RICHTLINIE FÜR EXTERNE DIENSTLEISTER, LIEFERANTEN UND KOOPERATIONSPARTNER

INFORMATIONSSICHERHEIT

rd electronic GmbH
Keltening 9
D-82041 Oberhaching
Telefon 089 / 2378 8900 ● info@rd-electronic.de

Version:	1.0.0.0
Status:	Freigabe
letzte Änderung:	16.12.2022
erstellt am:	08.12.2022
gültig / Überarbeitung bis:	Unbefristet
Autor / Eigentümer:	ISB
ISM-Klassifizierung:	Öffentlich

Äderungsmanagement / Historie

Ausgabe	Datum	Autor	Beschreibung
0.0.0.1	08.12.2022	ISB	Erstellung
1.0.0.0	16.12.2022	ISB	Redaktionelle Änderungen

Dokumentprüfung und -freigabe

Ausgabe	Datum	Person	Beschreibung
1.0.0.0	19.12.2022	EDV/IT	Prüfung
1.0.0.0	20.12.2022	GF	Freigabe

Inhaltsverzeichnis

1 Einordnung, Zweck und Geltungsbereich

Diese Vorgaben zur Informationssicherheit (IS) gelten für alle AUFTRAGNEHMER, wie Dienstleister, Lieferanten und Kooperationspartner, der rd electronic GmbH, die im Bereich der Informationstechnologie (IT), der elektronischen Datenverarbeitung (EDV) oder Technik tätig werden. Sie gelten nicht für AUFTRAGNEHMER, die eine reine Lieferungsleistung ohne Arbeitsanteil an technischen Systemen erbringen. Die rd electronic GmbH als AUFTRAGGEBER und der/die AUFTRAGNEHMER werden nachfolgend gemeinsam PARTEIEN genannt.

Die spezifischen Rechte und Pflichten der AUFTRAGNEHMER im Zusammenhang mit der Informationssicherheit werden in der hier vorliegenden Richtlinie beschrieben. Der Geltungsbereich umfasst alle INFORMATIONEN von denen der AUFTRAGNEHMER im Zuge der Auftragserfüllung oder ZUSAMMENARBEIT Kenntnis erlangt.

1.1 Veröffentlichung dieser Richtlinie

- Internes Kollaborationstool, ISMS
- Extern allgemein über Website der Firma: https://rd-electronic.com/cond/

2 Beschreibung

2.1 Allgemeine Regelungen

2.1.1 Vertraulichkeit

VERTRAULICHE INFORMATIONEN sind alle verkörperten, elektronischen oder mündlichen INFORMATIONEN und Daten jeder Art, die die PARTEIEN im Rahmen einer ZUSAMMENARBEIT austauschen, einschließlich aller technischen und geschäftlichen Daten, wie personenbezogene Daten, Zeichnungen, Designs, Know-how, Verfahren, Materialien, geschäftlich/betriebliche Informationen aller Art, Erfindungen, in Muster oder Prototypen, zu verarbeitende Daten, Software, einschließlich Quellcodes, unabhängig davon, ob die INFORMATIONEN als „eingeschränkt“, „vertraulich“, „streng vertraulich“ oder mit einem ähnlichen Vermerk gekennzeichnet oder mündlich übermittelt wurden. Wurde mit dem AUFTRAGNEHMER eine „Vereinbarung zur Auftragsverarbeitung (AVV)“ getroffen, gelten diese Vorgaben zusätzlich. Die beschriebenen Vorgaben sind verpflichtend für digitale und analoge Aufzeichnungen, inklusive Bild- und Tonaufzeichnungen, Kopien und Zusammenfassungen.

- Alle INFORMATIONEN gelten bis zur Freigabe durch den Informationssicherheitsbeauftragten (ISB) oder durch den verantwortlichen Projektleiter der rd electronic GmbH als vertraulich.
- Vertrauliche INFORMATIONEN sind ausschließlich zur Vorbereitung und zur Durchführung der ZUSAMMENARBEIT zu verwenden.
- Veröffentlichungen im Rahmen von Abschlussarbeiten, Projektberichten, wissenschaftliche Publikationen u.s.w. sind nur nach Freigabe des ISB zulässig.
- AUFTRAGNEHMER verpflichten sich, INFORMATIONEN Dritten nicht zugänglich zu machen und sie nur Dritten (z.B. Zulieferern) und denjenigen ihrer Mitarbeiter zugänglich zu machen, die diese für die jeweilige ZUSAMMENARBEIT benötigen und die zu einer expliziten Geheimhaltung verpflichtet sind, soweit sie nicht auf Grund ihres Berufstandes oder Arbeitsvertrages einer generellen Geheimhaltungsverpflichtung unterliegen.
- Nicht freigegebene INFORMATIONEN, die AUFTRAGNEHMER/N anvertraut oder die bei der ZUSAMMENARBEIT bekannt werden, dürfen nicht unbefugt für eigene Geschäftszwecke verwendet werden.
- AUFTRAGNEHMER verpflichtet sich, INFORMATIONEN zu Prototypen streng geheim zu halten und sich über die verbindlichen Vorgaben bei dem Ansprechpartner der rd electronic GmbH / dem Prototypen-Eigentümer zu informieren.
- Die PARTEIEN haben sicherzustellen, dass die jeweiligen Maßnahmen zur Wahrung der Informationssicherheit (IS) einem der ZUSAMMENARBEIT angemessenem Informationssicherheitsniveau entsprechen.

- Personen bezogene Daten werden stets vertraulich und zweckgebunden behandelt, die DSGVO wird eingehalten.
- Die im Rahmen des Auftragsverhältnisses generierten bzw. zur Verfügung gestellten Daten und INFORMATIONEN gehören der rd electronic GmbH.
- Sofern Daten und INFORMATIONEN dem AUFTRAGNEHMER überlassen wurden, über die zu verfügen sich ein Dritter vorbehalten hat, sind diese Daten und INFORMATIONEN im Zweifel so zu behandeln, als gehörten sie der rd electronic GmbH.
- Gleichgültig, ob Schutzrechte bestehen oder nicht, können aus technischen Einzelheiten und Zusammenhängen keine Lizenz-, Nachbau-, Nutzungs- oder sonstige Rechte durch AUFTRAGNEHMER hergeleitet werden.

2.1.2 Meldepflichten

Sämtliche einer Geheimhaltungspflicht betreffenden Vorkommnisse sind unverzüglich der rd electronic GmbH mitzuteilen.

Die Kenntnis von Verstößen gegen Vorgaben zur Informationssicherheit (auch dritter Personen) oder sonstiger Risiken für die rd electronic GmbH oder ihrer Kunden verpflichtet zur sofortigen Meldung an den Projektleiter oder an den ISB der rd electronic GmbH.

Eine aus dem Projekt / der vertraglichen ZUSAMMENARBEIT ausscheidende Person des AUFTRAGNEHMERS ist der Projektleitung der rd electronic GmbH augenblicklich zu melden.

Der AUFTRAGNEHMER verpflichtet sich zur augenblicklichen Meldung von Sicherheitsereignissen und Gegenmaßnahmen mit Bezug zur Informationssicherheit bzw. dem Datenschutz, die die rd electronic GmbH oder deren Kunden betreffen könnten; das schließt bspw. potentielle Sicherheitslücken im Programmcode ein.

2.1.3 Umgang mit Arbeitsmitteln

Grundsätzlich sind in Netzwerken und in den Räumen der rd electronic GmbH nur die für Verfügung gestellten Arbeitsmittel, insbesondere Hardware / Software, zu verwenden.

Nur in besonderen, kritischen Ausnahmefällen und im geprüften Einzelfall ist die Anbindung von firmenfremder IT-Hardware an die interne Infrastruktur (Ethernet, WLAN, sonstige IT-Systemschnittstellen) möglich. Die dokumentierte Freigabe erfolgt gemeinsam durch die Abteilung EDV/IT und dem für das entsprechende technische System Verantwortlichen. Dabei darf keine schwachstellenbehaftete Software auf der firmenfremde IT-Hardware installiert sein. Zur Prüfung kann die Erstellung eines „software inventory“ durch den Beschäftigten des AUFTRAGNEHMERS in Gegenwart eines fachlich versierten Mitarbeiters des AUFTRAGGEBERS angeordnet werden.

Über die firmenfremde IT-Hardware darf keine gleichzeitige Weitervernetzung, z.B. über Mobilfunk, möglich sein.

Der Zugriff auf das Internet über ein Gästenetzwerk mit firmenfremder IT-Hardware ist nur nach Übergabe von entsprechenden Zugangsdaten durch einen Mitarbeiter der rd electronic GmbH möglich.

Die Nutzung des Internetzugangs ist verboten für Zwecke, die den Interessen rd electronic GmbH entgegen sprechen, dem Ansehen in der Öffentlichkeit schaden könnten, gegen die geltenden Rechtsvorschriften verstoßen oder nicht im Zusammenhang mit der ZUSAMMENARBEIT stehen.

2.1.4 Verbot eigener nicht beauftragter Aufzeichnungen

Jegliche nicht durch die ZUSAMMENARBEIT und Verträge legitimierte Aufzeichnungen sind untersagt. Als Aufzeichnungen gelten auch handschriftliche Notizen und Fotos.

2.1.5 Ansprechpartner für sicherheitsrelevanten Themen

Der AUFTRAGNEHMER verpflichtet sich für die ZUSAMMENARBEIT, eine natürliche Person als Ansprechpartner für alle sicherheitsrelevanten Themen schriftlich zu benennen. Änderungen sind unverzüglich anzuzeigen.

Bei der rd electronic GmbH ist der erste Ansprechpartner die Projektleitung. Diese zieht im Bedarfsfall den Informationssicherheitsbeauftragen hinzu.

2.1.6 Dokumentation und Belehrung der Beschäftigten

Der AUFTRAGNEHMER trägt dafür Sorge, dass Beschäftigte, die in der ZUSAMMENARBEIT Zugriff auf Informationswerte erhalten könnten im angemessenen Umfang zur Informationssicherheit und zum Datenschutz zu sensibilisieren und zu verpflichten; Nachweis über die Schulung bzw. Sensibilisierung der Mitarbeiter muss auf Nachfrage des AUFTRAGGEBERS erbracht werden können.

Die Sensibilisierungspflicht gilt auch für allgemeine Standards, gesetzliche Vorgaben, speziellen Arbeitsschutz und weitere.

2.1.7 Referenzen

Aus der ZUSAMMENARBEIT erschließt sich kein Recht, mit den Arbeiten bei der rd electronic GmbH als Referenz zu werben. Dies gilt nicht für den Fall einer ggf. mit der rd electronic GmbH abgeschlossenen Referenzkundenvereinbarung.

2.1.8 Entwicklungsprinzipien und Testumgebungen

Der AUFTRAGNEHMER hat grundsätzlich die Funktionalität der beauftragten Leistung, vor der Implementierung in das Produktivsystem, in einer unkritischen Umgebung nachzuweisen. Der Auftraggeber behält sich vor sich vor, eine entsprechende Testumgebung zur Verfügung zu stellen.

Sofern es in einem Auswahlverfahren zur Lieferung von den rd electronic GmbH unbekannter Hardware kommt, ist die Hardware in einer zeitlich begrenzten Teststellung zur Verfügung zu stellen. Der dafür beim AUFTRAGNEHMER entstehende Aufwand ist vorab mit den rd electronic GmbH zu klären.

Insofern der AUFTRAGNEHMER Software für den AUFTRAGGEBER entwickelt, müssen Prinzipien des „Security by Design“ eingehalten und die Entwicklung gemäß allgemein anerkannter Industriestandards erfolgen.

2.1.9 Einhaltung der Vorschriften (Compliance)

Urheber- und / oder sonstige gewerbliche Schutzrechtsvermerke in Dokumenten, Quellcode, etc. dürfen von AUFTRAGNEHMERN nicht entfernt, unkenntlich oder verfälscht werden.

AUFTRAGNEHMER halten Rechte von Urhebern ein und beachten die entsprechenden Lizenzbedingungen.

AUFTRAGNEHMER sind verantwortlich, sich über gültige Standards, Vorschriften, gesetzliche Vorgaben, speziellen Arbeitsschutz und Geheimhaltungsvereinbarungen, die die ZUSAMMENARBEIT betreffen, detailliert zu informieren und einzuhalten.

Der AUFTRAGNEHMER beteiligt sich nicht an Industriespionage; Hackertools (bspw. Netzwerksniffer oder anderweitige Software, die gegen eine kontrollierte Softwareumgebung sprechen) werden nicht im Umfeld der rd electronic GmbH eingesetzt (Ausnahme sind gesonderte, vertraglich beauftragte Penetrationstests).

2.1.10 Informationen zur Organisation der Sicherheit

Der AUFTRAGNEHMER muss Informationen zum implementierten Informationssicherheitsmanagementsystem (ISMS) offenlegen, auf deren Basis eine Bewertung möglich ist; einem Audit des AUFTRAGNEHMERS oder durch einen Dritten kann im Einzelfall zugestimmt werden, falls ISO/IEC 27001, TISAX, BSI oder äquivalente Nachweise nicht vorliegen.

Voraussetzung in jedem Fall ist, dass das implementierte ISMS kontinuierlich verbessert / auditiert und die Aufrechterhaltung der Informationssicherheit in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität sowie den gesetzlichen Anforderungen gewährleistet wird.

2.2 Zutritt

Der Zutritt zu Räumlichkeiten des AUFTRAGNEHMERS mit Informationswerten des AUFTRAGGEBERS in verkörperter und/oder elektronischer Form ist im Sinne eines Informationssicherheitsmanagements geregelt. Der AUFTRAGNEHMER verpflichtet sich Sorge zu tragen für die physische und umgebungsbezogene Sicherheit, d.h. unbefugter Zutritt in bspw. Räume, Büros, Anlieferungs- und Ladebereiche sowie Einrichtungen allgemein ist ausgeschlossen; es existieren Richtlinien für aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung.

Der physikalische Zutritt zu Arbeitsorten des AUFTRAGGEBERS wird nur nach Anmeldung und in ständiger Gegenwart von Beschäftigten des AUFTRAGGEBERS gewährt.

2.3 Zugang

Der AUFTRAGNEHMER bestätigt, dass sichere Anmeldeverfahren und Maßnahmen zur sicheren Aufbewahrung von Passwörtern, Tokens, Schlüssel etc. bei ihm implementiert sind; Richtlinien für sichere Passwörter, Schlüssel etc. werden angewendet.

Der Zugang zu den internen Datenverarbeitungsanlagen des AUFTRAGGEBERS erfolgt ausschließlich überwacht durch einen Mitarbeiter des AUFTRAGGEBERS. Die Weitergabe von Zugangsdaten von internen Datenverarbeitungsanlagen ist untersagt.

Der Austausch von elektronischen Daten mit Dritten erfolgt ausschließlich über extern gehostete und kontrollierte Systeme.

2.4 Zugriff

Allgemein gilt das „Prinzip der minimalen Berechtigungsvergabe“: Berechtigungen werden nur zugewiesen, wenn sie zur Bearbeitung erforderlich sind. Der AUFTRAGNEHMER hat nachzuweisen, welche seiner Beschäftigten auf die INFORMATIONEN der ZUSAMMENARBEIT zugreifen können.

2.5 Datensicherheit

2.5.1 Verfahren zum Datenaustausch

Der AUFTRAGNEHMER verpflichtet sich, dass ein Austausch sicherheitsrelevanter Daten ausschließlich verschlüsselt erfolgt, wobei kryptographische Lösungen stets gängigen und aktuellen Industriestandards entsprechen.

Informationswerte mit der Klassifizierung „eingeschränkt“, „vertraulich“ oder „streng vertraulich“ dürfen nur mit geprüften Empfängern ausgetauscht werden. „Vertrauliche“ oder „streng vertrauliche“ Daten müssen verschlüsselt übertragen werden, nachdem die Projektleitung der rd electronic GmbH der Übergabe und dem gewählten Kommunikationsweg schriftlich zugestimmt hat.

2.5.2 Umgang mit mobilen Datenträgern und Fremd-IT-Hardware

Der Einsatz von mobilen Datenträgern oder fremder IT-Hardware im Firmennetz der rd electronic GmbH ist grundsätzlich untersagt. Sollte die Nutzung dennoch erforderlich sein, ist in jedem Fall das Vorgehen mit der Projektleitung und der Abteilung EDV/IT der rd electronic GmbH abzustimmen.

Fremde IT-Hardware bzw. der mobile Datenträger ist vor Anschluss an Ausrüstung der rd electronic GmbH auf Schadsoftware und Risiken zu überprüfen. Des weiteren sind mobile Datenträger nur zulässig, insofern Datenübermittlungstools wie sftp, FILR3 etc. aus technischen Gründen vor Ort nicht herangezogen werden können.

Bei der Ablage von Daten mit der Klassifizierung „eingeschränkt“ und „vertraulich“ auf mobilen Datenträgern ist das Wechselmedium oder die Datei selbst zu verschlüsseln. Bei der Ablage von Informationswerten der Sicherheitsstufe „streng vertraulich“ ist ein verschlüsseltes Medium und zusätzlich die Verschlüsselung auf Dateiebene (bspw. 7z, zip, veracrypt, truecrypt) verpflichtend vorgeschrieben. Nach der Übertragung der Informationswerte von einem USB-Stick / einer USB-Festplatte ist die zeitnahe, kontrollierte Löschung der Datei/en vorzunehmen, sofern der Zweck erfüllt worden ist.

Der Einsatz bzw. das Auspacken von Datenträgern mit als „eingeschränkt“, „vertraulich“ oder „streng vertraulich“ klassifizierte Informationen darf nur in sicheren Umgebungen erfolgen; sie dürfen nie unbeaufsichtigt bzw. ungesichert gelassen werden.

2.5.3 Sicherung von Informationswerten, Prototypen und Projektstände

Informationswerte, Prototypen und Projektstände aus der ZUSAMMENARBEIT sind beim AUFTRAGNEHMER nur in einer gesicherten und abgestimmten Umgebung aufzubewahren.

2.5.4 Kontrolliertes / Sicheres Löschen

KONTROLLIERTES LÖSCHEN bedeutet, dass die gelöschten INFORMATIONEN nur noch mit sehr erheblichem Aufwand wieder hergestellt werden können.

SICHERES LÖSCHEN von Daten bedeutet, dass INFORMATIONEN selbst gelöscht und mindestens zwei Mal mit zufälligen Informationen überschrieben werden.

2.5.6 Schutz, Löschung und Rückgabe von Informationen

Der AUFTRAGNEHMER verpflichtet sich, geeignete technische und organisatorische Maßnahmen zum Schutz der INFORMATIONEN des AUFTRAGGEBERS zu ergreifen.

Der AUFTRAGNEHMER verpflichtet sich im Rahmen der gesetzlichen Bestimmungen nach Beendigung der konkreten ZUSAMMENARBEIT, aber auch bei Nichtzustandekommen dieser, ohne Aufforderung sämtliche VERTRAULICHE INFORMATIONEN in verkörperter und/oder elektronischer Form sowie sämtliche Kopien davon und eventuell übergebene Muster unverzüglich und vollständig zurück zu geben oder zu vernichten. Angemessene Nachweise sind nach Aufforderung des AUFTRAGGEBERS zur Verfügung zu stellen. Für die Vernichtung elektronischer Informationswerte wird kontrolliertes / sicheres Löschen eingesetzt.

Der AUFTRAGGEBER behält sich vor, eine Kontrolle dieser Maßnahmen beim AUFTRAGNEHMER durchzuführen.

2.5.7 Abwehr von Schadsoftware

Der AUFTRAGNEHMER sichert zu, dass wirkungsvolle Maßnahmen gegen Schadsoftware etabliert sind, die im direkten und indirekten Zusammenhang mit der ZUSAMMENARBEIT stehen, bspw.

- Installierte und aktive Anti-Schadcodeprogramme mit stets aktuellen Schadcode-Definitionen sowie aktivierte Firewalls.
- Zur Gefahrenabwehr betreibt der AUFTRAGNEHMER ein Schwachstellen- und Patchmanagement.
- Eingesetzte Betriebssysteme sind zeitgemäß und/oder zusätzlich abgesichert.

3 Schlussbestimmungen

Bei einem Verstoß gegen die hier genannten Bestimmungen durch den AUFTRAGNEHMER besteht für die rd electronic GmbH das Recht, die sofortige Herausgabe sämtlicher überlassener vertraulicher INFORMATIONEN, einschließlich Kopien aller Kopien, Abschriften jeder Art etc., zu verlangen oder den Nachweis der Unbrauchbarmachung einzufordern.

Die AUFTRAGNEHMER haften in vollem Umfang für Missbrauch und Weitergabe der zur Verfügung gestellten INFORMATIONEN.

Sollten einzelne genannte Bestimmungen ganz oder teilweise unwirksam oder nichtig sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen oder nichtigen Bestimmung tritt diejenige wirksame Bestimmung, die rd electronic GmbH und AUFTRAGNEHMER vereinbart hätten, um den gleichen Erfolg zu erzielen. Dies gilt für fehlende Bestandteile entsprechend.