COMPANY NAME

[City, Country].

Information Security Manual

ISMS 01/1

ISMS System	ISO 27001:2022
Issue Number	01
Issue Date	15.10.2022

COMPANY NAME

Information Security Manual

ISMS 01/1

ISMS System	ISO 27001:2022
Revision Number	01
Issue Date	15.10.2022
Copy Number	
Total Pages	
Issued To	

Address of Organization

	Prepared By	Approved By
Name		
Designation	**Information Security Head**	**Top Management**
Signature		

PROCEDURE FOR RISK ASSESSMENT

1.0 Purpose

The purpose of this procedure is to describe our methodology for asset identification and classification. It also includes procedure for preparation of risk assessment and treatment plan.

2.0 Scope

a. All main and associated activities having bearing on associated risks are covered for asset identification and classification.

b. It also includes procedure for risk assessment and preparation of treatment plan

3.0 Responsibility

3.1 Business head/IS head is responsible for ensuring that system is established for our approach to risk assessment arising from the Organization activities and services are identified and recorded. He is assisted by Information security head for asset identification and classification as well as evaluation of risk.

3.2 Functional Heads and Information security head are responsible for identifying the risk in their respective areas and evaluate the same for their impact on Information Security. They are also responsible for ensuring that risks are managed through objectives and targets by operational control measure or follow up of risk treatment plans.

4.0 Description Of Activity

4.1 The effective management of information security has always been a priority for the [IT Department], knowing as it does the high degree of reliance that ABC Infotech delivery functions place upon both IT-based and non IT-based systems.

However, there is still much to be gained by us and by the IT Department in introducing industry-standard good practice processes, not the least of which is the ability to become more proactive in our approach to Information Security and to gain and maintain a better understanding of our Customers needs and plans.

4.2 Risk Assessment Process

Risk is the happening of an unwanted event, or the non-happening of a wanted event, which affects a business in an adverse way. Risk is realised when:

- the objectives of the business are not achieved
- the assets of the business are not safeguarded from loss
- there is non-compliance with organisation policies and procedures or external legislation and regulation
- the resources of the business are not utilised in an efficient and effective manner
- the confidentiality, integrity and availability of information is not reliable

It is important that our organization has an effective risk management process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them.

4.3 Asset Identification and classification

Based on ISO 27001 requirements the identification or assets are done as per details given below

4.3.1 Assets

A full inventory of assets will be compiled and maintained by ABC Infotech The definition of an asset is taken to be “anything that has value to the organisation” and is therefore worthy of protection. This will include physical assets such as IT servers and operational machinery as well as information assets such as customer lists and application databases.

4.3.2 Threats

For each asset, the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft or sabotage.

4.3.3 Vulnerabilities

Circumstances which may be capitalised on by any specific threat will be detailed. Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of hacking) or the existence of paper files in a data centre (which could be exploited by the threat of fire).

4.3.4 Impacts

Finally an estimate of the impact that the loss of confidentiality, integrity or availability could have on the asset should be given.

All other assets are classified and valued as per details given in below and proper identification is given in the asset identification and classification records F/IS/01:

Asset Identification & Classification	
Department/ Functions	viz. Operations, General, BPO, etc.
Activity	viz. Hardware repairing, Data Process, Data storage, Paper-based documents, Networking equipment, Communication etc.
Asset Name	The generic asset name.
Asset Owner and Location	For each asset write the asset belongs to which location as well as owner details
Threat	Related threat to the assets like failure of network, Poor system performance, virus attack, Connectivity, Communication, infiltration, Theft, Wilful damage, Power failure etc.

PROCEDURE FOR ASSET CLASSIFICATION & CONTROL

1.0 Purpose: -

To describe a procedure for Asset Classification & Control. The purpose of this document is to set out how information assets will be labeled and the specific controls that must be used when handling information of a particular classification

2.0 Scope: -

This procedure covers all activities related to responsibility for assets, information labelling, asset classification, control & handling in our company.

3.0 Responsibility: -

3.1 The Business head is overall responsible for the activities related to asset classification and control. He is also responsible for reviewing & implementing measures as & when required for the same. He is assisted by Information security manager and IS head for all routine activity related to asset identification, CIA analysis of assets and establishing necessary information security in the organisation.

3.2 Functional heads are directly responsible for the implementation of procedure for information classification, asset labelling and handling.

4.0 Description of activity: -

4.1 In ABC Solutions Pvt. Ltd. each asset is clearly identified for its ownership and current locations. The various types of assets used in our company are as listed below.

a) Information assets: databases and data files, system documentation, user manuals, Training material, operational or support procedures, archived information;

b) Software assets: application software, system software, Training modules and Utilities;

c) Physical assets: computer equipment (processors, monitors, laptops, and modems), Communications equipment, servers, LCD projectors, other technical equipment (power supplies, air conditioning units), furniture and accommodation;

d) Services: computing and communications services, general utilities, e.g. training facility, Lighting, power, air-conditioning.

4.2 Classification Guidelines:

The information assets are mainly classified in our organisation in 2 ways considering the threat associated as well as nature of our work. All such assets are divided in KPO work areas. The Business Head decide sharing or restricting of information in these areas to respective functional heads and accordingly user rights are provided. Normally related process Lead and technical lead is not having information related to other customer and such access is also not given to them.

4.3 First of all we require understanding of the methodology of the information classification at Nama Solutions Pvt. Ltd. In our BPO business the Information that is directly received

Risk Assessment and Treatment Plan	
Sr. No.	**Date:**
Activity and Department	
Asset Name:	
Threat	
Affected Asset Attribute (C / I / A)	
Existing control	
Control Objective	
Business Harm	
Risk Factor (HS,S, L)	
Management Decision for risk treatment options	
Recommended controls for risk treatment	
control reference	
Resources required	
Personnel responsible for implementation	
Start Date	
End Date	
Retained residual risk	
Any change in ISQMS system	
Authorized by	

Department		ABC Infotech Centre	No.	F/IS/01
			Issue No.	01
Page	1 of 1	Asset Identification And Classification	Approved By	Management Representative

Sr. No.	Activity	Criteria	Asset Name	Threat	Vulnerability	C	I	A	AV Asset Value No	T	V	P	Business Impact (Risk AV xTxVxP)	Remarks (Present & controls needs if any)

C: Confidentiality / Scale (1-4)	**I : Integrity (1-4)**	**A : Availability (1-4)**
T: Threat Value (1-4)	**V : Vulnerability (1-4)**	**P : Probability of Occurrence (1-4)**
Note: 4 is high level on the scale & Risk = Asset Value x Threat x Vulnerability x Probability		
0-100 no significant 101 to 400 Significant and controls or Sop is required. Above 401 Highly significant and risk plan is required.		

Naman Infotech Centre

Document Information			
Document Name	**Statement of Applicability**	Document No.	**F/IS/11**
Classification	CONFIDENTIAL	Version	01.00
Owner		Release Date	
Intended User		No. of Sheets	

Ver. No.	Release Date	Rational for change	Summary of changes made	Author	Reviewed By	Approved By
01		New document.	New document.			

Management Approval

Name	Designation	Signature	Date

Acceptable Use Policy - Information Services

Policy

Rules for the acceptable use of information and of assets associated with information and information processing facilities is identified and clearly documented in ISMS procedures and policies. All the employees of COMPANY NAME Infotech are strictly instructed to follow this policy and implement policies and procedures documented in the ISMS system. The purpose of this policy is to ensure that all had read related documents and must implement the ISMS system in their day to day activities.

Acceptance of policy by Employee:

- I hereby acknowledge that I have read and understood all the security policies and procedures set by COMPANY NAME Infotech

  Please ensure you have read the following summary of the main points of the organization's policies with regard to information security

- I understand that the confidential data like client source code, database schemas, etc are the property of the company and I am not permitted to do an unauthorized transfer of the above mentioned data to the outside world by email, upload, download or any other way. I understand that it is my responsibility to safeguard this information from unauthorized use and will ensure that all copies are either destroyed or returned to The COMPANY NAME Infotech, when I have finished. If engaged at a client site, I will apply this same practice there as well

- I acknowledge that my use of COMPANY NAME Infotech computer and communications systems may be monitored and/or recorded for lawful purposes.

- I accept that I am responsible for the use and protection of the user credentials with which I am provided (user account and password, access token or other items I may be provided with)

- I will not use anyone else's user account and password to access company systems

- I will not attempt to access any computer system to which I not been given access

- I will protect any classified material sent, received, stored or processed by me according to the level of classification assigned to it, including both electronic and paper copies

- I will ensure that I label any classified material that I create appropriately according to published guidelines so that it remains appropriately protected

- I will not send classified information over the Internet via email or other methods unless appropriate methods (e.g. encryption) have been used to protect it from unauthorized access

- I will always ensure that I enter the correct recipient email address(es) so that classified information is not compromised

- I will ensure I am not overlooked by unauthorized people when working and will take appropriate care when printing classified information

- I will securely store classified printed material and ensure it is correctly destroyed when no longer needed

Information security incident management Procedure

1.0 Purpose

The purpose of an Incident Management process is to establish procedures and standards to handle any interruption to a working service that disrupts access or use of technology-related services. This will enable ABC Infotech to better meet service expectations and have procedures for analyzing and resolving problems and preventing their recurrence.

2.0 Scope

Incident Management begins with the recognition of a problem and ends when the problem has been closed and the solution validated. Problems invoking the Incident Management Process are those that interrupt or degrade a key campus service, impacting a large number of users or key campus functions.

Specifically, Incident Management addresses problems that interrupt or significantly impact access or performance, such as:

- Local and remote hardware and software problems
- Incomplete or unavailable functions and applications
- Local and remote facility problems
- Operational problems
- Local and remote network problems
- Process problems

3.0 Objectives

The objectives of an incident management process are to:

- Ensure that all problems are reported and recorded correctly
- Ensure that all problems are assigned appropriate priority
- Recognize and escalate recurring problems
- Ensure all outstanding problems are managed to resolution and the service is restored
- Identify, and escalate to management, issues that are not resolved within stated criteria.
- Review closed problems and validate their resolutions.
- Provide management with an overview of problems having an impact on the delivery of applications or system service.
- Advise management on methods to prevent problem recurrence, which includes documentation of occurrence and go-forward changes.
- Ensure communication to key users and their management, as well as senior management.

4.0 Key Success Factors

- Problem assignment – Appropriate people should be assigned to work on a given problem. Problems can be reassigned to other people or groups if they are outside of a given person's