INFORMATIONSSICHERHEITSRICHTLINIEN FÜR LIEFERANTEN

Im Rahmen der Zusammenarbeit mit der IPETRONIK GmbH (nachfolgend „Auftraggeber" genannt) erhält der Lieferant (nachfolgend „Auftragnehmer" genannt) Zugang zu Informationen, Systemen und Ressourcen, die für die Erbringung der vereinbarten Leistungen erforderlich sind. Der Schutz dieser Informationen sowie die Einhaltung der geltenden Vorgaben zur Informationssicherheit haben für die IPETRONIK GmbH höchste Priorität.

Mit dieser Bestätigung verpflichtet sich der Auftragnehmer die nachfolgenden Anforderungen zur Informationssicherheit einzuhalten.

1. Organisatorische Grundsätze

1.1 Benennung eines Ansprechpartners

Der Auftragnehmer benennt gegenüber dem Auftraggeber mindestens einen Ansprechpartner, der für die Abstimmung von Vorgaben zur Informationssicherheit sowie Fragen zur Umsetzung für den Auftraggeber zur Verfügung steht.

1.2 Schützenswerte Informationen

Schützenswerte Informationen im Kontext dieser Lieferantenvereinbarung sind alle Informationen mit einem Bezug zum Auftraggeber, die aufgrund ihres Informationsgehalts nicht der Öffentlichkeit oder unberechtigten Dritten zugänglich sein dürfen. Dies beinhaltet explizit auch Geschäfts- und Betriebsgeheimnisse sowie Informationen zu betrieblichen Abläufen des Auftraggebers. Schützenswerte Informationen sind beispielsweise: Dokumentationen, Zeichnungen, Skizzen, Pläne, Beschreibungen, Richtlinien und sonstige Regelungen, Konfigurationen, Zugangsdaten zu IT-Systemen und IT-Komponenten.

Sind Informationen nicht oder noch nicht durch den Auftraggeber klassifiziert oder handelt es sich um Informationen, die durch den Auftragnehmer erstellt werden, so ist der Schutzbedarf der Informationen durch den Auftragnehmer festzulegen. Der Schutzbedarf ist so zu wählen, dass dem Auftraggeber kein Schaden durch eine zu geringe Einstufung der Informationen entstehen kann, bspw. in Form der Kenntnisnahme durch unberechtigte Dritte aufgrund fehlender Schutzmaßnahmen. Beispiel der IPETRONIK-Klassifizierung:

	Öffentlich	**Intern**	**Vertraulich**	**Geheim**
Kennzeichnung	Keine	„intern" Alle nicht gesondert klassifizierten Dokumente und Informationen gelten als „intern".	"Vertraulich" Auf allen Seiten des Dokuments bzw. auf dem Informationsträger sichtbar anbringen.	"Streng vertraulich" Auf allen Seiten des Dokuments bzw. auf dem Informationsträger sichtbar anbringen.
„Farblich"	„Grüner Balken"	„Gelber Balken"	„Orangener Balken"	„Roter Balken"

1.3 Organisationsfremde IT-Dienste

Vor Verwendung von organisationsfremden Diensten, die zum Verarbeiten von Informationswerten des Auftraggebers eingesetzt werden, sind die Informationssicherheitsanforderungen zu ermitteln, umzusetzen und eine Risikobewertung durchzuführen. Es muss sichergestellt werden, dass der Auftragnehmer nur die organisationsfremden Dienste einsetzt, die nach Risikobewertung ein ausreichendes Maß an Sicherheiten bietet. Es muss immer Multifaktorauthentifizierung (MFA) zum Einsatz kommen.

1.4 Verwendung von Software

Vor Verwendung von Software, die zum Verarbeiten von Informationswerten des Auftraggebers eingesetzt werden, sind die Informationssicherheitsanforderungen zu ermitteln, umzusetzen und eine Risikobewertung durchzuführen. Es muss sichergestellt werden, dass nur freigegebene Software verwendet wird.

1.5 Einhaltung der Informationssicherheit in Verfahren und Prozessen

Der Auftragnehmer stellt sicher, dass die Anforderungen dieser Vereinbarung regelmäßig auf Einhaltung überprüft werden.

1.6 Meldung von Ereignissen und Vorfällen

Der Auftragnehmer meldet aufgetretene Sicherheitsereignisse oder -vorfälle mit einer Auswirkung auf Informationen des Auftraggebers unverzüglich dem Auftraggeber.

Die Meldung hat an helpdesk@ipetronik.com zu erfolgen und an den ISB daniel.knap@ipetronik.com. Sollte eine Meldung per E-Mail nicht möglich sein, dann hat die Meldung telefonisch an Nr. 07221 / 99 22 344 zu erfolgen. Die Meldung hat auch bei bloßem Verdacht zu erfolgen.

1.7 Auswahl von Personal

Der Auftragnehmer setzt nur fachlich geeignetes Personal ein. Der Mitarbeiter weist sich durch seinen Dienstausweis gegenüber IPETRONIK aus. Für Remote-Tätigkeiten stellt der Dienstleister durch geeignetes On- und Offboarding sicher, dass nur berechtigtes Personal die Arbeiten ausführen kann.

Diese Mitarbeiter sowie Unterauftragnehmer und Leiharbeiter kennen diese Vereinbarung und werden regelmäßig auf Informationssicherheit geschult und zur Geheimhaltung verpflichtet.

1.8 Mobiles Arbeiten

Beim mobilen Arbeiten ist ein sicherer Umgang mit Informationen des Auftraggebers unter Berücksichtigung des Schutzbedarfs und der Anforderungen dieser Vereinbarung zu gewährleisten. Der Zugang zum Netzwerk des Auftragnehmers erfolgt über eine gesicherte Verbindung (z. B. VPN) und über eine starke Authentifizierung.

1.9 Sicherheitszonen

Informationen des Auftraggebers werden in gesicherten Bereichen des Auftragnehmers aufbewahrt. Zutritte zu diesen gesicherten Bereichen werden dediziert vergeben. Bei Leistungserbringung beim Auftraggeber vor Ort gelten die etablierten Besucherregelungen des Auftraggebers. Diese sind vor Ort einsehbar.

1.10 Unterauftragnehmer

Jede Einbeziehung von Unterauftragnehmern durch den Auftragnehmer bedarf der Genehmigung durch den Auftraggeber, sofern der Unterauftragnehmer Informationen des Auftraggebers erhält oder verarbeitet. Vor Beginn der Beauftragung muss mit dem Unterauftragnehmer eine Geheimhaltungs-vereinbarung / NDA geschlossen werden (Siehe auch 1.11).

Vom Auftraggeber zugelassene Unterauftragnehmer sind durch den Auftragnehmer vor Aufnahme der Tätigkeit zur Einhaltung der vorliegenden Lieferantenvereinbarung zu verpflichten.

1.11 Verpflichtung zur Geheimhaltung

Der Auftragnehmer ist verpflichtet, schützenswerte Informationen des Auftraggebers geheim zu halten. Die Verpflichtung erfolgt über eine separate Geheimhaltungsvereinbarung (GHV/NDA). Muster hierzu erhält man von der Assistenz der Geschäftsführung in deutscher oder englischer Sprache.

2. IT-bezogene Regelungen

2.1 Umgang mit Informationsträgern

Informationen des Auftraggebers dürfen nur auf verschlüsselten Datenträgern gespeichert werden. Ist eine Verschlüsselung technisch nicht sinnvoll realisierbar, so sind die Zugriffe auf die Informationen durch geeignete andere Maßnahmen abzusichern. Bei Ausmusterung von Datenträgern auf denen Informationen des Auftraggebers gespeichert sind, sind diese sicher zu löschen oder gemäß ISO 21964 mit mind. Sicherheitsstufe 4 zu vernichten.

2.2 Berechtigungsmanagement und Kennwörter

Der Zugriff auf Informationen des Auftraggebers muss beim Auftragnehmer einer Zugriffssteuerung unterliegen. Es ist sicherzustellen, dass nur die Personen Zugriff auf Informationen des Auftraggebers erhalten, die für den Auftraggeber tätig werden. Die Zugriffssteuerung muss auf Basis personenbezogener Benutzerkonten erfolgen. Es gelten das Least-Privilege- und das Need-to-know-Prinzip.

Alle Benutzerkonten müssen mit komplexen Kennwörtern (mind. 12-stellige Kombination auf folgenden 4 Kriterien: Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen) ausgestattet sein. Bei Zugriff auf besonders schützenswerte Informationen des Auftraggebers muss der Zugriff zusätzlich über eine Multifaktor-Authentifizierung (MFA) abgesichert werden.

Die Kennwörter sind regelmäßig, mindestens einmal pro Jahr oder bei Kompromittierung umgehend zu ändern. Bei Einsatz vom MFA kann auf eine regelmäßige Kennwortänderung verzichtet werden. Bei Austritt von Personen, die für den Auftraggeber tätig sind, muss der Auftragnehmer deren Zugänge umgehend sperren.

2.3 Verschlüsselung der Datenübertragung

Die Übertragung schützenswerter Informationen des Auftraggebers hat verschlüsselt (Ende-zu-Ende-Verschlüsselung) zu erfolgen. Dies bezieht sich insbesondere auf die Übertragung schützenswerter Information per E-Mail oder Dateitransfer. Für den sicheren Datenaustausch stellt der Auftraggeber bei Bedarf eine Lösung für sicheres File-Sharing bereit.

2.4 Schutz vor Schadprogrammen

Der Auftragnehmer hat seine IT-Systeme vor Schadsoftware sowohl technisch als auch organisatorisch zu schützen, sofern auf diesen Informationen des Auftraggebers gespeichert sind. Die hierfür eingesetzte Software/Systeme werden automatisch aktualisiert. Der gesamte Datenbestand aller Systeme wird regelmäßig auf Schadsoftware überprüft.

2.5 Schwachstellenmanagement

Der Auftragnehmer stellt sicher, dass alle IT-Systeme und -Komponenten des Auftragnehmers, die im Rahmen der Leistungserbringung für den Auftraggeber zum Einsatz kommen, auf denen Informationen des Auftraggebers gespeichert werden oder über die Informationen des Auftraggebers übertragen werden, über einen aktuellen Software- und Patch-Stand verfügen. Bekanntgewordene Schwachstellen auf den IT-Systemen und -Komponenten des Auftragnehmers sind umgehend durch geeignete Maßnahmen zu schließen.

2.6 Fernzugriffe

Der Auftragnehmer stellt sicher, dass Fernzugriffe auf IT-Systeme oder -Komponenten des Auftraggebers personenbezogen eingerichtet sind. Es muss jederzeit sichergestellt sein, dass erfolgte Fernzugriffe einer Person eindeutig zuordenbar sind. Fernzugriffe auf IT-Systeme oder -Komponenten des Auftraggebers sind nur den Mitarbeitenden des Auftragnehmers bereitzustellen, die für den Auftraggeber tätig werden.

Für Fernzugriffe gelten grundsätzlich die Vorgaben zur Zugriffssteuerung gemäß Punkt 2.2. Eine Multifaktor-Authentifizierung (MFA) ist für Fernzugriffe verpflichtend. Fernzugriffe dürfen durch den Auftragnehmer ausschließlich für die Ausführung konkreter Aufträge genutzt werden.

2.7 Datensicherung

Der Auftragnehmer hat für die maßgeblichen IT-Systeme ein Sicherungs- und Wiederherstellungskonzept umgesetzt, sofern auf diesen Systemen Informationen des Auftraggebers speichert, für deren Speicherung er verantwortlich ist. Die einwandfreie Funktion der Datensicherung sowie die Wiederherstellbarkeit ist in regemäßigen Abständen zu prüfen.

IPETRONIK GmbH & Co. KG
Im Rollfeld 28
76532 Baden-Baden

+49 (0) 7221 9922 0
info@ipetronik.com