PREH GmbH

1. Zweck

Der Zweck dieses Dokumentes ist die Festlegung von Regelungen für die Informationssicherheit, welche von Partnerfirmen beim Umgang mit Informationen von PREH zu befolgen sind.

Die Richtlinie richtet sich an die Geschäftsführung und Mitarbeiter der Partnerfirmen.

2. Zielgruppen

Zielgruppe	Anmerkung
Partnerfirmen (Dienstleister/Lieferanten) mit Zugriff auf Informationen	Bis Kapitel 3.8
Partnerfirmen (Dienstleister/Lieferanten) mit Zugriff auf das IT-System der PREH	Bis Kapitel 4.3

3. Allgemeine Anforderungen

3.1 Klassifikation von Informationen

Wenn die Klassifikation nicht bekannt ist, dann muss die Klassifikation der Informationen bzw. Daten beim Ansprechpartner von PREH angefordert werden. Informationen sind über den Lebenszyklus hinweg entsprechend ihrer Einstufung zu schützen. Die aktuelle Einstufung der Informationen ist durch den Ansprechpartner von PREH zu bestätigen. Die Stufen der Klassifizierung orientiert sich am Whitepaper „Harmonisierung der Klassifizierungsstufen“ des VDA.

3.2 Kennzeichnung und Umgang mit Informationen

Klassifikation	Anforderungen
vertraulich	Kennzeichnung: PREH ist für die Definitionen der Kennzeichnung verantwortlich. Speicherung: verschlüsselt Transport: verschlüsselt (z. B. TLS) Entsorgung: Dokumente im Schredder entsorgen, mind. ISO21964 Sicherheitsstufe 4. Löschung der Daten auf Datenträgern.
Streng vertraulich	Kennzeichnung: Die PREH ist für die Definitionen der Kennzeichnung verantwortlich. Speicherung: verschlüsselt Transport: Ende-zu-Ende-Verschlüsselung Entsorgung: Dokumente persönlich im Schredder entsorgen, mind. ISO21964 Sicherheitsstufe 5 Sichere Löschung der Daten auf Datenträger.

3.3 Kontrolle auf Schadsoftware

Die Partnerfirma muss vor Lieferung bzw. Übertragung der Informationen diese auf Schadsoftware prüfen. Dies hat unter Verwendung aktueller Prüfzyklen und Analysemöglichkeiten zu erfolgen.

Wird bei der Partnerfirma eine Schadsoftware erkannt ist unverzüglich der Ansprechpartner von PREH zu informieren. Des Weiteren ist der Datenträger nicht mehr zu verwenden.

3.4 Backup der Informationen

Informationen sind so zu speichern, dass eine zentrale Datensicherung erfolgen kann. Bei nicht zentraler Speicherung ist der Mitarbeiter der Partnerfirma für die Datensicherung zuständig.

Die Datensicherungen sind zu schützen wie die normalen Informationen.

3.5 Clean Desk

Der Arbeitsplatz ist nach Beendigung der Arbeit sauber zu verlassen. Alle nicht mehr benötigten Dokumente und Informationen von PREH sind in einem abschließbaren Behälter zu verwahren. Es dürfen unberechtigte Dritte keinen Einblick in Dokumente bzw. Informationen von PREH erhalten.

3.6 Zugriffsrechte auf Informationen und Systeme

Zugriffsrechte auf Informationen von PREH sind nach dem Need-to-Know Prinzip zu vergeben. Diese sind regelmäßig zu prüfen und wenn notwendig zu überarbeiten. Zugriffe auf Informationen sind in ausreichender Form abzusichern (z. B. starke Authentifizierung).

3.7 Austausch von Informationen

Alle Datenträger, welche Informationen von PREH enthalten sind vor Verlust, Zerstörung, Manipulation und unberechtigten Zugriff zu schützen. Nicht mehr relevante Datenträger sind nach Standardverfahren (siehe 3.2) zu vernichten.

Der Datenaustausch darf nur über von PREH freigegebenen Datenaustausch-wegen durchgeführt werden. Dazu hat sich die Partnerfirma bei ihrem Ansprechpartner von PREH zu informieren.

Es ist durch die Partnerfirmen sicherzustellen, dass keine unberechtigten Dritten vertrauliche Informationen mithören können oder Einsicht auf diese erhalten. Beim Versand von E-Mails ist der Verteilerkreis auf das nötige Maß einzuschränken.

3.8 Umgang mit Informationssicherheitsvorfällen

Informationssicherheitsvorfälle, welche die Daten oder Systeme von PREH betreffen sind unverzüglich der Sicherheitsorganisation von PREH security@preh.de sowie dem Ansprechpartner von PREH zu melden.

Beispiele für Informationssicherheitsvorfälle sind Hacking, Diebstahl oder Verlust von Informationen von PREH.

3.9 Datenschutz & gesetzliche und vertragliche Anforderungen

Die jeweiligen landesspezifischen Vorgaben und Gesetzte zum Thema Datenschutz sind durch die Partnerfirmen einzuhalten.

Die Partnerfirmen sollte ein Compliance Management führen und in jedem Fall rechtliche und betriebliche Anforderungen umsetzen.

Es ist nur lizenzierte Software einzusetzen. Software darf nur durch autorisiertes Personal installiert werden.

Der Ansprechpartner für das Thema Informationssicherheit ist den Einkauf von PREH mitzuteilen.

Mitarbeiter der Partnerfirma sind zu den Anforderungen von PREH zu schulen. Dazu kann die „Sicherheitsrichtlinie für Partnerfirmen“ mit einbezogen werden.

4 Anforderungen an Partnerfirmen mit direktem Zugang in das Netzwerk von PREH

Die folgenden Anforderungen müssen von Partnerfirmen eingehalten werden, welche einer der aufgelisteten Kategorien zugeordnet sind:

- Partnerfirmen, denen ein Client durch PREH zur Verfügung gestellt wurde.
- Partnerfirmen, die einen Remote-Zugang (z. B. Citrix) oder andere VPN-Lösungen mit direktem Zugriff auf das Netzwerk der PREH besitzen.

Es spielt dabei keine Rolle, ob sich dabei der Mitarbeiter der Partnerfirma auf dem eigenen Gelände befindet oder auf dem Gelände von PREH.

Die Bereitstellung, Installation von Hardware und Software darf nur durch IT-Personal von PREH erfolgen. Die Veränderung von Einstellungen ist nur durch IT-Personal von PREH zulässig. Die Geräte von PREH dürfen nur durch die spezifisches IT-Personal von PREH geöffnet werden.

Auf den Geräten von PREH ist nur mit PREH-Daten zu arbeiten. Die Geräte sind ordentlich zu behandeln und vor Verlust zu schützen.

4.1 Umgang mit Anmeldeinformationen und -medien

Anmeldeinformationen und -medien (z.B. Passwörter, Token) dürfen nicht an unautorisierte Personen weitergeben werden. Wenn der Verdacht der Kompromittierung besteht ist das Kennwort des Accounts unverzüglich zu ändern.

Temporäre Passwörter sind bei erstmaliger Anmeldung zu ändern. Beim Verlassen des Arbeitsplatzes ist der Client zu sperren sowie Token mitzunehmen. Es dürfen nur Passwörter in Abhängigkeit der Klassifikation der verarbeiteten Informationen verwendet werden. Dazu sollten internationale oder nationale Vorgaben und Empfehlungen (z.B. NIST, BSI) berücksichtigt werden.

4.2 Zugriffsrechte auf Informationen und Systeme

Zugriffsrechte auf Systeme von PREH müssen über den Ansprechpartner beantragt werden. Eine Liste mit Mitarbeitern der Partnerfirma, welche Zugriff auf die Systeme erhalten, ist dem Ansprechpartner von PREH auf Nachfrage zur Verfügung zu stellen.

4.3 Zugang zum Netzwerk

IT-Geräte dürfen nur solange mit dem VPN zur PREH verbunden sein, wie sie für die Arbeit notwendig ist. Eine private Internetnutzung ist nicht gestattet.

Die Partnerfirma verpflichtet sich zur Einhaltung der Regelungen dieser Sicherheitsrichtlinie.

Partnerfirma

Ort, Datum

Unterschrift

Name:

Funktion:

Unterschrift

Name:

Funktion: