

Informationssicherheitsrichtlinie für Rahmenvertragspartner der Thüga Aktiengesellschaft

Inhaltsverzeichnis

1.	Einleitung	2
2.	Informationssicherheitsanforderungen an Externe.....	2
2.1	Grundlegende Sicherheitsanforderungen	2
2.2	Personal	3
2.3	Sicherheit von IT-Systemen.....	3
2.4	Sichere Softwareentwicklung	3
2.5	Physische Sicherheit von IT-Systemen	4
2.6	Nutzung von Cloud-Diensten	5
3.	Überprüfung der Umsetzung	6
4.	Sicherheitsvorfälle	6
5.	Schlussbestimmungen	7

1. Einleitung

Die Partnerunternehmen der Thüga Aktiengesellschaft sind dafür verantwortlich, eine sichere und zuverlässige Energieversorgung für ihre Kunden im jeweiligen Versorgungsgebiet sicherzustellen.

Grundlage dafür sind stabile Geschäftsprozesse, eine vertrauensvolle Zusammenarbeit mit Lieferanten und Dienstleistern sowie die konsequente Einhaltung gesetzlicher, regulatorischer und vertraglicher Vorgaben.

Informationssicherheit hat dabei eine zentrale Bedeutung. Nahezu alle betrieblichen Abläufe beruhen auf der Verarbeitung sensibler Informationen und sind auf funktionsfähige Informations- und Kommunikationssysteme angewiesen.

Dieses Dokument ergänzt den vorliegenden Rahmenvertrag zwischen Thüga Aktiengesellschaft, im Folgenden „Thüga“, und dem Auftragnehmer und regelt verbindlich die Informationssicherheitsanforderungen, die im Rahmen der Zusammenarbeit des Auftragnehmers mit den abrufberechtigten Unternehmen (Auftraggeber) einzuhalten sind.

Die folgenden Bestimmungen gelten für den Auftragnehmer und enthalten sowohl Pflichten des Auftragnehmers als auch Kontrollrechte des Auftraggebers und Thüga zur Sicherstellung eines angemessenen Schutzniveaus.

2. Informationssicherheitsanforderungen an Externe

2.1 Grundlegende Sicherheitsanforderungen

Mit der Annahme des Auftrags verpflichtet sich der Auftragnehmer zur Umsetzung angemessener Informationssicherheitsmaßnahmen nach dem aktuellen Stand der Technik. Diese Maßnahmen müssen geeignet sein, den Schutzbedarf der verarbeiteten Informationen und eingesetzten IT-Systeme angemessen zu erfüllen. Sie umfassen sowohl organisatorische als auch technische Maßnahmen zur Minimierung möglicher Sicherheitsrisiken.

Die in der vorliegenden Richtlinie beschriebenen Anforderungen für den Auftragnehmer und dessen Subunternehmer (sofern in direktem Zusammenhang mit der erbrachten Leistung stehend) ergeben sich mittelbar aus den gesetzlichen und regulatorischen Vorgaben, die für die NIS2-Unternehmen und Betreiber kritischer Infrastrukturen selbst gelten (z. B. gemäß IT-Sicherheitskatalog, EnWG, BSIg) und dienen der Unterstützung dieser Unternehmen bei der Einhaltung ihrer Pflichten. Die Anforderungen dieser Richtlinie sind unabhängig von datenschutzrechtlichen Vorgaben.

Als Orientierung bei der Auswahl, Planung und Umsetzung geeigneter Sicherheitsmaßnahmen gelten insbesondere folgende anerkannte Standards und Rahmenwerke:

- ISO 27001 und 27002
- BSI-Grundschutz
- BDEW Whitepaper 3.0
- CIS Controls (Center for Internet Security)
- VdS-Richtlinien 10000 ("Informationssicherheitsmanagement für KMU")
- VdS-Richtlinien 10005 ("Mindestanforderungen an die Informationssicherheit von Klein- und Kleinstunternehmen")

2.2 Personal

Der Auftragnehmer verpflichtet sich sicherzustellen, dass:

- ein verantwortlicher Ansprechpartner für die Informationssicherheit benannt wird, der dem Auftraggeber während der gesamten Vertragslaufzeit für alle Fragen und Belange rund um die Informationssicherheit zur Verfügung steht.
- ausschließlich qualifiziertes und vertrauenswürdigen Personal für die Erfüllung des Auftrages und damit verbundene Tätigkeiten, wie z. B. die Administration der IT-Systeme des Auftraggebers oder die Durchführung von Wartungsarbeiten, eingesetzt wird. Das eingesetzte Personal muss sowohl fachlich kompetent als auch zuverlässig sein, um den hohen Anforderungen der Informationssicherheit gerecht zu werden.
- relevante personelle Änderungen, die Auswirkungen auf die Auftragsdurchführung haben können, sind dem Auftraggeber unverzüglich mitzuteilen.
- alle eingesetzten Mitarbeitenden sowie gegebenenfalls eingebundene Subunternehmen nachweislich über ihre speziellen Verantwortlichkeiten und Verpflichtungen in Bezug auf Informationssicherheit sowie die Einhaltung kundenspezifischer Anforderungen informiert wurden.
- die Einhaltung der Maßnahmen zur Erfüllung der vorliegenden Richtlinie fortlaufend sichergestellt und nachvollziehbar dokumentiert wird. Die Dokumentation muss auf Anfrage dem Auftraggeber zur Prüfung zur Verfügung gestellt werden, s. Abschnitt 3.

2.3 Sicherheit von IT-Systemen

Sofern IT-Systeme des Auftragnehmers für die Erzeugung, Übertragung oder Speicherung von Daten des Auftraggebers eingesetzt werden, verpflichtet sich der Auftragnehmer zur Umsetzung folgender Sicherheitsmaßnahmen:

- Einsatz zuverlässiger und sicherer Hard- und Software: Der Auftragnehmer setzt für alle IT-Systeme, die im Zusammenhang mit dem Auftrag stehen, ausschließlich vertrauenswürdige und sichere Hardware- und Softwarelösungen nach dem Stand der Technik ein.
- Schutz vor unberechtigtem Zugriff: Der Auftragnehmer wendet geeignete Verfahren an, um unberechtigten Zugang zu IT-Systemen sowie unautorisierten Zugriff auf Informationen zu verhindern.
- Schutz vor Schadsoftware: Es werden angemessene Maßnahmen ergriffen, um die IT-Systeme vor Schadsoftware (z.B. Viren, Trojaner, Ransomware) zu schützen.
- Patchmanagement: Der Auftragnehmer implementiert und betreibt geeignete Verfahren zur Identifizierung und Behebung technischer Schwachstellen, insbesondere durch ein effektives Patchmanagement.
- Datensicherung und Wiederherstellung: Der Auftragnehmer sorgt für die regelmäßige Sicherung aller relevanten Datenbestände und stellt sicher, dass diese im Falle eines Vorfalls wiederhergestellt werden können.
- Prozesse für Änderungs- und Kapazitätsmanagement: Der Auftragnehmer betreibt wirkungsvolle und dokumentierte Prozesse für das Änderungs- und Kapazitätsmanagement.

2.4 Sichere Softwareentwicklung

Sofern der Auftragnehmer Software für den Auftraggeber entwickelt oder liefert, verpflichtet sich der Auftragnehmer zur Umsetzung folgender Maßnahmen zur sicheren Softwareentwicklung:

- **Sichere Entwicklungsumgebung:** Der Auftragnehmer gewährleistet eine sichere Entwicklungsumgebung, die den Schutz des Quellcodes sicherstellt. Dazu gehören unter anderem kontrollierte Zugriffsrechte, eine zuverlässige Versionskontrolle sowie Mechanismen zur Überwachung und Protokollierung von Änderungen.
- **Prüfinformationen und Datenmaskierung:** Für Test- und Entwicklungszwecke dürfen ausschließlich synthetische, anonymisierte oder pseudonymisierte Daten verwendet werden. Die Nutzung produktiver Echtdaten ist nur mit ausdrücklicher Genehmigung der IT-Sicherheitsabteilung und der Datenschutzbeauftragten zulässig. Sollen Daten aus produktiven Quellen für Tests genutzt werden, sind diese zu anonymisieren bzw. pseudonymisieren. Alle Betriebsinformationen, die zu Testzwecken in eine Prüfumgebung übertragen wurden, sind nach Abschluss der Tests sicher zu löschen. In Entwicklungs- und Testsystemen dürfen nur speziell gekennzeichnete Testkonten verwendet werden, die regelmäßig überprüft werden.
- **Einhaltung von Security-Leitlinien und Best Practices:** Der Auftragnehmer verpflichtet sich, in allen eingesetzten Entwicklungsumgebungen (z.B. .Net, Java, ABAP) etablierte Sicherheitsrichtlinien und bewährte Verfahren zur sicheren Softwareentwicklung umzusetzen. Geeignete Sicherheitsanforderungen sind während des gesamten Entwicklungsprozesses zu berücksichtigen, um Schwachstellen frühzeitig zu vermeiden.
- **Sicherheit in der Entwicklungsmethodik:** Der Auftragnehmer stellt sicher, dass Sicherheitsaspekte systematisch in die angewandte Softwareentwicklungsmethodik integriert sind. Dazu gehören regelmäßige Sicherheitsüberprüfungen, Codereviews und automatisierte Tests zur frühzeitigen Erkennung und Behebung von Schwachstellen.
- **Einsatz sicherer Repositories:** Für die Speicherung und Verwaltung von Quellcode und Entwicklungsartefakten verwendet der Auftragnehmer ausschließlich sichere Repositories. Diese müssen gegen unberechtigten Zugriff geschützt sein und über Mechanismen zur Integritätsüberprüfung verfügen.

Durch die konsequente Umsetzung dieser Maßnahmen stellt der Auftragnehmer sicher, dass die entwickelte oder gelieferte Software den Sicherheitsanforderungen des Auftraggebers entspricht und potenzielle Sicherheitsrisiken während des gesamten Entwicklungsprozesses wirksam minimiert werden.

2.5 Physische Sicherheit von IT-Systemen

Sofern die Verarbeitung, Speicherung oder Aufbewahrung von Daten Teil des Auftragsinhalts ist, verpflichtet sich der Auftragnehmer zur Umsetzung folgender Maßnahmen zur physischen Sicherheit:

- **Schutz physischer Bereiche:** Der Auftragnehmer ergreift wirksame Maßnahmen zum Schutz aller Flächen und Räume, die im Rahmen der Auftragserbringung genutzt werden.
- **Schutz vor unberechtigtem Zutritt:** Es werden geeignete Verfahren eingerichtet, um unbefugten Zutritt zu relevanten Flächen und Räumen zu verhindern.
- **Regelmäßige Überprüfung von Zutrittsberechtigungen:** Zutrittsberechtigungen zu Flächen und Räumen sowie Zugangs- und Zugriffsberechtigungen zu IT-Systemen und Informationen werden in regelmäßigen Abständen überprüft und bei Bedarf angepasst. So wird sichergestellt, dass nur befugte Personen Zugang zu sensiblen Bereichen und Daten haben.
- **Trennung von Datenbeständen:** Der Auftragnehmer sorgt dafür, dass produktive Datenbestände und Backupdaten räumlich oder technisch voneinander getrennt gespeichert oder aufbewahrt werden.

- Brandschutzmaßnahmen: Für relevante Bereiche werden geeignete bauliche, technische und organisatorische Maßnahmen zur Verhütung, frühzeitigen Erkennung und schnellen Eindämmung von Bränden umgesetzt.
- Unterstützende Versorgungseinrichtungen: In relevanten Räumen mit IT-Systemen betreibt der Auftragnehmer ausreichend dimensionierte und fachgerecht gewartete Versorgungseinrichtungen wie unterbrechungsfreie Stromversorgung (USV), Klimaanlage und Feuchtigkeitsmelder.

Durch diese Maßnahmen stellt der Auftragnehmer sicher, dass die Datenverarbeitung, -speicherung und -aufbewahrung unter hohen Sicherheitsstandards erfolgt und potenzielle Risiken wirksam minimiert werden.

2.6 Nutzung von Cloud-Diensten

Sofern im Rahmen der Auftragserfüllung Cloud-Dienste zur Verarbeitung, Speicherung oder Übertragung von Informationen des Auftraggebers eingesetzt werden, verpflichtet sich der Auftragnehmer zur Einhaltung folgender Anforderungen:

- Auswahl vertrauenswürdiger Anbieter: Der Auftragnehmer verwendet ausschließlich Cloud-Dienste von Anbietern, die nach anerkannten Sicherheitsstandards zertifiziert sind (z. B. ISO/IEC 27001, BSI C5). Die eingesetzten Dienste müssen ein angemessenes Schutzniveau für die verarbeiteten Informationen gewährleisten.
- Datenlokalisierung: Der Auftragnehmer stellt sicher, dass alle relevanten Daten grundsätzlich innerhalb der Europäischen Union verarbeitet und gespeichert werden. Eine Verarbeitung außerhalb der EU ist nur zulässig, wenn hierfür geeignete rechtliche Grundlagen bestehen, insbesondere durch den Abschluss von EU-Standardvertragsklauseln (Standard Contractual Clauses, SCCs), wie sie von der Europäischen Kommission bereitgestellt werden. In jedem Fall ist eine vorherige schriftliche Zustimmung des Auftraggebers erforderlich.
- Verschlüsselung und Zugriffsschutz: Alle Daten, die über Cloud-Dienste verarbeitet werden, sind sowohl bei der Übertragung als auch bei der Speicherung durch geeignete kryptografische Verfahren zu schützen. Der Zugriff auf die Daten muss durch rollenbasierte Berechtigungen und mehrstufige Authentifizierungsverfahren abgesichert sein.
- Transparenz und Dokumentation: Der Auftragnehmer dokumentiert die eingesetzten Cloud-Dienste und stellt dem Auftraggeber auf Anfrage eine Übersicht über die verwendeten Anbieter, Dienste und Speicherorte zur Verfügung. Änderungen an der eingesetzten Cloud-Infrastruktur, insbesondere ein Anbieterwechsel, sind vom Auftraggeber vorher freizugeben.
- Sicherstellung der Mandantentrennung: Der Auftragnehmer gewährleistet, dass die Daten des Auftraggebers technisch und organisatorisch von anderen Mandanten getrennt verarbeitet werden, um eine ungewollte Vermischung oder Einsichtnahme auszuschließen.

Durch diese Maßnahmen wird sichergestellt, dass die Nutzung von Cloud-Diensten im Rahmen der Auftragserfüllung unter Einhaltung hoher Sicherheitsstandards erfolgt und die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen des Auftraggebers gewahrt bleibt.

3. Überprüfung der Umsetzung

Der Auftragnehmer verpflichtet sich mit Annahme des Auftrags, die Einhaltung der vereinbarten Sicherheitsmaßnahmen regelmäßig zu überprüfen und nachvollziehbar zu dokumentieren. Dazu gehören insbesondere:

- **Interne Prüfungen:** Der Auftragnehmer führt in angemessenem Umfang regelmäßige interne Prüfungen durch oder beauftragt Dritte mit der Durchführung entsprechender Audits.
- **Überprüfungen durch den Auftraggeber:** Der Auftragnehmer ermöglicht dem Auftraggeber und Thüga auf Anfrage eine angemessene Überprüfung der Einhaltung und Umsetzung der Sicherheitsmaßnahmen. Dies kann beispielsweise durch Einsichtnahme in relevante Dokumentation oder durch abgestimmte Vor-Ort-Prüfungen erfolgen.
- **Bereitstellung von Reports:** Der Auftragnehmer stellt dem Auftraggeber und Thüga regelmäßig (mind. jährlich) Berichte zur Verfügung, die sicherheitsrelevante Kennzahlen, Erkenntnisse und Ergebnisse aus den durchgeführten Prüfungen enthalten. Die Berichte müssen nachvollziehbar dokumentiert und auf Anfrage näher erläutert werden.

Durch diese Maßnahmen wird sichergestellt, dass sowohl der Auftragnehmer als auch der Auftraggeber aktiv zur Einhaltung und Weiterentwicklung der Sicherheitsstandards beitragen.

4. Sicherheitsvorfälle

Sofern beim Auftragnehmer oder einem seiner Dienstleister Sicherheitsvorfälle bekannt werden, die Auswirkungen auf Informationen oder die Verfügbarkeit von IT-Systemen des Auftraggebers haben, verpflichtet sich der Auftragnehmer zu folgenden Maßnahmen:

- **Unverzögliche Information:** Der Auftragnehmer informiert den Auftraggeber unverzüglich über den Vorfall. Die Mitteilung muss alle verfügbaren Informationen enthalten, die für eine erste Bewertung des Vorfalls erforderlich sind.
- **Unterstützung bei Meldepflichten:** Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung etwaiger gesetzlicher oder regulatorischer Meldepflichten. Dazu gehört insbesondere die zeitnahe Bereitstellung aller relevanten Informationen für die Kommunikation mit zuständigen Behörden oder Meldestellen.
- **Analyse und Bewertung:** Der Auftragnehmer ergreift geeignete Maßnahmen zur Ermittlung der Ursachen und Auswirkungen des Vorfalls. Dies umfasst die Analyse der betroffenen Systeme und Daten sowie die Bewertung möglicher Risiken für die Informationssicherheit.
- **Dokumentation und Aufarbeitung:** Der Auftragnehmer sorgt für eine strukturierte und nachvollziehbare Aufarbeitung des Sicherheitsvorfalls. Hierzu gehört die rechtssichere Dokumentation aller relevanten Erkenntnisse und Maßnahmen sowie die Sammlung von Beweismitteln, sofern erforderlich.

Diese Maßnahmen dienen dazu, Sicherheitsvorfälle wirksam zu bewältigen, potenzielle Schäden zu minimieren und die Integrität sowie die Verfügbarkeit der IT-Systeme und Informationen des Auftraggebers zu schützen.

5. Schlussbestimmungen

Diese Informationssicherheitsrichtlinie ergänzt den bestehenden Rahmenvertrag zwischen Thüga und Auftragnehmer und ist ausschließlich im Zusammenhang mit diesem anwendbar. Sie wird von beiden Parteien unabhängig vom Rahmenvertrag unterzeichnet und kann separat gepflegt und aktualisiert werden.

Änderungen oder Ergänzungen dieser Richtlinie bedürfen der schriftlichen Zustimmung beider Parteien. Bei Fragen zur Auslegung oder Anwendung der Richtlinie steht der jeweils benannte Ansprechpartner für Informationssicherheit zur Verfügung.

.....
Ort, Datum

.....
Unterschrift Lieferant / Firmenstempel