Informationssicherheitspolitik

Informationssicherheitsleitlinie

Version und Datum	**V1.1**
Freigabedatum	**26.03.2024**
Verantwortlicher der Dokumentation	**Marvin Schmidt (ISB)**
Vertraulichkeitsstufe	**Öffentlich**

Freigabe des Dokumentes

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

Änderungshistorie

Version	**Historie**	**Datum**	**Ersteller**	**Freigabe**
V1	Erstellung	09.01.2022	Tobias Riede	GF
V1	Überarbeitung	26.03.2024	Marvin Schmidt	GF

Dokumentenverteiler

Berechtigte Rolle (Verteilerkreis)
Keine Einschränkung

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. Vorwort

TEAM23 ist auf IT-gestützte Prozesse angewiesen. In dieser Situation ist es unerlässlich die Informationssicherheit zu gewährleisten, um die nötige Zuverlässigkeit im geschäftlichen Alltag zu schaffen.

Bei TEAM23 ist die Informationssicherheit somit ein essenzieller Teil in unserem Wachstum, der uns ermöglicht, unseren bestehenden Weg zur ständigen Weiterentwicklung unseres Unternehmens zu gehen. Die Beziehung zu unseren Kunden wird gefördert und der vertrauliche Umgang mit deren Informationen und Daten gewährleistet. Darüber hinaus werden unsere Prozesse geschärft, dokumentiert und tragen so zu deren allgegenwärtigen Verfügbarkeit bei.

2. Zweck, Anwendungsbereich und Anwender

Zielsetzung dieser auf oberster Ebene angesiedelten Politik ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für Informationssicherheits-Management.

Diese Politik wird auf das gesamte Informationssicherheits-Managementsystem (ISMS) angewendet, und wie im Dokument zum ISMS Anwendungsbereich definiert. Sie orientiert sich an TISAX.

Anwender dieses Dokuments sind alle Mitarbeiter von TEAM23, sowie relevante externe Parteien.

3. Referenzdokumente

- ISO/IEC 27001 Norm – A.5.1
- TISAX Norm – 1.1.1
- Dokument zum ISMS Anwendungsbereich
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Erklärung zur Anwendbarkeit
- Liste rechtlicher, amtlicher, vertraglicher und anderer Anforderungen
- Verfahren zum Management von Informationssicherheits-Vorfällen

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

4. Informationssicherheit: Grundbegriffe

Vertraulichkeit – die Eigenschaft von Informationen, dass sie lediglich berechtigten Personen oder Systemen verfügbar gemacht werden

Integrität – die Eigenschaft von Informationen, dass sie lediglich von berechtigten Personen oder Systemen auf genehmigte Weise abgeändert werden können

Verfügbarkeit – die Eigenschaft von Informationen, dass sie lediglich berechtigten Personen zugänglich sind, wenn ein solcher Zugang notwendig ist

Informationssicherheit - Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

Informationssicherheits-Managementsystem – jener Teil des gesamten Managementprozesses, der sich mit Planung, Implementierung, Instandhaltung, Überprüfung und Verbesserung von Informationssicherheit befasst

5. Verwaltung der Informationssicherheit

5.1 Zielvorgaben und Messung

Die generellen Zielvorgaben des Informationssicherheits-Managementsystems sind die folgenden: Verbesserung des Images im Markt sowie eine Reduktion der Schäden durch potentielle Vorfälle. Diese Ziele stimmen mit den Geschäftszielen, der Strategie und den Geschäftsplänen der Organisation überein. Die Geschäftsleitung ist für die Überprüfung dieser generellen ISMS Zielvorgaben und für die Definition neuer Zielvorgaben verantwortlich.

Maßnahmenziele für einzelne Sicherheitsmaßnahmen oder Gruppen von Sicherheits-maßnahmen werden von Informationssicherheitsbeauftragten und/ oder durch das ISMS-Projektteam vorgeschlagen und von der Geschäftsleitung im Rahmen der Erklärung zur Anwendbarkeit genehmigt.

Alle diese Zielvorgaben müssen mindestens einmal jährlich überprüft werden.

TEAM23 bewertet und misst die Erfüllung dieser Zielvorgaben. Die Geschäftsleitung ist verantwortlich für die Festlegung der Methode, mit der die Erfüllung dieser Zielvorgaben gemessen wird. Die Bewertung/Messung wird mindestens einmal jährlich durchgeführt und durch den Informationssicherheitsbeauftragten und durch das ISMS-Projektteam analysiert und evaluiert die Messresultate und berichtet anschließend an die Geschäftsleitung in der Form von Input-Materialien für die Managementbewertung. Der Informations-sicherheitsbeauftragte ist dafür verantwortlich, die Details zu Messmethoden, Periodizitäten und Ergebnissen im Messbericht zu speichern.

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

5.2 Anforderungen an Informationssicherheit

Diese Informationssicherheitspolitik und das gesamte ISMS müssen sowohl den rechtlichen und gesetzlichen Anforderungen, als auch den vertraglichen Verpflichtungen entsprechen, die für die Organisation auf dem Gebiet der Informationssicherheit maßgeblich sind.

Eine detaillierte Auflistung aller vertraglichen und rechtlichen Anforderungen wird mit der Liste der rechtlichen, amtlichen und vertraglichen Verpflichtungen bereitgestellt.

5.3 Maßnahmen zur Informationssicherheit

Der Prozess bei der Auswahl von Maßnahmen (Sicherheitsmaßnahmen) ist der Methodik zur Risikoeinschätzung und Risikobehandlung definiert.

Die gewählten Maßnahmen und deren Implementierungs-Status sind in der Erklärung zur Anwendbarkeit aufgeführt.

5.4 Verantwortlichkeiten

Folgendes sind die grundsätzlichen Verantwortlichkeiten für das ISMS:

- Die Geschäftsführung ist dafür verantwortlich, sicherzustellen dass das ISMS entsprechend dieser Richtlinie umgesetzt und instandgehalten wird und dass alle notwendigen Ressourcen verfügbar sind.
- Der Informationssicherheitsbeauftragte/ ISMS-Projektteam sind für die Koordination des Betriebs des ISMS verantwortlich, sowie für die Berichterstattung über dessen Leistungsfähigkeit.
- Die Geschäftsführung muss das ISMS mindestens einmal jährlich überprüfen (bzw. immer im Falle von erheblichen Änderungen) und ein Protokoll dazu erstellen. Zweck dieser Überprüfung durch das Management ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.
- Der Informationssicherheitsbeauftragte/ ISMS-Projektteam sind ist für die Umsetzung von Informationssicherheits-Training und Programmen zur Bewusstseinsbildung (Awareness) für Mitarbeiter zuständig.
- Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit der Werte unterliegt der Verantwortung des Eigentümers der jeweiligen Werte.
- Alle Sicherheitsvorfälle oder Schwachstellen müssen an den Informationssicherheitsbeauftragten gemeldet werden. Sollten personenbezogene Daten betroffen sein, ist der Datenschutzbeauftrage zu involvieren.

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

- Der Informationssicherheitsbeauftragte/ ISMS-Projektteam definieren, welche sich auf Informationssicherheit beziehenden Informationen mit welchen (sowohl internen als auch externen) interessierten Parteien kommuniziert werden, durch wen und wann.
- Der Informationssicherheitsbeauftragte/ ISMS-Projektteam sind für die Aufstellung und Implementierung des Plans für Training und Awareness verantwortlich, dem alle Personen unterliegen, die eine Rolle im Informationssicherheits-Management inne haben.
- Die Führungskräfte Leben einer Vorbildrolle, um Informationssicherheit gegenüber Mitarbeitern förderlich zu kommunizieren. Diese leiten den Informationssicherheitsbeauftragten Verbesserungsvorschläge zu und Sie beziehen den Informationssicherheitsbeauftragten bei Veränderungen ein.
- Der Datenschutzbeauftragter bezieht den Informationssicherheitsbeauftragte ISB bei Änderungen oder Vorfällen ein sofern die Informationssicherheit betroffen ist
- Alle Mitarbeiter melden Informationssicherheitsvorfälle an den Informationssicherheitsbeauftragten und halten alle vorgeschriebenen Prozesse und Richtlinien ein.

5.5 Politik-Kommunikation

Der Informationssicherheitsbeauftragter hat sicherzustellen, dass alle Mitarbeiter von TEAM23 sowie entsprechende externe Parteien mit dieser Politik vertraut sind.

6. Unterstützung der ISMS Umsetzung

Hiermit erklärt die Geschäftsleitung, dass die ISMS Implementierung und deren kontinuierliche Weiterverbesserung mit geeigneten Ressourcen unterstützt werden, um alle in dieser Politik genannten Zielvorgaben zu erfüllen.

7. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab 26.03.2024

Der Eigentümer des Dokuments ist der Informationssicherheitsbeauftragte der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- Anzahl von Mitarbeitern und externen Parteien mit einer Funktion im ISMS, denen dieses Dokument nicht bekannt ist

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

- Mangelnde Übereinstimmung des ISMS mit Gesetzen und Vorschriften, vertraglichen Verpflichtungen und anderen internen Dokumenten der Organisation
- Mängel in Umsetzung und Aufrechterhaltung des ISMS
- Unklare Verantwortlichkeiten für die Umsetzung des ISM

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