

(Anhang 3)

## Informationssicherheitspolitik

**PFLITSCH** Informationssicherheitspolitik gilt in allen Bereichen des Unternehmens. Sie dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen. Diese Politik soll sicherstellen, dass alle Mitarbeiter, Partner und Dritte die Richtlinien und Verfahren befolgen, um die Informationssicherheit zu gewährleisten.

Das Hauptziel dieser Informationssicherheitspolitik ist es, Risiken für die Informationssicherheit zu minimieren, Geschäftsprozesse zu unterstützen und den gesetzlichen und vertraglichen Anforderungen gerecht zu werden. Dies wird durch die Implementierung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS) erreicht.

Grundsätze der Informationssicherheit:

**Vertraulichkeit:** wir schützen Informationen vor unbefugtem Zugriff und Offenlegung.

**Integrität:** wir schützen Informationen vor unbefugter Modifikation oder Zerstörung.

**Verfügbarkeit:** wir machen Informationen und IT-Systeme für berechtigte Benutzer stets verfügbar.

**Rechtmäßigkeit:** wir sorgen dafür, dass alle Informationsverarbeitungsprozesse den geltenden Gesetzen und Vorschriften entsprechen.

**Verantwortlichkeit:** wir verdeutlichen jedem Benutzer die von ihm durchgeführten Handlungen im Rahmen der Informationssicherheit zu verantworten.

Wir halten uns auf dem Stand der Technik und verpflichten uns zur **kontinuierlichen Verbesserung** des Informationssicherheitsmanagementsystems. Regelmäßig bewerten wir die Informationssicherheitsrisiken, um Schwachstellen und Bedrohungen zu identifizieren. Wir entwickeln und implementieren Maßnahmen zur Minderung der identifizierten Risiken.

Alle Mitarbeiter müssen regelmäßig Schulungen und **Sensibilisierungsmaßnahmen** zur Informationssicherheit durchlaufen. Neue Mitarbeiter müssen bei ihrem Eintritt in das Unternehmen eine Informationssicherheitseinführung erhalten.

Zugang zu IT-Systemen und -Einrichtungen ist auf autorisierte Personen beschränkt. Physische Sicherheitsmaßnahmen, wie z.B. Zutrittskontrollen, Videoüberwachung und Brandschutz, sind zu implementieren und zu überwachen.

Die Einhaltung dieser Informationssicherheitspolitik ist für alle Mitarbeiter und Partner verpflichtend. Diese Politik tritt mit ihrer Veröffentlichung in Kraft und bleibt bis auf Weiteres gültig.

Hückeswagen, 05.07.2024



Roland Lenzing  
Geschäftsführender Gesellschafter



Mathias Stendtko  
Geschäftsführender Gesellschafter