

" SECURITY ZONES - CODE OF CONDUCT"

1. Controller

Company	Austria Druckguss GmbH & Co KG
Address	Industriestraße 34, 8200 Gleisdorf
E-mail	info@austriadruckguss.com
Validity period	Unlimited
Revision Interval	3 years or in case of occasion
Confidentiality level	public

Gender Disclaimer

In order to ensure easier readability of the text, the explicit gender-specific spelling has been omitted in this guideline. For this purpose, the (usually shorter) masculine spelling was used as a simplification for both gender forms, so that these are to be understood as gender-neutral formulations.

2. Purpose and scope

This policy defines the binding rules for access to the company's designated security zones and is binding on all employees, external service providers and visitors.

It serves to protect information, IT systems and the company infrastructure in accordance with internal information security guidelines and the requirements of TISAX.

3. Classification of security zones

Security Zone 1 – Public Area (Green)

(e.g. reception, visitor area)

- Visitors are allowed to enter.
- No access to internal IT systems or confidential documents.
- Confidential information may not be discussed in this area.
- The clean desk policy must be adhered to at all times.

1. Safety Zone 2 – Controlled Area (Yellow)

(e.g. offices, internal workspaces)

- Access only for authorized employees.
- Visitors may only enter these areas if accompanied by an authorized employee.
- Visitor badges must be worn in a clearly visible manner at all times.
- The accompanying employee is responsible for the visitor.
- Doors must be kept closed and secured against unauthorized access.

2. Security Zone 3 – High Security Area (Red / Blue)

(server room / IT infrastructure, high voltage)

- Access only for authorized (IT) personnel.
- Every access must be logged and documented in a comprehensible manner.
- External persons will only be granted access after prior approval and under supervision.
- Unauthorized equipment must not be brought into the area.
- Physical security measures must not be circumvented or overridden.

4. General safety requirements

The following rules apply to all security zones:

- Access media (e.g. keys, ID cards or access cards) may not be passed on to third parties.
- Access badges must be worn in a clearly visible manner.
- Tailgating of other persons is prohibited.
- Workplaces must be locked or locked when leaving.
- Suspicious activity or security incidents must be reported immediately.

5. Security Incident Reporting

Security incidents or violations of this policy must be reported immediately to:

- IT Security
- the responsible supervisor

6. Compliance with the Directive

Violations of this policy may result in the following consequences:

- withdrawal of access authorisation,
- labour law or disciplinary measures,
- legal consequences, to the extent provided for by law.