Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister

Verwendung für Anforderungen der e-netz Südhessen AG und citiworks AG in Verbindung mit

informationssicherheitsrelevanten Lieferanten und Dienstleistern der Kategorien Typ 1, Typ 2 und Typ 3

Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister

Inhaltsverzeichnis:

1	**Informationssicherheitsprozess**	**4**
1.1	Geregelter Sicherheitsprozess zur Steuerung und Verbesserung der Informationssicherheit (T1, T2, T3)	4
1.2	Ansprechpartner für Informationssicherheit (T1, T2, T3)	4
1.3	Mitarbeiter und Dienstleister (T2, T3)	4
1.4	Anforderungen zum Stand der Technik (T2, T3)	5
1.5	Datenschutz (T2, T3)	5
2	**Technische und organisatorische Bestimmungen**	**6**
2.1	Softwareentwicklung (T3)	6
2.2	Zugriffs- und Zutrittsschutz (T1, T2, T3)	6
2.3	Kennwortanforderungen (T3)	6
2.4	Netzwerksicherheit (T2, T3)	6
2.5	Schadsoftwareschutz (T3)	7
2.6	Systemhärtung, Schwachstellen und Patch-Management (T3)	7
2.7	Administration von Systemen und Anwendungen (T3)	7
3	**Umgang mit klassifizierten Informationen (T1, T2, T3)**	**8**
3.1	Verarbeitung sensibler Informationen (T1, T2, T3)	10
3.2	Zugriffsschutz, Speicherung und Entsorgung (T1, T2, T3)	10
3.3	Übermittlung in Netzwerken (T1, T2, T3)	10
4	**Anforderungen an die Wartungsprozesse (T2, T3)**	**11**
4.1	Allgemeines (T2, T3)	11
4.2	Sichere Systemkonfiguration von Wartungskomponenten (T3)	11
4.3	Fernwartung (T3)	11
5	**Meldung von Informationssicherheitsvorfällen (T1, T2, T3)**	**13**

Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister

Zweck

IKT-Systeme, ICS und angebotene IKT-Dienstleistungen im Geltungsbereich des ISMS müssen nach anerkanntem Stand der Technik in der Informationssicherheit gemäß den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt, in Betrieb genommen, dokumentiert und betrieben werden. Details der vorgesehenen Sicherheitsmaßnahmen sind im Angebot sowohl in technischen als auch organisatorischen Belangen zu beschreiben. Die Anforderungen nach § 11 EnWG sowie insbesondere der IT-Sicherheitskatalog der BNetzA sind einzuhalten

Die Umsetzung der Anforderungen ist zu beschreiben. Alle Abweichungen davon sind im Angebot zu benennen und zu begründen. Der Einsatz von Nachunternehmern und/oder Dritten ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer hat für alle Nachunternehmer wie für sein eigenes Handeln einzustehen.

Geltungsbereich und Zielgruppen

Dieser Vertragsbestandteil enthält die Anforderungen an Drittunternehmen, um die Sicherheitsanforderungen der e-netz Südhessen AG und citiworks AG zu gewährleisten.

Die nachfolgenden Anforderungen sind verbindlicher Bestandteil der Liefer- und Wartungsverträge. Jegliche Abweichungen von den Anforderungen sind dem Auftraggeber (im Folgenden AG genannt) schriftlich mitzuteilen und von diesem explizit zu genehmigen.

Drittunternehmen (im Folgenden Dienstleister oder DL genannt), die Dienstleistungen oder Produkte im Geltungsbereich des ISMS erbringen oder liefern, müssen grundlegende Anforderungen an die Sicherheit ihrer informationsverarbeitenden Systeme erfüllen und geeignete organisatorische Abläufe in Bezug auf sichere interne IT-Abläufe zusichern. Der AG behält sich vor, für unten genannte Maßnahmen entsprechende Nachweise anzufordern.

Werden Subdienstleister durch den DL eingesetzt, so sind diese Anforderungen ebenfalls für den Subdienstleister bindend. Der Einsatz von Subdienstleistern ist dem AG anzuzeigen.

Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister

1 Informationssicherheitsprozess

1.1 Geregelter Sicherheitsprozess zur Steuerung und Verbesserung der Informationssicherheit (T1, T2, T3)

Der Dienstleister muss in seinem Unternehmen einen geeigneten Sicherheitsprozess zur Planung, Steuerung, Kontrolle und Verbesserung der Informationssicherheit etabliert haben, über den die Umsetzung der hier geforderten technischen und organisatorischen Maßnahmen sichergestellt wird.

Dies kann beispielsweise in Form eines Informations-Sicherheitsmanagementsystems (ISMS) bzw. einer Zertifizierung nach ISO/IEC 27001 oder der Steuerung interner Abläufe bzw. des Betriebs der IT-Infrastruktur, z. B. nach ITIL, erfolgen. Der Nachweis einer Zertifizierung und/oder eines Lieferantenaudits kann in begründeten Einzelfällen erforderlich werden.

Der Dienstleister hat bei Einsatz von Subdienstleistern und Drittthersteller-Produkten diese zu benennen sowie die Umsetzung der Anforderungen aus der Dienstleistungsvereinbarung sicherzustellen und zu dokumentieren.

1.2 Ansprechpartner für Informationssicherheit (T1, T2, T3)

Der Dienstleister verfügt über einen Ansprechpartner zur Informationssicherheit, der für die Umsetzung und Überprüfung von Informationssicherheitsmaßnahmen verantwortlich und der zu Fragen der Informationssicherheit gegenüber dem Auftraggeber auskunftsfähig und auskunftsberechtigt ist.

Die vollständigen Kontaktdaten des Ansprechpartners sind dem AG mitzuteilen.

1.3 Mitarbeiter und Dienstleister (T2, T3)

Die Mitarbeiter und Subdienstleister des DL sind über die sicherheitstechnischen Anforderungen des AG zu informieren.

Die besondere Bedeutung der Informationssicherheit muss durch entsprechende Security-Schulungen für Mitarbeiter des DL unterstrichen werden. Dabei sind die besondere Sensibilität im Umgang mit vertraulichen und sensiblen Daten sowie die sicherheitstechnischen Anforderungen herauszustellen.

Die Mitarbeiter müssen hinsichtlich des vertraulichen Umgangs mit Informationen, die ihnen im Zuge ihrer Tätigkeit bekannt werden, verpflichtet werden. Dies kann bspw. durch entsprechende Regelungen im Arbeitsvertrag oder eine separate Erklärung erfolgen.

Scheiden Mitarbeiter des DL aus dem Unternehmen aus oder wechseln ihr Aufgabengebiet, ist durch geeignete Maßnahmen sicherzustellen, dass sicherheitssensitive Zutritts- und Zugriffsberechtigungen zu Systemen und Informationen des AG entzogen werden sowie Einwahlmöglichkeiten dieser Mitarbeiter in das Daten- / Prozessnetz und die Fernwartungsumgebung des AG ausgeschlossen sind. Die Accounts der betroffenen Mitarbeiter sind zumindest zu deaktivieren. Der AG behält sich vor, für oben genannte Maßnahmen entsprechende Nachweise anzufordern.
Der AG behält sich vor, Mitarbeiter von Dienstleistern, die in Kontakt mit als besonders sensibel kategorisierten Informationen oder Anlagen kommen, einer Sicherheitsüberprüfung unterziehen zu lassen bzw. für diese einen entsprechenden Sicherheitsnachweis einzufordern.

Werden Subdienstleister durch den DL eingesetzt, so sind diese Anforderungen ebenfalls für den Subdienstleister bindend. Der Einsatz von Subdienstleistern ist dem AG anzuzeigen.

1.4 Anforderungen zum Stand der Technik (T2, T3)

Der DL hat die Verfahren zur Etablierung des Stands der Technik darzustellen, dazu gehört zum Beispiel die Beschreibung der Anforderungserfüllung gemäß des BDEW Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" und das BSI Dokument " Empfehlungen zu Entwicklung und Einsatz von in Kritischen Infrastrukturen eingesetzten Produkten". Zu diesem Zweck stellt der AG auf Anfrage dieses Whitepaper sowie eine Übersicht der relevanten Standards und Anforderungen zur Leistungserbringung zur Verfügung.

Der Nachweis der Anforderungserfüllung kann durch vorhandene Zertifizierungen erbracht werden (z.B. Produktzertifizierung nach IEC 62443).

(T3) In Abstimmung mit dem AG erfolgt die Dokumentation der Informationssicherheitsanforderungen in Form eines Pflichtenheftes durch den DL.

1.5 Datenschutz (T2, T3)

Der Schutz personenbezogener Daten ist bei der Erbringung von Dienstleistungen für die e-netz Südhessen und citiworks ein wichtiges Anliegen. Die Verarbeitung personenbezogener Daten (z.B. Mitarbeiter, Kunden sowie Geschäftspartner) sind in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit durchzuführen. Die „Konzernrichtlinie Datenschutz“ des ENTEGA Konzerns regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bestehenden Verantwortlichkeiten. Alle Dienstleister und Lieferanten sind zur Einhaltung der Richtlinie verpflichtet. Die Konzernrichtlinie wird bei Bedarf zur Verfügung gestellt.

Sollte eine Weitergabe dieser Informationen an Dritte (bspw. an Behörden o.ä.) erforderlich und rechtlich – insbesondere datenschutzrechtlich – notwendig sein, so können diese nur nach vorheriger Zustimmung der e-netz Südhessen und citiworks unter Einbeziehung des Datenschutzbeauftragten sowie der IT-Sicherheitsbeauftragten der e-netz Südhessen und citiworks erfolgen.

Umfasst die Dienstleistung eine Verarbeitung personenbezogener Daten, so ist eine Vereinbarung zur Datenverarbeitung im Auftrag gemäß den Anforderungen des Art. 28 DSGVO mit dem Dienstleister abzuschließen. Die genannten Vertragsmuster werden gemäß Dienstleistungsumfang zur Verfügung gestellt.

Gesetzliche Löschtermine und Aufbewahrungsfristen sind datentypengenau zu beachten und zu dokumentieren. Der Dienstleister hat die Einhaltung der Lösch- und Sperrfristen von personenbezogenen Daten im Dienstleistungsumfang sicherzustellen und eine dem Dienstleistungsumfang entsprechende Dokumentation zur Verfügung zu stellen.

2 Technische und organisatorische Bestimmungen

2.1 Softwareentwicklung (T3)

Softwareentwicklung für die e-netz Südhessen und citiworks ist nach aktuellen Qualitäts- und Informationssicherheits-standards zu betreiben. Aufgrund der Zertifizierungen der e-netz Südhessen und citiworks, werden hierzu die notwendigen Anforderungen aus aktuellen Standards und relevanter Normen in den Entwicklungszyklus einer Anwendung eingebunden, um durch geeignete Vorgaben die Qualität und Sicherheit der Software zu gewährleisten. Hierbei ist entscheidend, dass an den verschiedenen Stellen, an denen Gefährdungen auftreten können, diesen durch entsprechende Maßnahmen entgegengewirkt wird.

Die Softwareentwicklung adressiert an vielen Stellen Themen der Qualität und Informationssicherheit. So sind verschiedene Aspekte zu bewerten und zu beschreiben. Dazu gehören die Auswahl der Sprache, die Architektur und die Datenhaltung. Die Entwicklung ist mittels Standards durchzuführen, die die Einhaltung von Qualitäts- und Sicherheitskriterien sicherstellen und die Abnahme des Ergebnisses durch geeignete Tests nachvollziehbar macht.

Ergänzend zu den Anforderungen des ISMS der e-netz Südhessen und citiworks sind die Vorgaben an die Softwareentwicklung zu beachten, die in Form Technischer Richtlinien die Anforderungen an Softwareentwicklung innerhalb der e-netz Südhessen und citiworks beschreiben. Diese werden bei Bedarf dem AN zur Verfügung gestellt.

2.2 Zugriffs- und Zutrittsschutz (T1, T2, T3)

(T1, T2) Räume oder Bereiche beim Dienstleister, in denen Informationen elektronisch verarbeitet oder gespeichert werden, müssen durch geeignete Maßnahmen vor unberechtigtem Zutritt geschützt werden.

(T3) Alle informationsverarbeitenden Systeme des DL, von denen ein Zugriff auf die Systemumgebung des AG oder dem AG zugeordnete sensible Informationen mittelbar oder unmittelbar möglich ist, müssen mit einem sicheren logischen Zugangsschutz versehen sein. Dabei ist eine Multi-Faktor-Authentifizierung anzustreben (z. B. Kombination aus Benutzername/Passwort und einer ergänzenden Identifizierung mit Hilfe eines Hardwaretokens, einer Smartcard o. Ä. oder eines biometrischen Merkmals).

2.3 Kennwortanforderungen (T3)

An die Kennwörter für informationsverarbeitende Systeme und Komponenten werden besondere Anforderungen gestellt, der DL muss deshalb eine verpflichtende Kennwortrichtlinie definiert haben.

Diese Richtlinie muss mindestens den Anforderungen an Kennwörter des AG entsprechen. Diese Anforderungen wird der AG dem DL zur Verfügung stellen.

2.4 Netzwerksicherheit (T2, T3)

Das interne Datennetzwerk des DL wird von öffentlichen oder externen Netzen durch geeignete Maßnahmen nach dem Stand der Technik getrennt (z. B. Firewall).

Drahtlose Netzwerke müssen nach Stand der Technik gesichert werden, insbesondere muss ein unbefugter Zugriff auf die System- und Wartungsumgebung des AG oder dem AG zugeordnete sensible Informationen sicher verhindert werden.

2.5 Schadsoftwareschutz (T3)

Der DL muss sicherstellen, dass alle informationsverarbeitenden Systeme mit einem aktiven und aktuellen Schutz vor Schadsoftware versehen sind, soweit sich dies technisch realisieren lässt.

Insbesondere für diejenigen Systeme, von denen mittel- oder unmittelbar Zugriffe auf die System- und Wartungsumgebung des AG möglich sind (z. B. Parametrierlaptops, Terminalserver, Web-, Mail- und Dateiserver usw.) ist ein stringenter Schadsoftwareschutz sicherzustellen.

Der DL muss sicherstellen, dass der Schadsoftwareschutz nicht durch Mitarbeiter deaktiviert wird.

Bei Pattern-basierten Lösungen ist dafür Sorge zu tragen, dass die Schadsoftware-Pattern unverzüglich aktualisiert werden.

Neben den Arbeitsplatzsystemen muss der Schutz vor Schadsoftware auch Kommunikationsverbindungen, wie Web-, E-Mail- und Datentransfer, umfassen.

2.6 Systemhärtung, Schwachstellen und Patch-Management (T3)

Systeme sind nach anerkannten und dokumentierten Verfahren (z. B. CIS-Standards) zu konfigurieren bzw. zu parametrieren, dazu gehört z. B. die dokumentierte Systemhärtung.

Betriebssysteme, Firmware oder Applikationen von IT-Komponenten des DL sind unverzüglich durch Softwareupdates des jeweiligen Herstellers zu aktualisieren, wenn durch diese Updates Sicherheitslücken geschlossen oder Schwachstellen beseitigt werden.

Zu diesem Zweck ist ein Patchmanagement zu etablieren, welches sicherstellt, dass Patches vom Hersteller bezogen sowie nach Dringlichkeit kategorisiert und durch einen geregelten Prozess installiert werden können.

2.7 Administration von Systemen und Anwendungen (T3)

Die technischen und organisatorischen Anforderungen an die Administration von Anwendungen und Systemen der e-netz Südhessen und citiworks durch Dienstleister und beauftragte Dritte sind zu beachten und umzusetzen. Sie können sich aufgrund der privilegierten Rechte, Zugriff zu Informationen verschaffen, deren Schutzbedürfnis ggf. erhöht ist. Gerade deswegen gelten für Administratoren besondere Sorgfalts- und Verschwiegenheitspflichten. Sie haben durch ihre Berechtigungen erweiterten oder gar unbeschränkten Zugriff auf die Infrastruktursysteme, sowie die darüber vorgehaltenen Informationen.

Die für die Beauftragung benötigten Informationen werden dem Auftragnehmer dem Dienstleistungsumfang entsprechend zur Verfügung gestellt.

3 Umgang mit klassifizierten Informationen (T1, T2, T3)

Der DL muss die Vorgaben zur Klassifizierung von Informationen des AG einhalten und seine Mitarbeiter dahingehend nachweislich unterweisen.

Alle Informationen des AG sind ihrer Vertraulichkeitsklasse entsprechend eindeutig eingeordnet und gekennzeichnet. Die Informationsklassifizierung richtet sich dabei nach dem möglichen Einfluss auf das Geschäft des AG, der sich aus einer vorsätzlichen oder nicht beabsichtigten Bekanntgabe der Informationen ergeben kann.

Der AG hat die nachfolgenden Vertraulichkeitsklassen festgelegt, aus denen sich jeweils unterschiedliche Konsequenzen für die Handhabung der relevanten Informationen ergeben.

Tabelle 1: Vertraulichkeitsklassen

Vertraulichkeits-klasse	Beschreibung
(S0) - öffentlich	Eine Verbreitung bleibt regelmäßig ohne Beeinträchtigung der Interessen des EN-TEGA-Konzerns, eines Unternehmens im ENTEGA-Konzern, seiner Mitarbeiter, Vertragspartner, Kunden oder Dritter. Die Dokumente sind standardmäßig mit dem Vermerk "S0 - öffentlich" gekennzeichnet. Beispiele: Informationen ohne vertraulichen oder geheimen Charakter, die für die Öffentlichkeit bestimmt sind, bspw.: Werbung; Öffentlichkeitsarbeit
(S1) - intern	Eine Verbreitung kann regelmäßig für die Interessen des ENTEGA-Konzerns, eines Unternehmens im ENTEGA-Konzern, seiner Mitarbeiter, Vertragspartner, Kunden oder Dritter nachteilig sein. Die Dokumente sind standardmäßig mit dem Vermerk "S1 - intern / Konzern" oder "S1 - intern / <Gesellschaftskürzel>" gekennzeichnet. Beispiele: Informationen ohne vertraulichen oder geheimen Charakter, die nicht für die Öffentlichkeit bestimmt sind, bspw.: Betriebliche Informationen an Mitarbeiter; Arbeitsanweisungen
(S2) - vertraulich	Eine Verbreitung kann regelmäßig für die Interessen des ENTEGA-Konzerns, eines Unternehmens im ENTEGA-Konzern, seiner Mitarbeiter, Vertragspartner, Kunden oder Dritter schädlich sein. Die Dokumente sind standardmäßig mit dem Vermerk "S2 - vertraulich" oder "S2 - vertraulich / Berechtigte <Gesellschaftskürzel / OE>" gekennzeichnet. Beispiele: • Bestimmte sensible personenbezogene Daten, bspw. private Adressen etc. (je nach Schutzbedarf) • Verträge • Betriebs- und Geschäftsgeheimnisse Hinweis: Jeweilige Einstufung in Abhängigkeit des Risikos bei (ungewollter) Verbreitung
(S3) - geheim	Eine Verbreitung kann regelmäßig die Sicherheit von Mitarbeitern des ENTEGA-Konzerns gefährden oder den Interessen des ENTEGA-Konzerns, eines Unternehmens im ENTEGA-Konzern, seiner Mitarbeiter, Vertragspartner, Kunden oder Dritter schweren Schaden zufügen. Die Dokumente sind standardmäßig mit dem Vermerk "S3 - geheim" oder "S3 - geheim / Berechtigte <Gesellschaftskürzel / OE>" gekennzeichnet. Beispiele: • KRITIS-Informationen • Besonders sensible personenbezogene Daten, bspw. medizinische Informationen • Betriebs- und Geschäftsgeheimnisse Hinweis: Jeweilige Einstufung in Abhängigkeit des Risikos bei (ungewollter) Verbreitung
(S4) - streng geheim	Eine Verbreitung kann regelmäßig den Bestand/Existenz von Unternehmen des ENTEGA-Konzerns oder lebenswichtige Interessen des ENTEGA-Konzerns, eines Unternehmens im ENTEGA-Konzern, seiner Mitarbeiter, Vertragspartner, Kunden oder Dritter gefährden. Die Dokumente sind standardmäßig mit dem Vermerk "S4 – streng geheim" oder "S4 – streng geheim / Berechtigte <Gesellschaftskürzel / OE>" gekennzeichnet. Beispiele: • KRITIS-Informationen • Besonders sensible personenbezogene Daten, bspw. medizinische Informationen • Betriebs- und Geschäftsgeheimnisse Hinweis: Jeweilige Einstufung in Abhängigkeit des Risikos bei (ungewollter) Verbreitung

3.1 Verarbeitung sensibler Informationen (T1, T2, T3)

Zu den besonders schützenswerten Daten der Vertraulichkeitsklassen „S2 vertraulich“, „S3 – geheim“ und „S4 – streng geheim“ des AG werden insbesondere die folgenden Informationen gezählt:

- Informationen zur Konfiguration und Implementierung von Sicherheitsmaßnahmen
- Passwörter und Authentisierungsinformationen
- Netzwerkpläne, -konfigurationen und IP-Adress-Informationen
- Aufbau und Konfiguration von Systemen und Komponenten der IT- und Prozessleittechnik des AG.

Diese Daten werden im Sinne der hier dargestellten Sicherheitsanforderungen auch als "sensibel" bezeichnet und können zusätzlich den oben aufgeführten Vertraulichkeitsstufen „S2 vertraulich“, „S3 – geheim“ und „S4 – streng geheim“ unterliegen.

Informationen, die von wirtschaftlichem Wert sind, Gegenstand von angemessenen Geheimhaltungsmaßnahmen sind oder bei denen ein berechtigtes Interesse an der Geheimhaltung besteht, werden gemäß den Vorgaben des Geschäftsgeheimnisgesetzes behandelt und entsprechend gekennzeichnet.

3.2 Zugriffsschutz, Speicherung und Entsorgung (T1, T2, T3)

Werden Daten des AG durch den DL verarbeitet, so hat dieser sicherzustellen, dass der Zugriff auf diese Daten auf einen minimalen Kreis berechtigter Mitarbeiter eingeschränkt wird.

Werden sensible Daten auf mobilen Komponenten gespeichert (z. B. Notebooks, mobile Datenträger etc.), sind diese durch eine Verschlüsselung nach Stand der Technik zu sichern.

Werden IT-Systeme oder Komponenten des DL, auf denen sensible Daten des AG gespeichert sind, zur Reparatur gegeben oder einer Entsorgung zugeführt, muss gewährleistet sein, dass diese Daten nicht für Dritte, auch nicht unter Verwendung von Daten-Wiederherstellungstechnologien, lesbar oder anderweitig auswertbar sind.

Der Stand der Technik zur sicheren Vernichtung von Informationen ist nachweislich anzuwenden.

3.3 Übermittlung in Netzwerken (T1, T2, T3)

Datenverkehr, über den sensible Informationen zwischen AG und DL über ein unsicheres Netz (z. B. Internet) ausgetauscht werden, muss mit Hilfe anerkannter technischer Verfahren gegen Manipulation oder Einsichtnahme geschützt werden.

(T2, T3) Dafür sind in der Regel VPN-Lösungen einzusetzen, deren kryptographische Algorithmen dem aktuellen Stand der Technik entsprechen.

(T2, T3) Der VPN-Tunnel muss nach Beendigung der Kommunikation abgebaut werden; eine dauerhafte Einrichtung eines solchen Tunnels zwischen AG und DL ist untersagt.

(T1, T2, T3) Werden per E-Mail sensible Informationen zwischen AG und DL ausgetauscht, so muss der Mailverkehr kryptographisch gesichert werden. Der DL trägt Sorge für die entsprechenden technischen Voraussetzungen auf seiner Seite.

4 Anforderungen an die Wartungsprozesse (T2, T3)

Unter "Wartung" werden alle vom DL erbrachten Servicemaßnahmen verstanden, die sich auf die Komponenten oder Systeme der technischen IT-Umgebung des AG auswirken.

Servicemaßnahmen können beispielsweise sein:

- Instandhaltungs- und Reparaturarbeiten
- Fehleranalyse- und Fehlerbehebungsarbeiten
- Installation von Softwareupdates oder neuen Firmware- oder Betriebssystemen bzw. Applikationen
- System-, Geräte oder Software-Anpassungen, Neuparametrierungen u. Ä.

Wartungsarbeiten können innerhalb eines Remote-Zugriffs über eine Fernwartungsinfrastruktur bei DL und AG, als auch in Form von Vor-Ort-Arbeiten (z. B. Anschluss mobiler Geräte an das Netzwerk oder die IT- und Prozesstechnikkomponenten des AG) durchgeführt werden.

4.1 Allgemeines (T2, T3)

Wartungsarbeiten durch den DL erfolgen ausschließlich durch qualifiziertes und geschultes Personal. Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen des AG nachweislich zu schulen, ggf. sind entsprechende Sicherheitsüberprüfungen nachzuweisen.

Alle zur Wartung genutzten Systeme müssen mit einem sicheren logischen Zugangsschutz versehen sein sowie vor einem unberechtigten physischen Zugriff geschützt werden.

Die anderweitige Nutzung von für Wartungsarbeiten genutzten Systemen / Komponenten ist durch den DL zu untersagen. Dies gilt auch für den Fall, dass auf den Systemen eigens für die Wartung installierte virtuelle Maschinen (Betriebssystem und Applikationen) verwendet werden.

4.2 Sichere Systemkonfiguration von Wartungskomponenten (T3)

Für Wartungsarbeiten sind ausschließlich Systeme zu verwenden, die anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik sicher konfiguriert und gehärtet sind.

Die Systeme müssen beim Wartungszugriff über einen aktiven Schadsoftwareschutz, basierend auf aktuellsten AV-Pattern, verfügen.

4.3 Fernwartung (T3)

Fernwartungszugriffe dürfen nur über die vom AG zur Verfügung gestellten Fernwartungszugänge realisiert werden.

Die zur Fernwartung berechtigten Mitarbeiter sind dem AG namentlich mitzuteilen.

Fernwartungszugriffe dürfen auf Seiten des DL nur aus einem nach Stand der Technik gesicherten und gegen unberechtigte Zugriffe geschützten Wartungsnetzwerk erfolgen. Sollen Fernwartungszugriffe direkt von Arbeitsplatzsystemen oder anderen Systemen (z. B. mobile Systeme, Heimarbeitsplatz) erfolgen, muss dies dem AG mitgeteilt und von diesem explizit genehmigt werden.

Fernzugriffe werden auf einem Terminalserver / Jumphost in einer separaten Sicherheitszone des AG terminiert. Der AG legt die technisch / organisatorischen Parameter für die Einwahl fest und übermittelt diese an den DL. Der DL benennt die

für die Wartungsarbeiten benötigten Programme und Tools, welche auf den Systemen bereitgestellt werden müssen, stellt diese zur Installation zur Verfügung und stellt notwendige Aktualisierungen sicher.

Ein direkter Zugriff auf die zu wartenden Systeme des AG unter Umgehung des Terminalservers / Jumphost ist nicht zulässig.

5 Meldung von Informationssicherheitsvorfällen (T1, T2, T3)

Wenn beim DL ein Informationssicherheitsvorfall vorliegt, der Auswirkungen auf die vom DL an den AG gelieferten Produkte oder Dienstleistungen hat oder auf andere Weise die Informationssicherheit des AG gefährdet, ist der DL verpflichtet, den AG unverzüglich darüber zu informieren.

Wenn Zweifel darüber bestehen, ob es sich tatsächlich auch um einen Informationssicherheitsvorfall handelt, muss dies trotzdem gemeldet werden.

Kontaktaufnahme

Hotline Informationssicherheit:	06151-701 8088
E-Mail-Adresse e-netz:	Lieferantenverpflichtung@e-netz-suedhessen.de
Post-Anschrift e-netz:	e-netz Südhessen AG Dornheimer Weg 24 64239 Darmstadt
E-Mail-Adresse citiworks:	Lieferantenverpflichtungen@citiworks.de
Post-Anschrift citiworks:	citiworks AG Frankfurter Straße 110 64293 Darmstadt