SECURETECH SOLUTIONS

GOVERNANCE CHARTER

2024

PURPOSE

The purpose of this Governance Charter is to establish a framework for effective governance, risk management, and compliance at SecureTech Solutions. This document outlines the mission, vision, objectives, roles, responsibilities, and decision-making processes necessary to achieve our cybersecurity goals

MISSION STATEMENT

To protect the integrity, confidentiality, and availability of SecureTech Solutions' information assets while ensuring compliance with applicable laws and regulations.

VISION STATEMENT

To be a leader in cybersecurity governance, creating a culture of security awareness and proactive risk management that aligns with our business objectives.

OBJECTIVES

01

Risk Identification

Proactively identify, assess, and prioritize risks to the organization's information assets.

02

Regulatory Compliance

Ensure adherence to relevant laws, regulations, and industry standards.

03

Stakeholder Engagement

Foster collaboration among stakeholders to promote a shared understanding of risk and compliance.

04

Continuous Improvement:

Regularly review and enhance governance practices to adapt to changing risks and regulatory environments.

SCOPE

This governance framework applies to all employees, contractors, and third-party partners of SecureTech Solutions involved in the management and protection of information assets.

KEY ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Oversees the overall cybersecurity strategy.
- Reports to the executive team on risk status and compliance.

Governance, Risk, and Compliance (GRC) Team Lead

- Manages governance, risk, and compliance efforts.
- Coordinates risk assessments and compliance audits.

IT Compliance Officer:

- Ensures adherence to regulations and internal policies.
- Monitors compliance status and reports findings to the GRC Team Lead.

Department Heads

- Responsible for implementing governance policies within their departments.
- Ensure their teams are trained on compliance requirements.

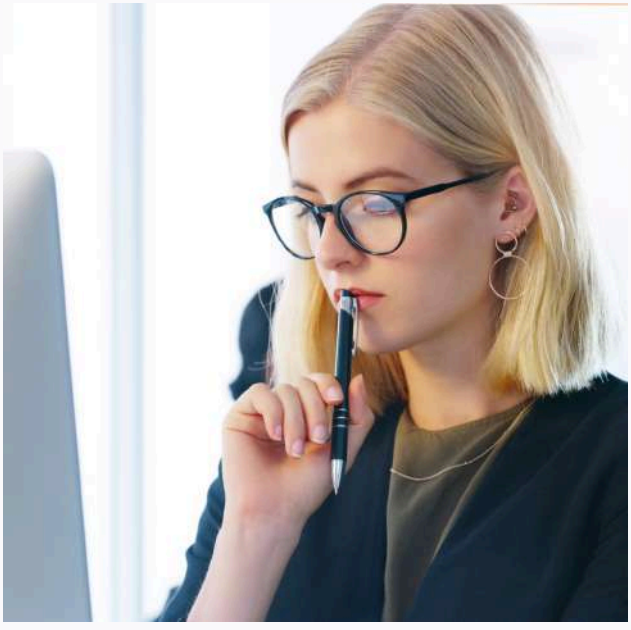
DECISION-MAKING PROCESSES

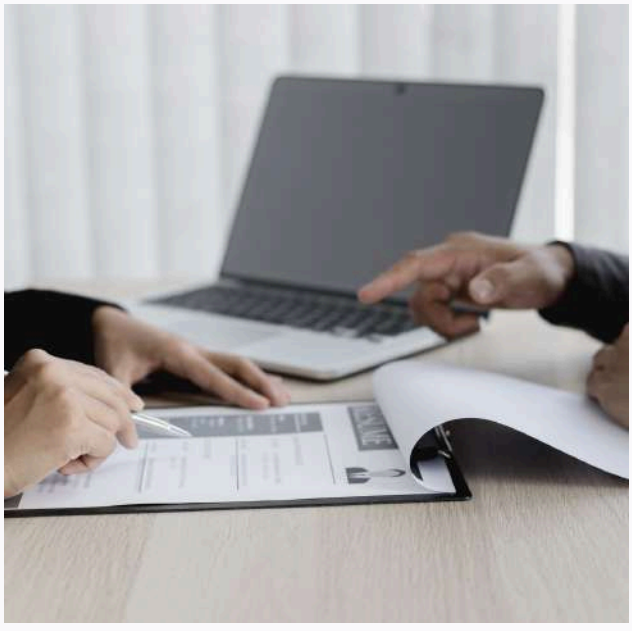
Authority Levels

- The executive team has the authority to approve major policy changes.
- The GRC Team Lead has the authority to approve risk mitigation strategies.

Escalation Procedures

- Issues requiring higher-level approval should be escalated to the executive team through the GRC Team Lead.





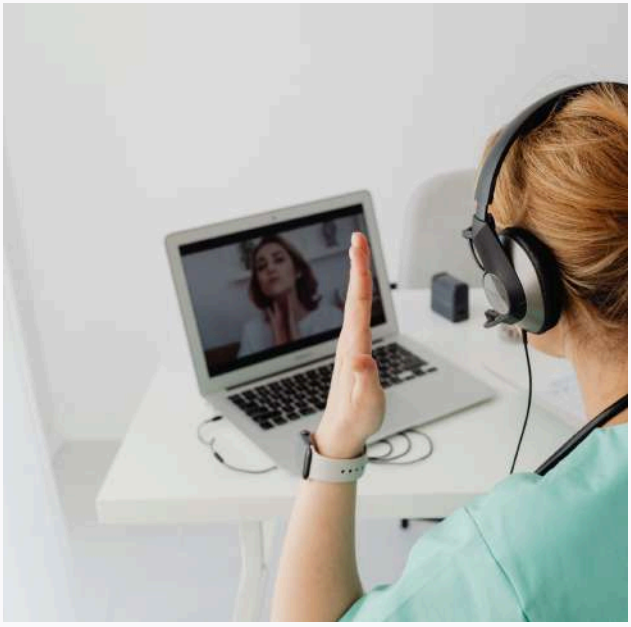
COMMUNICATION CHANNELS

Regular Meetings

Schedule monthly meetings to discuss governance, risk, and compliance updates.

Reporting

Provide quarterly reports to the executive team outlining risk assessments, compliance status, and any emerging issues.



MONITORING AND REVIEW

- Conduct annual reviews of the governance framework to ensure its effectiveness.
- Implement feedback mechanisms to incorporate stakeholder input into governance practices.

DOCUMENTATION

All roles, processes, and decisions related to governance will be documented and stored in a centralized repository to maintain transparency and accountability.

STAKEHOLDER INVOLVEMENT

Key stakeholders will be involved in the development and review of this Governance Charter to ensure it meets the organization’s needs and addresses potential concerns.

APPROVAL

This Governance Charter is approved by the executive team of SecureTech Solutions as of 15 January 2024.

Jane Smith
Chief Information Security Officer
SecureTech Solutions

John Doe
Chief Executive Officer
SecureTech Solutions