Nexus Select Malls

Data Privacy Policy

Version 1.1

Document Information	
Title	Data Privacy Policy
Version	1.1
Effective Date	
Policy Owner	InfoSec Team
Policy Reviewed By	Head – IT and Security Ops
Policy Approved By	CTO
Review Period	Annually

Revision History			
Version	**Date Created**	**Author / Title**	**Change Description**
1.0	November 2024	InfoSec Team	Draft Data Privacy Policy
1.1	November 2024	InfoSec Team	Reviewed and updated the Policy

Table of Contents

1. POLICY STATEMENT 4
2. PURPOSE 4
3. SCOPE 4
4. FRAMEWORK AND DEFINITION 4
5. ROLES AND RESPONSIBILITIES 5
6. DATA PRIVACY POLICY 5
7. REFERENCE 6

1. Policy Statement

Nexus Select Malls is committed to safeguarding the privacy and protection of Personal Identifiable Information (PII) and Sensitive Personal Information (SPI) of its internal and external stakeholders. This policy ensures that data privacy is maintained through appropriate procedures, technology, and adherence to applicable legal and regulatory requirements. The organization follows a process-based approach aligned with the NIST Cybersecurity Framework for implementing and monitoring data privacy practices.

2. Purpose

The purpose of this policy is to establish clear guidelines for the responsible handling of Personal Identifiable Information (PII) and Sensitive Personal Information (SPI). It aims to protect the privacy rights of stakeholders by ensuring secure collection, processing, storage, disclosure, and disposal of personal data. The policy is designed to promote compliance with applicable legal and regulatory requirements, foster trust, and uphold the organization's commitment to data privacy.

3. Scope

This policy applies to all employees, third-party personnel, and systems involved in the handling of PII and SPI at Nexus Select Malls. It encompasses the processes, technology, and practices used to collect, process, store, disclose, and dispose of personal information in accordance with legal and regulatory requirements. It ensures that data privacy measures are consistently applied across all organizational operations and stakeholder interactions.

4. Framework and Definition

This policy aligns with the NIST Cybersecurity Framework, focusing on the **'PROTECT'** function.

Key terms include:

S. No.	Keyword	Definition
1.	PII	Personal Identifiable Information that can uniquely identify an individual.
2.	SPI	Sensitive Personal Information, such as financial or health data.
3.	Privacy Notice	A document informing stakeholders about data collection, use, and protection.

5. Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Establish and monitor privacy policies and practices. Conduct regular assessments to ensure compliance.
Grievance Officer	• Address privacy-related grievances in accordance with legal requirements
IT Team	• Implement privacy controls and maintain secure systems for storing and processing PII and SPI.
HR Department	• Conduct training sessions on data privacy for employees and third-party personnel.
Users	• Comply with data privacy policies and report any privacy incidents promptly.

6. Data Privacy Policy

1. Nexus Select Malls shall perform an assessment of the cloud service provider (CSP) prior to onboarding.
2. The Nexus Select Malls team shall include the necessary legal, non-disclosure, business continuity, and disaster recovery clauses in the CSP contract.
3. Responsibility for privacy and protection of Personal Identifiable Information (PII) and Sensitive Personal Information (SPI) of all internal/external stakeholders shall be established.
4. The organization shall designate a Grievance Officer to address privacy-related grievances from stakeholders, if applicable.
5. Processes and procedures shall be established to protect PII and SPI data in accordance with the applicable compliance requirements.
6. Organizations should consider hiding sensitive data (e.g. PII, SPI, etc.) by using techniques such as data masking, pseudonymization, or anonymization taking applicable legislation into consideration.
7. Personal data of stakeholders shall be securely stored, in manual or electronic form in accordance with the applicable compliance requirements.
8. Privacy training shall be administered to all the staff and authorized third-party personnel who handle sensitive personal information.
9. Changes to the Legal and regulatory landscape related to privacy shall be monitored and any impact from such changes shall be identified and addressed.
10. An online privacy notice shall be made available for stakeholders during the collection of PII and SPI data.
11. Privacy notice shall clearly and conspicuously describe how Nexus Select Malls collects, uses, stores, and discloses personal information.
12. The organization shall obtain stakeholder consent prior to the collection, processing, and transfer of PII and SPI data.

13. Upon the customer's request, the organization shall provide mechanisms to correct or amend the stakeholder's personal information.
14. If the stakeholder withdraws his/her consent to use his/her personal information by Nexus Select Malls, the organization shall consider not providing services for which the information was sought, but data will be retained as per legal and regulatory requirements.
15. The organization shall limit the collection of sensitive personal information that is necessary and relevant for the purposes for which information is being collected.
16. PII and SPI data shall only be collected by reasonable, lawful, and fair means.
17. The organization shall limit the use of sensitive personal information for the purposes identified in the privacy notice.
18. The personal information of stakeholders shall only be disclosed for the purposes outlined in the privacy notice.
19. Personal information of stakeholders shall be retained for only as long as necessary to fulfill the stated purpose or based on legal or regulatory requirements.
20. Incidents that involve misuse, unauthorized access, or disclosure of sensitive personal information shall be categorized and handled as privacy incidents.
21. The Grievance Officer shall address stakeholder privacy-related complaints in accordance with legal or regulatory requirements.

7. Reference

Version	Document
-	Nexus Malls – ISMS Policy
	Nexus Malls – Incident Response Plan