		[Insert Registered Legal Entity Name Here]
Document number: P4S		Document Title: **Access Control Policy**
Version: 1.0	Effective Date:	Document Owner:

X	Policy		Standard		Procedure		Form		Register		Other

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 5.15	
ISO/IEC 27002:2022	Controls: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev.5	AC-1 to AC-5	
EU GDPR	Article 32	
EU NIS2	Article 21(2)(b)	
EU DORA	Article 9	
COBIT 2019	APO07, DSS01	

<table>
<tr><td colspan="4"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="4">Document number:
P4S</td><td colspan="8">Document Title:
<b>Access Control Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:</td><td colspan="8">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

Purpose

1.1. This policy defines how the organization manages access to systems, data, and facilities to ensure that only authorized individuals can access information based on business need.

1.2. It establishes clear rules for user provisioning, modification, monitoring, and removal to minimize the risk of unauthorized access and to support compliance with applicable laws and standards.

1.3. The policy enforces the principle of least privilege, requiring that access be limited to the minimum necessary to perform job functions.

2. Scope

2.1. This policy applies to all individuals who use or manage access to the organization’s IT systems, networks, data, or facilities, including:

2.1.1. Employees

2.1.2. Contractors

2.1.3. Temporary workers

2.1.4. External IT service providers

2.2. It covers access to:

2.2.1. Company applications, file shares, and databases

2.2.2. Email, VPN, and remote access systems

2.2.3. Cloud-based services used for business purposes

2.2.4. Physical access to secure facilities, such as offices or server rooms

2.3. This policy is enforceable across all devices (company-issued or approved BYOD), platforms, and locations.

3. Objectives

3.1. Ensure that access rights are granted only after formal approval based on role and business justification.

3.2. Prevent unauthorized or excessive access to sensitive data, systems, or infrastructure.

3.3. Define clear procedures for provisioning, modification, and termination of user access.

3.4. Require regular access reviews and automated or manual logging to support audits.

3.5. Support technical enforcement of access restrictions through configuration and monitoring.

4. Roles and Responsibilities

4.1. General Manager

4.1.1. Approves this policy and ensures resources are available to implement effective access controls.

4.1.2. Approves exceptions and reviews annual access audits.

4.2. IT Manager / External IT Provider

4.2.1. Handles provisioning, modification, and termination of user accounts.

4.2.2. Maintains an Access Control Register with all activity (creations, changes, removals).

4.2.3. Implements role-based access controls (RBAC) and enforces strong authentication (e.g., MFA).

4.2.4. Reviews access logs for suspicious activity and reports issues to the General Manager.

4.3. Department Managers

4.3.1. Approve access requests for their staff and verify access aligns with duties.

4.3.2. Notify the IT Manager of role changes or employment terminations.

4.3.3. Participate in periodic access reviews.

4.4. **Employees and Contractors**

4.4.1. Must request access through proper channels and only use it for business purposes.

[…….]