RICHTLINIE ZUR INFORMATIONSSICHERHEIT FÜR LIEFERANTEN

KROMBERG & SCHUBERT

Inhaltsverzeichnis

0. Vorwort 2
1. Anwendungsbereiche 3
2. Nutzung von Kroschu IT-Systemen 3
3. Umgang mit Kroschu-internen Daten 4
4. Nutzung von Kroschu IT-Equipment und Software 4
5. Informationsklassifizierung 5
6. Datenschutz bei externem Betrieb von IT-Infrastruktur 5
7. Meldung von informationssicherheitsrelevanten Vorgängen 5

Rev.	Datum	Erstellt von	Geprüft von	Freigegeben von Datum
00	21.10.2019	M. Winkler	T.Träder B. Hoffmann-Genser	21.10.2019
01	01.09.2022		M. Winkler	auf Aktualität geprüft
02	21.08.2025	V.Sergl	M.Winkler	

0. Vorwort

Das Unternehmen Kromberg & Schubert (nachfolgend Kroschu) entwickelt und produziert im Kerngeschäft komplexe Bordnetzsysteme an über 40 internationalen Standorten für die Automobilindustrie. Zusätzlich zählt heute neben der Produktion von Sonderleitungen auch Kunststofftechnik zum Leistungsspektrum.

Das engagierte Zusammenspiel von Entwicklung, Produktion und Qualitätsmanagement hat bei Kromberg & Schubert oberste Priorität, um jede Lösung perfekt umzusetzen.

Informationen sind ein wesentlicher Wert für unser Unternehmen, unsere Kunden und Geschäftspartner und müssen daher angemessen geschützt werden. Arbeits- und Geschäftsprozesse basieren immer stärker auf IT gestützten Lösungen und Anbindungen.

Die Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik wird deshalb immer wichtiger.

Kroschu ist gemäß TISAX zertifiziert. Um die Einhaltung des Standards auch in Zusammenarbeit mit Lieferanten und dessen Unterlieferanten zu gewährleisten, sind die folgenden Anforderungen an die Informationssicherheit als Mindestanforderung für Lieferanten einzuhalten.

Mit dieser Richtlinie werden grundsätzliche Regelungen zur Sicherstellung der Informationssicherheit innerhalb der Geschäftsbeziehung zwischen Kroschu und den Lieferanten vereinbart. Sie dient der Einhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen von Kroschu.

1. Anwendungsbereiche

Folgende Anwendungsbereiche sind von den Regelungen dieser Richtlinie ausdrücklich betroffen:

- Ingenieurbüros und Lieferanten für Konzeptstudien- / Design für Neuentwicklungen
- Lieferanten aus dem Bereich Maschinenbau sofern eine Sondermaschine beauftragt werden soll
- Lieferanten für Prototypen, welche die Herstellung und Entwicklung von innovativen Neuentwicklungen übernehmen –> Bauteile, welche auch in ähnlicher Ausfertigung noch nicht am Markt verfügbar sind

2. Nutzung von Kroschu IT-Systemen

Die Nutzung von IT-Geräten und Daten von Kroschu durch Mitarbeiter von externen Lieferanten bedarf der ausdrücklichen Zustimmung des zuständigen Fachbereiches. Dieser hat das Recht die Nutzung jederzeit zu unterbinden (z.B. bei Missbrauchsverdacht). Kroschu kann das Mitbringen tragbarer IT-Systeme, Mobiltelefone, Kameras, etc. verbieten oder auf bestimmte Bereiche einschränken.

Der Kreis der autorisierten Mitarbeiter des externen Lieferanten muss namentlich festgelegt werden und ist nach dem „need-to-know"-Prinzip möglichst eng zu halten. Mitarbeiter des externen Lieferanten, welche Zugang zu Kroschu IT-Systemen bekommen, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften, internen Regelungen sowie der Geheimhaltungsvereinbarung zu verpflichten.

Dies gilt entsprechend auf für Mitarbeiter von beauftragten Subunternehmern.

Die Weitergabe von Informationen an Dritte ist ausdrücklich untersagt, es sei denn Kroschu stimmt diesem Vorgang ausdrücklich zu.

Durchführung von IT-Support:

Die durchgeführten Arbeiten sind zu dokumentieren (Umfang, Ergebnis, Zeitpunkt). Arbeiten die das Betriebssystem oder systemnahe Software betreffen dürfen durch den externen Lieferanten ausschließlich weisungsgebunden durchgeführt werden.

3. Umgang mit Kroschu-internen Daten

Bei der Übertragung und/oder Verarbeitung von Kroschu internen Daten durch den externen Lieferanten sind folgende Punkte zwingend zu beachten:

- Kroschu interne Daten sind vor jeglichem Missbrauch und Datenklau z.B. durch eine Schadsoftware zu schützen. Bei Verdacht auf Befall durch eine Schadsoftware dürfen die betroffenen Geräte und Datenträger nicht mehr benutzt werden.

- Die von Kroschu überlassenen Daten müssen durch Backup-Sicherungen abgesichert werden.

- Auf den von Kroschu zur Verfügung gestellten IT-Geräten dürfen keine Daten oder Informationen von weiteren Kunden, die nicht zur Kroschu gehören, verarbeitet werden.

- Die Daten von Kroschu sind nach den Regeln der Mandantentrennung von anderen Kundendaten des externen Lieferanten zu trennen.

- Datenträger sind gegen Verlust, Zerstörung und Verwechselung sowie gegen Zugriff von Unbefugten zu sichern. Nicht mehr benötigte Daten sind einer sicheren Entsorgung zuzuführen.

- Bei allen Gesprächen über schützenswerte Informationen, inklusive Telefongespräche, ist darauf zu achten, dass diese nicht unbefugt mitgehört werden können.

- Bei Transport von Datenträgern bzw. Geräten, die Datenträger enthalten ist dafür zu sorgen, dass alle notwendigen und geeigneten Vorkehrungen getroffen werden (z.B. Verschlüsselung), die vor Einsichtnahme, Veränderung und Löschung der Informationen durch Unbefugte schützen.

4. Nutzung von Kroschu IT-Equipment und Software

Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen. Von Kroschu bereitgestellte Geräte (z.B. Laptops, Mobiltelefone) dürfen nur mit Genehmigung von Kroschu vom jeweiligen Betriebsgelände entfernt werden. Ein Verlust der Geräte ist unverzüglich anzuzeigen.

Zur Erleichterung der auftragsbezogenen Kommunikation kann ein E-Mail-Account innerhalb der Kroschu-Domain eingerichtet werden. Die Nutzung des internen E-Mail-Dienstes ist ausschließlich im Zusammenhang mit dem Auftrag gestattet. Ebenso ist die Weiterleitung von E-Mails an externe Empfänger nur auftragsbezogen gestattet. Eine automatische Weiterleitung von an E-Mails an externe Postfächer ist ausdrücklich verboten.

5. Informationsklassifizierung

Im Rahmen der Informationsklassifizierung (in Bezug auf die Vertraulichkeit) werden die möglichen Auswirkungen (potentielle Schäden) für Kroschu für den Fall bewertet, dass Informationen ungewollt einem unberechtigten Empfängerkreis offengelegt werden.

Der Lieferant hat mittels eines geeigneten Rechtekonzepts sicherzustellen, dass die durch Kroschu übermittelten Informationen geschützt sind. Kroschu behält sich das Recht vor, die entsprechenden Konzepte vom Lieferanten anzufordern und auf ihre Einhaltung zu überprüfen.

6. Datenschutz bei externem Betrieb von IT-Infrastruktur

Bei externem Betrieb der IT-Infrastruktur (z.B. Netzwerke, Server) und/oder Cloud-Lösungen ist sicherzustellen, dass:

- externe Administratoren keinen Zugriff auf den Inhalt der Daten haben und
- die Anforderungen zur Verschlüsselung gemäß VDA ISA Control 10.1 (Cryptography)

eingehalten werden (Referenz zu ISO 27002:Control 10.1.1)

7. Meldung von informationssicherheitsrelevanten Vorgängen

Der Lieferant verpflichtet sich ein Verfahren zur Sicherstellung der Nachweisbarkeit bei Informationssicherheitsereignissen gemäß Kritikalitätsstufen zu erstellen und aufrechtzuerhalten.

Aufgetretene informationssicherheitsrelevante Vorgänge sind Kroschu unverzüglich unter folgender Emailadresse zu melden:

informationsecurity@kroschu.com