



# IT GOVERNANCE AND MANAGEMENT POLICY

This document is a simplified version for technical portfolio demonstration purposes, focusing on strategic structure and alignment with COBIT, ISO, or ITIL frameworks.



**Company Name:** NovaTech Solutions Ltd.

**Document Type:** IT Governance and Management Policy

**Version:** 1.0

**Approving authority:** Executive Board

**Effective date:** 01/01/2026

**Ciclo de revisão:** Annually or after significant changes

## ■ Objective

This policy establishes the principles, structures, and responsibilities for the governance and management of Information Technology (IT) at NovaTech Solutions Ltd.

The objective is to ensure that IT:

- Is aligned with business strategy
- Delivers measurable value
- Manages risks effectively
- Complies with applicable laws, regulations, and standards



## ■ Scope

### This policy applies to:

- All IT systems, services, infrastructure, and data;
- All employees, contractors, and third parties involved with IT;
- All business units of NovaTech Solutions Ltd.



## ■ Principles of governance

IT governance at NovaTech is guided by the following principles:

- **Strategic alignment:** IT initiatives must support business objectives;
- **Value delivery:** IT investments must generate measurable benefits;
- **Risk optimization:** IT risks must be identified, assessed, and managed;
- **Resource management:** IT resources must be used efficiently;
- **Performance measurement:** IT performance must be monitored and reported.

# ■ Governance Structure

## IT Management

- Implements approved strategies and policies;
- Manages IT operations and services;
- Ensures compliance with governance requirements.

## Risk and Compliance Function

- Oversees IT risk management;
- Supports audits and regulatory compliance;
- Monitors adherence to internal policies.

## ■ IT risk management

NovaTech adopts a structured approach to IT risk management in order to:

- Identify IT-related risks;
- Assess risks based on probability and impact;
- Define and implement risk treatment plans;
- Monitor and report risks periodically;
- Risk management activities are aligned with the organization's risk appetite and integrated with Enterprise Risk Management (ERM).

## ■ Information Security Governance

Information security is governed by an Information Security Management System (ISMS) designed to protect:

- Confidentiality;
- Integrity;
- Availability of information assets.
- Security controls are selected based on risk assessment and aligned with recognized standards such as ISO/IEC 27001.

## ■ IT Service Management

IT services are governed to ensure:

- Consistent service delivery;
- Compliance with Service Level Agreements (SLAs);
- Continuous improvement of services.
- Service management practices support business continuity and customer satisfaction.

## ■ Performance Monitoring and Reporting

IT performance is monitored using defined metrics and indicators, including:

- Service availability;
- Incident and problem trends;
- Project delivery performance;
- Risk and compliance status.

Reports are submitted periodically to governance bodies.

## ■ Compliance

All IT activities must comply with:

- Internal policies;
- Applicable laws and regulations;
- Contractual obligations;
- Recognized governance and security frameworks;

Non-compliance may result in corrective action.

## ■ Continuous Review and Improvement

This policy is reviewed annually or when significant changes occur in:

- Business strategy;
- Technological landscape;
- Regulatory environment.

Continuous improvement is promoted to increase the maturity of IT governance.

## ■ Reference Frameworks

This policy is aligned with:

- COBIT 2019
- ISO/IEC 38500
- ISO/IEC 27001
- ITIL 4

## ■ Disclaimer

This document represents a fictional case developed for professional and educational purposes and does not reflect any real organization.