Cybersecurity Regelungen für Geschäftspartner

Datum: 24.04.2023

Version: 1.1

Veröffentlicht von: REMECH Systemtechnik GmbH

1. Anwendungsbereich

Diese Regelungen gelten für Geschäftspartner der REMECH Systemtechnik GmbH (nachfolgend REMECH genannt), die im Rahmen eines Vertragsverhältnisses Zugang oder Zugriff auf IT-Systeme, -Applikationen, -Netze oder Informationen[1] haben.

Die hierin definierten Regeln und Grundsätze gelten unabhängig davon, ob der Geschäftspartner IT-Systeme von REMECH oder eigene IT-Systeme nutzt, der Geschäftspartner in Räumlichkeiten von REMECH arbeitet oder nicht, oder ein Anschluss zu IT-Ressourcen von REMECH erfolgt (z.B. zu einem IT-System oder einer IT-Applikation).

Die Cybersecurity Klauseln einer zugrunde liegenden Vereinbarung bleiben hiervon unberührt.

1.1. Verantwortlichkeiten

Der Geschäftspartner von REMECH erhält Zugang zu IT-Systemen, Anwendungen, Netzwerken oder Informationen, um seinen vertraglichen Verpflichtungen nachzukommen und die Effizienz der Geschäftsabwicklung zu steigern.

Dies erfordert Maßnahmen zum Schutz von IT-Systemen, Anwendungen, Netzwerken und Informationen, um unbeabsichtigte Offenlegung, unbefugten Zugriff, Manipulation, Computerviren, Hacking, Cyberangriffe und andere IT-Sicherheitsbedrohungen zu verhindern. Zu diesem Zweck ist es erforderlich, dass die Geschäftspartner von REMECH die folgenden Regeln und Grundsätze einhalten und dass Schutzmaßnahmen nicht auf andere Weise deaktiviert, umgangen oder geändert werden. Alle diese Maßnahmen sind in Übereinstimmung mit Cybersecurity Standards (z.B. ISO27001) nach dem Stand der Technik durchzuführen.

Der Geschäftspartner verpflichtet sich zusätzlich zu den sonstigen vertraglichen Vereinbarungen, die hierin definierten Regeln und Grundsätze zu beachten sowie diese Unterlage seinen Mitarbeitern und allen Subunternehmern, die Zu-gang oder Zugriff auf IT-Systeme, -Applikationen und -Netze von REMECH oder Informationen erhalten, zur Kenntnis zu bringen, sie auf die Einhaltung zu verpflichten und die Einhaltung in geeigneter Weise zu überprüfen.

Im Weiteren werden Geschäftspartner und seine Mitarbeiter zusammenfassend als Geschäftspartner bezeichnet.

[1] "Informationen" bedeutet in hier Informationen oder Daten (nicht zugänglich im öffentlichen Bereich), die auf Grundlage aller Arten und Formaten, einschließlich digitaler Formate (z.B. Daten, die auf elektronischen oder optischen Medien gespeichert sind) oder physischer (z.B. Papier), numerischer, audiovisueller, grafischer, kartografischer, narrativer oder immaterieller Formate (z.B. Know-how), erhalten, erzeugt, ausgetauscht, gesammelt oder gespeichert werden und entweder im Besitz von REMECH sind oder im Auftrag von REMECH - Kunden und Lieferanten verarbeitet werden und dem Geschäftspartner zugänglich sind.

Der Geschäftspartner ist verpflichtet, die Richtlinien und Vorschriften von REMECH für die Sicherheit von IT-Systemen, Anwendungen und Netzwerken einzuhalten.

Erfüllen Geschäftspartner ihre vertraglichen Verpflichtungen aus der Ferne/Remote (weder bei REMECH noch auf Geschäftspartnergelände), so hat der Geschäftspartner sicherzustellen, dass seine Mitarbeiter zusätzlich zu den Regeln und Grundsätzen in diesem Dokument und der zugrunde liegenden vertraglichen Vereinbarung auch die Fernarbeits-richtlinien nach dem Stand der Technik des Geschäftspartners einhalten (z.B. durch Sensibilisierungstrainings für sicheres Arbeiten von zu Hause).

2. Regeln und Grundsätze

2.1. Schulung des Geschäftspartnerpersonals

Zur Erfüllung der vertraglichen Verpflichtungen soll der Geschäftspartner nur Personal engagieren, das auf dem Stand der Technik der Informationssicherheit (und ggf. sicherer Programmierung) ausgebildet ist, und sicherstellen, dass deren Wissen regelmäßig (mindestens einmal pro Kalenderjahr) aufgefrischt wird. Die Geschäftspartner machen sich mit den Informationssicherheitsrichtlinien, -standards und -vorgaben von REMECH vertraut und nehmen auf Verlangen von REMECH an Schulungen zur Informationssicherheit teil. Der Geschäftspartner wird REMECH im Voraus informieren, wenn Personal ausgetauscht wird, welches für die Erfüllung der vertraglichen Verpflichtungen benötigt wird.

2.2. Umgang mit Informationen

Der Geschäftspartner nutzt die von REMECH / Siemens[2] bereitgestellten Kommunikations- und Kollaborationslösungen für den Austausch von Informationen (siehe "IT-Services für sichere Datenübertragung und Zusammenarbeit externer Geschäftspartner mit REMECH - Siemens"), sofern zwischen den Parteien nichts anderes vereinbart ist.

Jedwede Form der Verschleierung oder Fälschung der Identität oder der Bedeutung von verwendeten Informationen durch den Geschäftspartner ist verboten.

2.2.1. Schutz von Informationen

Alle Informationen sind unabhängig von ihrer Erscheinungsform und ihrem Informationsträger gemäß ihrer Einstufung vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.

Für Informationen von REMECH sind drei Schutzklassen vorgesehen: „Intern“, „Vertraulich“ und „Streng vertraulich“. Entsprechend der Schutzklasse sind bei der

[2] REMECH Systemtechnik GmbH ist eine 100% Tochterfirma der Siemens AG und nutzt von Siemens bereitgestellte IT-Dienste

Kennzeichnung/Erstellung, Verteilung, Versand und Übertragung, Aufbewahrung und Speicherung sowie bei der Entsorgung/Vernichtung/Löschung Schutzmaßnahmen erforderlich, die mit zunehmendem Schutzbedarf höher werden.

Der Geschäftspartner legt in Absprache mit dem Ansprechpartner bei REMECH den Vertraulichkeitsgrad der von ihm erstellten Informationen fest. Bei überlassenen Informationen ist der Geschäftspartner verpflichtet, die von REMECH definierten Schutzmaßnahmen einzuhalten.

Informationen dürfen nur auf IT-Systemen, -Applikationen und Dateiablagesystemen gespeichert und verarbeitet werden, die einen adäquaten Schutz dieser Informationen gewährleisten, d.h. Informationen mit Schutzklasse "Vertraulich" sind verschlüsselt zu speichern und zu transferieren, während Informationen mit der Schutzklasse "Streng vertraulich" durchgehend (Ende-zu-Ende) verschlüsselt sein müssen.

Der Geschäftspartner darf ohne vorherige Zustimmung von REMECH oder ohne anderweitige vertragliche Vereinbarung zwischen den Parteien weder Kopien noch Vervielfältigungen von Informationen erstellen, löschen, untersuchen oder modifizieren.

2.2.2. Übermittlung von E-Mails

Der sichere Austausch von E-Mails bezieht sich auf E-Mail-Korrespondenz, die von oder zwischen Mitarbeitern und Auftragnehmern des Geschäftspartners, IT-Systemen, Anwendungen und REMECH stammt.

E-Mails, die die Integrität und Vertraulichkeit der Informationen und die Identifizierung des Absenders gewährleisten müssen, sind, unter Einhaltung von Standards nach dem Stand der Technik (z. B. NIST SP800-177R1, TN-1945 oder BSI ISi-Mail-Server), digital zu signieren und Ende-zu-Ende zu verschlüsseln, sofern sie Informationen mit den Schutzklassen "Vertraulich" oder "Streng vertraulich" beinhalten (z.B. mit dem S/MIME-Standard http://www.siemens.com/digital_id_en; siehe " IT-Services für sichere Datenübertragung und Zusammenarbeit externer Geschäftspartner mit REMECH - Siemens "[3]).

Dies umfasst z.B. folgenden Informationsaustausch:

- E-Mails mit kommerziellen oder rechtlichen Auswirkungen
- E-Mails, die eine Benutzerinteraktion bedürfen
- E-Mails, die sich auf den Austausch kritischer Sicherheitsinformationen beziehen
- E-Mails, die potenzielle schädliche Inhalte enthalten (z. B. URLs, Anhänge)

Die automatische Weiterleitung eingehender E-Mails an externe Postfächer, E-Mail-Spam, Missbrauch von REMECH - E-Mail-Adressen (z.B. Hinzufügen von E-Mails zu

[3] REMECH Systemtechnik GmbH ist eine 100% Tochterfirma der Siemens AG und nutzt von Siemens bereitgestellte IT-Dienste

Mailinglisten ohne ausdrückliche Zustimmung) sowie die Übermittlung vertraulicher oder streng vertraulicher Informationen per Fax ist untersagt.

2.2.3. Löschung von Informationen

Der Geschäftspartner hat alle Informationen auf allen seiner Informationsträger, die für die Erbringung der vertraglich vereinbarten Aufgaben oder Tätigkeiten nicht mehr benötigt werden, zuverlässig zu löschen, es sei denn, die Aufbewahrung ist vertraglich vereinbart oder nach den geltenden Gesetzen und Vorschriften erforderlich.

Informationen, die in elektronischer oder Papierform vorliegen, werden in Abhängigkeit von ihrer Vertraulichkeit unter Beachtung von Standards nach dem Stand der Technik (z.B. BS EN 15713 – Schutzstufe 6, NIST SP800-88, DIN 66399-2) gelöscht, bereinigt und entsorgt (d.h. Informationen mit Schutzklassen "Vertraulich" oder "Streng vertraulich" sind unwiederbringlich zu vernichten).

2.3. Zugangs- und Zutrittsberechtigungen

Bei Bedarf und wenn nicht anderweitig zwischen den Parteien vereinbart, soll, in Abhängigkeit der Schutzstufe des jeweiligen IT-Systems, der jeweiligen Anwendung und des jeweiligen Netzwerks, der Geschäftspartner Zugriff ausschließlich über REMECH Zugangslösungen auf das Netzwerk und die Informationen von REMECH erhalten (z.B. über die angebotene Geschäftspartnerzugangslösung von REMECH/Siemens[4]).

Der Geschäftspartner muss seinen Zugang zu REMECH protokollieren und jede Verbindung zwischen dem Intranet von REMECH und seiner Umgebung vor dem Zugriff von Dritten schützen.

Der Geschäftspartner darf erhaltene Systemzugangs- und Zulassungsberechtigungen (z.B. Passwort- oder Zugangskarten) nur zur Erfüllung seiner vertraglich vereinbarten Aufgaben und Tätigkeiten nutzen. Solche Systemzugangs- und Zulassungsberechtigungen sind auf den Grundsätzen "least privilege", "need to know" und "segregation of duties" anzuwenden.

Der Geschäftspartner wird REMECH zeitnah informieren, wenn sich Änderungen bzgl. der Mitarbeiter oder Subunternehmer mit entsprechendem Zugang zu Informationen ergeben.

Die Zulassungen, alle damit verbundenen technischen Konfigurationen oder kryptografischen Materialien sind vertraulich zu behandeln und dürfen weder an Dritte weitergegeben noch veröffentlicht werden.

[4] REMECH Systemtechnik GmbH ist eine 100% Tochterfirma der Siemens AG und nutzt von Siemens bereitgestellte IT-Dienste

Der Geschäftspartner darf diese Zugangslösung und die damit verbundenen Sicherheitsmechanismen nicht umgehen oder missbrauchen.

2.4. Schutz von Systemen und des Datenzugriffs

IT-Systeme und Informationsträger, die von den Geschäftspartnern genutzt oder von REMECH zur Erfüllung der vertraglichen Verpflichtungen zur Verfügung gestellt werden, müssen durch Maßnahmen nach dem Stand der Technik vor unbefugtem Zugriff geschützt werden, einschließlich der physischen Sicherheit für die Arbeitsumgebung des Geschäftspartners.

2.4.1. IT-Systeme und Informationsträger von REMECH

IT-Systeme und Informationsträger von REMECH werden auf der Grundlage von REMECH-Regeln und -Vorschriften gesichert und regelmäßig überwacht. Solche Sicherheitsmaßnahmen dürfen vom Geschäftspartner nicht umgangen oder manipuliert werden. Bei der Nutzung solcher IT-Systeme und Informationsträger lässt der Geschäftspartner die gebotene Sorgfalt walten, was zumindest die folgenden Schutzmaßnahmen umfasst:

• Nutzung des Diebstahlschutzes für mobile Systeme.

• Kein Missbrauch oder unberechtigter Zugriff bei der Nutzung von gemeinsamen Ressourcen.

• Verwendung von unterschiedlichen Passwörtern pro Benutzerkonto (Anonyme- und Gast-Zugänge sind zu de-aktivieren).

• Zugriffsrechte dürfen ohne vorherige Zustimmung von REMECH nicht erhöht werden.

• Ausschalten von sprachgesteuerten Smart Devices oder etwaigen Webcams im Arbeitsbereich, die nicht für dienstliche Zwecke benötigt werden (z.B. Amazon Alexa, Apple Siri).

• Abmelden und sicheres Aufbewahren der Geräte, wenn sie nicht genutzt werden.

• Papierdokumente mit vertraulichen oder streng vertraulichen Informationen dürfen nicht offen zugänglich sein oder unbeaufsichtigt bleiben. Sie müssen unter Benutzung geeigneter Schutzmechanismen weggeschlossen werden.

2.4.2. IT-Systeme und Informationsträger im Eigentum des Geschäftspartners

In Ergänzung zu Abschnitt 2.4.1 sind die folgenden zusätzliche Mindestschutzmaßnahmen für IT-Systeme und Informationsträger im Eigentum des Geschäftspartners umzusetzen:

- Installation der aktuellen Bios-Version und Aktivierung des Bios-Passworts.

- Keine Nutzung von dauerhaft lokalen Administrationsrechten.
- Aktivierung des Bildschirmschoners des Betriebssystems mit Passwortschutz (als Systemsperre für unbeaufsichtigte IT-Systeme).
- Aktivierung von Festplatten- und Dateiverschlüsselung.
- Schutz vor Viren und ähnlicher Schadsoftware nach dem Stand der Technik, sofern die IT-Systeme oder Informationsträger solchen Risiken ausgesetzt sind. Für PC-Systeme ist ein aktueller und permanent aktiver Virenschutz einschließlich eines „Endpoint Detection and Response Agents“ zu verwenden.
- Absicherung des Netzwerkzugangs mindestens durch ein Passwort zum Schutz vor unerlaubtem und bösartigem Netzwerkverkehr (z. B. Whitelisting).
- Keine Verwendung von Standard-Passwörtern. Löschung von Initialpasswörtern nach Erhalt und Verfall nach 24 Stunden.
- Passwörter müssen aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen erstellt werden. Passwörter müssen mindestens 12 Zeichen enthalten (26 Zeichen für Administratorkonten). Für PINs sind frei wählbare Ziffern zu verwenden. Passwörter müssen alle 180 Tage (45 Tage für privilegierte Administratorkonten) geändert werden, es sei denn, das Passwort ist Teil einer Zwei-Faktor-Authentifizierung. Die letzten 10 Passwörter dürfen nicht wiederverwendet werden.
- Für den Zugriff auf vertrauliche und streng vertrauliche Informationen ist eine Zwei-Faktor-Authentifizierung erforderlich.
- Während des Zugriffs auf REMECH IT-Systeme und Netzwerke darf keine zusätzliche Internetverbindung des Geräts möglich sein.
- Keine Verwendung von Netzwerk- oder Systemanalysegeräten ohne die ausdrückliche vorherige Genehmigung von REMECH.
- Angeschlossene Netzwerkgeräte und darauf eingesetzte Software von Drittanbietern müssen regelmäßig gewartet werden und der Geschäftspartner muss sicherstellen, dass der aktuelle Patch-Level eingespielt ist.

2.5. Informationspflichten, Cybersecurity Kontakt, Kontrolle

2.5.1. Informationspflichten

Der Geschäftspartner informiert die definierten Ansprechpartner von REMECH (u.a. Cybersecurity-Ansprechpartner, Vertragsinhaber) über Betriebsstörungen, Feststellung von Fehlern und Schadensfaktoren (z.B. Computerviren, Programmstörungen) in allen für die Zusammenarbeit genutzten IT-Systemen, Anwendungen, Netzwerken oder Software.

Stellt der Geschäftspartner Schwachstellen oder Sicherheitsvorfälle fest oder liegt ein entsprechender Verdacht vor, wird REMECH unverzüglich darüber informiert, z. B. bei Verdacht auf Missbrauch oder Offenlegung von PINs/Passwörtern.

2.5.2. Cybersecurity Kontakt

Neben den jeweiligen REMECH-Ansprechpartnern sind in den folgenden Fällen die entsprechenden REMECH-Cyber-Security-Kontaktadressen unverzüglich zu informieren, sofern potenziell oder tatsächlich eine Verletzung von Informationen, IT-Systemen, Applikationen, Netzwerk oder Informationsträgern vorliegt:

=> Sicherheitsvorfall / Schwachstelle: infosec@remech.de

2.5.3. Kontrolle

REMECH behält sich das Recht vor, die Einhaltung dieser Regeln und Grundsätze durch den Geschäftspartner wie hier beschrieben zu überwachen. Die an die Netzwerke von REMECH angeschlossenen IT-Systeme werden nach dem Stand der Technik auf Sicherheitslücken geprüft. Identifizierte Schwachstellen müssen vom Geschäftspartner unverzüglich behoben werden. Alle sicherheitsrelevanten Patches und Hotfixes, die von Dritten freigegeben werden, müssen installiert werden, sofern sie im Zusammenhang mit den vertraglichen Verpflichtungen stehen.

Der Geschäftspartner hat darüber hinaus die Einhaltung der hier festgelegten Regeln und Grundsätze in geeigneter Weise zu protokollieren und zu überwachen und dabei die gesetzlichen Vorgaben (z.B. Aufbewahrungsfristen) zu beachten.

Verstößt der Geschäftspartner gegen die hierin enthaltenen Regeln und Grundsätze, kann dies zur Sperrung seines Zugangs zu den Standorten und IT-Systemen von REMECH führen und vertragliche oder rechtliche Konsequenzen nach sich ziehen.

2.6. Beendigung der Zusammenarbeit

Bei Beendigung der Geschäftsbeziehung mit REMECH, einschließlich der Beendigung der Geschäftsbeziehung mit einem Mitarbeiter des Geschäftspartners, und sofern nicht anders vereinbart oder von REMECH verlangt, sind die folgenden Aktivitäten vom Geschäftspartner durchzuführen und schriftlich zu bestätigen:

- Rückgabe aller IT-Systeme, Geräte, Informationen, Informationsträger, Papierunterlagen und Arbeitsmittel (inkl. Zugangskarten).
- Rückgabe aller gewährten Zugänge und Angabe zum Zwecke der Deaktivierung oder Löschung (z.B. Zugang zu Dateifreigaben, Service-Accounts, etc.).
- Löschung von Informationen auf allen Informationsträgern und Vernichtung von Papierdokumenten gemäß Ziffer 2.2.3.
- Deinstallation der von REMECH zur Erbringung der vertraglichen Leistung zur Verfügung gestellten Software (z.B. Virtual Client Software).