

NexTtech Limited



Supplier Security Policy

A. Document Information:

Document Ref No. : NEXTECH-ISMS-L2-006
Document Title : Supplier Security Policy
Revision No. : 00
Issue Date : 05 December 2020
Document Owner : Head of HR
Prepared by : HR Dept., NEXTECH
Approved by : CTO

B. Document Distribution List:

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

Table of Contents

1. Introduction	3
1.1 Purpose	3
1.2 Scope	3
2. Ownership and Responsibility	3
3. Workflow chart	3
4. Supplier Security Policy	4
4.1 Information Security Sensitive Products & Services	4
4.2 Due Diligence	4
5. Roles and Responsibilities	4
5.1 General Roles	4
5.2 Specific Roles and Responsibilities	4
5.2.1 Role: Incharge HR	4
5.2.2 Role: CISO	4
5.2.3 Role: CTO	4
5.2.4 Role: Management Committee	5

1. Introduction

1.1 Purpose

The objective of this policy to ensure that suppliers of services to NEXTECH operate in accordance with the expected information security standards specified within NEXTECH policies, procedures and contracts. This will account for external supplier requirements in meeting company goals and objectives in relation to information security.

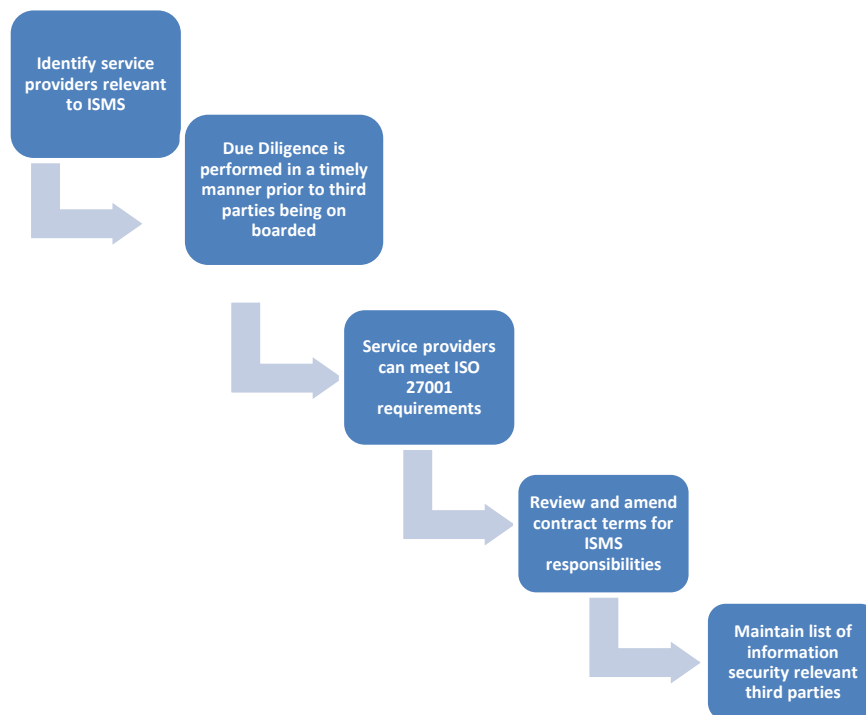
1.2 Scope

This policy defines the necessary controls which are to be applied on suppliers who has any kind of relevance to Information Security, either by the type of product or service they provide or by way of their interaction with the organization.

2. Ownership and Responsibility

In-charge HR

3. Workflow chart



4. Supplier Security Policy

4.1 Information Security Sensitive Products & Services

CISO in consultation with all departmental heads will prepare a list of product and services that NEXTECH outsources or purchases from third party vendors that are sensitive to Information Security. Whenever any such product or services is required by NEXTECH, the relevant departmental head will inform In-charge HR via email regarding the product or service. In-charge HR will update the mentioned list accordingly. This list will be reviewed and updated by Incharge HR yearly basis.

4.2 Due Diligence

While issuing the Request for Quotation (RFQ) to any third party vendor regarding any service or product mentioned in the aforementioned list, CISO, and related Head of the Departments, would be included. The prospective vendor must agree with the terms and condition mentioned in ToR while submitting the quotation. CISO will ensure that the ToR adequately satisfy the requirements of ISO 27001:2013.

5. Roles and Responsibilities

5.1 General Roles

Not Applicable

5.2 Specific Roles and Responsibilities

5.2.1 Role: Incharge HR

Responsibility
<ol style="list-style-type: none"> 1. Propose review the policy and familiarize himself with this policy 2. Update the List of vendors yearly or as being informed by the other departmental heads. 3. Consistently apply it in NEXTECH business activities

5.2.2 Role: CISO

Responsibility
<ol style="list-style-type: none"> 1. Ensures that all necessary ISO 27001:2013 controls are incorporated into the ToR for RFQ. 2. Help Incharge HR technically while implementing the policy. 3. Review product and services before keeping those in the list.

5.2.3 Role: Managing Director/ CTO

Responsibility
<ol style="list-style-type: none"> 1. Approving the policy. 2. Periodical review to identify relevance and applicability of change in the policy. 3. Provide all technical & Administrative support to In-charge HR and CISO.

5.2.4 Role: Management Committee

Responsibility
<ol style="list-style-type: none">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.