

1. Verhaltensregel zur Informationssicherheit

Um die Informationssicherheit sicherzustellen, gelten folgende verbindliche Regelungen:

- Jegliche Art von Bild- oder Tonaufzeichnungen ist untersagt.
- Das Verteilen oder Nutzen mobiler Datenträger (z.B. USB-Sticks) ist ohne Genehmigung verboten.
- Die Mitnahme von Dokumenten, Zeichnungen oder sonstigen Informationen ist untersagt.
- Die Installation oder das Anschließen eigener IT-Geräte an unsere Systeme oder Maschinen ist strikt untersagt.

Sollten Sie ausnahmsweise auf die oben genannten Mittel angewiesen sein, ist dies ausnahmslos vorab mit unserer IT-Leitung oder Informationssicherheitskoordinator abzustimmen.

Die dazugehörenden Richtlinien und Prozessbeschreibungen sind in unserem Managementsystem integriert und für alle Mitarbeiter verfügbar.

2. Regeln zur Arbeitssicherheit & Verhalten im Notfall

Ihre Sicherheit hat für uns höchste Priorität. Bitte beachten Sie daher die folgenden Verhaltensweisen.

Verhalten im Brandfall

- **Ruhe bewahren:** Handeln Sie überlegt und vermeiden Sie Panik.
- **Melden & Warnen:** Wählen Sie den Notruf 112 und warnen Sie Personen in Ihrer Umgebung.
- **Gebäude verlassen:** Nutzen Sie die gekennzeichneten Fluchtwege. Benutzen Sie keine Aufzüge. Schließen Sie Türen hinter sich. Gehen Sie zügig, aber rennen Sie nicht.
- **Sammelstelle aufsuchen:** Begeben Sie sich zum nächstgelegenen Sammelplatz und warten Sie auf Anweisungen.

Allgemeine Sicherheitshinweise

- **Erste Hilfe:** Melden Sie jeden Unfall oder jede Verletzung umgehend Ihrem Ansprechpartner, damit unsere Ersthelfer informiert werden können.
- **Rauchverbot:** Das Rauchen ist nur in den ausgewiesenen Außenbereichen gestattet.

3. Meldungen und Verbindlichkeit:

- **Melden von Sicherheitsvorfällen:** Bitte informieren Sie bei Verdacht auf einen Informationssicherheitsvorfall umgehend Ihren Ansprechpartner, den Informationssicherheitskoordinator oder die IT-Leitung.
- **Verbindlichkeit der Regelungen:** Alle hier genannten Regeln sind verbindlich einzuhalten. Zuwiderhandlungen können zu einem Hausverbot sowie zu zivil- oder strafrechtlichen Konsequenzen führen

Kontakt bei Fragen zur Informationssicherheit

Fragen können an Ihren jeweiligen Ansprechpartner, dessen Vorgesetzten oder direkt an den Informationssicherheitsbeauftragte gestellt werden:

Frau Carolin Mederer
Email: c.mederer@prologistik.com
Telefon: +49 2581 783 463 0

Vielen Dank für Ihre Kooperation!

Freigegeben durch die Geschäftsleitung
Datum: 25.06.2025

Informations- & Arbeitssicherheit für Besucher bei der proLogistik Group

Sehr geehrte Besucherinnen und Besucher,

im Rahmen unseres Managementsystems möchten wir Sie auf wichtige Verhaltensregeln in unserem Haus hinweisen.

Als Besucher verpflichten Sie sich, diese entsprechend umzusetzen und einzuhalten.

Vielen Dank!

1. VERTRAULICHKEIT zu wahren
2. VERFÜGBARKEIT sicherzustellen
3. VERÄNDERBARKEIT nicht zu zulassen



Schutzziel

VERTRAULICHKEIT

Vertraulichkeit bezeichnet die Eigenschaft, dass Informationen für unautorisierte Personen oder Prozesse nicht zugänglich sind und von diesen auch nicht offengelegt werden können. Die Vertraulichkeit ist beispielsweise verletzt, wenn ein Angreifer Kommunikation abhört.

- Unsere personenbezogenen Daten sind vor Dritten zu schützen.
- Kundenbezogene Daten und Informationen, wie z. B. Zeichnungen, gegenüber nicht befugten Dritten vertraulich zu schützen.



Schutzziel

VERFÜGBARKEIT

Die Verfügbarkeit bezeichnet die Eigenschaft, dass eine Information oder ein Wert für einen berechtigten Nutzer verfügbar und nutzbar ist, sobald dieser es verlangt. Die Verfügbarkeit kann beispielsweise durch Elementarschäden oder Katastrophen, aber auch durch von Hackern verursachte Verschlüsselungen von Daten bedroht sein, die dann „freigepresst“ werden.

- Informationen müssen jederzeit schnell und sicher verfügbar sein.
- Gesetzliche Archivierungsfristen müssen eingehalten werden.



Schutzziel

INTEGRITÄT

Als Integrität wird eine Eigenschaft bezeichnet, die Werte im Hinblick auf ihre Richtigkeit und Vollständigkeit schützt. Eine Integritätsprüfung erkennt jede Veränderung einer digitalen Information oder Nachricht. Hierzu zählen alle denkbaren Manipulationen, wie das Einfügen oder Löschen von Zeichen, das Wiedereinspielen einer Nachricht, das Umordnen von Daten oder Nachrichten sowie Duplikate.

- Zugänge und Passwörter müssen geschützt werden.

