Acceptable Use Policy (AUP) – External System Access & Use of Personal Devices

Contents

Version	date	Amendment	Author
1.0	02.12.2025	First publication	Praster Christian

1. Purpose and Scope

This policy defines the mandatory rules for all individuals accessing Tyrolit Group systems, applications, or portals from external locations. This includes:

- Employees using privately owned or non-company devices (Bring Your Own Device – BYOD)
- External service providers, partners, suppliers, freelancers, and other third parties granted access to company systems using non-Tyrolit Group devices.

The aim of this policy is to protect the confidentiality, integrity, and availability of Tyrolit Group data as well as the digital identity of all users.

2. General User Responsibilities

All users agree to the following:

- Treat all data accessible through the portal as confidential.
- Use information only as required for their assigned tasks.
- Do not copy, share, or use Tyrolit Group data for private purposes.
- Protect login credentials carefully and never share them with others.
- Immediately report incidents such as device loss, suspected account misuse, or other suspicious activities.
- Do not manipulate, or alter data without authorization.
- Do not attempt to bypass system boundaries, permissions, or security mechanisms and report situations where you believe that you have been able to.

3. Protection of Digital Identity (Identity Protection)

3.1 Importance of Identity Protection

Each user's digital identity is a critical security element and must be adequately safeguarded.

3.2 Handling of Credentials

- Passwords must never be shared with anyone, including colleagues, supervisors, or IT staff.
- Passwords must be strong, unique, and meet internal security requirements.
- Automatic password storage in browsers, apps, or non-approved password managers is not permitted.
- Credentials may only be stored in password solutions officially approved by Tyrolit Group.
- Users must properly log out after each session.

3.3 Multi-Factor Authentication (MFA)

- MFA is mandatory where technically available.
- Devices or tokens used for MFA must not be shared.
- Loss or compromise of an MFA device must be reported to IT immediately.

3.4 Protection Against Identity Theft & Social Engineering

- Unknown emails, links, or attachments must not be opened.
- Users must remain alert to phishing, smishing, vishing, or fake login pages.
- Sensitive identity-related information must not be shared via email, phone, or messaging tools.
- If in doubt contact informationsecurity@tycom.at for assistance in validating the legitimacy of information received.

3.5 Logging of Identity-Related Activities

- Login attempts and security-relevant activities may be logged for security, compliance and contractual purposes.

4. Requirements for Personal or External Devices (BYOD)

4.1 Basic Security Requirements

Devices used to access Tyrolit Group systems must comply with the following:

- Up-to-date operating system and regular security patches
- Active and updated anti-malware software
- Screen lock using PIN, password, or biometrics
- No insecure apps, jailbreaking, rooting, or modified operating systems

4.2 Network and Connection Rules

- Access is only allowed through secure networks.
- Public Wi-Fi may only be used if a secure connection (e.g., VPN) is enabled.
- Tools that attempt to bypass security controls are prohibited.

4.3 Separation of Private and Business Data

- Tyrolit Group data may only be processed within approved and secure applications.
- Private and business accounts, browser profiles, or apps must be used separately.
- Storing Tyrolit Group data in private cloud services is not permitted.

5. Requirements for use of the Tyrolit Group IT-Systems

- Only authorized software and applications may be used.
- Installing private software for handling Tyrolit Group data is not permitted.
- Company licenses may only be used for business purposes.
- Downloads from unknown or untrusted sources are not allowed.

6. Data Processing, Data Protection, and Compliance

- All users must comply with applicable data protection laws and internal regulations.
- Personal data may only be processed in accordance with legal requirements.
- Local storage of sensitive or confidential company data on private or external devices is strictly prohibited.
- Data may only be processed or stored within Tyrolit Group approved infrastructure.

7. Security Incidents and Reporting Obligations

Users agree to:

- Report security incidents or suspicious activity immediately.
- Not attempt their own repairs, bypasses, or interventions.
- Inform informationsecurity@tycom.at immediately in the event of identity misuse or unauthorized access.

8. Termination of Access and Revocation of Permissions

Upon termination of employment, cooperation, or in the event of a security risk:

- All access rights and accounts will be deactivated.
- The IT department must be informed proactively and in advance so that all accounts, accesses, and permissions can be safely and fully disabled.
- Accidently stored credentials (e.g., in password managers, apps, or browsers) must be removed.

9. Violations and Consequences

Violations of this policy may result in:

- Restriction or suspension of system access
- Disciplinary measures
- Termination of contractual relationships
- Claims for damages or legal action

10. Acceptance and Validity

By logging into the system, the user confirms that they have read, understood, and accepted this policy.
The obligation to maintain identity protection and confidentiality continues even after termination of employment or contractual relationships.

11. Contact

If you have any questions about this policy, please contact informationsecurity@tycom.at This guideline is regularly reviewed and updated as necessary.