Richtlinie für Lieferanten

Richtlinie

Version und Datum	**V1.0**
Freigabedatum	**25.03.2024**
Verantwortlicher der Dokumentation	**ISB**
Vertraulichkeitsstufe	**Öffentlich**

Freigabe des Dokumentes

Datum	**Freigabe durch**	**Unterschrift**
09.04.2024	Fabian Ziegler	

Änderungshistorie

Version	**Historie**	**Datum**	**Ersteller**	**Freigabe**
V1	Erstellung	12.02.2024	Marvin Schmidt (ISB)	GF

Dokumentenverteiler

Alle internen Rollen

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

Inhaltsverzeichnis

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,

www.team23.de | **Geschäftsführer** Fabian Ziegler | **Registergericht Augsburg,** USt-IdNr.:DE308873371,

Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Festlegung der Vorschriften für Beziehungen zu Lieferanten und Partnern.

Dieses Dokument gilt für alle Lieferanten und Partner, welche die Fähigkeit zur Beeinflussung der Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen von TEAM23 besitzen.

Anwender dieses Dokuments sind das Top-Management von TEAM23, sowie alle anderweitigen Personen, die bei TEAM23 verantwortlich für Lieferanten und Partner sind.

2. Referenzdokumente

- VDA ISA 5.1 – 6.1 Supplier Relationships
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Informationssicherheitspolitik

3. Betroffene Lieferanten

3.1 Lieferanten und Geschäftsbeziehungen

Unter folgenden Bedingungen werden Lieferanten in Bezug auf Informationssicherheit bewertet und Zusatzvereinbarungen über Informationssicherheit abgeschlossen:

- Zugriff oder Verarbeitung interner Dokumente und Informationen
- Zugriff auf das interne Netzwerk oder die Systeme
- Dauerhafter Zutritt zu den Geschäftsräumen
- Zutrittsberechtigung zu Räumen, in denen sensible Informationen verarbeitet werden
- Wartung, Bereitstellung oder Entwicklung sensibler IT-Systeme oder Dienste
- Wenn die Risikoanalyse ergibt, dass die Lieferantenbeziehung Einfluss auf die Erreichung der Informationssicherheitsziele haben kann.

Folgende Ausnahmen bestehen:

- Erfüllt der Vertrag bzw. die Leistungsbeschreibung mit dem Lieferenten bereits die Sicherheitsanforderungen (Bewertung durch den ISB), muss auf keine Zusatzvereinbarung bestanden werden.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

3.2 IT-Systeme

Die Beschaffung von Standardkomponenten kann ohne separate Lieferantenfreigabe erfolgen. Folgende Mindestanforderung sind hierbei zu beachten:

Kategorien	***Anforderungen***
Serverhardware	- Unterstützung von UEFI und Secure Boot - Netzteilredundanz - Supportvereinbarung (mindestens 3 Jahre vor Ort)
Clienthardware	- Secure Boot - Unterstützung Bitlocker
Peripherie-Geräte	- Erfüllung der spezifischen gesetzlichen Regularien

4. Beauftragung von Lieferanten

Die Beauftragung eines Lieferanten, der unter die hier definierten Kriterien für betroffene Geschäftspartner fällt, erfolgt grundsätzlich erst nach Freigabe durch den ISB.

Je nach Tätigkeit wird der Lieferant auf eine Geheimhaltungsvereinbarung (NDA) und die Zusatzvereinbarung mit Lieferanten verpflichtet.

Die Lieferanten werden im ISMS bewertet, welche Anforderungen an sie in Bezug auf die Informationssicherheit gestellt werden (normal, hoch oder sehr hoch).

Für die Freigabe ist jeweils eine Risikobewertung durchzuführen, die die Risiken durch die Nutzung des Dienstleisters wie folgt kategorisiert:

- **Normal:** Die Sicherheitsmaßnahmen des Lieferanten sind dem Schutzbedarf der zu verarbeitenden Informationen bzw. der bereitgestellten Systeme angemessen.
- **Hoch:** Die Sicherheitsmaßnahmen des Lieferanten sind angemessen, jedoch fehlen einige Elemente (z.B. funktionierendes ISMS, Auskünfte über Sicherheitsmaßnahmen oder der Vertrag enthält einige Komponenten nicht).
- **Sehr hoch:** Es ist nicht erkennbar, dass die Sicherheitsmaßnahmen des Lieferanten angemessen für das angestrebte Schutzniveau sind.

Unser Unternehmen akzeptiert maximal die Risikoeinstufung „Hoch“.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

Liegt das Risiko mit dem Lieferanten über diesem Niveau, werden risikomindernde Maßnahmen implementiert und auf Basis dessen eine neue Bewertung durchgeführt. Hierzu gehören:

- Nachbesserung des Vertrags
- Bestimmung von Zusatzvereinbarung oder Vertragsstrafen
- Durchführung von Lieferantenaudits, um kritische Bereiche und die Einhaltung getroffener Regeln zu prüfen
- Bereitstellung von Zertifikaten zum Nachweis eines Informationssicherheitsmanagementsystems

Die abzuschließenden Zusatzvereinbarungen müssen wenigstens den Mindestanforderungen aus diesem Dokument entsprechen.

Alternativ wird der vom Lieferanten bereitgestellte Vertrag durch den ISB auf diese Anforderungen geprüft.

Die Freigabe des Lieferanten wird durch den ISB dokumentiert und kommuniziert.

5. Überprüfung von Lieferanten

Die Risikobewertung aller Lieferanten wird regelmäßig wiederholt und überprüft.

Wird als risikominimierende Maßnahme ein Lieferantenaudit definiert, ist dies mindestens jährlich im Rahmen des regulären Auditprogramms einzuplanen und durchzuführen.

6. Mindestanforderungen an Verträge

Sollte es keine Vereinbarung geben wird die Dokumentvorlage "Zusatzvereinbarung mit Lieferanten" genutzt. Diese stellt einen umfassenden Vertrag dar.

7. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab 25.03.2024

Der Eigentümer des Dokuments ist der ISB, der das Dokument mindestens einmal jährlich prüft und gegebenenfalls aktualisiert.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX