Dokumentenverwaltung

Aktuelle Version	1.3
Letzte DMS-Version	1.3
Freigabestatus	freigegeben

Änderungshistorie

Version	Datum	Kommentar	Autor (Kürzel)
1.0	20.10.2025	Erstellung	pejo
1.1	28.11.2025	Überarbeitung und Ergänzung	pejo/Ft
1.2	04.12.2025	Korrektur und Ergänzung	pejo/TPM/Ma
1.3	25.03.2026	Anpassungen Stauferwerk	pejo

Zielgruppen der Richtlinie

Zielgruppe	zuständig	Art der Bestätigung
Auftragnehmer	Einkauf & Materialwirtschaft	Bestandteil der Bestellung, gültig ohne Widerspruch
Dienstleister	Einkauf & Materialwirtschaft	Bestandteil der Bestellung, gültig ohne Widerspruch
Sonstige Akteure	Informationssicherheitsbeauftragter	Information – Überwachung der Umsetzung – ggf. Anpassung

Inhalt

1. Grundlagen 3
2. Präambel....3
3. Geltungsbereich 3
4. Definitionen....4
4.1 Informationswerte....4
4.2 Sicherheitsmaßnahmen 6
5. Pflichten des Auftragnehmers 6
5.1 Vertraulichkeit und Weitergabe 6
5.2 Beendigung des Vertragsverhältnisses: Rückgabe und Löschen von Werten 7
5.3 Sicherer Datenaustausch 7
5.4 Einhaltung von Gesetzen und Vorschriften 7
5.5 Datenschutz 7
5.6 Meldepflichten des Auftragnehmers und Meldewege....8
6. Zutrittskontrollen und Sicherheitszonen 8
7. Privilegierte Zugangs- und Zugriffsrechte auf IT-Systeme 8
8. Weitere Regelungen für schutzbedürftige Werte....9
8.1 Regelungen für Besitzer von Schließberechtigungen 9
8.2 Regelungen für die Entsorgung 10
8.3 Regelungen für den Transport 10
8.4 Regelungen zur Beschaffung von TK & EDV-Systemen....10
8.5 Regelungen zur Reparatur und Wartung außer Haus 10
9. Überprüfungsrecht zur Einhaltung von Sicherheitsvorgaben 11

1. Grundlagen

Die gesetzlichen Anforderungen für diese Richtlinie ergeben sich aus:

- IT-Sicherheitsgesetz
- Energiewirtschaftsgesetz – EnWG
- DSGVO, BDSG, LDSG, EU Data-Act, AI-Act, CRA, ...

In Verbindung mit den folgenden regulatorischen Anforderungen:

- IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG
- DIN ISO/IEC 27001/27002
- DIN ISO/IEC 27019

In ihrer jeweils geltenden Fassung.

2. Präambel

Die **Stauferwerk GmbH & Co. KG** (im Folgenden **Auftraggeber** genannt) betreibt ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001.

In seiner Sicherheitsrichtlinie hat der Auftraggeber seine Informationssicherheits-Politik und -Ziele festgelegt. Die Sicherheitsrichtlinie wird auf Anfrage vom Auftraggeber zur Verfügung gestellt.

Bei Rückfragen zu dieser Richtlinie oder zum ISMS im Allgemeinen, wenden sie sich an den Informationssicherheitsbeauftragten. – **isb@stauferwerk.de**

3. Geltungsbereich

Diese Sicherheitsrichtlinie gilt für alle Rechtsgeschäfte des Auftraggebers mit seinen Vertragspartnern, Lieferanten, Dienstleistern, sowie deren Subdienstleistern (nachstehend **Auftragnehmer** genannt). Sie umfasst Mitarbeiter, Repräsentanten, Nachunternehmer und Vertriebspartner, sowie andere zugehörige Organe des Auftragnehmers.

Diese allgemeine Sicherheitsrichtlinie ist **Bestandteil einer vertraglichen Vereinbarung** (z.B. Einzelvertrag, Rahmenvertrag) mit dem Auftragnehmer und hat im Falle von Abweichungen und Widersprüchen gegenüber den Einkaufsbedingungen des Auftraggebers Vorrang, sofern sie vor Vertragsschluss übermittelt/zugänglich gemacht wird.

Sie kann durch zusätzliche spezifische Sicherheitsrichtlinien in den Verträgen oder Service-Level-Agreements (SLA) durch den Auftraggeber ergänzt werden, die ihrerseits im Fall von Abweichungen und Widersprüchen Vorrang haben.

4. Definitionen

4.1 Informationswerte

Die Informationssicherheit zielt auf den Schutz von Informationen ab, die in Telekommunikations- und elektronischen Datenverarbeitungssystemen (TK & IT-Systeme) verarbeitet, gespeichert oder übertragen werden.

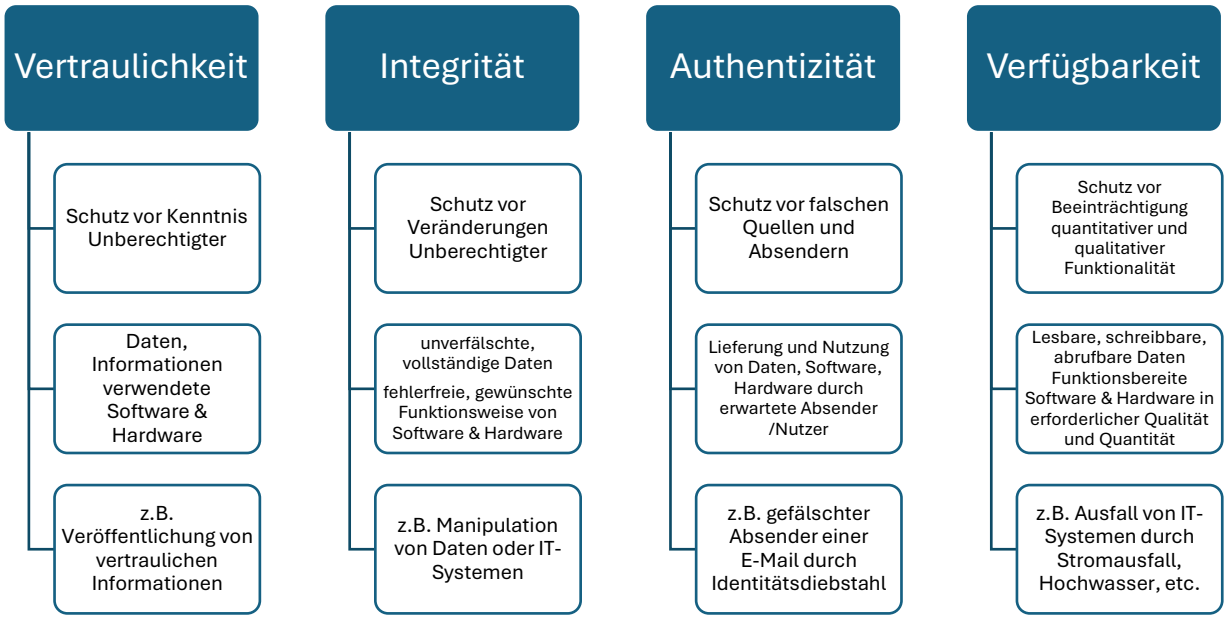


Abbildung 1: aus Hampe, Liane – Schutzbedarfsfeststellung der Schlüssel zum effizienten ISMS - xmera.de

Eine Schutzbedürftigkeit entsteht für alle relevanten Informationen – das hat Auswirkungen auf die Prozesse, Anwendungen, Systeme, Hardware und die Standorte, sowie die dafür eingesetzten Dienstleister.

Beim Auftraggeber als kritische Infrastruktur KRITIS, sind neben den abgebildeten Werten auch physische Anlagen, die eine Relevanz für die Netzführung haben betroffen.

Sicherheitsrichtlinien sind darauf ausgerichtet Werte zu schützen, indem sie Regelungen beinhalten, die auf vier Schutzziele der Informationssicherheit abzielen:



Die Klassifikation von Informationswerten wird in drei Kategorien vorgenommen:

- öffentlich: Weitergabe an jeden Empfänger möglich.
- intern: Weitergabe an alle internen und externen Mitarbeiter des Auftragnehmers.
- vertraulich: Personenkreis, der mit einem Auftrag, Projekt durch den Auftragnehmer betraut ist und notwendigerweise über die Informationen Kenntnis besitzen muss

Nicht klassifizierte Informationswerte, von denen der Auftragnehmer im Rahmen seiner Tätigkeit für den Auftraggeber Kenntnis erlangt, sind ebenfalls **vertraulich** zu behandeln.

Dokumente, welche der Auftragnehmer für den Auftraggeber erstellt, sind in Absprache mit dem Auftraggeber zu klassifizieren, sowie mit Datum und Version zu kennzeichnen.

4.2 Sicherheitsmaßnahmen

Sicherheitsmaßnahmen müssen den **Stand der Technik** einhalten. Der Auftragnehmer entscheidet über die Auswahl von Sicherheitsmaßnahmen, soweit keine konkreten Vorgaben, z.B. in Service-Level-Agreements, etc. bestimmt sind.

Es können z.B. folgende Quellen für den Stand der Technik herangezogen werden:

- Stand der Technik-Kataloge (z.B. BDEW, Teletrust, ...)
- ISO-Guidelines zu Informationssicherheitsmaßnahmen (z.B. ISO/IEC 27002, ...)
- BSI IT-Grundschutzkataloge

In ihrer jeweils aktuellen Fassung.

Sicherheitsmaßnahmen sind **angemessen**, wenn der technische und wirtschaftliche Aufwand nicht außer Verhältnis zu den Folgen einer Störung der Verfügbarkeit steht.

Sicherheitsmaßnahmen sind objektiv nachzuweisen und zu dokumentieren zum Beispiel durch Richtlinie, Verfahrensbeschreibungen, Arbeitsanweisungen, Protokolle etc.

Die Wirksamkeit der getroffenen Maßnahmen ist regelmäßig zu überprüfen und muss dem Zweck nach angemessen sein.

5. Pflichten des Auftragnehmers

Der Auftragnehmer sorgt innerhalb seines Unternehmens bei internen und externen Mitarbeitern für die **Kenntnis** und **Einhaltung** relevanter Inhalte dieser und ggf. weiterer vereinbarter Richtlinien. Bei Unsicherheit über die korrekte Anwendung obliegt es dem Auftragnehmer sich beim Auftraggeber zu informieren.

Der Auftragnehmer setzt einen **Ansprechpartner für Informationssicherheit** ein, der auf Anfrage an Werktagen zu den Geschäftszeiten des Auftragnehmers (Mo-Fr) unverzüglich über Maßnahmen zur Einhaltung dieser Sicherheitsrichtlinie Auskunft geben kann. Der Auftragnehmer hat für eine Vertretung zu sorgen.

Sub-Regel: Der Auftragnehmer ist verantwortlich für die Einhaltung dieser Sicherheitsrichtlinie auch bei von ihm eingesetzten Subdienstleistern.

Kosten im Zuge der Einhaltung dieser Sicherheitsrichtlinie trägt der Auftragnehmer.

5.1 Vertraulichkeit und Weitergabe

Der Auftragnehmer hat alle Informationswerte, die ihm vom Auftraggeber zur Verfügung gestellt werden, von denen er Kenntnis erlangt oder er für den Auftraggeber erstellt **vertraulich** zu behandeln unabhängig davon, ob diese gekennzeichnet sind.

Er muss Maßnahmen ergreifen, dass die Informationswerte des Auftraggebers, Dritten nicht zugänglich sind. Eine Weitergabe der Informationswerte an Dritte ist zustimmungspflichtig und

darf nur nach Genehmigung durch den Auftraggeber erfolgen. Dritte können auch Mitarbeiter des Auftragnehmers sein, die nicht notwendigerweise über diese Informationen verfügen müssen.

Der Auftragnehmer hat sicherzustellen, dass Informationswerte des Auftraggebers nur für vertragsgemäße Zwecke genutzt, vervielfältigt, gespeichert und weitergegeben werden.

Diese Pflichten bestehen auch **nach Beendigung** des Vertragsverhältnisses weiter.

Bei Bedarf werden erweiterte Geheimhaltungsvereinbarungen (NDA) geschlossen.

5.2 Beendigung des Vertragsverhältnisses: Rückgabe und Löschen von Werten

Vom Auftraggeber erhaltene Unterlagen und Werte (z.B. Schlüssel) sind nach Beendigung des Auftrages unverzüglich zurückzugeben.

Die Rückgabe ist zu dokumentieren.

Der Auftragnehmer sorgt für eine geregelte und vollumfängliche Übergabe der Arbeitsergebnisse, d.h. er übergibt relevante Daten, z.B. Dokumente, Skripte, Konfigurationsdateien etc. und dokumentiert diese angemessen.

Alle schutzbedürftigen Informationswerte mit direktem Bezug zum Auftraggeber, die der Auftragnehmer auf seinen IT-Systemen gespeichert hat oder aufbewahrt sind sicher zu löschen bzw. sicher zu vernichten, soweit keine Genehmigung einer dauerhaften Speicherung/Aufbewahrung durch den Auftraggeber erteilt wurde. Als sichere Löschverfahren gelten die vom Bundesamt für Sicherheit in der Informationstechnik als sicher eingestuften Verfahren.

Der Auftragnehmer weist auf Risiken der Vernichtung von Informationswerten hin. Der Auftragnehmer ist verpflichtet, die Vernichtung oder Löschung schriftlich zu bestätigen.

5.3 Sicherer Datenaustausch

Für den sicheren Datenaustausch ist eine durch den Auftraggeber zur Verfügung gestellte Plattform zu verwenden. Die übertragenen Daten sind zu verschlüsseln.

5.4 Einhaltung von Gesetzen und Vorschriften

Der Auftragnehmer hat die gesetzlichen Bestimmungen und Vorschriften, die im Zuge seiner Dienstleistung relevant sind einzuhalten. Hierzu gehören z.B. Datenschutz, Arbeitsschutzgesetze, Urheberrecht und der Schutz geistigen Eigentums.

5.5 Datenschutz

Ansprechpartner für die folgende Regelung ist der Datenschutzbeauftragte des Auftraggebers (Erich Zimmermann - e.zimmermann@zida-gmbh.de).

Der Auftragnehmer hat die gesetzlichen Bestimmungen zum Datenschutz einzuhalten.

5.6 Meldepflichten des Auftragnehmers und Meldewege

Zertifizierungsnachweise: Der Auftragnehmer hat den Verlust oder die Aussetzung von sicherheitsrelevanten Zertifizierungen unverzüglich schriftlich gegenüber dem Auftraggeber anzuzeigen, sofern der Geltungsbereich des jeweiligen Zertifikats in die Leistungserbringung für den Auftragnehmer involviert ist.

Meldung von Informationssicherheits-Ereignissen: Der Auftragnehmer hat Ereignisse, die im Zusammenhang mit seiner Dienstleistung für den Auftraggeber stehen, unverzüglich zu melden. Ereignisse und Umstände sind zu dokumentieren.

Die Meldung erfolgt gegenüber dem Informationssicherheitsbeauftragten des Auftraggebers. Unter **isb@stauferwerk.de**.

6. Zutrittskontrollen und Sicherheitszonen

Es ist vor bzw. mit Betreten eines Gebäudes das vorherige Anmelden beim Besuchsempfänger und im Kundenzentrum notwendig. In bestimmten Sicherheitszonen kann das Fotografieren oder das Mitbringen tragbarer IT-Systeme, Mobiltelefone, Kameras eingeschränkt oder untersagt werden.

Sicherheitszonen dürfen nur in Begleitung einer Aufsichtsperson betreten werden.

7. Privilegierte Zugangs- und Zugriffsrechte auf IT-Systeme

Sind zur Erfüllung des Auftrags durch den Auftragnehmer Administrationsrechte notwendig, müssen diese beantragt, begründet und der benötigte Zeitraum bestimmt werden. Der Auftragnehmer hat anzuzeigen, wenn die Rechte nicht mehr benötigt werden. Administrationsrechte sind personengebunden und dürfen ausschließlich von der berechtigen Person zur Erbringung der vertraglichen Leistung genutzt werden.

Passwörter dürfen nur der berechtigten Person bekannt sein. Soweit systemtechnisch möglich sind Initialpasswörter unverzüglich zu ändern.

Dem Auftragnehmer ist es untersagt nicht explizit freigegebene **Hardware und Software** mit IT-Systemen des Auftraggebers zu verbinden.

Ist der Betrieb von Hard- und Software für die Erfüllung des Auftrages notwendig, ist zuvor eine Genehmigung bei der IT-Abteilung des Auftraggebers einzuholen und zu begründen. Wichtige Voraussetzung zur Erteilung der Genehmigung können der Nachweis der Nutzung eines Virenschutzsystems mit aktueller Virensignaturdatenbank sowie ein Patchmanagement-Prozess des Auftragnehmers sein, der gewährleistet, dass auf eingesetzter Hardware korrekt lizenzierte

Software und regelmäßig aktualisierte Sicherheits-Patches für die Betriebssystem-Software und Anwendungen (z.B. Browser) installiert sind.

Soweit der Auftragnehmer IT-Systeme, Anwendungen oder Komponenten des Auftraggebers **konfiguriert, wartet, parametriert** hat er sicherzustellen, dass der Datenstand vor seinem Eingriff wieder hergestellt werden kann.

Dokumentiert werden muss mindestens:

- Umfang und Zweck des Eingriffes
- Name des Ausführenden, Datum, Uhrzeit
- Risikobehaftete Einstellungen (Nutzen, Schadensfolgen, genehmigender Mitarbeiter des Auftraggebers)

Remote-Access-Anbindungen sind untersagt. Unter Remote-Access Anbindungen fallen Methoden, welche Zugang auf IT-Systeme des Auftraggebers über Netzwerke ermöglichen und dabei Übertragungsstrecken Dritter verwenden (z.B. öffentliche Netzwerke, GPRS etc.).

Sind zur Erfüllung des Auftrags durch den Auftragnehmer Remote-Access Anbindungen notwendig, müssen diese genehmigt, begründet und eine sichere Anbindung gewährleistet werden. Die Nutzung genehmigter Remote-Access-Zugänge ist durch den Auftragnehmer vor jedem Einsatz unter Nennung des Zweckes und des Mitarbeiternamens des Auftragnehmers anzuzeigen. Der Lösungsweg wird durch die IT-Abteilung des Auftraggebers vorgegeben.

8. Weitere Regelungen für schutzbedürftige Werte

8.1 Regelungen für Besitzer von Schließberechtigungen

Unter Schließberechtigungen sind Zutrittsrechte zu verstehen, die es dem Auftragnehmer erlauben sich Zutritt zu Flächen, Gebäuden und Räumen zu verschaffen und sich dort unbeaufsichtigt aufzuhalten. Für Besitzer von Zutrittsmitteln für Türschließsysteme, wie z.B. Schlüssel, Transponder, Mitarbeiterausweise, mechatronische Schlüssel usw. ist zu beachten:

- Zutrittsmittel müssen sicher verwahrt werden, damit diese nicht von anderen Personen genutzt werden können.
- Der Verlust ist unverzüglich gegenüber dem Auftraggeber anzuzeigen.
- Zutrittsrechte sind personengebunden und dürfen nur von der berechtigten Person eingesetzt werden.
- Die Mitnahme anderer Personen ist nur nach Erlaubnis durch den Auftraggeber gestattet.
- Zutrittsrechte dürfen nur für die Erfüllung der vertraglichen Dienstleistung genutzt werden.
- Die Nichtbeachtung dieser Regeln kann zu einem vorübergehenden oder dauerhaften Entzug der Zutrittsmittel führen.

8.2 Regelungen für die Entsorgung

Mit „Entsorgung“ ist jegliche Art Außerbetriebsetzung gemeint, insbesondere auch die Nutzung in anderen Kontexten, z.B. Aufbereitung (Refurbishing), Verkauf an Dritte, Entsorgung auf Mülldeponien und Wertstoffhöfen etc.

Der Auftragnehmer hat schutzbedürftige Werte nur nach Einholung einer schriftlichen Erlaubnis des Auftraggebers zu entsorgen, hierunter fallen z.B. ausgedruckte Informationswerte, insbesondere alle IT-Systeme mit Speichermedien verschiedenster Art. Jegliche Art der Entsorgung muss entsprechend der Art des schutzbedürftigen Wertes angemessene Vorkehrungen treffen, die verhindert, dass Unberechtigte Kenntnis von Daten und Informationen des Auftraggebers erlangen können.

Das gilt auch für IT-, Cloud- oder KI-Dienstleister des Auftragnehmers, bei denen die Daten des Auftraggebers gespeichert werden.

8.3 Regelungen für den Transport

Unter Transport ist jegliche örtliche Veränderung, auch die Übertragung von Daten gemeint, z.B. außerhalb von Betriebsgeländen oder aus definierten Schutzzonen heraus. Der Auftragnehmer hat mindestens angemessene Vorkehrungen gegen Diebstahl, Beschädigung und Manipulation zu treffen. Soweit die Bereitstellung von Transportbehältnissen nicht in seinem Auftragsumfang enthalten ist, hat er dies vom Auftraggeber einzufordern bzw. nicht seinen Ansprüchen genügende Umstände bestätigen zu lassen.

Der Auftragnehmer hat ferner zu dokumentieren, wann er den Wert, von wem und in welcher Verpackungsform erhalten hat, sowie wer diesen transportiert und wann der Empfänger diesen erhalten hat (z.B. auf Reparaturauftrag, Begleitzettel, Versandschein etc.).

Daten sind grundsätzlich in EU-Ländern zu verarbeiten und dürfen nicht in Drittländer (z.B. USA, China, Indien) übertragen werden. Der Standort des Datenverarbeitungssystems ist dem Auftraggeber bekanntzugeben.

8.4 Regelungen zur Beschaffung von TK & EDV-Systemen

Soweit der Auftragnehmer TK & EDV-Systeme beschafft, können weitere Regelungen vereinbart werden.

8.5 Regelungen zur Reparatur und Wartung außer Haus

Soweit der Auftragnehmer schutzbedürftige Werte außerhalb der Betriebsstätten des Auftraggebers repariert, können weitere Regelungen vereinbart werden.

9. Überprüfungsrecht zur Einhaltung von Sicherheitsvorgaben

Der Auftraggeber darf die Einhaltung dieser Sicherheitsrichtlinie sowie ggf. weiterer vereinbarter Sicherheitsvorgaben an allen Betriebsstätten des Auftragnehmers und von Subunternehmern des Auftragnehmers überprüfen, die in die Leistungserbringung einbezogen sind.

Ziel von Überprüfungen ist, die Feststellung inwieweit vom Auftraggeber Sicherheitsvorgaben in vereinbarten Informationssicherheitsrichtlinien des Auftraggebers umsetzen.

Rahmenbedingungen von Überprüfungen sind:

- vom Auftraggeber zu **begründen**
- außerhalb der Betriebsstätten des Auftragnehmers anzumelden
- dürfen nicht außer **Verhältnis** zwischen Nutzen und Aufwand sein
- müssen dem Schutzbedarf der an der Leistungserbringung beteiligten schutzbedürftigen Werte berücksichtigen
- dürfen Geschäftsprozesse des Auftragnehmers oder von Subunternehmen nicht beeinträchtigen.

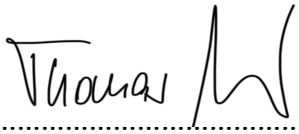
Häufigkeit: Überprüfungen können einmal pro Jahr bzw. aus besonderem Anlass auch öfters erfolgen.

Methoden zur Überprüfung der angemessenen Auswahl und wirksamen Umsetzung von Sicherheitsmaßnahmen können sein:

- Abfrage von entsprechenden Zertifizierungen ISO 27001 oder vergleichbar
- Besichtigung von Betriebsstätten des Auftragnehmers
- Befragung von Mitarbeitern, die in die Leistungserstellung für den Auftraggeber eingebunden sind.
- Erhebung einer Selbstauskunft per Fragebogen zum Anwendungsgrad von Sicherheitsmaßnahmen i.S. des Anhang A, DIN ISO/IEC 27001.
- Einblick in interne Richtlinien, externe Auditberichte von Zertifizierungsgesellschaften bzw. vom externen Auditor unterzeichnete relevante Auszüge davon.
- Softwareanbieter haben ein digitales Software-Bill-of-Materials (SBOM) bereitzustellen, welches der Auftraggeber in automatisierten Systemen zum Schwachstellenmanagement verarbeiten darf

Freigegeben durch die Geschäftsführung der Stauferwerk GmbH & Co. KG:

Geislingen, 25.03.2026



.....

Für die Stauferwerk GmbH & Co. KG – Thomas Peter Müller