# ACCEPTABLE USE POLICY

Version 1.3 | Effective Date: February 15, 2025 | Classification: INTERNAL

## 1. PURPOSE

This Acceptable Use Policy defines the appropriate use of TNO information technology resources, systems, and services. It is designed to protect the organization, its employees, and its information assets from harm resulting from misuse of IT systems and resources.

## 2. SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at TNO, including all personnel affiliated with third parties who access TNO networks and systems. This policy applies to all equipment, systems, and services owned or leased by TNO, as well as to all activities conducted using TNO resources.

## 3. POLICY REQUIREMENTS

### 3.1 General Principles

1. Company resources shall only be used for authorized business purposes and in accordance with applicable policies and laws.

2. Limited personal use is permitted provided it does not interfere with work duties, consume significant resources, or violate any other policies.

3. All users are expected to exercise good judgment regarding appropriate use of TNO resources.

4. TNO reserves the right to monitor and audit systems and review data stored on its resources for compliance and security purposes.

### 3.2 Authorized Uses

1. Creating, viewing, and editing business documents

2. Business communication via approved channels

3. Accessing business applications and databases needed for job functions

4. Professional research and development activities

5. Work-related web browsing and information retrieval

6. Professional development and training

7. Other business-related activities approved by management

### 3.3 Prohibited Activities

1. Employees shall not use company systems to access inappropriate content, including pornographic, hateful, or offensive materials.

2. Sharing confidential information with unauthorized individuals

3. Violating copyright or intellectual property laws

4. Creating or distributing malicious code or attempting to breach security measures

5. Using resources for personal commercial purposes or financial gain

6. Engaging in online gambling, gaming, or non-business streaming activities

7. Excessive use of company resources for personal matters

8. Circumventing security controls or IT policies

9. Using company resources for political campaigns or activities

10. Harassing, discriminatory, or defamatory communications

11. Any illegal activities or actions that expose the company to legal liability

### 3.4 Software and Application Use

1. Software must not be installed without approval from IT department

2. Only licensed and approved software may be installed on company systems

3. Users must not disable or circumvent security features or anti-malware tools

4. Peer-to-peer file sharing applications are prohibited unless specifically authorized

5. Cloud storage services must be company-approved and used in accordance with data classification policies

### 3.5 Email and Communication

1. Company email is primarily for business communications

2. Mass emails must be business-related and sent only when necessary

3. Forwarding of business emails to personal accounts is prohibited

4. Email signatures must comply with corporate standards

5. Users must exercise caution with email attachments and links to prevent malware and phishing

### 3.6 Network and Internet Use

1. Remote access must use approved VPN or secure connection methods

2. Bandwidth-intensive activities should be limited during business hours

3. Streaming media should be limited to business purposes

4. Public Wi-Fi networks should be used with caution and always with VPN

5. Users must not attempt to bypass network security controls

### 3.7 Mobile Devices and Remote Work

1. Mobile devices accessing company resources must be password-protected

2. Company data on mobile devices must be encrypted

3. Lost or stolen devices must be reported immediately

4. Remote work must comply with all security policies and standards

5. Public computers should not be used to access company resources

### 3.8 Social Media Use

1. Users representing the company on social media must follow brand guidelines

2. Confidential information must never be shared on social media

3. Personal social media use should be minimal during work hours

4. Users should not claim to represent the company unless authorized

5. All social media communications should be professional and respectful

## 4. MONITORING AND PRIVACY

1. TNO reserves the right to monitor all activities on company systems without prior notice

2. Users should have no expectation of privacy when using company resources

3. Monitoring will be conducted in accordance with applicable laws and regulations

4. Personal devices used for business purposes may be subject to monitoring and security requirements

## 5. COMPLIANCE AND ENFORCEMENT

1. Violations of this policy may result in disciplinary action up to and including termination

2. Illegal activities will be reported to law enforcement

3. Temporary suspension of access privileges may be enforced during investigations

4. Contractors or temporary staff who violate this policy may have their contracts terminated

5. The IT department and managers are responsible for enforcing this policy

## 6. EXCEPTIONS

1. Exceptions to this policy must be approved in writing by the IT Security Manager or CISO

2. Exceptions will be documented and reviewed periodically

3. Temporary exceptions may be granted for specific business needs

4. All exceptions must include compensating controls where appropriate

## 7. RESPONSIBILITY

1. All users are responsible for understanding and complying with this policy

2. Managers are responsible for ensuring their staff understand and follow this policy

3. IT staff are responsible for implementing technical controls to support this policy

4. The Security team is responsible for monitoring compliance and investigating violations

## 8. REVIEW

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

APPROVED BY:

Thomas Wilson, Chief Information Officer

Date: February 15, 2025