# Information security policy for third parties

Replacement for: -

| | | Name | Department | Date |
|---|---|---|---|---|
| melecs | Created /changed | Thomas P. | QMS | 2024-06-07 |
| | Checked | Hermann L. | PI | 2024-06-07 |
| | Released | Erich L. | SVP OP | 2024-06-18 |

**Table of contents**

# 1 Objective

This policy sets out the organisational requirements and rules on information security to be observed by third parties when handling information from Melecs EWS GmbH locations in Austria, hereinafter referred to as MELECS, must be observed.

The terms information and data in this document refer exclusively to information and data of MELECS. Third parties are defined as contractual partners who, on the basis of contractual relationships, supply products/services with an impact on information security for MELECS.

This policy does not apply to customers of MELECS.

This policy is addressed to the management of third parties. The third party's management must ensure that its employees and agents who process MELECS information are bound by this Information Security Policy.

This document addresses the security requirements to three target groups. The following table shows which target group is addressed by which Section.

| Section | Target group |
|---|---|
| 4 | All information security third parties |
| 5 | Third parties who work in MELECS IT infrastructure |
| 6 | Third parties who have access to or provide MELECS information outside the MELECS IT infrastructure |

Depending on the collaboration model, a third party can belong to several target groups at the same time.

# 2 Scope of application

This policy applies to all Austrian MELECS sites.

# 3 General safety regulations for all third parties

## 3.1 Classification of information

The aim of classification is to categorise the information into levels according to its protection requirements. Depending on the classification, different protection measures are required.

All MELECS information must be classified according to its confidentiality. The confidentiality classifications may change at certain milestones.

If documents or information are created by third parties for MELECS, the confidentiality classification must be requested from the MELECS contact person and labelled accordingly.

## 3.2 Further requirements

- Information security incidents (e.g., malfunctions, breaches of the policy, cyber-attacks) that affect the client's information or IT systems must be reported immediately to informationsecurity@melecs.com or the Melecs contact person with the information required to assess the criticality. Further information on the incident must be made available to the client on request.

- If an attack using malware is suspected or detected, the affected IT devices and storage media may no longer be used to process MELECS information.
- Suspected vulnerabilities and weaknesses in MELECS' IT systems must be reported immediately to informationsecurity@melecs.com.
- In the event of suspected loss of internal, confidential or secret information of the Client, this must be reported immediately to the contact person at MELECS.
- The disclosure of data or information to other third parties is only permitted with the written authorisation of the owner of the information.
- Documents and storage media containing MELECS information worthy of protection must be protected against loss, destruction, confusion and unauthorised access. As soon as the data on the storage medium is no longer required, it must be securely deleted. Storage media that are no longer required must be physically destroyed.
- IT devices not managed by MELECS must be secured in accordance with the state of the technology. The error-free processing of information and protection against unauthorised changes must be ensured.
- For all conversations and data transmissions (including telephone conversations, video and web conferences) that concern or contain confidential or strictly confidential information of MELECS, it must be ensured that these cannot be intercepted or read without authorisation.
- In particular, no public (in terms of confidentiality "insecure") Internet translation services (including those using AI methods) may be used for translations of documents containing confidential or strictly confidential information of MELECS. Approval by the client in advance is required.

# 4 Additional requirements for third parties

The following is a list of additional requirements for third parties working in the MELECS infrastructure.

## 4.1 Definition

A third party may only work in the Melecs infrastructure if:

- IT devices (physical or virtual end devices) are provided by MELECS, or
- the connection is made via remote access solutions with access to the internal MELECS network, or
- the connection of the third party is made directly to the internal MELECS network or
- access-protected applications provided by MELECS via the Internet are used.

This applies regardless of whether the third party is located at a MELECS site.

## 4.2 Requirements

- When taking IT devices that are not supervised by MELECS onto the company premises or into security areas, it must be noted that these IT devices may not be brought into the MELECS network (with the exception of the guest WLAN). Exceptions are regulated as described in Section *4.5 Use of MELECS network services*.
- IT equipment provided by MELECS-IT must be handled properly and protected against loss or unauthorised modification.
- IT equipment provided by MELECS may only be removed from MELECS's premises with MELECS's authorisation.
- The provision or installation of hardware and software may only be carried out or arranged by MELECS-IT.
- Only the hardware, software and storage media provided by MELECS may be used.
- Opening the IT device provided by MELECS and making changes to the hardware (e.g., installing/removing components) and changing security settings (e.g., in the web browser) is only permitted for MELECS-IT. The removal of usage restrictions (e.g., "jailbreaking" or "operating system rooting") is not permitted.
- The use or subsequent modification of programmes is only permitted with the approval of MELECS-IT.
- Only MELECS data may be processed on the IT devices provided by MELECS.
- Every third party is responsible for ensuring that information, programmes and IT devices are only used and utilised properly within the scope of the respective task.
- The sending of non-official information is not permitted.
- The use of private software and data on the IT devices provided by MELECS is not permitted.
- Hardware (e.g., laptop, USB sticks, USB hard drives) and software that is no longer required must be returned immediately, but no later than at the end of the contract.
- Repairs to IT equipment provided by MELECS may only be arranged by MELECS.
- The loss of hardware provided by MELECS must be reported immediately by the respective user to the responsible contact person and at informationsecurity@melecs.com without delay.

- IT devices and data carriers on which personal, confidential or strictly confidential data are stored may only leave MELECS sites in encrypted form.

## 4.3 Handling of classified information

Information may only be made accessible to an authorised group of people within the scope of the agreed activities and in compliance with the relevant regulations. The need-to-know principle must be observed.

To protect internal, confidential or strictly confidential information, the relevant IT devices must be set up in such a way that access by unauthorised persons is prevented and the risk of unauthorised persons gaining access is minimised.

Information must be protected from unauthorised access throughout its entire life cycle in accordance with its current confidentiality classification. The following rules apply:

| Confidentiality level | Requirement |
|---|---|
| **OFFEN / OPEN** | • No labelling requirement - can be labelled as OPEN<br>• Reproduction and disclosure: no restrictions<br>• Storage: no restrictions<br>• Destruction: no restrictions |
| **INTERN / INTERNAL** | • No labelling requirement – can be labelled as INTERNAL<br>• Reproduction and disclosure: only to authorised third parties within the scope of the activity or area of application.<br>• Storage: protection against unauthorised access.<br>• Destruction: in accordance with ISO/IEC 21964, protection class 2 (paper: particle size max. 160mm², hardware: multiple fragmented and deformed particle size max. 2000mm²) |
| **VERTRAULICH / CONFIDENTIAL** | • Indication of the confidentiality level VERTRAULICH or CONFIDENTIAL on the first page of the document.<br>• Reproduction and disclosure: only to a limited group of authorised third parties within the scope of the activity and scope of application AND with the prior approval of the information owner by Melecs. The person distributing the information is responsible for appropriate distribution channels to protect the information and data from unauthorised access and/or eavesdropping.<br>• Storage: protection against unauthorised access. Access only for a restricted group. Encrypted external storage media.<br>• Destruction: in accordance with ISO/IEC 21964, protection class 2 (paper: particle size max. 160mm², hardware: multiple fragmented and deformed particle size max. 2000mm²).<br>• Transport/transfer: Confidential documents must be sent in sealed, neutral envelopes. E-mails only using TLS encryption. |
| **STRENG VERTRAULICH / STRICTLY CONFIDENTIAL** | • Indication of the confidentiality level STRENG VERTRAULICH or STRICTLY CONFIDENTIAL on each page of the document.<br>• Reproduction and disclosure: only to a very restricted group of authorised third parties (e.g., name list) within the scope of the activity and scope of application AND with the prior approval of the information owner by Melecs. All data must be encrypted. Depending on the application, further technical or organisational security measures must be used (e.g., prohibition of forwarding and printing). only to a very restricted group of authorised third parties (e.g., name list) within the scope of the activity and scope of application AND with the prior approval of the information owner by Melecs. |

| | |
|---|---|
| 🟥 | • Storage: protection against unauthorised access. Access only for a very restricted group (e.g., closed user group). All data is stored in encrypted form. Access only for a very restricted group (e.g., closed user group).<br>• Destruction: in accordance with ISO/IEC 21964, protection class 2 (paper: particle size max. 160mm², hardware: multiple fragmented and deformed particle size max. 2000mm²).<br>• Transport/transfer: Strictly confidential documents must be sent in sealed, neutral outer envelopes. A second inner envelope must be placed in these, which is labelled and protected with the classification "STRICTLY CONFIDENTIAL". Emails only using TLS encryption. Files only encrypted via Melecs Cloud or encrypted PDF and password forwarding via SMS. |

The requirements for handling information also apply to IT systems.

## 4.4 Handling of user accounts

User accounts and passwords are the most important protection against unauthorised network access and unauthorised use of applications and information.

The following guidelines for handling user accounts and passwords must be followed by all users:

- User accounts or access authorisations that are no longer required must be reported immediately to the responsible contact person so that they can be deleted or blocked.
- Passing on authentication tools (e.g., authenticator apps) is not permitted.

It is very important that secure passwords are used and that password confidentiality is maintained. The following points must be observed:

- minimum length 12 characters
- For user accounts with extended rights, the minimum length should be increased to 15 characters.
- Complex passwords consist of at least 3 of the following 4 criteria:
    - combination of capital letters (A-Z)
    - lowercase letters (a-z)
    - numbers (0-9)
    - special characters (#,!,&, etc.)
- change every 360 days
- the last 10 passwords must not be used
- the user can only change a password the next day
- after 10 failed attempts to enter a password, the domain account will be blocked for 30 minutes
- the password must not contain the account name or parts of the user's full name.

**Important information:**

- Change the initial password immediately.
- The passwords must be chosen in such a way that they cannot be easily guessed by third parties. First names, surnames, birthdays and names of relatives are not suitable for password selection. The same applies to trivial passwords with combinations of numbers (e.g., Melecs123456!).
- Passwords should not correspond to trivial keyboard combinations, such as "Qwertzui12§" on German keyboards.
- Each user must only use their personalised access data. The use of group accounts is generally not intended; unconditional exceptions must be authorised by internal processes.

- Under no circumstances may users pass on individual passwords to other users, administrators, superiors or outsiders.
- When entering passwords, you must ensure that the entry cannot be observed by other persons.
- Under no circumstances should passwords be entered on untrusted systems or at an unexpected command line.
- Passwords must not be saved, stored or transmitted unencrypted in plain text.
- The storage of company passwords/access data in other password memories (e.g., browsers for auto-completion) is not permitted.
- Always clearly separate private and business use and always use different passwords for different user accounts.
- Passwords for service accounts (i.e., accounts for machine-to-machine communication (M2M)) must have a minimum length of 32 characters, be complex (upper case letters, lower case letters, numbers and special characters), be generated with a secure random generator and be configured in such a way that active login by the user is not possible with them.

### 4.5 Use of MELECS network services

Only MELECS IT devices may be connected to the network. (Exception guests WLAN)

The connection of network-compatible IT devices not managed by MELECS to the MELECS network is only permitted if this procedure has been explicitly authorised by the Client for the IT device in question. Prior to this, the third party must ensure that the IT device to be introduced is secured in accordance with the state of the art. Exceptions must be checked in advance by MELECS IT Security and authorised by the CIO or his representative.

### 4.6 Additional requirements for mobile work

The employees of the third party are responsible for ensuring that the relevant regulations on information security and data protection are fully complied with during mobile working. Work documents, data and information must not be visible or accessible to unauthorised persons either in public places or in private rooms, nor must it be possible to eavesdrop on them.

The connection of hardware (e.g., mouse, keyboard, USB sticks) to the hardware provided by MELECS is only permitted if it has been provided by MELECS.

Image output devices (e.g., monitors, projectors) that are not provided by MELECS may be used if the connection is wired and no wireless transmission is used.

IT equipment provided by MELECS must be physically protected against theft and misuse:

- If an IT device is left unattended in a vehicle, this must be done in such a way that it is not visible from the outside.
- When travelling by air or rail, IT devices must be transported in hand luggage.
- If an IT device is left unattended for a longer period of time, it must be switched off.

## 5 Additional requirements for third parties

Additional requirements for third parties who have access to or provide MELECS information outside MELECS IT infrastructure.

A third party has access to MELECS information outside MELECS IT infrastructure if it processes MELECS information in its own IT infrastructure or hosts it for MELECS or other third parties on behalf of MELECS.

### 5.1 Requirements

Unless otherwise contractually agreed, the third party's information security regulations shall apply. The information on information security collected during the supplier selection process and the agreements made can be checked by the client.

## 6 Sanctions

Violations of this policy will be examined on a case-by-case basis in accordance with the applicable legal and contractual provisions and penalised accordingly.

Deviations from this policy that affect the level of security are only permitted after consultation with the contact person and approval by the CIO or their representative and must always be limited in time.