Global Information Technology Policy

Version: 1.0 Public

SCOPE

Camurus is dedicated to protecting the confidentiality, integrity and availability of Camurus information assets to support business-decisions and operations at all times.

This policy describes the high-level guiding principles to be followed when using information technology to conduct Camurus' business as well as information security principles.

ROLES AND RESPONSIBILITIES

The IT Director, reporting to the executive management team, is responsible for this policy and to ensure IT enables and supports Camurus with relevant IT tools and services.

The requirements stated in this policy and supporting standards must be followed by all users (employees, contractors, consultants, temporary workers and other workers and affiliates).

POLICY KEY PRINCIPLES

Responsible Use

Camurus IT resources must be used responsibly and only for business purposes. Individuals must contribute to a stable and secure IT environment by reporting incidents and suspicious use, sharing data only with known collaborators and being mindful when interacting with social media (posting, likes or tagging) as it may affect Camurus and its reputation. Systems and IT services must be used as intended.

Information Protection

All company data must be protected and only shared with its intended audience (the public, internal users or restricted to certain functions/persons). Information must only be shared when necessary and stored securely in approved systems.

Software and Licenses

Only approved and licensed software shall be installed on company devices. Unauthorized or pirated software is strictly prohibited. Camurus reserves the right to remove any software or applications that pose a security risk.

Security

To maintain security, only devices provided by Camurus may connect to the internal network and individuals must keep track of and secure company devices for which they are responsible. Lost devices or suspected security incidents must be reported immediately. Remote work must be conducted through secure, company-approved VPN connections. Continuous online security awareness training courses are performed by employees.

The IT risk assessment is reviewed yearly to monitor potential security risks and the need for mitigation strategies.

Access Control

Access to systems must follow the principle of least privilege. Multi-factor authentication must be used where supported, and passwords must be strong, confidential, and never shared. Any suspicion of compromised passwords must be reported to IT immediately.

Data Privacy

Personal data must be handled in compliance with data protection laws such as GDPR (Privacy notice). Sensitive data must be encrypted both at rest and in transit. Third-party email or storage services must not be used for company business.

Artificial Intelligence (AI)

When using artificial intelligence tools, individuals must act responsibly and securely. Confidential information must never be shared with unapproved AI tools. AI-generated content must meet Camurus standards and legal requirements.