1 Geltungsbereich

Die Richtlinie richtet sich an die Geschäftsführung und Mitarbeitende der Kooperationspartner.

1.1 Zielgruppen

Zielgruppe	Verbindliche Anforderungen enthalten in:
Freelancer / Dienstleister / Lieferanten mit Zugriff auf Informationen	Kapitel 1-2
Freelancer / Dienstleister / Lieferanten mit Zugriff auf das IT-System von Albert Weber	Kapitel 1-3
Freelancer / Dienstleister / Lieferanten mit Zugriff auf Komponenten und Bauteile von Albert Weber	Kapitel 1-2, 4

1.2 Zweck

Der Zweck dieses Dokumentes ist die Festlegung von Regelungen für die Informationssicherheit, welche von Kooperationspartnern beim Umgang mit Informationen und schutzbedürftigen Komponenten sowie Bauteile zu befolgen sind.

2 Allgemeine Anforderungen

2.1 Klassifikation von Informationen

Die Partnerfirma muss die Klassifikation der Informationen bzw. Daten beim Ansprechpartner von Albert Weber (z.B. Projektleiter) anfordern. Informationen sind über den Lebenszyklus hinweg entsprechend ihrer Einstufung zu schützen. Die aktuelle Einstufung der Informationen ist durch den Ansprechpartner der Albert Weber zu bestätigen. Die Stufen der Klassifizierung orientiert sich am Whitepaper „Harmonisierung der Klassifizierungsstufen“ des VDA.

2.2 Kennzeichnung und Umgang mit Informationen

Klassifikation	Anforderungen
Vertraulich	Kennzeichnung: Der Informationseigentümer ist für die Definitionen der Kennzeichnung verantwortlich. Speicherung: verschlüsselt Transport: verschlüsselt

	Entsorgung: Dokumente im Schredder entsorgen, mind. DIN 66399 Sicherheitsstufe 4. Löschung der Daten auf Datenträgern.
Streng vertraulich	Kennzeichnung: Der Informationseigentümer ist für die Definitionen der Kennzeichnung verantwortlich. Speicherung: verschlüsselt Transport: Ende-zu-Ende- Verschlüsselung Entsorgung: Dokumente persönlich im Schredder entsorgen. mind. DIN 66399 Sicherheitsstufe 5 Sichere Löschung der Daten auf Datenträger.

2.3 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 der Albert Weber zu informieren. Des Weiteren ist der Datenträger nicht mehr zu verwenden.

2.4 Backup der Informationen

Informationen sind so zu speichern das eine zentrale Datensicherung erfolgen kann.

Bei nicht zentraler Speicherung ist der/die Mitarbeiter*in der Partnerfirma für die Datensicherung zuständig.

Die Datensicherungen sind zu schützen wie die darauf gesicherten Informationen.

2.5 Clean Desk

Der Arbeitsplatz ist nach Beendigung der Arbeit sauber zu verlassen. Alle nicht mehr benötigten Dokumente und Informationen der Albert Weber sind in einem abschließbaren Behälter zu verwahren.

Es dürfen unberechtigte keinen Einblick in Dokumente bzw. Informationen von Albert Weber erhalten.

2.6 Zugriffsrechte auf Informationen und Systeme

Zugriffsrechte auf Informationen von Albert Weber 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).

2.7 Austausch von Informationen

Alle Datenträger welche Informationen des Auftraggebers enthalten sind vor Verlust, Zerstörung, Manipulation und unberechtigten Zugriff zu schützen. Nicht mehr relevante Datenträger sind nach Standard Verfahren zu Vernichten.

Der Datenaustausch darf nur über vom Auftraggeber freigegebenen Datenaustauschwegen durchgeführt werden. Dabei hat sich der Zulieferer über diese beim Auftraggeber zu Informieren.

Es ist durch die Kooperationspartner sicherzustellen das keine unberechtigte Person während Gesprächen Zugriff auf Informationen der Stufe vertraulich oder streng vertraulich erhalten.

Der Versand von Ketten E-Mails ist zu unterlassen.

2.8 Umgang mit Informationssicherheitsvorfällen

Informationssicherheitsereignisse, welche die Daten oder Systeme von Weber betreffen sind unverzüglich der Sicherheitsorganisation von Albert Weber Informationssicherheit@a-weber.com sowie der Projektleitung zu melden.

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

2.9 Datenschutz & Gesetzliche und Vertragliche Anforderungen

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

Die Kooperationspartner haben ein Compliance Management zu führen und rechtliche und betriebliche Anforderungen umzusetzen.

Es ist keine nicht Lizenzierte Software einzusetzen. Software darf nur durch autorisiertes Personal installiert werden.

Der Ansprechpartner für das Thema Informationssicherheit ist dem Einkauf Albert Weber mitzuteilen (z.B. in der QSV).

Mitarbeiter*innen der Kooperationspartner sind zu den Anforderungen von Albert Weber zu schulen. Dazu kann diese Sicherheitsrichtlinie mit einbezogen werden.

3 Anforderungen an Kooperationspartner mit direktem Zugang in das Netzwerk der Albert Weber

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

- Kooperationspartner denen ein Client durch die Albert Weber-IT zur Verfügung gestellt wurde.
- Kooperationspartner die einen Remote-Zugang (z.B. Citrix) oder andere VPN-Lösungen mit direktem Zugriff auf das Netzwerk von Albert Weber besitzen.

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

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

Auf den Geräten der Albert Weber ist nur mit Daten von Albert Weber zu arbeiten.

Die Geräte sind ordentlich zu behandeln und vor Verlust zu schützen.

3.1 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 des Schutzbedarfes der verarbeiteten Informationen verwendet werden. Dazu sollten internationale oder nationale Vorgaben und Empfehlungen (z.B. NSIT, BSI) berücksichtigt werden.

3.2 Zugriffsrechte auf Informationen und Systeme

Zugriffsrechte auf Systeme von Albert Weber müssen über den Projektverantwortlichen beantragt werden. Eine Liste mit Mitarbeitern der Kooperationspartner, welche Zugriff auf die Systeme erhalten, ist der Projektleitung von Albert Weber auf Nachfrage zur Verfügung zu stellen.

3.3 Zugang zum Netzwerk

IT-Geräte dürfen nur solange mit dem VPN zum Auftraggeber verbunden sein wie sie für die Arbeit notwendig ist. Direktes Surfen im Internet ist nicht gestattet.

4 Schutz von Komponenten und Bauteile

Die auftraggebende Projektleitung von Albert Weber ist grundsätzlich für die Einstufung der Schutzbedürftigkeit von Komponenten und Bauteilen verantwortlich.

Die Einstufung wird in Abhängigkeit vom potenziellen Schaden für den Endkunden (z.B. OEMs) bzw. für Albert Weber festgelegt. Dabei wird in drei Schutzstufen eingeteilt.

4.1 Schutzstufen

4.1.1 Stufe 1 - normaler Schutzbedarf

Der potenzielle Schaden ist geringfügig, kurzfristiger Natur und auf ein einzelnes Projekt begrenzt. Komponenten und Bauteile mit einem normalen Schutzbedarf müssen mindestens in einem kontrollierten Bereich hergestellt, bearbeitet oder gelagert werden. Diese Bereiche dürfen nicht frei zugänglich sein.

Üblicherweise fallen alle nicht-designrelevanten Komponenten und Bauteile nach SOP (Start of Production) in diese Sicherheitsstufe.

Komponenten und Bauteile mit normalen Schutzbedarf weise keine Kennzeichnung bzgl. Schutzbedarf auf.

4.1.2 Stufe 2 - hoher Schutzbedarf

Der potenzielle Schaden ist beträchtlich oder mittelfristiger Natur oder nicht auf ein einzelnes Projekt begrenzt. Komponenten und Bauteile mit hohem Schutzbedarf müssen mindestens in einem eingeschränkten Bereich hergestellt, bearbeitet oder gelagert werden. Diese Bereiche sind nur einem begrenzten Personenkreis zugänglich.

Üblicherweise fallen alle nicht-designrelevanten Komponenten und Bauteile vor SOP sowie designrelevanten Komponenten und Bauteile nach SOP in diese Stufe.

Komponenten und Bauteile mit hohem Schutzbedarf werden durch einen halbgefüllten Kreis gekennzeichnet (⦿).

4.1.3 Stufe 3 - sehr hoher Schutzbedarf

Der potenzielle Schaden ist für die Albert Weber existenzbedrohend oder langfristiger Natur oder nicht auf ein einzelnes Projekt begrenzt. Komponenten und Bauteile mit einem sehr hohem Schutzbedarf müssen in einem Prototypenbereich hergestellt, bearbeitet oder gelagert werden. Diese Bereiche sind nur einem streng begrenzten Personenkreis zugänglich. Diese Bereiche müssen im Rahmen eines TISAX® Assessments freigegeben werden.

Üblicherweise fallen designrelevante Komponenten und Bauteile vor SOP in diese Sicherheitsstufe.

Komponenten und Bauteile mit sehr hohem Schutzbedarf müssen durch einen ausgefüllten Kreis gekennzeichnet (●).

4.2 Anforderungen an den Schutz von Komponenten und Bauteilen

4.2.1 Physische und umgebungsbezogene Sicherheit für Komponenten und Bauteile der Stufe 3 – sehr hoher Schutz

Diese Maßnahmen sollten in das Sicherheitszonenkonzept der Kooperationspartner aufgenommen werden. Insbesondere müssen folgende Themenfelder betrachtet werden:

Sicht- und Einblickschutz

Der Sicht- und Einblickschutz ist in allen Bereichen zu gewährleisten, in denen designrelevante Komponenten und Bauteile hergestellt, bearbeitet oder gelagert werden. Dies umfasst sowohl relevante Glasflächen als auch Schutzmaßnahmen zur Verhinderung der Einsicht bei geöffneten Türen, Toren oder Fenstern.

Schutz vor unbefugtem Betreten und Kontrolle des Zugangs

Ein Zutrittskonzept für die zu sichernden Bereiche ist zu erstellen, welches die Vergabe der Zugangsrechte regelt und dokumentiert. Dies kann sowohl durch mechanische als auch elektronische Zugangssysteme erfolgen.

Einbruch Überwachung (Einbruch Schutz)

Für Räumlichkeiten, in denen designrelevante Komponenten und Bauteile gelagert werden, wird dringend empfohlen eine funktionsfähige Einbruchmeldeanlage zu installieren. Alternativ zur Einbruchmeldeanlage kann eine Bewachung durch einen Wachdienst erfolgen.

4.2.2 Umgang mit Komponenten und Bauteilen

Transport

Als schutzbedürftig eingestufte Komponenten und Bauteile sind auf dem Transportweg (Land, Wasser, Luft) vor unberechtigter Einsichtnahme, unberechtigter Bildaufzeichnung und Zugriff zu schützen. Alle sicherheitsrelevanten Vorfälle sind über dem zuständigen Projektleiter der Weber zu melden.

Lagerung

Die Lagerung von als schutzbedürftig eingestuften Komponenten und Bauteilen ist nur in geeigneten Örtlichkeiten zulässig. Die Lagerung der schutzbedürftigen Komponenten und Bauteilen muss unter Einhaltung der Trennung von unterschiedlichen Auftraggebern erfolgen.

5 Änderungshistorie

Revision	Ausgabe Datum	Änderungs-beschreibung	Name Ersteller	Geprüft / Freigegeben	
				Name Prozesseigner	Name QM-Experte
A	03.08.21	Erstausgabe	T. Bornträger	Dr. R. Breu E. Wizgall M. Bleimehl M. Pleikies T. Bornträger	T. Bornträger