📄 Software Installation and Usage Policy

Document ID: POL-IT-2025-001
Effective Date: June 23, 2025
Last Updated: June 23, 2025
Owner: IT Security & Compliance Department
Applies To: All employees, contractors, and third-party users accessing company-owned devices or systems.

---

1. Purpose

This policy outlines the regulations and guidelines for installing and using software on all organization-owned or managed computing devices. Its objective is to maintain cybersecurity, ensure software compliance with licensing agreements, optimize system performance, and reduce risks to data and network integrity.

---

2. Scope

This policy applies to:

- All desktop computers, laptops, mobile devices, and virtual machines owned or managed by the organization.
- All employees, contractors, interns, consultants, and third-party partners.
- On-premises and remote work environments.

---

3. Definitions

- **Authorized Software**: Software pre-approved by the IT department or listed in the Authorized Software List.
- **Prohibited Software**: Any software explicitly disallowed due to security, licensing, ethical, or productivity reasons.

- **Shadow IT**: Use of unauthorized applications or services without IT knowledge or approval.

- **Installation**: The process of downloading, copying, or setting up software on a computing device.

---

4. General Principles

- All software installations must be approved by the IT department unless already pre-approved in the Authorized Software List.

- Employees are **not permitted** to install or use any software that has not undergone security, legal, and compatibility evaluation.

- Regular software audits will be performed to detect unauthorized software.

---

5. Authorized Software

Employees may install and use the following categories of software **with no additional approval** (assuming use aligns with business needs):

5.1 Productivity Software

- Microsoft Office Suite (Word, Excel, PowerPoint, Outlook)

- LibreOffice

- Google Workspace (Docs, Sheets, Slides) via browser

- Notepad++ / Sublime Text / Visual Studio Code

5.2 Collaboration & Communication Tools

- Microsoft Teams

- Slack (company-managed workspaces only)

- Zoom (enterprise version)

- Cisco Webex

5.3 Development Tools

- Git & GitHub Desktop
- Docker (with container approval)
- Visual Studio, Eclipse, IntelliJ IDEA (licensed versions)
- Postman
- Jupyter Notebook (local only)
- Python, Node.js, Java SDKs (as required per project)

5.4 Cybersecurity & Monitoring Tools

- VPN client (company-approved only)
- Antivirus (company-standard only)
- Endpoint Detection and Response (EDR) tools as configured by IT

---

6. Restricted Software Categories

The following categories of software are **prohibited** or **require specific justification and approval**:

6.1 Prohibited Software

These must never be installed under any circumstances:

- Torrenting applications (e.g., BitTorrent, uTorrent)
- Pirated or cracked software
- Remote access tools not provisioned by IT (e.g., TeamViewer, AnyDesk)
- Cryptocurrency mining applications

- Unauthorized password managers or browser extensions
- Dark web browsers (e.g., Tor Browser)
- Hacking tools or penetration testing frameworks (e.g., Metasploit, Kali Linux) unless on approved test environments

6.2 Requires IT Approval

- Open-source tools not listed in section 5 (e.g., GIMP, Inkscape, RStudio)
- AI or ML frameworks (e.g., TensorFlow, PyTorch) on local machines
- Simulation software or data visualization tools
- Software requiring admin privileges
- Third-party email clients
- Any software that involves storing or transmitting customer or employee data

---

7. Installation Process

7.1 Requesting New Software

1. Submit a Software Installation Request (SIR) through the IT Service Portal.
2. Include business justification, licensing info, and compatibility requirements.
3. The IT department will evaluate the software for:
    - Security vulnerabilities
    - License compliance
    - Performance impact
    - Data handling

7.2 Approval Timeline

- Standard software: 1–3 business days
- Specialized or sensitive software: Up to 10 business days
- Denials will include rationale and, where possible, alternative solutions

---

8. Licensing & Compliance

- Only properly licensed software may be installed.
- Employees must not attempt to bypass licensing restrictions or use personal licenses on company devices.
- Open-source software must comply with organizational open-source usage policy.
- The organization retains the right to uninstall any non-compliant software without notice.

---

9. Monitoring & Auditing

- Software usage and installation will be monitored continuously.
- Audits will be conducted quarterly.
- Violations will be logged, and users may be subject to disciplinary action, including removal of access or termination.

---

10. Roles and Responsibilities

Role	Responsibility
Employees	Request software approval, comply with this policy
IT Department	Review requests, maintain software inventory, monitor usage
Security Team	Evaluate software for vulnerabilities

Procurement	Ensure proper licensing and vendor vetting

11. Exceptions

Any deviations from this policy must be approved in writing by the Head of IT Security and logged in the Exception Register. Temporary exceptions may be granted for:

- Short-term projects
- Research and development environments
- Emergency situations

12. Enforcement

Non-compliance with this policy may lead to:

- Revocation of system access
- Mandatory retraining
- Disciplinary action, up to and including termination
- Legal liability in case of data breach or license violation

13. Related Policies

- Information Security Policy
- Data Protection Policy
- Acceptable Use Policy
- Open Source Software Policy
- Remote Work Policy

14. Revision History

Version	Date	Summary
1.0	2025-06-23	Initial release