Everest engineering

Software use policy

ISM.17

Version 0.2.3

July 1 2025

Contents

1 Software Use Policy

1.1 1. Purpose

The purpose of this policy is to outline the appropriate use of software, including SaaS (Software as a Service) and AI tools, at Everest Engineering. This policy aims to ensure legal compliance, protect company resources, and promote a productive and secure working environment.

It should be read in conjunction with the AI Code of Conduct.

1.2 Scope

This policy applies to all employees, contractors, and other individuals with access to company software, both within the company and while consulting at client businesses.

It covers all software used, including but not limited to:

- Proprietary software developed in-house
- Licensed commercial software
- Open-source software
- Cloud-based applications (SaaS)
- AI tools and applications

1.3 3. Acceptable Use

- **SaaS and Cloud Services**: Employees must use SaaS and cloud-based services in accordance with the company's guidelines and service agreements. Only approved SaaS applications should be used, and employees must follow any usage limits and data handling procedures specified by the service providers.
- **AI Tools**: Employees must use AI technology responsibly and ethically, avoiding any actions that could harm others, violate privacy, or facilitate malicious activities. Employees must actively work to identify and mitigate biases in AI systems, ensuring systems are fair, inclusive, and non-discriminatory. Employees should recognise the limitations of AI and always use their judgment when interpreting and acting on AI-generated recommendations. Employees are ultimately responsible for the outcomes generated by AI systems under their purview and must be prepared to explain and justify those outcomes to both internal and external stakeholders.
- **Software Use with Clients**: When consulting at client businesses, employees must familiarise themselves with the client's policies and procedures and use client-provided software or tools in accordance. Employees must be transparent in their use of any additional software, ensuring that clients, partners, and stakeholders are informed about the technology's involvement in relevant projects and decision-making processes. In cases where the client's policy and Everest Engineering's policy are misaligned, the stricter policy shall take precedence. If the two policies cannot be reconciled, the client's policy will take priority. However, if adherence to the client's policy would put Everest Engineering at risk, the employee must inform their direct manager, the CTO, and the security officer for further guidance and resolution.
- **Licence Compliance**: Employees must adhere to licensing agreements and terms of use associated with all software. Unauthorised use, duplication, or distribution of software is prohibited.
- **Compliance with Laws and Regulations:** Technology must be used in compliance with all applicable laws and regulations, including data protection, privacy, and intellectual property laws.
- **Software Updates**: Employees should ensure that all software, including SaaS applications and AI tools, is kept up-to-date with the latest patches and updates as recommended by the vendor or IT department.

1.4 Prohibited Use

- **Piracy and Illegal Copies**: The use of pirated software or illegal copies is strictly prohibited. This includes using cracked versions of software or bypassing licensing restrictions.
- **Malicious Software**: The installation or use of software that may harm Everest or its client's network or systems, such as malware, spyware, or adware, is forbidden.
- **Inappropriate AI Use**: The use of AI tools for unethical purposes, including but not limited to unauthorised data scraping, discriminatory practices, or invasion of privacy, is prohibited.

1.5 Security and Data Protection

- **Data Security**: Employees must ensure that software used on company devices and client systems does not compromise the security or integrity of company or client data. This includes using strong passwords and ensuring software access is restricted to authorised personnel.
- **Data Handling at Client Sites**: When working at client sites, employees must follow client-specific data protection protocols and ensure that sensitive data is handled in compliance with client agreements and applicable regulations. Such data must be anonymised or pseudonymised whenever possible and stored securely to protect client confidentiality and privacy. Employees should exercise caution when inputting sensitive data into tools and prioritise secure data transfer methods. Clients must be made aware if their data is going to be fed into any third party application (e.g. AI meeting transcribing tool) and given the option to opt-out.
- **Data Backup**: Employees are responsible for backing up critical data. Store data / documents in Everest-managed cloud systems, e.g. Google Drive, Docs, Sheets, rather than local copies to ensure data redundancy and reduce the chance of a data breach, e.g. lost laptop. Ensure similar practices are followed when working with client data if applicable and based on the tools provided by the client.

1.6 Software Management

- **Requests and Approvals**: Legal software required to complete your role may be installed provided it is from a reputable vendor and does not introduce a risk to Everest or Everest's clients.
- **Required Software**: Installed software provided by Everest, e.g. inventory management, virus scanner, should not be installed or switched off.
- **Inventory Management**: The IT department will maintain a Software & Tools Register of all software licences and ensure compliance with licensing terms. This includes managing software used on client projects, SaaS subscriptions, and AI tools.

1.7 Compliance and Enforcement

- **Monitoring**: Everest reserves the right to monitor software use to ensure compliance with this policy. This includes auditing software installations, licence usage, and adherence to guidelines for SaaS and AI tools.
- **Consequences**: Violations of this policy may result in disciplinary action, up to and including termination of employment. Legal actions may also be pursued for violations involving illegal software use, security breaches, or misuse of AI tools.