SECURITY PROCEDURES

Version 1.0 | Last Updated: June 12, 2023

Introduction

This document outlines the security procedures for TNO systems and data. All employees should follow these guidelines to ensure information security.

Access Management

1. Users should select secure passwords for their accounts.
2. Administrator passwords should be at least 8 characters long and include a mix of letters and numbers.
3. System access should be reviewed periodically by department managers.
4. When employees leave the company, their accounts should be disabled.
5. Shared administrator accounts may be used for emergency access to critical systems.

Data Handling

1. Confidential data should be protected with appropriate measures.
2. When transferring sensitive information, users should consider encryption options.
3. Department managers are responsible for determining which data needs to be backed up.
4. Old files should be removed when no longer needed.
5. Data should be retained according to departmental needs.

System Security

1. Systems should have antivirus software installed where possible.
2. Critical security patches should be applied within 90 days.
3. Standard users should not have administrative privileges.
4. Remote access to company systems should use VPN when available.
5. Local system passwords can be reset by the helpdesk on request.

Incident Handling

1. Users should report suspicious activities to their supervisor.
2. IT staff will investigate security concerns as they arise.
3. Records of major security incidents should be maintained.
4. Department heads should be notified of security breaches affecting their area.

Compliance

1. These procedures should be followed by all employees.
2. Exceptions may be granted with manager approval.
3. The IT department is responsible for security implementation.

Contact the IT helpdesk for any questions regarding these procedures.