TIVOLI GROUP
مجموعة تيفولي

OFFICIAL ANNOUNCEMENT

Policy Name: Software Installation Policy on Company Computers

Date: 01/07/2026
Effective date: 01/07/2026
Issued By: Human Resources Department

Purpose

The purpose of this memo is to establish a clear policy governing the installation of software on all company-owned computers, laptops, servers, and any devices connected to the company intranet. This policy aims to protect the company's IT infrastructure, ensure data security, maintain system stability, and comply with legal and licensing requirements.

Scope

This policy applies to:

1. All employees of Tivoli Group and temporary staff
2. All company-owned or company-managed computers and devices
3. Any software, applications, or system tools
4. Any installation that may affect PCs, operating systems, networks, servers, or the company intranet

Software Installation Approval Requirement

1. No software installation is permitted without prior written approval.
2. For any software installation, a formal request must be submitted to the Chief Human Resources Officer (CHRO) for approval before proceeding.
3. Approval must be obtained regardless of whether the software is free, paid, trial-based, open-source, or required for business operations.
4. Software installations requested by departments or individuals will only proceed after CHRO approval and coordination with the IT department.

TIVOLI GROUP
مجموعة تيفولي

Installation Process

The employee submits a software installation request to the CHRO, clearly stating:

1. Purpose of the software
2. Whether the software connects to external networks or systems

Upon approval by CHRO, the IT department will review the request for:

1. Compatibility
2. Security risks
3. Licensing compliance
4. Impact on existing systems and the intranet

Only the IT department is authorized to install approved software on company devices.

Prohibited Actions

The following actions are strictly prohibited:

1. Installing software without CHRO approval
2. Downloading or installing unauthorized applications, tools, or utilities
3. Installing software that interferes with system performance, security, or network stability
4. Modifying system settings, security configurations, or intranet-related components without authorization
5. Using personal software licenses on company devices

Accountability and Responsibility

Any employee installs or causes the installation of unauthorized software will be fully accountable for but not limited to

1. System failures
2. Data loss or breaches
3. Network disruptions
4. Intranet downtime
5. Legal, financial, or operational consequences

Will be subject to disciplinary action in accordance with company policies.

TIVOLI GROUP
مجموعة تيفولي

Security and Compliance

1. All software must comply with company cybersecurity standards and data protection policies.
2. Unauthorized software may expose the company to malware, ransomware, or data breaches and will be removed immediately by IT.
3. The company reserves the right to audit all systems and computers to ensure compliance with this policy.

Exceptions

1. Any exception to this policy must be approved in writing by the CHRO and CEO.
2. Emergency installations, if required, must still be documented and formally approved after execution.

Clarification,

Please contact the Human Resources Team.

Sincerely yours,

Anwar Ghaida
Chief Human Resources Officer