Informationssicherheits-leitlinie extern

für Hersteller, Dienstleister und externe Mitarbeiter der ÜZ

Ebene 1

Version: 3.0

Klassifizierung: Öffentlich

Dokumentenhistorie

Version	Datum	Bearbeitet durch	Änderung
1.0	18.09.2020	Alexander Schenk	Finalisierung vor Veröffentlichung
2.0	11.10.2021	Alexander Schenk	Finalisierung vor Veröffentlichung
3.0	20.07.2022	Christoph Zallmann	Finalisierung vor Veröffentlichung

Prüfung

Geprüft durch (Vorname u. Nachname, Unterschrift)	Version	Datum
Christoph Zallmann (ISB)	3.0	23.09.2022

Freigabe

Freigegeben durch (Vorname u. Nachname, Unterschrift)	Version	Datum
Jürgen Kriegbaum Kriegbaum Juergen Digital unterschrieben von Kriegbaum Juergen Datum: 2022.09.28 07:40:11 +02'00'	3.0	

Hinweis: Ausgedruckte Dokumente unterliegen NICHT dem Änderungsdienst!

ÜZ Mainfranken eG

Schallfelder Str. 11

97511 Lülsfeld

Inhaltsverzeichnis

1 Einleitung

Die Betreiber Kritischer Infrastrukturen haben eine besondere Verpflichtung, ihre Dienstleistungen bezüglich Verfügbarkeit, Vertraulichkeit und Integrität auf einem hohen Niveau anzubieten und bereitzustellen. Die ÜZ Mainfranken eG (nachfolgend ÜZ genannt) ist sich dieser Verantwortung bewusst. Bei der Erbringung ihrer Dienstleistungen setzt die ÜZ auch Produkte ein, die ihr von Herstellern bereitgestellt werden, und greift auf Dienstleistungen dieser Hersteller und weiterer Unternehmen zurück (im Folgenden nur als Produkte bezeichnet). Von der Produktqualität hängt damit wesentlich auch die Qualität der von der ÜZ bereitgestellten Dienstleistungen ab. Weisen solche Produkte eine Störung auf, kann dies auch zu einer Störung der kritischen Dienstleistung der ÜZ führen.

Freiwillige Transparenz und Maßnahmen der Hersteller sowie direkte gesetzliche Anforderungen an Mindestqualitäten in Bezug auf die Sicherheit und Funktionalität der von Herstellern bereitgestellten Produkte können die Komplexität sowie eine Gefährdung der Erbringung der kritischen Dienstleistung durch ÜZ verringern.

Das vorliegende Dokument soll Herstellern, Dienstleistern und externen Mitarbeitern einen Einblick in das Informationssicherheits-Managementsystem (ISMS) der ÜZ geben. Des Weiteren werden die prinzipiellen und wichtigsten Sicherheitsanforderungen, hier mit Fokus auf die Informationssicherheit, an diese externen Partner der ÜZ (im Folgenden als Auftragnehmer bezeichnet) definiert.

2 Geltungsbereich

Die vorliegende Informationssicherheitsleitlinie gilt für alle Hersteller, Dienstleister und externe Mitarbeiter der ÜZ, die in den Geschäftsprozessen „Netzführung“ oder „Housing Rechenzentrum“ (kurz Housing RZ) involviert sind. Ein entsprechender Hinweis sowie die Verpflichtung auf diese Leitlinie erfolgt über die schriftliche Beauftragung durch die ÜZ – Näheres hierzu ist im Sicherheitskonzept „Lieferantenmanagement“ der ÜZ beschrieben.

3 Informationssicherheit bei der ÜZ

3.1 Allgemeines

Die ÜZ ist sich der Bedeutung der bei ihr verarbeiteten Informationen im Rahmen ihres gesetzlichen Auftrages und unter Berücksichtigung ihrer Geschäftsziele bewusst. Alle Beteiligten (Kunden, Dienstleister, Lieferanten, Partner, Mitglieder der Genossenschaft, etc.) müssen sich darauf verlassen können, dass die ÜZ die Sicherheitsverantwortung für die von ihr verarbeiteten Informationen gewissenhaft wahrnimmt und vor missbräuchlicher Verwendung schützt. Um ihre Informationen zu schützen und ihre Geschäftsziele zu verwirklichen, hat die ÜZ ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 eingeführt sowie in Teilbereichen zertifizieren lassen und verpflichtet sich durch Zustimmung der Geschäftsführung, dieses aufrecht zu erhalten und ständig zu verbessern.

Damit kommt die ÜZ auch den im IT-Sicherheitskatalog gemäß § 11 Absatz 1a des Energiewirtschaftsgesetzes formulierten Anforderungen für einen sicheren Betrieb des Stromnetzes inkl. der Netzleitstelle nach („IT-SiKat“).

Über eine Unterzertifizierung wird sichergestellt, dass das „Housing Rechenzentrum“ („Housing RZ“) ebenfalls den Anforderungen der ISO/IEC 27001 gerecht wird. Hierbei stellt die ÜZ die Infrastruktur (Gebäude, Klimatechnik, Notstromversorgung, …) zum Betrieb von Rechenzentren durch Dritte zur Verfügung.

3.2 Stellenwert der Informationssicherheit

Alle wesentlichen, strategischen und operativen Funktionen und Aufgaben werden durch informationsverarbeitende Systeme (Informationstechnik, kurz IT) maßgeblich unterstützt. Informationen sind somit grundlegende Faktoren für den Geschäftsbetrieb und für die Erreichung der Unternehmensziele und stellen Unternehmenswerte der ÜZ dar.

Um das Informationssicherheits-Managementsystem der ÜZ zu steuern, zu kontrollieren und kontinuierlich zu verbessern hat die ÜZ einen Informationssicherheitsbeauftragen (kurz ISB) benannt.

Aufgrund der Qualität der verarbeiteten Daten sind auch gesetzliche Vorgaben hinsichtlich des Datenschutzes (Schutz personenbezogener Daten) und der Risikoabwehr (Gefährdungshaftung) zu erfüllen. Für die Koordinierung zur Umsetzung der datenschutzrechtlichen Anforderungen (z.B. EU-Datenschutz-Grundverordnung) hat die ÜZ einen Datenschutzbeauftragten (DSB) unternehmensintern etabliert. Zur Risikobeurteilung und Risikoabwehr betreibt die ÜZ ein unternehmensweites Risikomanagement.

3.3 Ziele der Informationssicherheit

Ziel des Managements der Informationssicherheit ist es, im Rahmen der gesetzlichen Anforderungen, eine kontinuierliche und wirtschaftlich angemessene Steuerung solcher Risiken sicher zu stellen, die in Verbindung mit der Verarbeitung, dem Transport und der Speicherung von Informationen stehen. Dies gilt insbesondere für Informationen, die für die Sicherheit des Netzbetriebes sowie dem Housing RZ erforderlich sind. Die Informationssicherheit betrifft Informationen, die in elektronischer oder gedruckter/schriftlicher Form vorliegen, aber auch mündlich übermittelte Informationen, z. B. in Telefonaten oder Gesprächen an öffentlichen Orten.

Zur Wahrung der Informationssicherheit dienen die folgenden Schutzziele:

- **Vertraulichkeit**
  Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen ohne Erlaubnis des Eigentümers.
- **Integrität**
  Integrität bedeutet Schutz vor Modifikation von Informationen durch nicht berechtigte Personen und stellt die Richtigkeit, Konsistenz und Vollständigkeit von Informationen dar.
- **Verfügbarkeit**
  Verfügbarkeit bedeutet, dass Prozesse, Informationen, Funktionen und Informationssysteme immer dann verfügbar sind, wenn ein autorisierter Benutzer sie bearbeiten bzw. in Anspruch nehmen will. „Verfügbar“ heißt in diesem Zusammenhang auch, dass der Zugriff auf Informationen, Funktionen und Betriebsmittel bedarfsgerecht gewährleistet ist.

3.4 Informationssicherheitsgrundsätze

Für den Betrieb des Informationssicherheits-Managementsystems gelten folgende Grundsätze:

1. Für Unternehmenswerte wie Informationen, IT-Systeme und IT-Anwendungen sind Eigentümer benannt, die für die Sicherheit der jeweiligen Unternehmenswerte verantwortlich sind.
2. Risiken aus der Nutzung der Informationen und Informationssysteme werden frühzeitig identifiziert und auf ein akzeptiertes Restrisiko minimiert. Hierzu betreibt die ÜZ ihr IS-Risikomanagement.
3. Kosten und Nutzen von Sicherheitsmaßnahmen stehen in einem angemessenen Verhältnis, ggf. werden Maßnahmen über einen längeren Zeitraum umgesetzt.
4. Vorgaben und Maßnahmen orientieren sich an anerkannten Standards und Best Practices zur Informationssicherheit. Systeme und Komponenten werden gemäß den Erkenntnissen aus dem IS-Risikomanagement der ÜZ behandelt.
5. Gesetzliche, vertragliche und sonstige Vorgaben für die Informationssicherheit werden identifiziert und durch angemessene Maßnahmen umgesetzt. Zur Identifizierung werden Informati-

onen von einschlägigen Fachquellen sowie von Fachverbänden ausgewertet (Gesetzgeber, Regulierungsbehörde, VDE, BDEW, …). Die Umsetzung und Berücksichtigung erfolgt in den entsprechenden Fachbereichen bzw. Teams der ÜZ.

6. Zugriff, Zugang (Benutzerverwaltung mit unterschiedlichen Rollen und Rechten) und Zutritt (Schließsysteme, Zutrittskontrollsysteme, …) zu den Informationswerten sind auf das notwendige Maß beschränkt.
7. Alle wesentlichen Aktivitäten und Ereignisse im Bereich der Informationssicherheit müssen transparent und im erforderlichen Umfang nachvollziehbar sein. Zur Dokumentation und Beschreibung wurden die Leitlinien (intern und extern) sowie Richtlinien und Sicherheitskonzepte ausgearbeitet. In Abhängigkeit vom Umfang und der Art und Weise der Aufgabenerfüllung durch den Auftragnehmer kann es erforderlich sein, dass dieser die entsprechenden Richtlinien und Sicherheitskonzepte beachten muss. Dies ist bei Bedarf und im Zweifel mit dem ISB der ÜZ abzustimmen.
8. Verfahren für den Betrieb bzw. die Wiederherstellung des Betriebs der wesentlichen Informationssysteme wurden dokumentiert.
9. Für die an der Verarbeitung von Informationen beteiligten Beschäftigten sowie Auftragnehmern werden angemessene Vorkehrungen zur Gewährleistung der Vertrauenswürdigkeit getroffen.
10. Die Beschäftigten werden hinsichtlich des sicheren Umgangs mit Informationswerten informiert, geschult und sensibilisiert. Sie sind angehalten, die entsprechenden Vorgaben umzusetzen. Entsprechendes gilt erforderlichenfalls auch für Auftragnehmer.
11. Die Wirksamkeit der Vorgaben und Maßnahmen zur Informationssicherheit werden kontinuierlich überprüft und verbessert. Zur Überprüfung werden die verschiedenen Audits gemäß dem ISMS-Auditprogramm der ÜZ durchgeführt und entsprechend dokumentiert.

4 Pflichten und Aufgaben externer Partner

4.1 Allgemeines

Generell ist es die Verantwortung des Auftragnehmers, die durch die ÜZ festgelegten Anforderungen einzuhalten. Darüber hinaus muss der Auftragnehmer von Produkten oder Dienstleistungen für Kritische Infrastrukturen die in der Industrie anerkannten Standards der Informationssicherheit und andere regulatorische Standards und Vorgaben für Dienstleistungen bzw. Produkte beachten. Hierdurch soll sichergestellt werden, dass die Sicherheitsaspekte bereits bei der Entwicklung, Produktion und Bereitstellung von Produkten berücksichtigt werden.

Sollte der Auftragnehmer weitere Subunternehmen beauftragen, die an der Herstellung beteiligt sind oder die wesentliche Bedeutung für die Erbringung der Dienstleistung haben, so muss der Auftragnehmer dafür Sorge tragen, dass die Subunternehmen die vorliegende Leitlinie und erforderlichenfalls weitere Richtlinien und Sicherheitskonzepte ebenfalls berücksichtigen und einhalten. Der Auftragnehmer ist hierbei für die Weiterleitung und Überwachung der entsprechenden Anforderungen zuständig. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber der ÜZ auf Anfrage nachzuweisen. Der Auftragnehmer muss die ÜZ im Vorfeld von Entscheidungen über die Auslagerung von Betriebs- oder Dienstleistungen informieren und eine entsprechende Freigabe von der ÜZ einholen.

Jeder, der im Namen des Auftragnehmers agiert und/oder entfernten oder lokalen Zugriff auf das Informationssystem der ÜZ benötigt, muss bei Bedarf Informationen zu seiner Identität bereitstellen. Der Auftragnehmer stellt ferner sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall dennoch eintritt.
Der Auftragnehmer darf nur Personen (Mitarbeiter des Auftragnehmers) und Subunternehmen beauftragen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen.

4.2 Systemhärtung

Um die Auswirkungen potentieller Sicherheitsrisiken zu minimieren, muss der Auftragnehmer dafür Sorge tragen, dass die von ihm gelieferten bzw. betriebenen Systeme und Komponenten gehärtet sind. Hierbei gelten folgende Grundsätze:

- Aktueller Stand der Technik: Der Auftragnehmer hat dafür Sorge zu tragen, dass seine Produkte bei Veräußerung bzw. Erfüllung der Dienstleistung mit Blick auf die Informationssicherheit den anerkannten Regeln und dem aktuellen Stand der Technik entsprechen. Anforderungen an sichere Steuerungs- und Telekommunikationssysteme können z.B. dem BDEW-Whitepaper entnommen werden.
- Minimale Installationsprinzipien: Es ist darauf zu achten, dass nur die für den eigentlichen Betrieb (Zweck) sowie erforderlichenfalls für Monitoring- und Protokollierungszwecke notwendige(n) Softwarekomponente(n) installiert werden.
- Netzwerkdienste und Kommunikationsports: Jeder nicht benötigte Netzwerkzugang und Kommunikationsport muss deaktiviert sein bzw. die Möglichkeit hierzu bestehen.
- Konfigurationsstandards: Der Auftragnehmer stellt sicher, dass die von der ÜZ vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.
- Standardpasswörter: Der Auftragnehmer stellt sicher, dass Standardpasswörter geändert werden bzw. er die ÜZ auf deren Verwendung hinweist.
- Backdoors: Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, welche die verwendeten Sicherheitsmechanismen umgehen können.

4.3 Vulnerability- und Patch-Management

Der Auftragnehmer muss seine Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, bspw. in Form eines sogenannten Vulnerability-Managements, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Es basiert auf der Transparenz der Funktionalität, der technischen Architektur und von Unterkomponenten einschließlich der Betriebssysteme, Datenbanken, Server (z.B. Web, Telnet, SSH), Middleware und Bibliotheken. Diese wird verwendet, um neue Schwachstellen in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen zu beurteilen. Auf Anforderung ist dies der ÜZ nachzuweisen. Sind vom Auftragnehmer entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der Auftragnehmer verpflichtet, umgehend die Schwachstellen an die ÜZ zu melden.
Sollten bei Produkten oder Systemen Fehlfunktionen eintreten oder mit Hinblick auf die Wahrung der Informationssicherheit kritische Schwachstellen erkannt werden, so ist der Auftragnehmer dazu verpflichtet, der ÜZ entsprechende Updates und Patches zur Behebung der Schwachstelle zur Verfügung zu stellen. Auch für den Fall, dass keine schriftliche Vereinbarung getroffen wurde, muss der Auftragnehmer der ÜZ seine Unterstützungsleistung im Rahmen seiner verfügbaren Ressourcen auf Anfrage durch die ÜZ bereitstellen. Er darf sich einer solchen Anforderung der ÜZ nicht grundsätzlich verweigern. Sich daraus ergebene Aufwände, die nicht vertraglich vereinbart sind, kann der Auftragnehmer selbstverständlich unter vorheriger Abstimmung mit der ÜZ in Rechnung stellen.
Nähere und detailliertere Regelungen (z.B. über Reaktionszeiten, Service-Level, Kosten, …) können über einen Service- und Wartungsvertrag zwischen der ÜZ und dem jeweiligen Auftragnehmer vereinbart werden.

4.4 Fernwartungszugänge

Fernwartungszugänge sind auf das Nötigste zu beschränken. Die Nutzung dieser Zugänge muss protokolliert werden. Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Assets und Services der ÜZ gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Er ist dafür verantwortlich, dass seine betroffenen Mitarbeiter geschult sind und sensibilisiert werden. Fernwartungszugänge dürfen nur unter Abstimmung zwischen dem jeweiligen Auftragnehmer, den Fachbereichen der ÜZ (z.B. Team Netzführung oder Team LWL) und dem Team Informationstechnik der ÜZ eingerichtet und betrieben werden. Die Fernwartungszugänge sind hierbei nach dem jeweils aktuellen Stand der Technik einzurichten (z.B. sichere VPN-Verschlüsselung) und bei Bedarf im laufenden Betrieb auf die jeweils aktuellen Sicherheitsanforderungen anzupassen. Nähere und detailliertere Regelungen (z.B. über konkrete Ausgestaltung) können über einen Service- und Wartungsvertrages zwischen der ÜZ und dem jeweiligen Auftragnehmer vereinbart werden.

4.5 Zutrittsschutz

Für die Liegenschaften der ÜZ wurden Sicherheitszonen definiert. Je nach Sicherheitszone bestehen restriktive Zutrittsregelungen und Zutrittsberechtigungen. Sollte es erforderlich sein, dass Mitarbeiter des Auftragnehmers Zutritt zu den Liegenschaften der ÜZ benötigen, um die beauftragten Dienstleistungen ausführen zu können, so müssen diese Personen im Vorfeld bei der Vermittlung der ÜZ angemeldet, beim Eintreffen registriert (Besucherausweis) und von einem Mitarbeiter der ÜZ betreut werden. Nähere Details und Informationen hierzu sind im Sicherheitskonzept „Physikalische Sicherheit“ der ÜZ beschrieben.

4.6 Informationssicherheitsvorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potentiell einen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte der ÜZ haben könnten, umgehend und unverzüglich dem ISB der ÜZ zu melden. Der Auftragnehmer muss im Falle eines Vorfalls auf Nachfrage der ÜZ Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen. In Abstimmung mit dem ISB der ÜZ werden dann erforderliche Sofortmaßnahmen eingeleitet und Konsequenzen angestoßen. So handelt es sich beispielsweise auch um einen Informationssicherheitsvorfall, wenn ein Mitarbeiter des Auftragnehmers gegen die bestehenden Vorgaben und Regelungen der ÜZ verstößt. Entsprechendes gilt auch beim Einsatz möglicher Subunternehmen – näheres hierzu siehe Kapitel 4.1. Das genaue Verfahren zur Behandlung von Informationssicherheitsvorfällen ist im entsprechenden Sicherheitskonzept der ÜZ beschrieben.

4.7 Kontrolle und Audits

Neben etablierten Abnahmeprüfungen und Leistungsnachweisen muss der ÜZ, bzw. den durch die ÜZ beauftragten Aufsichtsbehörden oder Dritten, durch den Auftragnehmer gestattet werden, darüberhinausgehende Kontrollen und Audits durchzuführen. Dies kann einmal oder mehrmals geschehen. Die Prüfungen werden hierbei auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Kosten, die Dauer und die Organisation des jeweiligen Audits werden jeweils einvernehmlich vereinbart. Dies kann beispielsweise in Form einer Werksbesichtigung oder Werksabnahme erfolgen. Näheres zu den Lieferantenaudits ist im Sicherheitskonzept „Lieferantenmanagement“ der ÜZ beschrieben.

5 Durchsetzung

Verstöße gegen diese Informationssicherheitsleitlinie können zur Aufhebung der Dienstleistungsvereinbarung führen. Ebenso behält sich die ÜZ in Abhängigkeit des Verletzungsgrades in Bezug auf die Informationssicherheit vor, gegen den jeweiligen Auftragnehmer entsprechende rechtliche Schritte einzuleiten.

6 Unterzeichnung

Durch die Unterzeichnung dieser Informationssicherheitsleitlinie für Hersteller, Dienstleister und externe Mitarbeiter durch die Geschäftsführung der ÜZ (siehe Seite 1) ist diese ab sofort gültig und in allen enthaltenden Punkten ausnahmslos anzuwenden.

Verteilung: Einstellen auf die Homepage der ÜZ Mainfranken und Verweis bei entsprechenden Beauftragungen über das Team Einkauf/Materialwirtschaft der ÜZ