UNNATI
Organisation for Development Education

IT AND DATA PROTECTION POLCY

Though some issues related IT and Data Protection has been included in UNNATI's Staff Service Regulation, 1995 (last changes effective from 01/11/2021), specifically in Regulation No. 18 (Secrecy) and Regulation No. 15 (Use of Office Infrastructure), this policy is designed to clearly outline UNNATI's stance on IT and Data Protection, as well as its approach to addressing such cases.

1. Purpose

This IT and Data Protection Policy outlines UNNATI Organisation for Development Education's approach to managing and protecting personal data and sensitive information. It also defines the use of IT systems and data management practices to ensure compliance with applicable laws.

2. Scope

This policy applies to all employees, contractors, consultants, volunteers, fellow and interns who access or use UNNATI's IT systems and handle personal data or confidential organisational information.

3. Definitions

- Personal Data: Any information that relates to an identified or identifiable individual (Data Subject), such as name, contact details, or IP address.
- Sensitive Data: Data that reveals race, ethnicity, political opinions, religious beliefs, health data, etc.
- Data Subject: The individual to whom the personal data relates.
- Data Controller: The entity that determines the purposes and means of processing personal data.
- Data Processor: The entity that processes personal data on behalf of the Data Controller.

4. IT Systems Usage

All employees are responsible for using IT systems in a way that ensures security and confidentiality of information. Employees must:

- Use company-provided devices for work-related purposes only.
- Refrain from unauthorized software installation or hardware changes.
- Avoid sharing login credentials with anyone, including coworkers.

5. Data Protection Principles

UNNATI will adhere to the following principles regarding personal data:

- Lawfulness, Fairness, and Transparency: Process personal data in a lawful, fair, and transparent manner.
- Data Minimization: Collect only the personal data that is necessary for the intended purpose.
- Accuracy: Keep personal data accurate and up-to-date.
- Storage Limitation: Retain personal data only as long as necessary.
- Confidentiality and Integrity: Secure personal data against unauthorized access or accidental loss.
- Accountability: Be able to demonstrate compliance with these principles.

6. Data Subject Rights

Data Subjects have the following rights regarding their personal data:

- Right of Access: To request access to their personal data held by UNNATI.
- Right to Rectification: To request correction of inaccurate or incomplete data.
- Right to Erasure: To request deletion of their data, subject to certain conditions.
- Right to Restrict Processing: To request that UNNATI limits the processing of their data.
- Right to Data Portability: To obtain and reuse their data for their own purposes across different services.
- Right to Object: To object to the processing of their data in certain circumstances.

7. Data Breach Reporting

In the event of a data breach, UNNATI will:

- Communicate with affected individuals if their personal data is at risk.
- Document the breach and any remediation actions taken.

8. IT Security Measures

UNNATI will implement the following IT security measures to protect data:

- Access Control: Ensure only authorized users have access to sensitive data.
- Firewalls and Antivirus: Use firewalls and regularly updated antivirus software to protect against threats.
- Data Backups: Regularly back up critical data and store it securely.
- Network Security: Monitor and secure the company’s network from unauthorized access or cyber-attacks.

9. Employee Responsibilities

All employees must:

- Follow the guidelines provided in this policy when accessing or using IT systems.
- Report any suspected data breach or security incident immediately to the reporting officer or the Policy Steering and Compliance Committee.

- Keep their systems up-to-date by installing updates and patches provided by the IT department.

10. Training and Awareness

UNNATI will undertake orientation of all employees to ensure they understand their responsibilities under this policy, including the handling of personal data and proper use of IT systems.

11. Third-Party Access and Data Sharing

Third parties who access UNNATI's IT systems or process data on behalf of the company must:

- Adhere to the data protection principles outlined in this policy.
- Sign data processing agreements before accessing any personal data or IT systems.
- Ensure appropriate security measures are in place to protect data.

12. Data Retention and Disposal

UNNATI will retain personal data only for as long as it is needed for the purposes for which it was collected, or as required by law. When personal data is no longer needed, it will be securely disposed of in line with data retention policies.

13. Monitoring and Review

This policy will be regularly reviewed by the Director and the Policy Compliance Committee. To ensure its effectiveness the Director and PCC may propose necessary amendments and updates will be communicated to employees and other stakeholders.

Approved by:
Binoy Acharya
Director

December 31, 2024