Information Security Management System Proposal

Prepared by: Michael Jordan
Date: 6-23-2025

Purpose:

The purpose of this ISMS proposal is to address identified gaps between SecureTech's current practices and ISO 27001 requirements. This document outlines prioritized controls, justifications, and actionable implementation plans to strengthen SecureTech's information security posture.

Objective:

To provide a clear, actionable roadmap for closing compliance gaps and ensuring adherence to ISO 27001 standards.

Section 1: Identified Gaps

Gap A: SecureTech lacks multi-factor authentication for access to sensitive systems.
Impact: Without MFA, administrative accounts are at higher risk of compromise through stolen or weak credentials, increasing the likelihood of unauthorized access and data breaches.
Relevant ISO 27001 Control: A.9 Access Control

Gap B: Current incident response practices are inconsistent, with no centralized logging system in place.
Impact: Ineffective logging and monitoring delay threat detection and containment, increasing exposure to extended breaches.
Relevant ISO 27001 Control: A.16 Incident Response

Gap C: Backup procedures rely solely on weekly full backups, with no daily incremental backups in place.
Impact: This leaves SecureTech vulnerable to significant data loss in the event of system failures, ransomware attacks, or accidental deletions between weekly backups.
Relevant ISO 27001 Control: A.12 Operations Security

Section 2: Recommended Controls

Control A: A.9 Access Control
Rationale:
Implementing MFA provides an essential second layer of authentication, significantly reducing the risk of unauthorized access to critical systems.

Control B: A.16 Incident Response
Rationale:
Centralized logging and consistent incident monitoring ensure faster detection, escalation, and resolution of security incidents.

Control C: A.12 Operations Security
Rationale:
Daily incremental backups mitigate the risk of data loss and ensure operational continuity, particularly in the event of cyberattacks or hardware failure.

Section 3: Implementation Plan

Control	Action Steps	Timeline	Resources Needed	Monitoring Processes
A.9 Access Control	- Deploy and configure MFA solution - Apply MFA to all privileged accounts - Train staff	3 months	MFA software licenses, training materials, IT security staff	Quarterly audits of MFA application and access logs
A.16 Incident Response	- Implement centralized logging tool - Integrate with alerting system - Train IR team on analysis	1 month	SIEM tool, training time, infrastructure support	Weekly log reviews, monthly audit reports

A.12 Operations Security	- Upgrade systems to support daily incremental backups - Automate backups and alerts - Test recovery monthly	2 months	Backup software upgrades, scripting resources, test environments	Daily backup success logs, monthly recovery test validations

Conclusion

This ISMS proposal addresses SecureTech’s most pressing ISO 27001 compliance gaps. By implementing multi-factor authentication, improving incident detection through centralized logging, and upgrading backup operations, SecureTech will significantly enhance its security maturity. These prioritized actions are aligned with best practices and offer high-impact improvements toward reducing risk and achieving ISO 27001 certification readiness.