RONALGROUP

# CORPORATE

## SUPPLIER INFORMATION SECURITY GUIDELINE

**RONAL GROUP: JULY 2023**

**Änderungsprotokoll**

| Version | Datum | Abteilung | Beschreibung der Änderung |
|---|---|---|---|
| 1 | Juli 23 | Information Security | Erarbeitung des Dokuments |

**Bestätigung & Unterzeichnung**

Mit dieser Unterschrift bestätigen Sie ihre Absicht, die Anforderungen der im vorliegenden Dokument der RONAL GROUP "**Supplier Information Security Guideline**" einzuhalten und angemessene wie auch zumutbare Massnahmen zu treffen und umzusetzen.

| Datum der Genehmigung | Name des Unternehmens | Kontaktperson: Vor- & Nachname | Rolle | Unterschrift |
|---|---|---|---|---|
| | | | | |

# Inhaltsverzeichnis

# 1 Geltungsbereich

Diese Anweisungen gelten für alle Dritte, die schutzbedürftige Informationen für die RONAL AG, sowie für die gesamte RONAL GROUP (alle zugehörigen Tochtergesellschaften) entsprechend den vertraglichen Vereinbarungen verarbeiten.

# 2 Zweck und Definitionen

Diese Handlungsleitlinie definiert Regeln für Informationssicherheit, die von Dritten beim Umgang mit Informationen und IT-Geräten (z.B. PCs, Arbeitsplätze, Laptops, Smartphones oder Tablet-PCs) zu befolgen sind.

Dritte sind definiert als Vertragspartner, die Dienstleistungen für die RONAL AG auf Basis vertraglicher Beziehungen erbringen. Tochtergesellschaften und Marken der RONAL AG, sowie Gesellschaften, an denen die RONAL AG Mehrheitsbeteiligungen hält, sind von dieser Definition ausgeschlossen.

# 3 Dokumentenstruktur und Zielgruppe

Diese Richtlinie richtet sich an die Geschäftsleitung der Dritten, deren Mitarbeiter sowie deren Erfüllungs-/Verrichtungshilfen. Dieses Dokument enthält drei Kapitel. Die folgende Tabelle führt die Dokumentenstruktur und die jeweilige Zielgruppe pro Kapitel auf.

| **Kapitel** | **Zielgruppe** |
|---|---|
| 4 | Alle Dritte |
| 5.1 | Dritte, die in der RONAL Infrastruktur arbeiten. |
| 5.2 | Dritte, die RONAL Informationen außerhalb der RONAL Infrastruktur Zugriff haben. |
| 5.3 | Dritte, die RONAL Informationen in Verbindung mit Prototypen bearbeiten |

Ein Dritter kann je nach Zusammenarbeitsmodell gleichzeitig zu mehreren Zielgruppen gehören.

# 4 Allgemeine Anforderungen an alle Dritten

Die Dritten verpflichten sich, die Umsetzung gängiger Informationssicherheitsstandards nach den Anforderungen des VDA-ISA (siehe Anhang, Kapitel 7.1.a) in seiner jeweils gültigen Form in ihrem Unternehmen bzw. ihrer Organisation sicherzustellen.

Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk), welche Daten oder Systeme des Auftraggebers betreffen, sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, Kapitel 7.3.b).

Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen des Auftraggebers sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, Kapitel 7.3.b).

Beim Verdacht auf Verlust von vertraulichen oder geheimen Informationen des Auftraggebers muss dies sofort an die zuständige Stelle gemeldet werden (siehe Anhang, Kapitel 7.3.b).

# 5 Zusätzliche Anforderungen an Dritte

Beschreibung der zusätzlichen Anforderungen, welche an Dritte gestellt werden, die in- oder ausserhalb der RONAL Infrastruktur arbeiten und Zugriff auf RONAL Informationen haben oder welche RONAL Informationen in Verbindung mit Prototypen verarbeiten.

## 5.1 RONAL Infrastruktur (intern)

Ein Dritter arbeitet in der RONAL Infrastruktur, wenn:

- Clients (physische oder virtuelle Endgeräte) von RONAL oder verbundenen Unternehmen zur Verfügung gestellt werden, oder
- die Anbindung über Remote-Access-Lösungen (wie z.B. Pulsecure) erfolgt mit Zugriff auf das interne RONAL Netzwerk, oder
- die Anbindung des Dritten direkt an das interne RONAL Netzwerk erfolgt.

Dies ist unabhängig davon, ob sich der Dritte auf dem Gelände von RONAL oder einem verbundenen Unternehmen befindet oder nicht.

Für diese Dritten gelten die folgenden **Anforderungen**:

- Regelungen der RONAL bezüglich des Mitbringens von nicht dem Auftraggeber gehörenden IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche müssen eingehalten werden.
- Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.
- Die Vorschriften des Herstellers zum Schutz der Geräte sind einzuhalten.
- Durch den Auftraggeber zur Verfügung gestellte Geräte (z.B. Laptops, Mobiltelefone) dürfen nur nach erfolgter Genehmigung vom Werksgelände des Auftraggebers mitgenommen werden.
- Dienstleister dürfen die Bereitstellung oder Installation von Hardware und Software nur über die für sie zuständige Abteilung des Auftraggebers durchführen oder initiieren.
- Bezüglich der Nutzung der zur Verfügung gestellten Hard- und Software gelten die Regelungen der RONAL (siehe Anhang, Kapitel 7.3.c).
- Das Öffnen des IT-Gerätes und das Durchführen von Veränderungen an der Hardware (z.B. Ein-/Ausbau von Festplatten, Speicherbausteinen) sowie manuelle Veränderungen der Sicherheitseinstellungen (z.B. Browsereinstellungen) ist nur den zuständigen Stellen (siehe Anhang, Kapitel 7.3) gestattet.

- Der Einsatz oder das nachträgliche Verändern von Programmen des Auftraggebers ist nur zulässig, wenn diese von den zuständigen Stellen (siehe Anhang, Kapitel 7.3.b) genehmigt wird.
- Auf den zur Verfügung gestellten IT-Geräten sind keine Daten von weiteren Kunden, die nicht zum Konzern gehören, zu verarbeiten.
- Das Verwenden von IT-Geräten oder Daten des Auftraggebers durch Mitarbeiter des Dienstleisters erfordert die ausdrückliche Zustimmung des Auftraggebers. Der Auftraggeber ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z.B. bei Missbrauch).
- Weiterhin sind die Regelungen, Hinweise und Merkblätter auf der RONAL Webseite zu beachten.

## 5.2 RONAL Infrastruktur (extern)

Zusätzliche Anforderungen für Dritte, die RONAL Informationen außerhalb der RONAL Infrastruktur im Zugriff haben:

- Diese Dritten sind an die eigenen Regularien zur Informationssicherheit gebunden.
- Die Umsetzung von Maßnahmen zur Informationssicherheit ist gemäß TISAX®[1] für hohen Schutzbedarf nachzuweisen.

## 5.3 Prototypen

Zusätzliche Anforderungen für Dritte, die RONAL Informationen in Verbindung mit Prototypen verarbeiten:

- Diese Dritten sind an die eigenen Regularien zum Prototypenschutz gebunden.
- Die Umsetzung von Maßnahmen zum Prototypenschutz ist gemäß TISAX®[1] für hohen Schutzbedarf in Verbindung mit Prototypenkomponenten nachzuweisen.

# 6 Abweichungen und Ausnahmen

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang, Kapitel 7.3.b) und dem Auftraggeber zulässig.

[1] **T**rusted **I**nformation **S**ecurity **A**ssessment e**X**change, siehe www.tisax.org

# 7 Anhang

## 7.1 Mitgeltende Dokumente

a. Information Security Assessment des Verbands der Automobilindustrie e.V.
(Download von der Website des VDA - www.vda.de)
b. Regelungen, Hinweise und Merkblätter auf der RONAL Webseite

## 7.2 Gültigkeit

Diese Informations-Sicherheitsregelung tritt zum Zeitpunkt der Veröffentlichung in Kraft. Aktualisierte Inhalte dieser Regelung sind innerhalb eines Übergangszeitraums von sechs Monaten umzusetzen.

Nächstes Überprüfungsdatum: **31. Oktober 2023**

## 7.3 RONAL spezifische Ausprägungen

a. RONAL Zentrale

Tel.: +41 62 389 05 10
Mail: info@ronalgroup.com

b. Verantwortlichkeit Informationssicherheit:
infosec@ronalgroup.com

c. Jeder Auftragnehmer ist dafür verantwortlich, dass Informationen, Programme und IT-Geräte nur für Unternehmenszwecke und im Rahmen der jeweiligen Aufgabenstellung ordnungsgemäß eingesetzt und genutzt werden.
Das Versenden von Daten mit nicht dienstlichem Inhalt ist unzulässig.
Die Nutzung des Internets zu privaten Zwecken ist nur im Rahmen von im Unternehmen bestehenden Regelungen zugelassen.
Der Einsatz privater Software und Daten auf den von RONAL gestellten IT-Geräten ist verboten.