camurus®

IT Policy on data use, storage, and loss of prevention

Effective: 12 January, 2023
Version: 1.0

SCOPE

The Scope of this policy is to:

- Employees, contractors, consultants, temporaries, and other workers (“USER” or “USERS”) who have access to Camurus´s data.

OVERVIEW

Camurus creates, gathers and manages data. This data is used in communication, collaboration and the maintenance and development of Camurus and its products. To protect Camurus and all its interests, all data must be kept safe and secure.

ROLES AND RESPONSIBILITIES

Role	Responsibility and Obligations
IT Manager	• Ensure a policy defining Camurus requirements data usage, data storage and data loss prevention is established
All Employees	• Follow and to respect this Company Policy

POLICY

This policy ensures that all Camurus´s data is secured from intrusion, improper distribution and deletion. Inappropriate use exposes Camurus to risks including virus attacks, compromise of network systems and services, improper dissemination of company information and data, and legal issues.

Data and user classification

Camurus creates, gathers and manages data which is divided into 5 different user classes.

- Public
- Private
- Corporate
- Confidential
- Restricted

Public information

Released to the public (e.g. press releases, public presentations, posted on webpage etc.)

Private information

Private data that may in some cases be located on a Camurus device.

Corporate information

Accessible for all “USERS”.

Confidential information

Restricted to certain line functions, projects or other groups within Camurus. Camurus acknowledges that all “USERS” will have access to Confidential data at some time, whether it is stored electronically or printed, or even spread verbally. Confidential data is only confidential to the public but should not be widely spread within Camurus.

Restricted information

Only accessible for a few users and prohibited to read or try to access. Files containing restricted data should be mark with labels “Restricted”. Example of restricted data is:

- Board materials
- Financial data
- Human resources data
- Business development data
- Agreements

Access restriction

Data require varying degrees of protection against being inappropriately disclosed, with “Restricted” data being the most protected and “Public” the least.

The right to access, save new information, and to process and change already existing data, is governed by eligibility level as outlined in the table below.

Data/user class	Authentication for access	Access provisioning	Audit log	Encryption
Public	Not required	Automatically	None	None
Private	Two-factor authentication	Automatically	Logging, monitoring	None
Corporate	Two-factor authentication	IT department	Logging, monitoring	Optional
Confidential	Two-factor authentication	IT department	Logging, monitoring	Optional
Restricted	Two-factor authentication	IT department	Logging, monitoring	Required

Encryption

Data classified with protection level higher than “Private” but lower than “Restricted”, must have option to be encrypted. Encryption should be made so that only intended users can gain access to the data whether located on servers, sent by email or located on other storage devices.

Data stored in SharePoint and OneDrive is always encrypted, if possible always create and send links to data stored in SharePoint and OneDrive instead of email or USB storage.

Data classified with protection level “Restricted” must be encrypted as above.

External devices

The main rule is that external devices (USB drive, USB hard drive etc.) are not to be used to store Camurus data unless classified as “Public” or “Private”.

In some cases, external devices that are Camurus approved, can be used for storage of “Corporate” or “Confidential” data. Users may never leave such device unattended.

Camurus approved devices can be found received from Camurus IT department.

Unless it cannot be avoided, it is in rare and extreme cases allowed to store “Restricted” data on external device. If such devices, and the data on it, is lost, this must be reported to line manager and IT department as soon as possible.

Privacy filters

When working in a public environment or when using public transportation, a privacy filter should be used to protect the information revealed on the screen. Always assume that people can see what you are working on, and you should therefore take necessary measures to avoid any disclosure of Camurus data.

Data loss prevention

For data stored on your computer desktop or on local computer drives no backup is done.

To prevent loss of data, all data must be stored on SharePoint or OneDrive

POLICY COMPLIANCE

Compliance Measurement

The IT department will verify compliance to this policy through automatic monitoring systems.

Exceptions

Any exception to the policy must be approved by the immediate line manager and IT department in advance.

Non-Compliance

Non-compliance is automatically monitored by IT systems and reported to IT manager. Users are informed if mistakes have been made in compliance to this policy.

Confirmed misconduct could result in disciplinary action up to and including termination of employment.