IT Sicherheit-Mindeststandards für externe Partner
(Technische und organisatorische Maßnahmen)

Der Auftragsverarbeiter/Auftragnehmer (kurz „AN“) verpflichtet sich im Rahmen der Erfüllung der mit dem Verantwortlichen/Auftraggeber (nachfolgend kurz „AG“) vereinbarten Leistungen folgende IT Sicherheit-Mindeststandards für externe Partner (Technische und organisatorische Maßnahmen) vollinhaltlich zu erfüllen. Die Verpflichtung gilt für alle Mitarbeiter das AN inklusive der Mitarbeiter von eventuell beauftragten Subunternehmen.

Der AN hat alle Maßnahmen zu treffen, durch die

- die zufällige oder unrechtmäßige Zerstörung von Daten verhindert sowie
- die Vertraulichkeit von Daten des AG oder des voestalpine Konzerns gewahrt wird.

Jeder Sicherheitsvorfall (versehentliche oder rechtswidrige Zerstörungen, Verlust, Veränderung, unberechtigte Offenlegung oder Zugriff auf Daten) wird unabhängig von der Verursachung unverzüglich dem AG mitgeteilt. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs (z.B. Datenverlust, Zerstörung oder Löschung von Dateien, Befall von Computerviren, Ausfall sämtlicher Hardwarekomponenten, Ausfällen von Software als Konsequenz von Programmierungsfehlern und falscher Konfiguration) oder anderen Unregelmäßigkeiten beim Umgang mit Daten des AG. Zudem werden allfällig darüber hinausgehende vertraglich vereinbarte Verpflichtungen beachtet.

Darüber hinaus erfüllt der AN insbesondere nachstehende Vorgaben:

Risikomanagement (regelmäßige Überprüfung, Bewertung und Evaluierung)

- Es existiert eine regelmäßige Risikoanalyse in Bezug auf materielle und immaterielle Schäden die im Rahmen der Verarbeitungstätigkeit bzw. bei den zugrundeliegenden Systemen auftreten können.
- Pläne zur Sicherstellung der betrieblichen Kontinuität werden regelmäßig getestet und aktualisiert, um sicherzustellen, dass diese effektiv sind.
- Der AN hat regelmäßig dem Risiko angemessene Aktivitäten (z.B. Penetration Tests, Security Audits) zur Überprüfung der Wirksamkeit der getroffenen Maßnahmen durchzuführen und die Ergebnisse dem AG auf Anfrage zur Verfügung zu stellen.

Zutrittskontrollen

- Es existiert ein physisches Sicherheitskonzept unter Berücksichtigung der Sicherheitszonen (z.B. öffentliche Bereiche, Büro, Rechenzentrum, Hochsicherheitsbereich). Informationsverarbeitende Geräte werden mittels Sicherheitssperren physisch vor unbefugtem Zugang und Zugriff sowie vor Beschädigung oder Eingriffen geschützt.
- IT-Sicherheitsbereiche werden durch angemessene Zutrittskontrollen geschützt, um sicherzustellen, dass nur autorisiertem Personal Zutritt gewährt wird. Insbesondere werden Berechtigungen bei Veränderung oder Ausscheiden eines Mitarbeiters angepasst bzw. deaktiviert.
- Zugangs- bzw. Zugriffsrechte aller Mitarbeiter, Auftragnehmer und Dritter auf Informationen und informationsverarbeitenden Einrichtungen werden deaktiviert, wenn ihre Anstellung, ihr Vertrag oder ihre Vereinbarung endet.
- Alle in Rechenzentren der voestalpine zutrittsberechtigten Mitarbeiter des AN befolgen die Sicherheitsrichtlinien in Rechenzentren der voestalpine (Verhalten im Brandfall, etc.) und bestätigen

schriftlich die erfolgte Einschulung. Die obligatorischen Sicherheits- und Umwelteinweisungen werden absolviert und bestätigt.

Zugriffkontrollen

- Im Rahmen der Aufgabenverteilung wird vom AN festgelegt, welche seiner Mitarbeiter und von ihm beauftragte Personen zum Zugang zu den Systemen des AG berechtigt sind. Diese Festlegung und die Definition des jeweiligen Berechtigungsumfangs erfolgt einvernehmlich mit dem AG.
- Berechtigungen werden restriktiv, angepasst an die Erfordernisse zur Aufgabenerfüllung der Mitarbeiter des AN („need to know"-Prinzip) vergeben und nachvollziehbar dokumentiert.
- Die Anzahl der Systemadministratoren wird auf ein notwendiges Minimum beschränkt.
- Im Auftrag des AG betriebene Systeme werden vom AN angemessen von der Bedienung durch Unbefugte geschützt.
- Benutzerberechtigungen werden regelmäßig auf Aktualität und Notwendigkeit zur Aufgabenerfüllung überprüft.
- Benutzerberechtigungen werden entzogen, wenn sie nicht mehr benötigt werden.
- Der Zugriff auf Daten erfolgt mittels eines sicheren Anmeldeverfahrens und einer sicheren Passwort Policy (z.B. starke Passwörter, regelmäßige Passwortwechsel).
- Geräte des AN (z.B. Notebook, externe Speichermedien), auf denen (sofern für die Auftragserfüllung unbedingt erforderlich) temporär Daten des AG gespeichert werden, sind mit entsprechenden Zugriffsschutz (zumindest sichere Passwörter sowie eine nach dem aktuellen Stand der Technik ausreichende Verschlüsselung) ausgestattet.
- Remote Access (Fernzugriff) über das Internet ist nur erlaubt, falls die folgenden Voraussetzungen erfüllt sind:
    - Die Kommunikation über das Internet erfolgt getunnelt, verschlüsselt und mit starker Authentifizierung (z.B. Einmalpasswort als zweiter Faktor).
    - Die Berechtigungen sind eingeschränkt auf das erforderliche Minimum.
    - Das eingesetzte Produkt erlaubt neben der Remote Access Verbindung technisch nicht gleichzeitig weitere Verbindungen in das Internet.
- Alle voestalpine Vermögensgegenstände, die der AN in Verwendung hat (z.B. Notebook, Mobiltelefon, etc.), werden bei Beendigung des Vertrages, Abschluss der vereinbarten Leistungserbringung bzw. nach Aufforderung des AG – nach Wahl des AG – unverzüglich zurückgegeben oder vernichtet.
- Der AN nimmt zur Kenntnis, dass seine Aktivitäten, die er auf Systemen des voestalpine Konzerns durchführt, protokolliert werden.

Netzwerkkontrollen

- Durch den AN werden die nach dem Stand der Technik üblichen Sicherheitsvorkehrungen bei den Netzübergängen eingesetzt (z.B. Firewalls, VPN Zugänge, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) etc.). Es erfolgt insbesondere eine sichere Abschottung der Systeme mittels einer Firewall gegenüber externem Zugriff aus öffentlichen Netzwerken.
- Technische Einrichtungen werden korrekt instand gehalten und gepflegt, um ihre Verfügbarkeit und Vollständigkeit sicherzustellen.
- Die Geräte, die die Mitarbeiter des AN verwenden, erfüllen dem Stand der Technik entsprechende Sicherheitsanforderungen (z.B. Antivirus, Firewall, aktueller Patchstand, etc.).

Weitergabekontrollen

- Der Transport von Daten auf Notebooks oder externen Speichermedien oder ähnlichem stellt ein hohes Risiko dar und wird daher auf das absolut mögliche Minimum reduziert. Falls es nicht vermeidbar ist, wird größte Sorgfalt angewendet. Die Vertraulichkeit wird durch den Einsatz von Verschlüsselungstechniken sichergestellt, welche dem jeweils aktuellen Stand der Technik entsprechen.
- Sofern der AN Zugriff auf Systeme des AG erhält, darf der AN ohne Genehmigung des AG keinerlei Daten dieser Systeme in Einrichtungen außerhalb des voestalpine Konzerns speichern (z.B.: Cloud, etc).
- Wenn Datenträger oder Medien nicht mehr länger benötigt werden, werden diese verlässlich, sicher und fachgerecht entsorgt oder vernichtet, damit es unmöglich ist, die betreffenden Daten zu lesen oder wiederherzustellen. Diese Entsorgung bzw. Vernichtung wird vom AN nachweislich dokumentiert und dem AG auf Verlangen bestätigt.

Speicherkontrollen

- Betriebssysteme und betriebsrelevante Anwendungen werden überwacht und Informationssicherheitsereignisse werden aufgezeichnet. Unberechtigte Zugriffe werden protokolliert, um eventuelle Missbräuche von Systemen und Informationen zu verhindern. Um sicherzustellen, dass auftretende Informationssystem-Probleme erkannt werden, werden Betriebs- und Fehlerprotokolle periodisch ausgewertet.
- Aktivitäten von Systemadministratoren und -operatoren werden protokolliert.

Weisungskontrollen

- Die Zuständigkeiten für die Verarbeitung personenbezogener Daten sind klar geregelt (Verantwortlicher, Auftragsverarbeiter, Subauftragsverarbeiter, usw.).
- Der AN hat seine Mitarbeiter und die von ihm beauftragten Personen (insbesondere von allenfalls beauftragten Subunternehmen) auf die Wahrung der Vertraulichkeit der ihnen im Rahmen der Leistungserbringung bekanntwerdenden Informationen - auch über die Dauer der Leistungserbringung und des Arbeitsverhältnisses hinaus - nachweislich verpflichtet (Vertraulichkeitsvereinbarung).
- Alle Mitarbeiter erhalten entsprechende bewusstseinsbildende Schulungen und regelmäßig aktualisierte Informationen über IT-Informationssicherheit sowie Datenschutz, sofern diese für ihre Arbeit von Bedeutung sind.
- Dem AN zugängliche Daten werden ausschließlich für den vereinbarten Zweck verwendet. Jegliche Daten des AG bzw. des voestalpine Konzerns dürfen daher beim AN nur temporär für den vorgesehenen Zweck verarbeitet werden. Bei Beendigung des Vertrages, Abschluss der vereinbarten Leistungserbringung bzw. nach Aufforderung des AG werden jegliche Daten – nach Wahl des AG – unverzüglich zurückgegeben oder unwiederbringlich gelöscht. Ergänzende diesbezügliche Vereinbarungen sind zu berücksichtigen.
- Subauftragsverarbeiter/Subauftragnehmer, welche Zugang zu Daten des AG erhalten, müssen sämtliche zwischen dem AN und dem AG vereinbarte technische und organisatorische Maßnahmen einhalten.

Verfügbarkeitskontrollen

- Businesskritische, informationsverarbeitende Systeme werden vor Stromausfällen und Ausfällen anderer Versorgungseinrichtungen geschützt.
- Verfahren wurden eingerichtet, um eine schnelle, effektive und planmäßige Reaktion auf Informationssicherheitsvorfälle sicherzustellen.
- Es existieren regelmäßige Backups der Daten.
- Die Wiederherstellbarkeit der Daten wird regelmäßig überprüft.
- Business Continuity Pläne und Notfallpläne wurden entwickelt und umgesetzt, um den Betrieb aufrechtzuerhalten oder wiederherzustellen, und um die Verfügbarkeit von Daten im erforderlichen Maß und im erforderlichen Zeitraum nach Unterbrechungen oder Ausfällen von kritischen Geschäftsprozessen sicherzustellen.

Trennungskontrollen

- Der Zugriff auf die unterschiedlichen Bereiche folgt einem geregelten Freigabeprozess durch autorisierte Personen beim AN. Es besteht ein Berechtigungskonzept, welches verhindert, dass Mitarbeiter des AN, welche nicht für den AG Aufgaben erfüllen, Zugriff auf Daten des AG haben.
- Die Mitarbeiter des AN wurden unterwiesen, dass die Daten ausschließlich zu den vorgesehenen Zwecken verarbeitet werden dürfen.
- Die Verarbeitung von Daten unterschiedlicher Kunden (Mandanten) des AN erfolgt in logisch oder physisch getrennten Infrastrukturen.

Compliance

- Die Geräte, die von Mitarbeitern des AN im Netzwerk von voestalpine betrieben werden, dürfen nur vom AN lizensierte Software enthalten.
- Der AN hat die Verpflichtung alle erforderlichen Informationen zum Nachweis der Einhaltung, der in den IT Sicherheit-Mindeststandards für externe Partner (Technische und organisatorische Maßnahmen) niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen die vom AG oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, nach mindestens siebentägiger Vorankündigung dem AG zu ermöglichen und dazu beizutragen. Bei Verdacht oder Hinweis auf gravierende Verletzungen dieser Bestimmungen durch den AN oder Dritten ist dem AG der sofortige Systemzugriff bzw. der sofortige Zutritt zu den verwendeten Räumlichkeiten zu gewähren. Mängel und Unzulänglichkeiten, die im Zuge eines Audits erkannt werden, müssen umgehend behoben werden.