NexTtech Limited

Business Continuity Policy

A. Document Information:

Document Ref No.	: NEXTECH-ISMS-L2-008
Document Title	: Business Continuity Policy
Issue No.	: 00
Issue Date	: 15 November 2020
Document Owner	: CISO
Prepared by	: CISO
Approved by	: MD/CTO

B. Document Distribution List:

SN	Designation
1.	CTO
2.	CISO
3.	In-charge HR
4.	Departmental Heads

Table of Contents

1. Introduction

The dependence of today's enterprises on ICT is significant. For an organization that uses IT extensively for its operations, not just recording of transactions; non-availability of its information systems could mean the end of its existence. Confidentiality, Integrity and Availability (CIA) of information systems must be ensured to protect the business from risks relating to IT.

A business continuity plan (BCP) is a management process to ensure the continuity of businesses in the event of a disaster. BCP is a process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue without interruption or essential change. Business Continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.

BCP will facilitate the identification of how quickly critical business functions and/or processes of NEXTECH can return to full operation following a disaster. It will delineate the business impact of disaster scenarios on the ability to deliver product or to support mission-critical services. BCP will also facilitate identification of the resources required to resume business operations to a survival level.

1.1 Purpose

The consequences of an extended interruption due to a disaster or security failure must be analyzed to determine the impact on NEXTECH's information security, and to determine the recovery time necessary to restore normal business operations. Business Continuity Plan must include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential business operations.

The requirements in this policy meet ISO 27001:2013 standard.

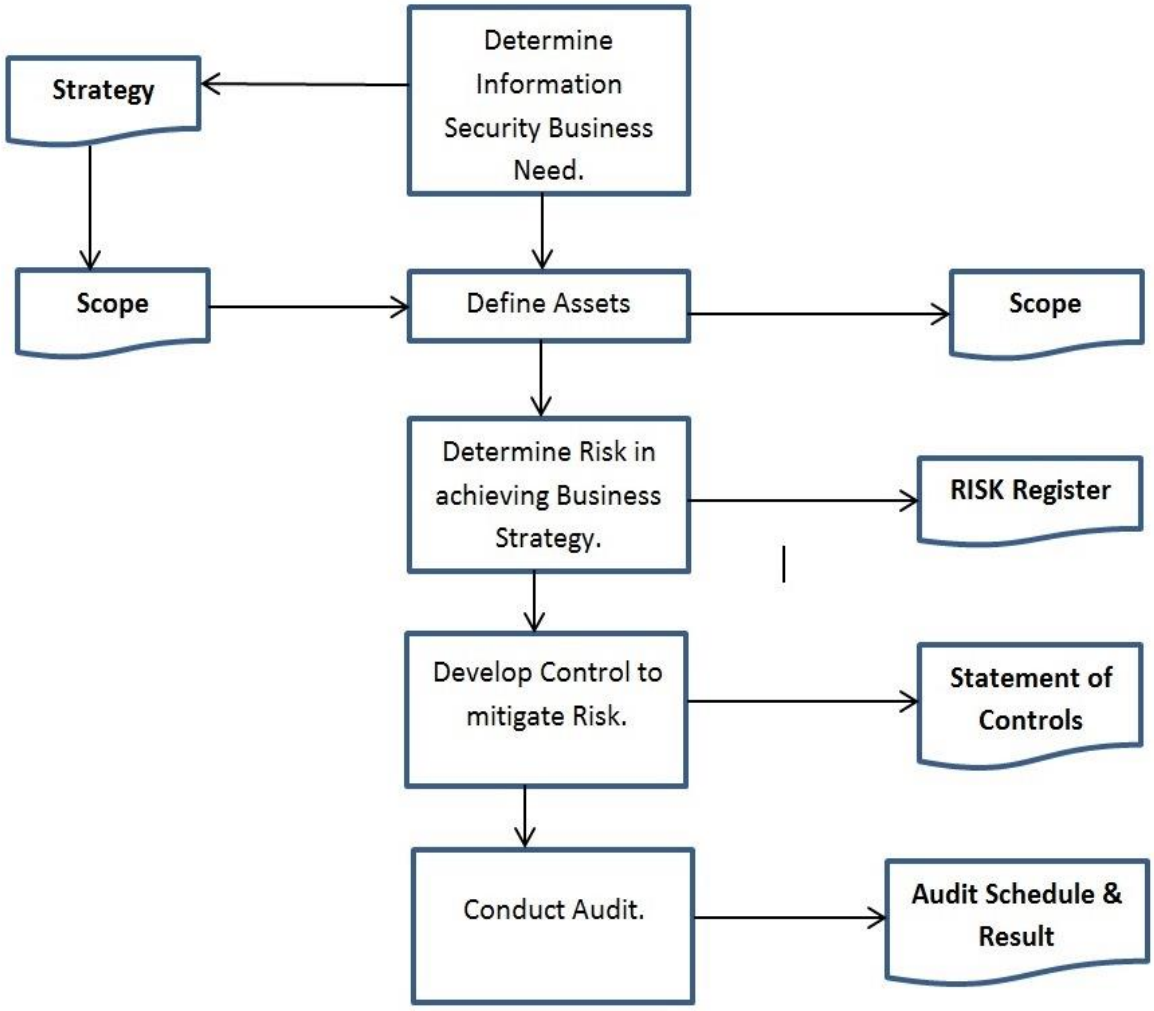
1.2 Scope

The scope of this policy is limited to the IT infrastructure, and the data and applications of the NEXTECH environment. To ensure interruptions to normal NEXTECH business operations are minimized, and critical NEXTECH business applications and processes are protected from the effects of major failures or disasters, CISO of NEXTECH needs to plan, develop, implement and periodically test its business continuity plan that can meet the recovery requirements of all critical business processes and applications related to information security.

2. Ownership and Responsibility

CISO

3. Workflow chart



4. Business Continuity Policy

NEXTECH Business continuity policy is briefed below:

4.1 IT Disaster and Declaration Plan

This plan should be invoked if an event, internal or external, has occurred or threatens to occur, which seriously damages NEXTECH's ability to continue normal business. In all situations the safety, health and well-being of people is the absolute overriding concern. Situations that qualify would certainly include but not be limited to:

- Widespread loss or damage of IT equipment at the NEXTECH Primary Data Centre
- Temporary or permanent loss of access to the site due to fire, natural disaster, terrorism, or any other event of similar nature.
- Large scale fire, flood or explosion affecting a whole building or the whole site
- Medical epidemic situation affecting staff or staff in critical areas
- Events resulting in significant staff casualties
- Unexpected power down or unlimited grid failure
- Terrorism, vandalism, political unrest etc.

- Large scale fire in the vicinity
- Any other similar situation capable of creating the disruption

4.2 Declaration Authorization

NEXTECH business continuity management team (ABCMT) as below:

SL No	Authorized Person	Work Phone	Home Phone	Cell Phone
1	MD			01713045492
2	CTO			01713092756
3	CISO			01713092756
4	Incharge HR			01755584720

4.3 Disaster Declaration Time

A disaster declaration must be made within thirty minutes (30) from the incident that disrupted normal NEXTECH business operations, unless the time needed to clear the disaster event is less than the time needed to move operations to the Recovery Facility.

4.4 Declaration Statement

A disaster declaration is a formal statement by the top management which starts the implementation of the BCP.

4.5 Recovery Site Information

The data center of NEXTECH is collocated with ASA. There is a well-defined contract to deliver the service between ASA and NEXTECH. ASA (Currently NEXTECH has no Data Center and DR site. NEXTECH shall set up DC and DR with their own cost or shall give the responsibility to a third party which) is fully responsible for keeping 99% uptime. A disaster recovery site (DRS) is being planned within Bangladesh at a strategically safe location, like different seismic zone from Dhaka. Till that time, the data is backed up daily in G-suit. However, presently we are not having any application failover arrangement.

4.5.1 Detail Information for Data Center (DC)

Address: 2nd Floor, ASA Tower, 23/3 Bir Uttam ANM Nuruzzaman Sharak
Shyamoli, Mohammadpur, Dhaka-1207, Bangladesh
Phone: +88 02 58155627, +88 02 58155175, +88 02 58155609
Fax: +88 02 9121861, +88 02 8116205
Email: asa@asabd.org

4.6 Strategies to address loss of Site or Site 1 Primary Server Room

The following options, amongst others will be considered, if there is a need to recover either a damaged site or part of a site that requires extensive rebuilds activity. In all cases the Recovery team will be guided by the Managing Director in deciding the appropriate strategy in the circumstances.

Key Dependency in all operations is the ability to provide appropriate Power and Networking and Physical Security.

- Utilizing spare capacity in the existing NEXTECH Office.
- Leasing space

- Convert part of an existing NEXTECH Building into a Secure Data Store
- IT Recovery to the Site 1 DR Server Room.

4.7 Dependencies Identification

4.7.1 Functional Dependencies

The success of this plan in supporting NEXTECH's overall Business Continuity depends on the following:

- Information Service Continuity Team (ISCT), drives the overall recovery activities after any major disruption.
- The unfold and maintain high level Business Continuity (BC) and Disaster Recovery (DR) Processes with the Management Committee.
- All installed infrastructure is the responsibility of IT Department to ensure appropriate BC and DR is in place and executed in time of necessity.

4.7.2 Specific Systems Dependencies

We will require the following systems to be operation in order to carry out recovery operations:

System/Dependency	Contact/Reason for Dependency
Restore systems in case of emergency	Name: Designation: Sr, System Engineer Contact:
Local / Remote access to system according to the access policy	Name: Designation: Sr, System Engineer Contact:
Physical access	Name: Designation: In charge HR Contact:
Hardware supply	Name: Designation: Sr, System Engineer Contact:
Emergency Internet service support	Name: Designation: Sr, System Engineer Contact:

4.8 Business Continuity Procedure

The essence of our Business Continuity Plan is to ensure the NEXTECH business has its processes and procedures supported by a risk assessment and containment plans, which are reviewed at least annually.

Strict configuration management control will be exercised by the use of formal installation and asset recording standards.

Any changes to configurations for whatever reason will be subject to the formal change control.

4.8.1 Risk Management

NEXTECH will maintain a Master Risk Register which is subject to regular review by the Senior Management Team. This Master Risk Register will contain all significant risks not only those of a business continuity nature specifically. Business Continuity Risks will be separately mentioned in the Risk Register and will be addressed progressively. Appendix A contains a general risk register.

All sites will be subject to regular process audits with follow up corrective action plans. Currently these include:

- ISO 27001: Information and Physical Security
- Security Audits
- Infrastructure Vulnerability Assessments

Additionally, ad hoc audits will be actioned as required and the master risk register will be actively reviewed and appropriate actions taken.

4.8.2 Essential Records

The ability to recover from a serious situation is determined by accurate records of the business.

A defined list of essential records is held in **Appendix B** with defined responsibilities.

4.9 Disaster Escalation Plan and Checklist

An escalation plan and checklist will be maintained for ease of operation and the ability to utilize resource at other sites. The normal escalation process will invoke the gathering of the Service Continuity Team with Management Committee and ensure that both teams are in full communication during and after the Recovery Operation.

4.10 Governance

The main governance instruments of the BC and DR Plan for NEXTECH will be the Management Committee.

The Managing Director will liaise with the Business Continuity Team to ensure a schedule of tests for the NEXTECH estate when such test is planned.

4.11 Data Backup

End user data backup: There is a directory for every users in the Network data storage. Users are recommended to back up their personal data at least once a week.

Application data backup: NEXTECH IT infrastructure is designed to provide hardware level redundancy. Therefore the data stored in the network storage system, is having real time redundancy. Moreover, Network storage data is copied as backup in a portable Hard Disk every Sunday morning. The same data is copied in the G-suit at the same time.

Database Backup: Application data is copied as backup into G-suit everyday.

4.12 Testing the Plan

The plan will be tested at least annually. This test may constitute a Table Top BC Exercise or a fully-fledged test where recovery to an alternative location is trialed. Disaster Recovery testing of the business-critical applications and IT infrastructure will be carried out on an annual basis in accordance with the planning schedule detailed in the Business Continuity planning calendar of events.

A detail testing way forward is depicted in appendix C.

4.13 Guidance for Staff in a Disaster Situation

IN ANY DOUBT DUE TO CIRCUMSTANCES AT THE TIME ALWAYS TAKE THE SAFE OPTION – IF THIS IS STAY AT HOME THEN DO THIS AND MAKE CONTACT BY PHONE AS SOON AS IT IS POSSIBLE TO DO SO.

- First Priority is to ensure your own safety and that of your family.
- Phone your manager or if not available another manager on another location as soon as reasonably possible.
- If you are pre-identified to work from home in an emergency then **DO NOT GO TO A SITE UNLESS INSTRUCTED (in many cases it is safer to stay at home)**.
- Go to the first-choice site AFTER a 24-working-hour period unless otherwise advised.

4.14 Acceptable Downtime & Business Recovery Point

Each disruption has some downtime on business. But unlimited downtime is not acceptable to the NEXTECH management. So, NEXTECH Management has some desirable set point regarding downtime & resumption of business. Recovery Point Objective (RPO) & Recovery Time Objective (RTO) are pre-set by the management for each business process/function.

For successful recovery from a disaster, the Management as well as Disaster Recovery Team must be aware of the two important driving factors:

1. Recovery Time Objective (RTO)
2. Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

Recovery Time Objective (RTO) is the maximum down time the Management can tolerate, that is, RTO is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) occurs in order to avoid unacceptable consequences associated with a break in business continuity.

For example, if RTO of a system is 1 (one) hour, the Recovery Team should be prepared to restore the system in operational condition within one hour after a disaster occurs.

RTO can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. This would include alternate or manual workaround procedures to meet the RTOs.

In multi-environment and dependent systems, RTO is the minimum tolerable downtime of the most critical system.

In business continuity planning, RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance. RTO must be accepted by the Management.

Recovery Point Objective (RPO)

Recovery Point Objective (RPO) is the point in time backwards up to which recovery can be tolerated by the Management, that is, maximum data / transaction loss the Management can tolerate due to a major incident.

For example, if RPO of a system is 1 (one) hour, the Recovery Team should be prepared to restore Data up to 1 (one) hour back in Production (LIVE) System when a disaster occurs and start business operation freshly, that is, management is agreed to accept maximum 1 (one) hour's data loss.

When real time data is replicated to remote DR Site and after a disaster business operation is started from DR Site, then RPO will be ideally Zero.

Both RTO & RPO are significant in respect of Business Continuity. If an organization fails to set up and meet proper RTO and RPO, dissatisfaction of the clients will increase and reputation of the organization will be threatened.

Generally low RTO & low RPO is recommended by the management, but it may require sacrifice of cost to be involved. So to set up RTO & RPO trade-off is maintained among cost, tolerance of the clients and tolerance of the business owners.

4.15 List of Critical NEXTECH Business Ratings with RTOs/RPOs

Critical Business processes:

For the purpose of the BIA, critical business processes/services are determined to be the technical or ICT services and the supporting resources which need to be recovered in the shortest possible time (RTO) and which would have the greatest impact to the NEXTECH business.

Criticality level of business processes:

Criticality of Business Processes	Criticality description	Maximum Tolerable Period of Disruption
Highly Critical = 1	• This describes all business resources which should be available immediately on demand. • The unavailability of the IT resource would cause intolerable impact to the business of NEXTECH resulting in catastrophic failure to the business. • Manual processing is feasible but not practical.	Must be available in less than 3 hours
Critical = 2	• This describes all business resources which should be available within a few hours. • The unavailability of the business resource would cause serious impact to the business of NEXTECH resulting in service being significantly and substantially degraded. • Processes could be performed manually for very limited period.	Must be available between 3 and 6 hours.
Marginal = 3	• This describes all business resources which marginally affects business but should be available within a day. • The unavailability of the business resource would cause some noticeable and minor impact to the business of NEXTECH • Process could be performed manually for an extended period at a substantial cost and effort.	Must be available between 6 and 24 hours
Negligible = 4	• This describes all business resources where availability is not critical, and it is sufficient for this asset to be available within 72 hours. • Destruction of the resource or unavailability of business services provided via the resource will have a negligible effect on business operations. • Process could be performed manually and can be delayed until normalcy is restored or new systems procured.	Must be available between 24 and 72 hours

Non-Critical = 5	• This describes all business resources that the organization can do without for an extended period of time (over 72 hours). • Destruction of the resource or unavailability of business services provided via the resource will have NO effect on business operations.	Must be available after 72 hours

4.16 Identify Recovery Priorities for Critical Business Processes / Services

According to RTO & RPO business processes/services of NEXTECH can be prioritized as following:

Priorities of Business Processes / Services	Related to ICT System Resource/Component	Criticality Level	RTO (HRS)	RPO (HRS)
JIRA	NEXTECH Hosting Server	1	3	6
HR System	NEXTECH Hosing Server	1	3	6
Data Center	Electrical Generator	1	3	N/A
Local / Remote access to system according to the access policy	NEXTECH Remote Access Hosing Server	2	6	N/A
Physical access	NEXTECH Physical Access Hosing Server	3	24	N/A
Hardware supply	NEXTECH Inventory System	4	24	N/A
Emergency Internet service support	ISP Provider	1	3	N/A

5. Roles and Responsibilities

5.1 General Roles

Not Applicable

5.2 Specific Roles and Responsibilities

5.2.1 Role: Incharge HR

Responsibility
1. Propose review the policy and familiarize himself with this policy. 2. Plan and organize training for new joiners. 3. Arrange training for staffs according to the training plan and on special request from other departmental heads.

5.2.2 Role: CISO

Responsibility
1. Develop the Annual Training Plan 2. Develop training material based on the requirement and conduct the training. 3. Execute this policy and analyze the relevance of the policy in the context of ISMS. 4. Report to the management.

5.2.3 Role: CTO

Responsibility
1. Approving the policy. 2. Approving the annual training plan. 3. Periodical review to identify relevance and applicability of change in the policy. 4. Provide all technical & Administrative support to CISO.

5.2.4 Role: Management Committee

Responsibility
1. Providing support for effective implementation of the policy. 2. Periodical review of performance of the policy and providing resources as necessary. 3. Proving leadership.

Appendix A – Generic Risk Assessment

Note: For detailed risks see the Master Risk Plan. This Appendix contains broad level guidance only.

Threat	Potential Causes	Counter Measures in Sites
Fire	Arson	Security measures 24/7 on sites. Buildings have perimeter fences with CC Camera.
	Electrical	All electrical work to current national standards by qualified personnel. Facilities reviewed by Electrical Contractor.
	Air Conditioning	Equipment under regular maintenance by qualified contractors.
	House Keeping	Cleaning standards defined and imposed by H&S.
	External	Reviews on external environment.
Water	Sea	All sites fall in the lowest possible category of EA flood likelihood.
	River	All sites fall in the lowest possible category of EA flood likelihood.
	Flood Water	All sites fall in the lowest possible category of EA flood likelihood.
	Burst Pipes	Regular building maintenance plus leak detection.
Environment	Dust / Dirt	Cleaning to defined standards
	Temperature	Monitored on 24/7 basis by Maintenance staffs
	Air Conditioning	Monitored on 24/7 basis by Maintenance staffs
	Denial of Access	Sites are monitored 24/7/365.
	Power Failure	Resilient power supplies
	Building Defects	Regular Building Maintenance + Site Surveys
Natural Causes	Earthquake	All buildings to relevant current Building standards.
	Lightning	Lightening Conductor systems fitted in the building.
	Flood	All sites fall in the lowest possible category of EA flood likelihood.
	Subsidence	All buildings to relevant current Building standards.
People	Malice, including Terrorism, Sabotage, Hacking, Vandalism	Staff vetting processes. Strict access control processes. Regular Security audits and reviews.
	Industrial Action	Unions not permitted or recognised by NEXTECH.

Threat	Potential Causes	Counter Measures in Sites
		Remote operation is possible.
	Negligence	Controlled access by trained staff On-going training and development of staff in line with technology requirements.
Equipment Failure	Plant	Resilience designed into facilities
	Computers	Maintenance is done by qualified internal staffs.
	Software	Maintenance is done by qualified internal staffs.

Appendix B – Essential Records

Record	Responsibility	Notes

Appendix C – Test Process

The test process will be generic and adapted on each occasion to the circumstances. In several cases it will need to be a desk checking scenario. Some tests will be planned into normal PPM (Planned Preventative Maintenance) schedules

- In all cases tests will be carried out as far as possible in a range of scenarios.
- All test activity will at all times be clearly identified as a Test.
- Various functions such as Management teams will be pre-warned a test is to take place, but not given specifics of the scenario.
- A scenario will be set up on a unit and a time log of activities maintained throughout the process.
- Specific guidance will be given in the test briefing.
- Following the test, a review will take place and lessons learnt published and corrective actions progressed through the relevant department and the Management Team.

Appendix D – Security Incidents

Security Incidents may lead to the invocation of the Business Continuity Plan

Security Incidents & Reporting

- A security incident is defined as being

"Any failure to observe a requirement of the security policy which has led to a security failure or has produced a condition which could lead to a security failure"

- All suspected or real security incidents must be reported immediately
- Contact the IT Helpdesk immediately and inform your line manager
- Helpdesk will log a call and the security incident will be investigated

Some examples of security incidents which must be reported include:

1. Attempts to gain entry to NEXTECH facilities by unauthorised staff whether successful or not
2. Suspicious requests for information about identifiers and passwords or the nature of NEXTECH's business
3. Loss, or inability to account for the whereabouts of client media or documents
4. Access to company classified data by persons not entitled to view it
5. Situations where you find classified documents in a public area
6. NEXTECH vehicles apparently being followed
7. NEXTECH sites being watched and/or photographed

DR to be prepared based storage in cloud.