SECURITY ASSESSMENT SUMMARY

Assessment ID: SEC-ASSESS-2025-03

Date: March 30, 2025

Assessor: James Wilson

Overview

This assessment evaluated security controls against TNO's Corporate Information Security Policy and Password Policy. The assessment identified several areas of PARTIAL COMPLIANCE that require attention.

Key Findings

Access Control Assessment

Role-based access control is implemented, but inconsistently across departments. Least privilege principles are generally followed, but exceptions exist without documentation. Quarterly access reviews are being conducted, but two departments missed the last review cycle. Terminated user account deactivation occurs within policy timeframes. Multi-factor authentication is implemented for most but not all privileged accounts (approximately 85% coverage). Service account documentation exists but has not been reviewed in the last 8 months.

Compliance Level: PARTIALLY COMPLIANT

Password Management Assessment

Password length requirements are consistently enforced at 12 characters. Password complexity requirements are configured correctly. Password history is maintained, but only for the previous 6 passwords instead of the required 10. Password expiration is set correctly to 90 days. Account lockout is configured for 5 failed attempts as required. Temporary password change enforcement is functioning properly.

Compliance Level: PARTIALLY COMPLIANT

Data Protection Assessment

Encryption for data in transit is implemented using TLS 1.2+. However, approximately 15% of storage locations containing sensitive data do not have at-rest encryption enabled. Data classification is generally followed, but inconsistently applied to new projects. Data transfer approvals are documented, but encryption is not consistently verified. Media sanitization procedures are compliant. Backup systems are operational but recovery testing is overdue by 2 months. Data retention periods are configured correctly.

Compliance Level: PARTIALLY COMPLIANT

Incident Response Assessment

Security incident reporting procedures are documented and available to employees. The incident response plan exists but has not been tested in the last 14 months, exceeding the annual testing requirement. Roles and responsibilities are defined but not updated to reflect recent organizational changes. Post-incident reviews are conducted but not consistently documented. Evidence preservation follows best practices.

Compliance Level: PARTIALLY COMPLIANT

System Security Assessment

Anti-malware protection is installed on all systems with current definition files. Patch management for critical systems is current, but approximately 20% of non-critical systems have patches pending beyond deployment schedules. Vulnerability remediation processes follow policy, but execution is delayed for medium-risk issues. Penetration testing for two critical systems is overdue. Host-based firewalls are enabled on all workstations but only 85% of servers. Remote access solutions use encrypted connections.

Compliance Level: PARTIALLY COMPLIANT

Compliance and Auditing Assessment

Audit logging is configured for security-relevant events on critical systems, but logging is inconsistent on secondary systems. Log protection measures are adequate. Security compliance reviews are conducted but not at the required frequency. Third-party providers have signed security agreements. Policy exceptions are documented, but several are past their review date.

Compliance Level: PARTIALLY COMPLIANT

Required Remediation Actions

1. Implement multi-factor authentication for all remaining privileged accounts.
2. Update password history settings to maintain 10 previous passwords.
3. Complete encryption deployment for all sensitive data storage locations.
4. Conduct and document the annual incident response plan test.
5. Complete pending system patches within 30 days.
6. Standardize audit logging across all systems.
7. Schedule penetration testing for overdue critical systems.

Conclusion

While foundational security controls are in place, several gaps must be addressed to achieve full compliance with organizational security policies.

Signed: James Wilson

Security Assessor