UNIFIED SECURITY AND PRIVACY COMPLIANCE POLICY
Version 1.0 | Effective Date: February 10, 2025 | Classification: INTERNAL

1. PURPOSE AND SCOPE

This unified policy establishes the framework for protecting both information security and data privacy at TNO. It applies to all employees, contractors, and third parties who access TNO systems or process TNO data.

2. SECURITY CONTROLS AND PRIVACY PRINCIPLES

2.1 Access Control and Data Subject Rights

1. All systems must implement role-based access control with least privilege
2. Multi-factor authentication is required for all privileged accounts
3. User access must be reviewed quarterly by managers
4. Data subjects have the right to access their personal data
5. Data subjects may request rectification or deletion of their data
6. All data subject requests must be processed within 30 days

2.2 Data Protection and Security

1. Sensitive data must be encrypted in transit and at rest
2. We collect the following types of personal information:
   - Contact details (name, email, phone)
   - Account credentials (username, password)
   - Usage data (features accessed, actions performed)
3. Regular security assessments must be conducted
4. Data retention periods must comply with legal requirements
5. Your data is processed according to the following principles:
   - Lawfulness, fairness, and transparency
   - Purpose limitation
   - Data minimization

2.3 Incident Response and Breach Notification

1. Security incidents must be reported to the Security team within 24 hours
2. Data breaches involving personal data must be reported to the DPO within 24 hours
3. The incident response team shall be notified immediately upon discovery of a security incident
4. Data breach notifications to authorities must be sent within 72 hours
5. Affected data subjects must be notified without undue delay
6. Incidents shall be categorized according to the following severity levels

2.4 System Security and Data Processing

1. All systems must maintain current anti-malware protection
2. Operating systems and applications must be kept updated
3. Your personal information is processed based on:

   - Performance of a contract
   - Legal obligations
   - Legitimate interests
   - Your consent (where applicable)
4. Host-based firewalls must be enabled
5. Regular vulnerability scanning must be performed

3. RESPONSIBILITIES

3.1 Security Responsibilities

1. Information Security Team: Implementation of security controls
2. System Administrators: System hardening and patching
3. Department Managers: Ensuring staff compliance with security requirements
4. All Employees: Following security procedures and reporting incidents

3.2 Privacy Responsibilities

1. Data Protection Officer: Oversight of privacy compliance
2. Data Stewards: Managing data within their departments
3. Privacy Team: Data protection impact assessments
4. All Employees: Handling personal data according to policy

4. INTERNATIONAL DATA TRANSFERS

1. Personal data transfers outside the EEA require appropriate safeguards
2. Transfer mechanisms include:
   - Standard Contractual Clauses
   - Binding Corporate Rules
   - Adequacy decisions
3. International transfers must be documented in the processing register
4. Data recipients must provide adequate security guarantees

5. MONITORING AND COMPLIANCE

1. Systems must maintain security audit logs
2. Data processing activities must be documented
3. Regular compliance assessments must be conducted
4. Privacy by design must be implemented for new systems
5. Security and privacy impact assessments are required for high-risk processing

6. EXCEPTIONS AND VIOLATIONS

1. Exceptions to this policy must be documented and approved
2. Security or privacy violations may result in disciplinary action
3. Repeated violations may result in termination
4. Legal actions may be pursued for serious violations

7. REVIEW

This policy shall be reviewed annually or when significant changes occur in the business, technology, or regulatory environment.

APPROVED BY:
Jennifer Walters, Chief Information Security Officer
Maria Chen, Data Protection Officer
Date: February 10, 2025