiatives to customers

HR- Lead

- The Head-HR shall budget for human resources for all information security related initiatives, facilitate implementation of Information Security Management System
- Initiate and maintain information security processes within HR function
- Incorporate relevant terms and conditions as required by ISMS in the contracts given to third party by the organization
- Identify and address legal and regulatory requirements and contractual security obligations that are applicable to the organization
- Ensure provisioning of basic training on Information Security as part of the induction program to the new employees
- Ensure provisioning of advances security training for individuals performing specific information security roles
- Initiate appropriate disciplinary action in concurrence with relevant heads of the departments in case of information security violations / breaches
- Ensure BCP and compliance to the BCP from HR perspective
- Communicate the various security processes and initiatives to employees

IT Associates (Operations / Support Functions)

- Follow the set policies & procedures as per the ISMS requirements
- Responsible for conforming to NextBewe Information Security Policy
  Required to bring to their manager or core team Coordinator s attention on areas of concern regarding Information Security
- Required to abide by the terms of the compliance with respective legislation

- Familiar themselves with all the necessary user-level policies and processes, as applicable to their role and function
- Reporting security incidents and/or weaknesses promptly to ISMS Coordinator or the respective managers or through incident management system.
- Ensuring effective implementation of ISMS

Administrative Officer

- Duties/Responsibilities
- Shall receive and dispatch office correspondence and deliveries
- Shall implement office documentation and maintenance of file inventory
- Shall keep and update staff records including attendance and related records
- Shall make requisition, procure and store of office essentials
- Shall supervise office logistics including negotiation of staff transportation, relationship management
- with transportation partners
- Shall be responsible for daily office routines including opening of office and closing opf office and
- coordination of security details
- Shall liaise with Team Leader and Account Manager regarding staff welfare including and not limited to health matters, claims and others
- Shall relate with the HR resources regarding staff on-boarding, trainings and other related matters
- Any other matter as may be assigned by the Country Manager

Annexure -3: Communication Matrix

S.No.	Subject (on what)	Responsibility (who)	Communicated to (with whom)	Mode of communication (How)	Frequency (When)
1	Information Security Policies	Corporate Communications	All NextBeweers	e-mail / Portal	As and when revised
2	ISMS objectives & effectiveness	Head- ISMS	Team Leads / Managers	ISMS Objectives Tracker	QBR / MRM
		Team Leads / Managers	Associates	Meetings	Quarterly / Half yearly
3	Incidents	IT Manager	Concerned Associate / TL / Mgr.	e-mail / Note	Immediately after the incident
4	Policies	Head- ISMS	All NextBeweers	Displays / Portal	As and when revised
5	NDA	Marketing, HR and Corporate services Teams	Customers, Vendors & Employees	Through Mail / Hard copy	Contract initiation / MOU
6	ISMS awareness	HR & Corporate Communications	New employees & NextBeweers	Induction training, Periodic mailers, NextBewe portal	At the time of joining, as and when required
7	Client	Respective Delivery heads / Client engagement team	Client SPOC	e-mails, Telecom	Weekly, monthly, QBRs
8	Interested parties	Corporate communications	SPOCs of interested parties	e-mails, Telecom	As and when required
9	Suppliers	Respective functional heads	SPOCs of suppliers	e-mails, Telecom	As and when required

ISMS Objectives

No	Metrics	Description	Measurement	Target	Frequency	Function responsible
1	Screening	Background verification checks on all candidates joined the organization	No. of employees covered for screening	100%	Every Quarter	TA
2	ISMS awareness training	All employees & contractors to receive awareness education and training on ISMS	No. of employees and contractors covered during training & test passed within 30 days of joining	100%	Every Quarter	HR
3	Disciplinary issues	Employees who have committed an information security breach	No. of incidences	0%	Every Quarter	HR
4	Ownership of assets	Assets maintained in the inventory are owned	No. of assets without ownership	0%	Quarterly	ALL FUNCTIONS
5	Labeling of information	Appropriate information labeling for all information assets	Number of information assets with appropriate labelling	100%	Every Quarter	
6	Reconciliation of user access rights	Asset owners to review users' access rights once in a month	Evidence of review of access rights by all functions / processes	100%	Every Month / quarter as applicable	
7	Clock synchronization	All clocks are synchronized to a single reference time source.	No. of systems not matching with server time	0	Every Month	IT
8	Security Incidences	No. of security incidents reported / observed or suspected information security weaknesses in systems or services.	No. incidents	0	Quarterly	IT

9	Internet up time	Availability of Internet	Availability	99.99 %	Monthly	IT