Compliance Report – SecureTech Solutions

Date: 6-13-2025

Prepared by: Michael Jordan

Audit Overview: Four major compliance gaps were discovered across these security domains: access control, incident logging, physical security, and policy updates. These findings posed a risk to achieving ISO 27001 certification readiness.

Findings:

1. Priority 1 – **Access Control Issues**
   - Explanation: Shared user ids are being used which makes it difficult to trace actions to a specific individual. ISO 27001 emphasizes unique IDs to ensure accountability. Not being in compliance can increase internal risk and data misuse.
   - Action Plan: Implement unique user IDs for all employees by the end of the quarter. Also, work with IT to disable all shared accounts.

2. Priority 2 – **Incident Logging**
   - Explanation: Our logging system is missing critical security events like failed login attempts and data access patterns. According to ISO 27001 it's essential that all incidents and events are captured to allow early detection of potential breaches.
   - Action Plan: Upgrade incident logging software (Splunk, etc.) to capture all security events including failed logins and access patterns within the next three months.

3. Priority 3 – **Physical Security**
   - Explanation: Employees are bypassing badge scanning to enter restricted areas, ISO 27001 strict access to secured areas.Tailgating is a security concern.
   - Action Plan: Physical security can be addressed by enforcing badge rules. Define tailgating as a violation of company policy.

4. Priority 4 – **Policy Updates**
   - Explanation: ISO 27001 mandates an annual review, to ensure policies remain relevant and align with evolving threats. It has not been reviewed in over a year.
   - Action Plan: Since policy hasn't been updated in over a year, time will need to be scheduled to review to ensure policies remain relevant and align with potential threats.