Compliance Gap Report

Date: 6-12-2025

Prepared by: Michael Jordan

Overview

The recent audit that was conducted at Secure Tech shows compliance gaps related to ISO 27001.

1. **Access Control:** Several employees are using shared user IDs, which is not aligned with SecureTech's access control policy.
2. **Incident Logging:** The incident logging system doesn't capture all security events, particularly failed login attempts and data access patterns
3. **Physical Security:** Some employees bypass badge scanners when entering restricted areas.
4. **Policy Updates:** The Information Security Policy is outdated and hasn't been reviewed in the last year

Prioritized Gaps:

5. **Access Control**: The sharing of user IDs offers no accountability or confidentiality, and increases the risk of internal risk and data misuse.
6. **Incident Logging**: Failing to log incidents and data access affects the detection and response to suspicious activity.
7. **Physical Security**: Physical security can be addressed by enforcing badge rules.
8. **Policy Updates**: Policy updates only need to be done annually, this can wait until next year.

Recommendations:

- Implement individual user IDs for all employees, and work with IT to disable all shared accounts by the end of the quarter.
- Update incident logging software (Splunk) to capture all relevant security events.