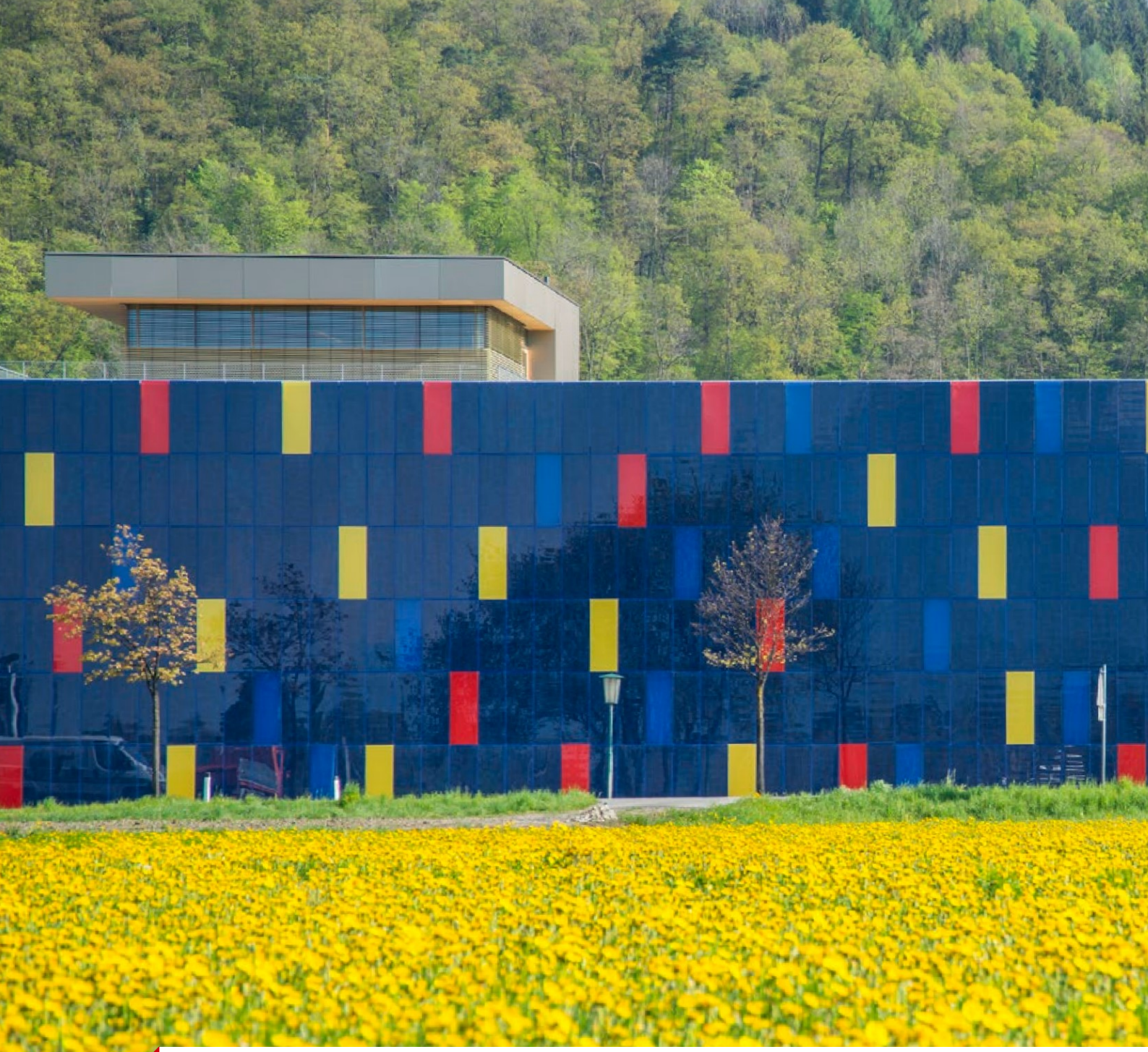

OMICRON

Information Security Guideline for Third Parties

Date: 2025-04-10 | **Status**: Released | **Classification**: C0 - Public

1 Introduction

The implementation of information security requirements is a benefit to all parties involved since it can improve and protect our reputation as trusted partners, boost operational efficiency and be a competitive advantage. For OMICRON, the awareness and engagement of external partners in maintaining their own suitable information security standards is essential for building and maintaining a trusted supplier relationship which contributes to the consequent provision of secure products and services by OMICRON, as well as protection of sensitive information.

The OMICRON Information Security Guideline for Third Parties outlines the Information Security requirements applicable to OMICRON's suppliers, external service providers (e.g., technical support, development cooperations) and other external partners who contribute to OMICRON's provision of products and rendering of services (altogether referred to as "Third Parties").

The security requirements outlined herein are applicable to Third Parties who:

- access, receive, process, or store information – including both personal and non-personal data – of OMICRON, their customers or business partners, as well as their employees;
- have access to OMICRON's corporate information systems, or
- provide certain services/products which are intended to be included in OT/Manufacturing services, as described below.

The following security requirements are designed to vary based on the level of risk the Third Party presents to OMICRON, depending on the type of OMICRON information the Third Party processes, network connection, and products and services provided by the Third Party, as well as data availability and resiliency requirements.

OMICRON reserves the right to update this document from time to time. The most recent version is accessible at https://www.omicronenergy.com/legal/.

2 General Requirements for Third Parties

The following general requirements must be implemented by **all Third Parties**:

- All Third Parties shall implement appropriate **technical and organizational information security measures** to ensure the confidentiality, integrity and availability of Third Party services. Good industry practices as defined by the requirements of ISO/IEC 27001 in its current version should apply as a reference value.
- All Third Parties are obliged to **ensure the protection of OMICRON information**, including non-public information of OMICRON's customers, business partners, and employees where access to such information has been directly or indirectly established during the business relation with OMICRON. "*OMICRON information*" includes any documents and records related to commercial and legal matters, trade secrets, technical knowledge and personally identifiable information, as well as other information designated as "confidential" or "strictly confidential" or otherwise recognizable as confidential based on its content; regardless of whether such information is in electronic, written or oral form.
- All Third Parties shall comply with any other **privacy or security policies or procedures** that OMICRON may provide or make available from time to time as the context and cooperation requires.
- If Third Parties involve additional parties in support of their services for OMICRON (e.g., sub-suppliers, processors), Third Parties must ensure that such **additional parties adhere to the same or similar Information Security standards** as described in this document. Upon request, Third Parties will disclose the name of such additional Third Parties to OMICRON and reasonably support with the verification of the implementation of the said standards.
- Regulations and instructions of the respective OMICRON group company on bringing **IT devices** that do not belong to OMICRON **on premises or into security areas of OMICRON** must be observed.
- All Third Parties must **report** the following events to OMICRON immediately upon discovery, ideally within 24 hours (see 7. Contact):
  - Information security incidents (e.g., vulnerabilities, violations of the information security regulations) concerning information, data or systems of OMICRON;
  - any suspected vulnerabilities and weak points concerning IT systems of OMICRON; and
  - any suspected loss or unauthorized disclosure of OMICRON information.

3 Special Requirements when Accessing OMICRON Infrastructure

3.1 Definition

A Third Party is accessing OMICRON infrastructure if:

- “Clients” (i.e. physical or virtual endpoint devices) are provided by OMICRON or its affiliated companies; or
- access to resources within OMICRON’s cloud environment (e.g., Microsoft M365 and Entra ID) are provided; or
- access to resources within OMICRON’s internal network are provided using remote access solutions (e.g., Citrix), or
- the Third Party has been connected directly to the internal OMICRON network (e.g., VPN connection).

These Third Parties may be located on the premises of OMICRON and its affiliated companies, or on the Third Parties’ premises.

3.2 Special Requirements

The following requirements must be observed by Third Parties who meet one or several criteria as defined in Section 3.1 above in addition to the general requirements stipulated in Section 2 of this Guideline:

- Clients provided by OMICRON must be handled correctly and protected from loss or unauthorized modification. The manufacturer's instructions for protection of the devices must be complied with.
- Clients provided by OMICRON (e.g., laptops, cellular phones) may only be taken outside OMICRON premises after approval.
- For Clients provided by OMICRON, Third Parties must only request or initiate procurement and installation of hardware and software via the OMICRON Service Desk.
- For Clients provided by OMICRON, only the OMICRON Service Desk is permitted to open the IT device, make changes to the hardware (e.g., installation/removal of hard drives and memory modules), and make manual changes to security settings (e.g., browser settings).
- Usage or subsequent modification of programs is only permissible with authorization of the OMICRON Service Desk.
- Usage of hard- and software provided by OMICRON is subject to internal regulations of OMICRON (e.g., OMICRON IT and Cybersecurity End User Policy).
- Data of any other customer that does not belong to OMICRON must not be processed on the provided IT devices.
- The use of Clients provided by OMICRON and OMICRON Information by the Third Party is only allowed for the fulfilment of and in accordance with the terms of the contract between the Third Party and OMICRON. Any exception requires the explicit consent of OMICRON. OMICRON is entitled to prohibit access/use at any time (e.g., in cases of misuse).

4 Other Special Requirements

Additional Information Security requirements may apply for **external software development partners** of OMICRON. If Third Parties are engaged in software development, they shall approach OMICRON to clarify such requirements.

5 Exceptions and Deviations

This Guideline must be observed by all Third Parties as defined in the scope of this document.

Deviations from this Guideline that reduce the intended security level are only allowed temporarily and after consultation with the OMICRON Information Security Team.

6 Enforcement

OMICRON strongly encourages Third Parties to adhere to this Guideline to foster a secure and trustworthy partnership.

OMICRON reserves the right to request written evidence on compliance with this Guideline, and to conduct on-site reviews to verify implemented measures.

In case of suspected or confirmed non-compliance with the standards stipulated in this Guideline by Third Parties, OMICRON may, in its sole discretion, decide to restrict access by such Third Parties and request immediate return or destruction of provided IT devices and information without any obligation towards the affected Third Party. In addition, OMICRON is entitled to terminate the agreements with the affected Third Party for cause. OMICRON further reserves the right to pursue legal action and demand full indemnification for any claims, fines and other negative consequences resulting out of the Third Parties' non-compliance with this Guideline.

7 Contact

Please find the points of contact related to Information Security, Product Security and Data Protection below.

Name	Purpose
OMICRON Information Security Team information.security@omicronenergy.com	Reporting of security incidents related to OMICRON's IT infrastructure and general inquiries regarding information security management at OMICRON.
OMICRON Product Security Team product.security@omicronenergy.com	Reporting of product security vulnerabilities and inquires related to the security of products and services of OMICRON.
OMICRON Data Protection Team data.protection@omicronenergy.com	Reporting of data breaches and inquiries related to the protection of personal data at OMICRON.

History

Version	Description	Date
1.0	Initial version	2024-08-27
1.1	Update of the contact details	2025-04-10

OMICRON electronics GmbH | Oberes Ried 1 | 6833 Klaus | Österreich
UID-Nr. ATU36297501 | Registration number FN34227i
+43 59495 0 | info@omicronenergy.com | www.omicronenergy.com