INFORMATION SECURITY AUDIT REPORT

Report ID: SEC-AUDIT-2025-Q1

Date: April 10, 2025

Auditor: Maria Chen, CISSP

Executive Summary

This audit report presents the findings of a comprehensive security review conducted between March 15-25, 2025. The audit evaluated compliance with TNO's Corporate Information Security Policy and Password Policy. Overall, the systems and processes reviewed demonstrate FULL COMPLIANCE with the organization's security policies.

Methodology

The audit included interviews with key personnel, configuration reviews, documentation analysis, and technical testing. All findings are supported by evidence collected during the audit process.

Detailed Findings

Access Control Review

All reviewed systems implement role-based access control as required. Access rights are granted following the principle of least privilege, and evidence shows quarterly user access reviews are being completed by managers. User account termination processes were tested and confirmed to meet the 24-hour deactivation requirement. All privileged accounts utilize multi-factor authentication. Service account documentation is up-to-date and shows evidence of semi-annual reviews.

Compliance Status: FULLY COMPLIANT

Password Management Review

Password configurations across all systems enforce a minimum 12-character length. Complexity requirements enforcing a combination of uppercase, lowercase, numbers, and special characters are properly implemented. Password history settings prevent reuse of the previous 10 passwords.

Maximum password age is correctly set to 90 days. Account lockout occurs after 5 failed authentication attempts. All default and temporary passwords must be changed upon first use.

Compliance Status: FULLY COMPLIANT

Data Protection Assessment

All sensitive data is encrypted both in transit using TLS 1.2+ and at rest using AES-256. Confidential information is properly classified and labeled according to the data classification policy. Data transfer approvals and encryption were verified through process review and sample testing. Media sanitization procedures comply with policy requirements. Backup systems are operational with regular testing. Data retention configurations match legal and regulatory requirements.

Compliance Status: FULLY COMPLIANT

Incident Response Evaluation

Security incident reporting procedures are well-documented and communicated. The incident response plan is current and was tested in February 2025. Roles and responsibilities are clearly defined in the incident response documentation. Post-incident review templates and completed examples were examined and found to be comprehensive. Evidence preservation guidelines follow forensic best practices.

Compliance Status: FULLY COMPLIANT

System Security Verification

All systems have up-to-date anti-malware protection installed. Operating systems and applications are current with security patches according to deployment schedules. Vulnerability remediation follows the documented risk-based approach. Penetration testing reports for critical systems from January 2025 were reviewed. Host-based firewalls are enabled on all applicable systems. Remote access solutions employ secure, encrypted connections.

Compliance Status: FULLY COMPLIANT

Compliance and Auditing Check

Audit logging is properly configured on all systems with security-relevant events being captured. Log files are protected from unauthorized access and modification. Regular security compliance reviews are scheduled and completed as required. Third-party service providers have signed security agreements. Exception documentation was reviewed and found to be properly approved.

Compliance Status: FULLY COMPLIANT

Recommendations

While all areas are in compliance, the following enhancements are recommended:

1. Consider implementing automated compliance monitoring tools to reduce manual review effort.
2. Evaluate passwordless authentication options for improved user experience and security.
3. Enhance the security awareness program with more frequent updates on emerging threats.

Conclusion

The organization demonstrates strong adherence to security policies with effective controls in place. No remediation actions are required at this time.

Signed: Maria Chen, CISSP

Information Security Auditor