# Acceptable use policy for IT in VELUX – External Users (public version).

## Contents

## 1. Document Information

| | |
|---|---|
| Document Title: | Acceptable use policy for IT in VELUX – external users |
| Type: | Policy |
| Effective Date: | 11-06-2025 |

## 2. Tracking and Approval

Not applicable in this version

## 3. Purpose

The purpose of this "Acceptable use policy for IT in VELUX – External Users" (hereinafter "Policy") is to define the requirements and responsibilities and thereby ensure proper use of IT in the VELUX Group by external users who have been granted access to VELUX IT systems, networks or data. (hereinafter "VELUX IT")

The Policy is intended to protect IT systems, employees, partners etc. in the VELUX Group from illegal or damaging actions by individuals, either knowingly or unknowingly.

Inappropriate/Incorrect use can potentially expose the VELUX Group to virus/malware attacks and compromise networks, systems and services. This can lead to direct financial losses and/or affect the VELUX reputation and relations to stakeholders in a negative way.

## 4. Scope

This policy applies to all external individuals or organisations who are not employees of VELUX such as contractors, consultants and others that have access to any VELUX IT System, application and/or network on premises, externally in the cloud, in administration, manufacturing or otherwise. (referred to as "External Users").

## 5. Policy

### 5.1. General use

a) All external users are responsible for exercising good judgement regarding appropriate use of information, IT Systems and network resources and are responsible for abiding by any other VELUX policies and standards which are part of the work order. In case of any uncertainty, external users should consult their manager or the VELUX employee responsible for the work that is being performed.

b) External users are required to complete security awareness training upon request by the VELUX Information Security team.

c) The access provided to VELUX IT is strictly personal and must not be used for any other- or private purposes.

d) VELUX company proprietary information stored on/in IT Systems and network resources remains the sole property of the respective VELUX legal entities. Each external user must

ensure, through legal or technical means, that proprietary information is protected in accordance with the VELUX Group and local VELUX company policies and procedures.

e) The external user has a responsibility to promptly report the theft, loss or unauthorized access disclosure of personal data about employees and customers and of all VELUX owned information.

f) Each external user may access, use or share personal data about employees, customers, partners etc. and all VELUX proprietary information, only to the extent it is authorized and necessary to fulfill the assigned job duties.

g) The external user has a responsibility to ensure, that confidential data, including personal data about employees, customers, partners etc. or all VELUX owned information (in paper or removable storage media format) is locked away when the external user is not able to monitor it.

h) If leaving a computer or a network resource unattended, the external user is required to lock it to ensure that unauthorized access cannot take place.

i) It is not allowed to have local administrator access to your VELUX laptop. If the need for administrator access occur, please contact helpdesk or local IT support.

j) Do not leave VELUX owned laptops or mobile devices in unsecure places, e.g. in a car or unattended at a training/conference center or similar. If it is absolutely necessary to leave it in a car, the car must be locked, and the laptop/mobile device must be stored in the boot of the car and not be visible from the outside.

k) Do not leave VELUX owned laptop or mobile device on your desk in the office at night. Either take it with you or make sure it is locked away.

l) Be extra careful when traveling (airports, airplanes, trains, busses, etc.). Keep the VELUX laptop with you at all times and only leave it with trusted parties. When using the VELUX laptop in public, it is recommended to use a privacy filter to avoid VELUX data to be visible.

m) Consider data sensitivity when having meetings at your desk or in public areas.

n) If the external user in any way is processing or storing information in the form of files, documents, e-mails etc., identified as a VELUX business record and containing personal data, this information must only be retained as long as the external user is in a working relationship with VELUX and there is a legitimate and ongoing business reason.

o) All activities conducted using VELUX IT Systems and network resources will be considered VELUX activities. Consequently, other VELUX employees can be granted access to the external user's e-mails, documents, IT Systems and network resources used by the external user.

p) If external users are processing or storing any kind of VELUX information, the external user must be informed about the categorization (classification) of the information. It is a management responsibility in the department employing or giving the external user access to VELUX information, to provide this classification information to the external user. This includes providing information on local procedures for handling personal data and access restrictions to information e.g. confidential information. Confidential and strictly confidential information must only be passed on with the acceptance of the information owner.

q) Except for VELUX owned information labelled as 'Public', information must not be published on social media accessible to anyone outside the VELUX Group.

r) Information must only be shared, published in e-mails or on social media when the receivers or members of the group have the right to/are cleared to access the information. E.g. confidential information must not be posted into public groups.

s) External users must only access AI platforms using a non-VELUX email address.

t) External users must only share generic non-VELUX information with AI platforms and must respect relevant privacy regulations

## 5.2. Unacceptable use

a) Use of any IT System or network resources for soliciting money or for advocating a religious or political cause is strictly forbidden.

b) To access, download or transmit any indecent, obscene, pornographic, racist, defamatory or other inappropriate material as well as the circulation by e-mail or other media of such material is an offence. Activity of this nature has potential criminal liabilities and relevant authorities will be informed where appropriate.

c) External users must not represent personal opinions in the name of VELUX through any electronic media and/or system.

d) External users must ensure that software, files or any other documentation are not copied or retransmitted in breach of copyright or intellectual property rights.

e) External users must not communicate personal data about employees, customers, partners etc. to external parties e.g. on public social media or in e-mails to externals.

f) If the external user has access to VELUX Group internal social media and e-mails, then this information must not be shared outside the VELUX Group.

g) If the external user has a VELUX e-mail address, this must not be used for creating profiles on social media like Facebook, Twitter, LinkedIn or other similar services, unless this has been approved by a relevant VELUX contact person.

h) External users must never forward VELUX e-mails to a third-party e-mail system unless this has been approved by a relevant VELUX contact person and VELUX IT&DE Information Security.

i) It is not allowed to use third-party e-mail systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct VELUX business, to create or memorialize any binding transactions, or to store or retain e-mail on behalf of VELUX. Such communications and transactions must only be conducted through channels approved by VELUX.

j) If the external user is using a VELUX Microsoft 365 account, it is not allowed to access OneDrive for Business, SharePoint and other systems from public and private computers.

k) It is unacceptable to use the VELUX email address for AI services as well as sharing VELUX information and/or personal identifiable information that would be in noncompliance with the guidelines stated in "VELUX Group Data Privacy Policy".

## 6. Update of Policy

The latest version of this Policy is available on VELUX One. The External User is responsible for using the latest version of this policy. Policy is reviewed at least annually.

## 7. Compliance, monitoring and auditing

An external user obtaining access to/using VELUX IT System and network resources accepts and acts in accordance with this policy. It is a management responsibility that any external User is aware of this policy.

For compliance, security and network maintenance purposes, authorized individuals within VELUX companies and trusted third parties may monitor IT Systems and network traffic at any time. This means, that all communication created, received or sent via VELUX IT equipment and network resources for any purpose might be subject to interception and review.

All user activity on VELUX IT may be logged and monitored. External users must not attempt to disable or circumvent logging mechanisms. VELUX reserves the right to audit any external user activity related to VELUX IT.

Moreover, the VELUX Group reserves the right to measure performance of IT Systems and the information processed or stored within all companies in the VELUX Group with the sole purpose of optimizing utilization. Access to personal data generated by performance management tools is restricted to authorized employees and according to a predefined process.

VELUX IT&DE Information Security will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits.

## 8. Termination

Access credentials must be returned or securely destroyed at the end of the engagement.IT must ensure all accounts and accesses are deactivated upon termination of the agreement

## 9. Exceptions

Inability to adhere to the policy must be reported to local management responsible for employing the external user and to VELUX IT&DE Information security. This can be done directly or via reporting to the department or company IT Security Coordinator.

Any exception to the policy must be approved in advance by providing relevant information to VELUX IT&DE Information Security who will clarify if an exception can be approved.

## 10. Non-Compliance

Any violation of this policy will be treated seriously and may lead to immediate termination of access, legal action and/or contract termination and liability for damages caused.