# Information Technology (IT), Cyber Security, and Data Privacy Policy

# Table of Contents


1. Purpose ..... 3
2. Scope ..... 3
3. Definitions ..... 3
4. Policy Commitments ..... 4
5. Roles and Responsibilities ..... 4
6. Communication and Training of the Policy ..... 4
7. Monitoring and Review ..... 5
8. Grievance Mechanism ..... 5
9. Related Policies ..... 5


| Version Number | Reviewed by | Approved Date | Approved By |
|---|---|---|---|
| **1.0** | **IT Head** | **14th Feb 2023** | **Board of Directors** |
| **1.1** | **IT Head** | **12th Aug 2024** | **Board of Directors** |
| **1.2** | **IT Head** | **17th May 2025** | **Board of Directors** |

## 1. Purpose

The purpose of this Information Technology (IT), Cyber Security, and Data Privacy Policy is to ensure the protection of sensitive information, maintain compliance with legal and regulatory requirements, and ensure the continuity of UFlex Limited (herewith to be referred as "UFlex") business operations. Specifically, the policy aims to:

- **Protect Sensitive Data**: Safeguard personal information and sensitive data from unauthorized access, use, or disclosure, both internally and externally.
- **Ensure Compliance**: Comply with all relevant legal and regulatory requirements, including data protection laws such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and other applicable industry standards.
- **Maintain Business Continuity**: Ensure that cybersecurity measures are in place to protect business-critical information, prevent data breaches, and support continuity in operations in case of a security incident or data loss.

This policy establishes the framework for safeguarding UFlex's information systems and sensitive data, ensuring that the company can continue to operate effectively while protecting the privacy of stakeholders.

## 2. Scope

The Policy applies to UFlex Limited and its 100% subsidiaries. The scope of the policy applies to all UFlex employees, contractors, third-party vendors, and any other stakeholders who interact with the company's IT infrastructure, data, or systems. The following are within the scope of this policy:

- **Systems**: All IT infrastructure, including hardware, software, and networking components used to store, process, and transmit data.
- **Data Types**: Personal information, including sensitive personal data such as financial records, health conditions, passwords, and biometric data, as well as non-sensitive data critical to business operations.
- **Personnel**: All employees, contractors, third-party vendors, and any other individuals who have access to UFlex's information systems and data.

## 3. Definitions

- **Personal Information**: Any information that can identify a person, such as names, addresses, contact details, and other personally identifiable information.
- **Sensitive Personal Data or Information**: Data that includes passwords, financial details, health records, sexual orientation, biometric data, and other sensitive details.
- **Data Classification**: A method of categorizing data according to its sensitivity level. Data will be classified into categories such as Public, Internal Use Only, Confidential, and Restricted, and will be treated accordingly.
- **Cybersecurity**: The practice of protecting UFlex's IT systems and data from cyber threats such as unauthorized access, data breaches, and malicious attacks.

- **Data Protection Laws**: Laws and regulations, such as the GDPR, CCPA, and the IT Act, that govern the collection, use, storage, and sharing of personal and sensitive data.

## 4. Policy Commitments

UFlex is committed to the following key principles:

- **Protecting Sensitive Data**: The Company will implement industry-standard security measures to protect sensitive personal data and ensure that all data is handled with the utmost confidentiality and security.
- **Ensuring Legal Compliance**: The Company will comply with all applicable laws, including GDPR, CCPA, and other data protection regulations that govern the collection, processing, and storage of personal and sensitive data.
- **Business Continuity**: The Company will implement business continuity practices to ensure that critical systems and data are protected and accessible, even in the event of a cyber-attack, data breach, or system failure.
- **Ongoing Risk Management**: The Company is committed to continually assessing and mitigating risks related to cybersecurity and data privacy, proactively managing potential threats to its IT infrastructure and sensitive data.
- **Data Lifecycle Management**: Clear guidelines will be established for data storage, transmission, and disposal, ensuring that sensitive information is protected throughout its lifecycle.

## 5. Roles and Responsibilities

- **Board of Directors**: The Board will provide oversight and ensure the company's adherence to this policy. The Board will also ensure that sufficient resources are allocated to implement and maintain data protection and cybersecurity measures.
- **Senior Management**: Senior management is committed to ensuring that this policy is implemented effectively across the organization. They will oversee the integration of security and data protection measures into daily operations.
- **IT Department**: Responsible for implementing and maintaining technical security measures, managing risks related to IT systems, and ensuring compliance with data protection regulations. They will also oversee the incident response plan and business continuity procedures.
- **Employees and Contractors**: All personnel must adhere to this policy and report any security breaches, vulnerabilities, or incidents to the designated grievance officer and IT department.
- **Grievance Officer**: Responsible for handling any complaints or grievances related to data protection, addressing them promptly and ensuring resolution in compliance with legal requirements.

## 6. Communication and Training of the Policy

- **Policy Communication**: This policy will be communicated to all employees, contractors, and relevant stakeholders through the company's intranet, website, and onboarding processes.
- **Training**: All personnel will receive mandatory training on data protection and cybersecurity measures. Training will cover the handling of personal and sensitive data, recognizing

cybersecurity threats, and understanding the importance of compliance with applicable data protection laws.

- **Ongoing Awareness**: The Company will provide regular refresher training and communication to ensure all employees are aware of the latest risks, best practices, and regulatory updates related to data privacy and cybersecurity.

## 7. Monitoring and Review

- **Risk Assessment**: UFlex will conduct regular risk assessments to identify potential threats to its information systems, data, and IT infrastructure. The company will continuously monitor for any vulnerabilities and implement corrective actions where necessary.
- **Compliance Audits**: Regular audits will be conducted to ensure compliance with this policy, as well as relevant laws and regulations such as GDPR and CCPA.
- **Continuous Improvement**: The company will update this policy periodically based on changes in legal requirements, emerging cybersecurity threats, and internal assessments. Senior management will review and approve any major changes to this policy.

## 8. Grievance Mechanism

**Reporting**: Any individual who has concerns or grievances regarding the handling of their personal or sensitive data may contact the Grievance Officer.
**Grievance Officer Contact**:

- **Name**: Mr. Dhiraj Kumar Singh
- **Email**: grievance@UFlexltd.com
- **Phone**: 01204002873

**Grievance Resolution**: All grievances will be acknowledged within 48 hours, and appropriate actions will be taken to address the concern. In cases where the grievance cannot be resolved immediately, the individual will be kept informed of the progress and outcome.

## 9. Related Policies

This policy should be read alongside the following policies of UFlex:

| S. No. | Policy |
|---|---|
| 1 | Code of Conduct |
| 2 | Whistle Blower Policy |
| 3 | Risk Management Policy |