INCUBATION CENTRE – DATA PRIVACY GUIDELINES

1. Purpose

These guidelines ensure the **protection, confidentiality, and responsible use of data** within the Incubation Centre by all users.

2. Scope

Applies to:

- All startups, founders, employees, interns, and visitors
- All forms of data: **digital, physical, and communication-based**

3. Data Responsibility

- Each user/startup is the **owner and custodian of their data**
- Users are responsible for securing:
  - Business data
  - Customer data
  - Intellectual property
- The Incubation Centre is **not responsible for data loss, theft, or breaches**

4. Acceptable Data Practices

Users must:

- Store data securely using **password protection and encryption (where applicable)**
- Use **licensed software and secure platforms only**
- Regularly update systems with **security patches and antivirus protection**
- Maintain proper **data backup mechanisms**

5. Prohibited Data Activities

The following are strictly prohibited:

- Unauthorized access to another user's data or systems
- Sharing confidential or sensitive data without consent
- Storing or transmitting **illegal, pirated, or harmful content**
- Attempting to hack, disrupt, or misuse network systems

6. Network & Internet Security

- Use only **authorized network access provided by the centre**
- Do not:
  - Share Wi-Fi credentials
  - Install unauthorized network devices
  - Engage in activities that compromise network integrity
- High-risk downloads and suspicious links must be avoided

7. Device & Access Security

- Devices must be **password-protected**
- Lock systems when unattended
- Avoid using **public/shared systems for sensitive work**
- Lost or compromised devices must be **reported immediately**

8. Confidentiality & IP Protection

- Respect the **confidentiality of other startups and users**
- Do not share, copy, or disclose any information without authorization
- Intellectual Property (IP) remains the **sole ownership of the respective startup/user**

9. Physical Data Security

- Secure important documents and files
- Avoid leaving sensitive information unattended
- Dispose of documents using **safe methods (shredding if required)**

10. Data Backup & Recovery

- Users are responsible for maintaining **regular backups**
- Backup systems should be stored securely (cloud/local)
- The centre does not guarantee **data recovery services**

11. Incident Reporting

- Any data breach, suspicious activity, or security concern must be **reported immediately** to the administration
- Prompt reporting helps minimize risk and impact

12. Compliance & Consequences

Non-compliance may result in:

- Suspension of network and facility access
- Termination of incubation privileges
- Legal action in case of serious violations

Guiding Principle

Protect your data. Respect others' data. Build responsibly.

Acknowledgement

I/We agree to comply with the Data Privacy Guidelines.

Name: _____

Startup Name: _____

Signature: _____

Date: _____