ISO 27017:2015 and ISO 27018:2019 Toolkit	
Level 1 – Manual & Policy	
Manual	
1.	Information Security Controls for Cloud Services Manual
Policy	
1.	Information Security Policy for Cloud Services
2.	Information Security Policy for Cloud Services (Development and Provision)
3.	Information Security Policy for Virtual Networks
4.	Return, Transfer and Disposal of PII Policy
5.	Secure Development of Cloud Services Policy
6.	Backup Policy
Level 2 – Procedures	
1.	Cloud Contracts Procedure
2.	Data Restoration Procedure
3.	PII Disclosure Procedure
4.	PII Geographical Processing Procedure
5.	Protection of Customer PII Procedure
6.	Return of Customer Assets Procedure
7.	Rights of PII Principals Procedure
8.	Temporary Files Procedure
9.	Data Center Access Procedure
Level 3 – Formats	
1.	Data Restoration Record
2.	PII Disclosure Record
3.	PII Geographical Processing Record
4.	Cloud Services Questionnaire
5.	Change Request Form
6.	List of Service Providers
7.	Master List of Records
8.	Objectives Monitoring Sheet
9.	Customer Complaint Report
10.	Internal Audit Non–Conformity Report
11.	Continual Improvement Plan
12.	Corrective Action Report

13.	Communication Report
14.	Training Calendar
15.	Risk Analysis Sheet

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

Scope

The purpose of this document is to provide customers, third parties, visitors, and other people with clear instructions on how to obtain access to and what to anticipate from the Organization Name data center.

Responsibility

The IT Managers or Asset Owners are responsible for granting permitted access to employees, including customers, suppliers, and other third parties.

Procedure

Data Center Access Principles

Based on the following tenets, access to Organization Name's data centers is permitted:

- Access to the data center should only be granted to those who have been approved by Organization Name
- All access should be for particular, permitted purposes
- An employee of Organization Name must constantly monitor over all visitors entering secure areas

2.2 Requesting Access to the Data Center

Reach us at +xx xxx xxx xxxx or send us an email at access@ [Company Name].com to request access to an Organization Name data center.

It will typically be necessary to give 24 hours' notice. Access is often only permitted during regular work hours, which are Monday through Friday from 9 am to 5:30 pm, excluding holidays.

2.3 Visitor Guidelines

The following regulations shall apply to all clients, third parties, and other visitors granted access to Organization Name's data center:

- The data center does not permit the use of food or beverages
- Smoking is not permitted anywhere on the site

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Scope

The scope of this document is to set out the way in which backups of information, software and system images are carried out, including regular testing.

2 Responsibility

This document applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Organization Name systems.

3 Procedure

Regular backups of essential business information must be taken to ensure that the organization can recover from a disaster, media failure or other form of error.

An appropriate backup cycle must be designed and used that meets business requirements, complies with Organization Name information security policy and is fully documented. Third parties that store organization information must also be required to ensure that the information is backed up appropriately.

In a cloud environment where the cloud service provider (CSP) is responsible for backups, the following criteria must be defined and agreed:

- Scope, schedule and location of backups
- Backup methods and data formats
- Retention periods for backups
- How the integrity of backups will be verified
- Use of encryption
- How backups are segregated in a multi-tenant cloud environment
- Frequency and method of reviews of backup and recovery procedures

For backups under Organization Name control, full documentation, including a complete record of what has been backed up, must be stored at an off-site location in addition to a copy at the site of origin.

INTERNAL AUDIT NON-CONFORMITY REPORT			
NC Report No:		Date:	
Department / Area:		Document Ref:	
Auditor:		Clause No:	
Audit Criteria:		Control #:	
Description of Non–Conformity:			
Person Responsible:			
Date of Completion	Planned:	Actual:	
Auditee: Signature		Auditor: Signature	
Root Cause of Non–Conformity:			
Action Taken to Resolve the Non–Conformities:			
Corrective Action Taken:			
Review of Action Taken:	**Status:**	☐ Closed	☐ Open
	Signature:		
	Date:		
Planned Date for Reviewing Effectiveness:			
Review of Effectiveness of Action Taken (Next Audit):			
Effectiveness Checked On	Date:	Sign:	