CORPORATE INFORMATION SECURITY POLICY

Version 2.3 | Effective Date: January 15, 2025 | Classification: INTERNAL

1. PURPOSE AND SCOPE

This policy establishes the framework for protecting the confidentiality, integrity, and availability of TNO's information assets. It applies to all employees, contractors, consultants, temporary staff, and other workers at TNO, including those affiliated with third parties who access TNO information systems.

2. POLICY REQUIREMENTS

2.1 Access Control Requirements

1. All systems and applications must implement role-based access control.
2. Access rights must be granted based on the principle of least privilege.
3. User access must be reviewed and certified by managers quarterly.
4. Terminated user accounts must be disabled within 24 hours.
5. Privileged accounts must utilize multi-factor authentication.
6. Service accounts must be documented and reviewed semi-annually.

2.2 Password Management

1. Passwords must be at least 12 characters long.
2. Passwords must contain a combination of uppercase, lowercase, numbers, and special characters.
3. Password history must be maintained to prevent reuse of the previous 10 passwords.
4. Password maximum age must be set to 90 days.
5. Accounts must be locked after 5 failed authentication attempts.
6. Default or temporary passwords must be changed on first use.

2.3 Data Protection

1. Sensitive data must be encrypted in transit and at rest.
2. Confidential information must be classified and labeled appropriately.
3. Data transfers outside the organization must be approved and encrypted.
4. Media containing confidential data must be securely sanitized before disposal.
5. Regular backups of critical data must be performed and tested.
6. Data retention periods must comply with legal and regulatory requirements.

2.4 Incident Response

1. Security incidents must be reported to the Information Security team within 24 hours.
2. An incident response plan must be documented and tested annually.
3. Roles and responsibilities during security incidents must be clearly defined.
4. Post-incident reviews must be conducted to identify improvements.
5. Evidence must be preserved according to forensic best practices.

2.5 System Security

1. All systems must have current anti-malware protection installed.
2. Operating systems and applications must be kept updated with security patches.
3. Security vulnerabilities must be remediated based on risk severity.
4. Critical systems must undergo annual penetration testing.
5. Host-based firewalls must be enabled where technically feasible.
6. Remote access must use secure, encrypted connections.

2.6 Compliance and Auditing

1. Systems must maintain audit logs of security-relevant events.
2. Audit logs must be protected from unauthorized access and modification.
3. Regular security compliance reviews must be conducted.
4. Third-party service providers must comply with TNO security requirements.
5. Exceptions to security policy must be documented and approved.

3. RESPONSIBILITIES

- Executive Management: Oversight and approval of the security policy.
- Information Security Team: Implementation and enforcement of the security policy.
- Department Managers: Ensuring their staff comply with the security policy.
- Employees: Understanding and adhering to all applicable security policies.

4. COMPLIANCE

Violations of this policy may result in disciplinary action, up to and including termination of employment. For contractors or consultants, violations may result in termination of the working relationship.

5. REVIEW

This policy shall be reviewed and updated annually, or more frequently if significant changes occur in the business or technical environment.

APPROVED BY:

Jennifer Walters, Chief Information Security Officer

Date: January 15, 2025