INFORMATION SECURITY & CYBERSECURITY POLICY

- **Purpose**
  To protect Zydus Wellness' information assets — people, data, systems and services — from unauthorized access, disclosure, alteration, or destruction and ensure business continuity. This policy establishes principles, responsibilities and minimum controls required across the organization and with third parties.

- **Scope**
  Applies to all employees, contractors, suppliers, joint ventures and any third party that stores, processes or transmits Zydus Wellness information or connects to its IT/OT environments (all locations, cloud, on-premises, endpoints, mobile devices).

- **Principles & Commitments**
  Zydus Wellness commits to:
  - Continuous improvement of information security systems.
  - Integrity and protection of data.
  - Monitoring and response to threats.
  - Clear individual responsibilities.
  - Third-party security requirements.

- **Governance & Roles**
  - Board / Risk Management Committee: oversight of cyber risk appetite and incidents.
  - CISO / Head — Information Security/CIO: implement ISMS, incident response, report to Board.
  - IT/OT Managers: implement technical controls and patching.
  - Business Unit Heads: ensure classification, access, and secure processes.
  - Employees / Contractors: follow rules, attend training, report incidents.

- **Risk Management & ISMS**
  Maintain ISMS aligned with ISO/IEC 27001 and adopt CERT-In guidance. Risk assessments must drive control selection and remediation plans.

- **Minimum Required Controls**
  Access & Identity : Role-based access, MFA, reviews.
  Endpoint & Network Security : MDM, protection, segmentation, secure remote access.
  Data Protection: Classification, encryption, backups.
  Application & Cloud : Secure SDLC, vendor hardening.
  Incident Response : Logging, monitoring, playbooks, regulatory notifications.
  Patching & Vulnerability : Regular scans, remediation SLAs.
  Physical Security : Access controls, CCTV at sensitive sites.
  BCP & DR : Tested DR plans, recovery objectives.

- **Third-Party & Supplier Security**
  Third parties must undergo assessments, contractual clauses, audits, and notify incidents impacting Zydus Wellness.

- **Monitoring, Reporting & Metrics**
  Key metrics include detection/response times, patch compliance, third-party assessments, and phishing resilience. CISO/CIO reports quarterly.

- **Training & Awareness**
  Mandatory onboarding and annual training for all; role-based training for privileged staff; immediate reporting of issues required.

- **Legal, Regulatory & Standards Compliance**
  Comply with Indian laws/regulations (CERT-In advisories), ISO/IEC 27001, and contractual obligations.

- **Policy Exceptions & Approvals**
  Exceptions must be documented, risk-assessed, and approved by CISO/CIO and business approver. Reviewed quarterly.

- **Enforcement & Sanctions**
  Non-compliance will lead to disciplinary action, up to termination or legal action if required.

- **Review Cycle**
  Policy reviewed annually or after significant incident/regulatory change, with continuous improvement cycles.

Place :

Date : 10/02/2025

Vineet Shrivastava
Head-Information Technology
Zydus Wellness

Zydus Wellness

Tarun Arora
Whole Time Director & CEO
Zydus Wellness