

# **Prohibition of Patched or Cracked Software Usage**

## **1. Purpose**

This policy is established to ensure the **legal, ethical, and secure use of software and tools** across Antier Solutions. The use of **patched, cracked, pirated, or unauthorized versions** of any software/tool poses serious **legal, financial, reputational, and cybersecurity risks** to both the individual and the organization. This policy sets clear guidelines prohibiting the use of such software within the company infrastructure.

## **2. Scope**

This policy applies to:

* All full-time, part-time, contractual employees, freelancers, and interns
* All devices used to access or operate within the Antier network, including but not limited to:  
  + Company-issued laptops/desktops
  + BYOD (Bring Your Own Device) systems connected to company resources
  + Remote desktops, cloud environments, or third-party systems with access to company data

## **3. Policy Guidelines**

### **3.1 Prohibited Use**

* **Under no circumstances** should any employee install, use, or distribute **patched, cracked, or pirated versions** of any software, tools, plugins, libraries, IDEs, operating systems, or digital products on any device used for company work.
* This applies to both **licensed commercial software** and **free or freemium tools** where altered versions bypass security, authentication, or payment mechanisms.

### **3.2 Zero Liability from the Organization**

* If any **patched/cracked software** is found on an employee’s system, **Antier Solutions will not be responsible** for:  
  + Data loss, corruption, or breaches
  + Device failures or malware infiltration
  + Any legal action or penalties resulting from unauthorized software use
* All consequences—legal, financial, reputational—will rest solely on the **individual responsible**.

### **3.3 Disciplinary Consequences**

* Any violation of this policy may result in:  
  + Immediate **seizure and audit** of the concerned system by the IT team
  + Issuance of a **formal warning or notice**
  + **Temporary or permanent suspension** of system/network access
  + **Salary deduction or recovery of damages**, if applicable
  + **Termination of employment** for repeated or severe violations
  + Legal action, depending on the nature of the infraction and external consequences (e.g., client breach, licensing violation)

## **4. Reporting & Monitoring**

* The **IT and InfoSec teams** will conduct regular audits and system scans to monitor for unauthorized software.
* Employees are encouraged to report any suspicious software or unethical practices anonymously to **itsecurity@antiersolutions.com**.
* All software installations must be approved and performed **only by the IT department** or through authorized company channels.

## **5. Approved Software Policy**

* A list of **approved and licensed software** will be maintained and made accessible via the internal portal or IT Helpdesk.
* If a required tool is not listed, employees should raise a formal request with justification to **it@antiersolutions.com** or their reporting manager.
* The company will purchase, license, or provide safe alternatives where required for job performance.

## **6. BYOD & Remote Work Considerations**

* Employees using personal devices for remote work must also adhere to this policy.
* **No cracked or modified software** is permitted even if used solely for accessing company platforms (e.g., email, VPN, task boards).
* BYOD systems may be randomly audited or requested for compliance verification by the IT team.

## **7. Acknowledgment & Compliance**

* All employees are required to **digitally acknowledge** this policy during onboarding or policy rollout.
* Ignorance of the policy **will not be considered a valid excuse** in the event of a violation.

## **8. Policy Review**

This policy will be reviewed annually or earlier if required due to regulatory changes, technological advancements, or security incidents.

## **Contact for Clarification**

For any questions or clarification related to this policy, please contact:  
 📧 **ithelpdesk@antiersolutions.com**