INFORMATIONSSICHERHEITSRICHTLINIEN FÜR LIEFERANTEN

Im Rahmen der Zusammenarbeit mit der IPETRONIK GmbH & Co. KG sowie aller Tochterfirmen (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 IPETRONIK höchste Priorität.

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

Organisatorische Grundsätze

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.

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

INFORMATION SECURITY POLICIES FOR SUPPLIERS

As part of the collaboration with IPETRONIK GmbH & Co. KG and all of its subsidiaries (hereinafter referred to as “Client”), the supplier (hereinafter referred to as “Contractor”) is granted access to information, systems, and resources necessary for the performance of the agreed-upon services. The protection of this information and compliance with applicable information security requirements are of the highest priority for IPETRONIK.

By providing this confirmation, the Contractor agrees to comply with the following information security requirements.

Organizational Principles

Designation of a Contact Person

The Contractor shall designate at least one contact person to the Client who will be available to coordinate information security requirements and address implementation-related questions on behalf of the Client.

Information Requiring Protection

Confidential information, as used in this Supplier Agreement, refers to all information related to the Client that, due to its content, must not be made available to the public or unauthorized third parties. This explicitly includes trade and business secrets as well as information regarding the Client’s operational processes. Examples of information requiring protection include: documentation, drawings, sketches, plans, descriptions, guidelines and other regulations, configurations, and access data for IT systems and IT components.

If information has not been classified – or has not yet been classified – by the Client, or if the information is created by the Contractor, the Contractor shall determine the level of protection required for the information. The level of protection must be selected in such a way that the Client suffers no harm as a result of the information being classified too low, for example,

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!

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"

in the form of unauthorized third parties gaining access to it due to lack of protective measures.
Example of the IPETRONIK classification:

	Public	Internal	Confidential	Secret
Classification	None	"Internal" All documents and information not specifically classified are considered "internal".	"Confidential" Affix visibly to all pages of the document or to the information carrier.	"Strictly Confidential" Affix visibly to all pages of the document or to the information carrier.
Color-coded	"Green Bar"	"Yellow Bar"	"Orange Bar"	"Red Bar"

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.

Third-Party IT-Services
Before using third-party services to process the client's information assets, the information security requirements must be identified and implemented, and a risk assessment must be conducted. It must be ensured that the contractor uses only those external services that, based on the risk assessment, provide an adequate level of security. Multi-factor authentication (MFA) must always be used.

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.

Use of Software
Before using software intended to process the client's information assets, the information security requirements must be identified and implemented, and a risk assessment must be conducted. It must be ensured that only approved software is used.

Einhaltung der Informationssicherheit in Verfahren und Prozessen
Der Auftragnehmer stellt sicher, dass die Anforderungen dieser Vereinbarung regelmäßig auf Einhaltung überprüft werden.

Compliance with Information Security in Procedures and Processes
The Contractor shall ensure that compliance with the requirements of this Agreement is regularly verified.

Nachweis- und Auditrecht
Der Auftraggeber ist berechtigt, die Einhaltung der in dieser Vereinbarung festgelegten Anforderungen zur Informationssicherheit in angemessenem Umfang zu überprüfen. Der Auftragnehmer stellt dem Auftraggeber hierzu auf Verlangen geeignete Nachweise zur

Right to Verification and Audit
The Client is entitled to verify, to a reasonable extent, compliance with the information security requirements set forth in this Agreement. The Contractor shall provide the Client with appropriate evidence for this purpose upon request. If necessary, the Client may, after prior consultation, conduct audits at the Contractor's

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!

Verfügung. Sofern erforderlich, kann der Auftraggeber nach vorheriger Abstimmung Audits beim Auftragnehmer durchführen oder durch einen beauftragten Dritten durchführen lassen. Der Auftragnehmer unterstützt die Durchführung in angemessenem Umfang und stellt die hierfür erforderlichen Informationen und Nachweise zur Verfügung.

premises or have them conducted by a third party commissioned by the Client. The Contractor shall assist in the conduct of such audits to a reasonable extent and shall provide the necessary information and evidence for this purpose.

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.knapp@ipetronik.com. Sollte eine Meldung per E-Mail nicht möglich sein, dann hat die Meldung telefonisch an +49 (0) 7221 / 99 22 344 zu erfolgen. Die Meldung hat auch bei bloßem Verdacht zu erfolgen.

Reporting of Event and Incidents

The Contractor shall immediately report to the Client any security events or incidents that have occurred and that affect the Client's information.

The report must be sent to helpdesk@ipetronik.com and to the ISB at daniel.knapp@ipetronik.com. If reporting via email is not possible, the report must be made by phone at +49 (0) 7221 / 99 22 344. The report must be made even in cases of mere suspicion.

Auswahl von Personal

Der Auftragnehmer setzt nur fachlich geeignetes Personal ein. Der Mitarbeiter weist sich durch seinen Dienstausweis gegenüber der 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.

Selection of Personnel

The Contractor shall employ only personal who are qualified for the job. Employees shall identify with IPETRONIK by presenting their employee ID cards. For remote work, the service provider shall ensure, through appropriate onboarding and offboarding procedures, that only authorized personnel can perform the work.

These employees, as well as subcontractors and temporary workers, are familiar with this agreement, receive regular training on information security, and are bound by a confidentiality obligation.

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.

Mobile Work

When working remotely, the Contractor must ensure that the Client's information is handled securely, taking into account the level of protection requited and the requirements of this agreement. Access to the Contractor's network must be via a secure connection (e.g. VPN) and strong authentication.

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.

Security Zones

The client's information is stored in the contractor's secure areas. Access to these secure areas is granted on a dedicated basis. When services are provided on the client's premises, the client's established visitors policies are available for review on site.

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!

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 Geheimhaltungsvereinbarung / NDA geschlossen werden. Vom Auftraggeber zugelassene Unterauftragnehmer sind durch den Auftragnehmer vor Aufnahme der Tätigkeit zur Einhaltung der vorliegenden Lieferantenvereinbarung zu verpflichten.

Subcontractors
Any engagement of subcontractors by the Contractor requires the Client's approval, provided that the subcontractor receives or processes the Client's information. A confidentiality agreement (NDA) must be concluded with the subcontractor before the start of the engagement.
Subcontractors approved by the Client must be required by the Contractor to comply with this Supplier Agreement before commencing work.

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

Confidentiality Obligations
The Contractor is obligated to keep the Client's confidential information secret. This obligation is governed by a separate confidentiality agreement (GHV/NDA). Templates for this are available from the Executive Assistant in German or English.

IT-bezogene Regelungen

IT-Related Regulations

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.

Handling of Data Storage Media
Client information may only be stored on encrypted data storage media. If encryption is not technically feasible, access to the information must be secured through other appropriate measures. When data storage media containing client information are decommissioned, they must be securely erased or destroyed in accordance with ISO 21964 at a minimum security level of 4.

Rückgabe und Lösung von Informationen nach Vertragsende
Nach Beendigung der Zusammenarbeit oder auf Aufforderung des Auftraggebers hat der Auftragnehmer sämtliche Informationen und Daten des Auftraggebers, einschließlich vorhandener Kopien, unverzüglich zurückzugeben oder sicher zu löschen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Die Löschung muss so erfolgen, dass eine Wiederherstellung der Informationen ausgeschlossen ist. Auf Verlangen des Auftraggebers ist die vollständige Löschung schriftlich zu bestätigen. Bestehen gesetzliche Aufbewahrungspflichten, sind die betreffenden Informationen weiterhin entsprechend den Anforderungen

Return and Destruction of Information Upon Termination of the Contract
Upon termination of the collaboration or at the Client's request, the Contractor shall immediately return all of the Client's information and data, including any existing copies, or securely destroy them, provided that no statutory retention requirements preclude such action. The deletion must be carried out in such a way that recovery of the information is impossible. Upon the Client's request, the complete deletion must be confirmed in writing. If statutory retention obligations exist, the information in question must continue to be protected in accordance with the requirements of this Agreement and must be deleted upon expiration of the retention obligation.

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!

dieser Vereinbarung zu schützen und nach Ablauf der Aufbewahrungspflicht zu löschen.

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.

Access Control and Passwords

Access to the Client's information at the contractor's premises must be subject to access control. It must be ensured that only those individuals who are working on behalf of the client are granted access to the client's information. Access control must be based on individual user accounts. The principles of least privilege and need-to-know apply.

All user accounts must be protected with complex passwords (a minimum 12-character combination meeting the following 4 criteria: uppercase letter, lowercase letters, numbers, and special characters). When accessing the Client's particularly sensitive information, access must additionally be secured via multifactor authentication (MFA). Passwords must be changed regularly, at least once a year, or immediately if compromised. If MFA is used, regular password changes are not required. Upon the departure of individuals working for the client, the contractor must immediately block their access.

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.

Encryption of Data Transmission

The transmission of the Client's sensitive information must be encrypted (end-to-end encryption). This applies in particular to the transmission of sensitive information via email or file transfer. To ensure secure data exchange, the Client shall provide a solution for secure file sharing as needed.

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.

Protection Against Malware

The Contractor must protect its IT systems against malware through both technical and organizational measures, provided that the Client's information is stored on these systems. The software and systems used for this purpose are automatically updated. The entire data inventory of all systems is regularly scanned for malware.

Schwachstellenmanagement

Der Auftragnehmer stellt sicher, dass alle IT-Systeme und -Komponenten des Auftragnehmers, die im Rahmen der Leistungserbringung für den Auftraggeber

Vulnerability Management

The Contractor shall ensure that all of its IT systems and components used in the provision of services to the Client, on which the Client's information is stored

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!

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.

or through which the Client's information is transmitted, have the latest software and patches installed. Any vulnerabilities discovered in the Contractor's IT systems and components must be addressed immediately through appropriate measures.

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. Eine Multifaktor-Authentifizierung (MFA) ist für Fernzugriffe verpflichtend. Fernzugriffe dürfen durch den Auftragnehmer ausschließlich für die Ausführung konkreter Aufträge genutzt werden.

Remote Access

The Contractor shall ensure that remote access to the Client's IT systems or components is configured on a per-person basis. It must be ensured at all times that any remote access can be unambiguously attributed to a specific individual. Remote access to the Client's IT systems or components shall be granted only to those employees of the Contractor who are working on behalf of the Client. Multi-factor authentication (MFA) is mandatory for remote access. The Contractor may use remote access exclusively for the performance of specific assignments.

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.

Data Backup

The Contractor has implemented a backup and recovery plan for the relevant IT systems, provided that the Contractor stores the Client's information on these systems and is responsible for its storage. The proper functioning of the data backup and the ability to restore data must be verified at regular intervals.

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!

Angaben zum Lieferanten / Supplier Information

Firmenname / Company Name:

Adresse / Address:

Land / Country:

Nachname, Vorname / Surname, Name:

Position:

Telefon / Phone:

E-Mail:

_____ _____

Ort/Place, Datum/Date Unterschrift/Signature

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

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

Dokumentenklassifizierung: ☒ öffentlich, ☐ intern, ☐ vertraulich, ☐ streng vertraulich

Any Reproduction or distribution without permission of IPETRONIK GmbH & Co.KG is prohibited!