NextTech Enterprise Information Security Policy

Policy Number: NT-IS-001
Effective Date: 01.01.2025

Review Cycle: Annual
Approved By: CEO, CISO

1. Purpose

This policy establishes NextTech's framework for safeguarding sensitive data, ensuring compliance with EU regulations (GDPR, NIS2), and mitigating cybersecurity risks across all business processes (O2C, P2P, R2R, H2R, IT, Logistics, and Customer Service).

2. Scope

Applies to:

- All employees, contractors, and third-party vendors
- IT systems (SAP S/4HANA, Azure Cloud, Salesforce)
- Physical and digital assets (manufacturing IoT, SaaS platforms)

3. Policy Statements

3.1 Data Classification & Handling

Classification	Examples	Access Control	Encryption
Confidential	Customer PII, Financial Data	Role-based (SAP GRC)	AES-256 at rest/transit
Internal	HR records, Process docs	NextTech employees only	TLS 1.3+
Public	Marketing materials	Unrestricted	N/A

Rules:

- Customer data retention: Max 5 years post-contract termination (GDPR Article 17).

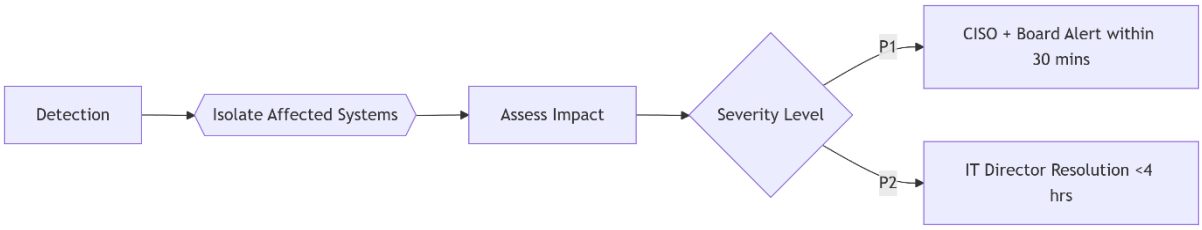
- SAP Fiori roles reviewed quarterly by Internal Audit.

3.2 Access Management

- **JML (Join-Move-Leave) Process:**
    - Onboarding: Access granted per **RACI matrix** within 24 hrs.
    - Offboarding: Automated revocation via **ServiceNow HR integration**.
- **Privileged Access:**
    - Requires VP approval + **MFA** (Microsoft Authenticator).
    - Sessions logged in **Azure Sentinel**.
- Blockchain-based Identity Management will be implemented

3.3 Incident Response

Escalation Protocol:



- **P1 Criteria:** Data breach, ransomware, or >1hr SaaS downtime.
- **Reporting:** All incidents logged in **ServiceNow GRC**; GDPR breaches reported to DPA within 72 hrs.

3.4 Secure Development

- **SaaS Products (Digital Twin):**
    - Code scans via **Checkmarx** before release.
    - Penetration testing biannually (CREST-certified vendors).
- **API Security:**
    - OAuth 2.0 mandatory for customer data access.
    - Rate limiting (1,000 requests/min) to prevent DDoS.

3.5 Physical Security

- **Manufacturing Sites:**
    - Biometric access for server rooms (Siemens ID system).
    - IoT devices on segregated VLANs.
- **Workstations:**
    - Auto-lock after 5 mins inactivity.
    - USB device use requires **Endpoint Privilege Management (EPM)** approval.

4. Compliance & Enforcement

- **Audits:** Quarterly by Internal Audit + external ISO 27001 recertification.
- **Violations:**
    - 1st offense: Mandatory training.
    - Repeat: Termination + legal action for GDPR breaches.

5. Roles & Responsibilities

Role	Accountability
CISO	Policy enforcement, threat intelligence
IT Managers	Patch management, access reviews
Employees	Report phishing via **PhishAlarm** button

6. Exceptions

- Must be documented via **Risk Acceptance Form** (approved by CISO).
- Valid for max 90 days unless renewed.