# Unterlagen zur Selbstauskunft von Dienstleistern der Stadtwerke Völklingen Netz GmbH

## Informationssicherheitsanforderungen

*Anforderungen für Dienstleister an ein Mindestniveau von Schutzmaßnahmen im Hinblick auf dessen IT-Systeme und Prozesse*

| | |
|---|---|
| Version | |
| Datum der Version | |
| Erstellt durch | |
| Genehmigt durch | |

| | |
|---|---|
| Gültig ab | Wiedervorlage |
| Stichworte (Tags) | ISMS Informationssicherheitsselbstauskunft Dienstleister |
| Klassifizierung | Vertraulich |
| Status | Geltend |
| Verteiler | Dienstleister im Geltungsbereich des ISMS |

# Inhaltsverzeichnis

# 1. Ziele und Anwendungsbereiche

Die hier defnierten Mindestanforderungen für Dienstleister im Betrieb der Prozessdatenverarbeitung sollen einen angemessenen Schutz der leittechnischen Komponenten und Infrastrukturen im Prozessumfeld gewährleisten. Dabei wird ein Mindestniveau von Schutzmaßnahmen festgeschrieben, welche von jedem Dienstleister im Hinblick auf dessen IT-Systeme und Prozesse zu erfüllen sind. Eine genaue Definition von umsetzungsrelevanten Techniken und produktspezifischen Lösungen ist nicht Bestandteil dieser Richtlinie, da die konkrete Planung und Umsetzung in der Verantwortung des jeweiligen Dienstleisters liegen.

Diese Richtlinie und deren Vorgaben sind von allen Dienstleistern einzuhalten, die Zugriff auf Komponenten und Infrastrukturen erhalten sollen, die von der Stadtwerke Völklingen Netz GmbH betrieben werden. Dazu zählen insbesondere:

- Dienstleister, die direkt oder über einen Remote-Zugang auf leittechnische Komponenten bzw. Infrastrukturen der Stadtwerke Völklingen Netz GmbH zugreifen,
- Dienstleister, die sensible Daten aus dem leittechnischen Bereich der Stadtwerke Völklingen Netz GmbH in eigenen IT- Systemen speichern oder verarbeiten.
- Dienstleister die Hardware / Software an Stadtwerke Völklingen Netz GmbH verkaufen bzw. installieren

Dienstleister sind angehalten eine qualifizierte Selbstauskunft über die Einhaltung und Umsetzung der im Folgenden festgeschriebenen Anforderungen zu erteilen. Dabei ist neben der textlichen Beschreibung der eingesetzten Maßnahme ein Realisierungsgrad der Umsetzung mit anzugeben. Mit dem Einreichen der Selbstauskunft verpflichtet sich der Dienstleister zur Einhaltung der Anforderungen dieser Sicherheitsrichtlinie. In Ausnahmen kann auf schriftlichen Antrag, abweichend von den im Folgenden geforderten Maßnahmen, eine Ausnahme durch den Informationssicherheitsbeauftragten der Stadtwerke Völklingen Netz GmbH – Herrn Thomas Heß genehmigt werden.

Alle auf diese Sicherheitsrichtlinie verpflichteten Dienstleister müssen die Einhaltung der vereinbarten Maßnahmen rechtlich verbindlich zusichern. Eine entsprechende Verpflichtungserklärung wird Bestandteil der Beauftragung. Die Selbstauskunft ist vor der erstmaligen Verpflichtung auf diese Sicherheitsrichtlinie vom Dienstleister einzureichen. Änderungen der IT-Umgebung des Dienstleisters, welche die Einhaltung der Sicherheitsrichtlinie betreffen, sind dem Informationssicherheitsbeauftragten der Stadtwerke Völklingen Netz GmbH – Herrn Thomas Heß mitzuteilen und ggf. eine aktualisierte Selbstauskunft einzureichen.

Die Stadtwerke Völklingen Netz GmbH behält sich vor, einmal pro Kalenderjahr oder bei konkreten Sicherheitsvorfällen und -verstößen, eine aktualisierte Selbstauskunft des Dienstleisters anzufordern und die Umsetzung der Sicherheitsrichtlinie durch ein Audit am Ort des Dienstleisters zu überprüfen.

Die Kontaktdaten des Informationssicherheitsbeauftragten der Stadtwerke Völklingen Netz GmbH lauten :

Thomas Heß
Hohenzollernstraße 10
66333 Völklingen
Telefonnummer : +49 6898 150 104
Mobil : +49 176 1001 0873
e-mail : bi@swvk.de

## 2. Verweise auf Regularien

Die aufgeführten Sicherheitsanforderungen stützen sich auf die Anforderungen des IT-Sicherheitskatalogs der BNetzA, sowie der dort zitierten Normen ISO 27001, 27002 und 27019.

## 3. Bewertung

Der Grad der Umsetzung einer Anforderung wird in den 3 Stufen gemessen:

- 0%: nicht begonnen
- 50%: teilweise umgesetzt
- 100%: voll umgesetzt

Beispiel :

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

| |
|---|
| |

Im Kommentarfeld können genauere Angaben zur Art und dem Grad der Umsetzung gemacht werden. Falls eine Anforderung bei einem Dienstleister nicht zutrifft, kann die Option „Nicht“ angekreuzt und im Kommentarfeld erläutert werden. Reicht das vorgesehene Kommentarfeld nicht aus, besteht die Möglichkeit in einem Anhang zu diesem Dokument zu den einzel abgefragten Punkten detaillierte Angaben zu machen.

# 4. Sicherheitsanforderungen

## 4.1. Allgemeines, Organisation

Für einen angemessenen Umgang mit Fragen der Informationssicherheit sind grundsätzliche Regelungen im Hause des Dienstleisters erforderlich.

### 4.1.1. Ansprechpartner für Informationssicherheit

Es ist ein Ansprechpartner zu benennen, der verbindliche Auskünfte zur Informationssicherheit im internen Bereich, als auch in Verbindung mit dem Projektumfang der Stadtwerke Völklingen Netz GmbH geben kann. Diese Aufgaben können auch von mehreren Mitarbeitern wahrgenommen werden, um auch im Falle der Abwesenheit eine Vertretung sicher zu stellen.

Name des Projekts, falls notwendig, bitte hier eintragen :

| |
|---|
| |

Ansprechpartner (Vor-, Zuname, Telefonnummer, Standort, Firma):

| |
|---|
| |

### 4.1.2. Berücksichtigung der Informationssicherheit

Im Rahmen der Beauftragung ist die Informationssicherheit sicherzustellen, beispielsweise durch die Formulierung umzusetzender IT-Sicherheitsanforderungen.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

| |
|---|
| |

### 4.1.3. Zugriffschutz für IT-Komponenten

Alle IT-Komponenten, von denen ein Zugriff auf die Ressourcen der leittechnischen Infrastruktur der Stadtwerke Völklingen Netz GmbH möglich ist, müssen mit einem Zugriffschutz vor unbefugter Benutzung geschützt sein. Es ist dabei sowohl der physische Zugriff als auch der logische Zugang zu schützen. Es ist sicherzustellen, dass nur namentlich benannte Mitarbeiter Zugang und Zugriff zu den leittechnischen Infrastrukturen erhalten.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

| |
|---|
| |

### 4.1.4. Verbot der privaten Nutzung

Alle IT-Komponenten, von denen ein Zugriff auf die Ressourcen der leittechnischen Infrastruktur der Stadtwerke Völklingen Netz GmbH möglich ist, dürfen nur für dienstliche Zwecke genutzt werden. Eine private Nutzung ist nicht zulässig. IT-Komponenten, für die eine private Nutzung nicht explizit ausgeschlossen ist, dürfen nicht für den Zugriff auf die leittechnischen Infrastrukturen und Komponenten der Stadtwerke Völklingen Netz GmbH verwendet werden. Dies gilt auch für die Komponenten der Dienstleister IT-Infrastruktur, die zum Zugriff auf die Ressourcen der Stadtwerke Völklingen Netz GmbH genutzt werden. Sofern IT-Komponenten zum Zugriff genutzt werden sind entsprechende Schutzmaßnahmen zu ergreifen und auszuweisen.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

| |
|---|
| |

### 4.1.5. Einsatz sicherer Passwörter

Passwörter, die zur Zugangssicherung verwendet werden, müssen eine hohe Passwortgüte besitzen (Mindestlänge, Groß-/Kleinschrift, Sonderzeichen und Zahlen). Der Dienstleister muss über eine entsprechende Passwortrichtlinie verfügen. Eine Verwendung von Passwort- Speicher-Programmen zur Projektumsetzung von Stadtwerke Völklingen Netz GmbH beauftragten Projekten bedarf einer Genehmigung durch die Stadtwerke Völklingen Netz GmbH nach Vorlage des Sicherheitskonzeptes

durch den Dienstleister. Ohne eine vorausgegangene Genehmigung dürfen keine Passwörter gespeichert werden.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.1.6. Notfallvorsorge

Der Dienstleister hat durch ein Business Continuity Management (BCM) sicher zu stellen, dass im Rahmen einer Notlage oder eines Krisenfalls die Aufrechterhaltung der nötigen Servicequalität und die schnellstmögliche Wiederherstellung aller für Stadtwerke Völklingen Netz GmbH bereitzustellenden Dienste gesichert ist.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

## 4.2. Umgang mit Informationen

### 4.2.1. Allgemeines

Informationen und Daten, die im Rahmen der Dienstleistertätigkeit anfallen oder dem Dienstleister bekannt werden, müssen vertraulich behandelt werden. Diese Informationen und Daten sind gemäß dieser Klassifizierung zu schützen und zu behandeln. Dies gilt insbesondere bei der Übertragung über öffentliche Netze, beim Versand als Briefpost und bei der Speicherung auf Datenträgern. Informationen und Daten (in elektronischer bzw. gedruckter Form), die nicht mehr benötigt werden, müssen nachweislich nicht wiederherstellbar gelöscht bzw. zerstört werden.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.2.2. Speicherung

Sofern vertrauliche oder sicherheitsrelevante Daten auf mobilen Datenträgern (Notebook, CDs, USB-Massenspeicher) gespeichert werden, müssen diese Daten kryptographisch stark verschlüsselt werden. Sofern die Daten auf externen Datenträgern gespeichert werden, hat der Dienstleister für den physikalischen Schutz und die sichere Verwahrung Sorge zu tragen.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.2.3. Datenübertragung

Werden vertrauliche oder sicherheitsrelevante Daten über öffentliche oder anderweitig nicht vertrauenswürdige Netzwerke übertragen, muss die Übertragung kryptographisch stark verschlüsselt sein. Daten dürfen dabei als E-Mail nur versendet werden, wenn diese ebenfalls kryptographisch stark verschlüsselt wurden. Es ist dabei zu beachten, dass den Stadtwerken Völklingen Netz GmbH eine Möglichkeit zur Entschlüsselung der Daten zur Verfügung steht.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.2.4. Informationsverarbeitung außerhalb der EU

Informationen und Daten, die im Rahmen der Dienstleistertätigkeit anfallen oder dem Dienstleister bekannt werden, dürfen nicht in ein Land außerhalb der EU übertragen, dort verarbeitet oder gespeichert werden.

Eine Bearbeitung von Informationen außerhalb der EU muss zuvor von der Stadtwerke Völklingen Netz GmbH genehmigt werden. Übertragung, Speicherung und/oder Verarbeitung erfolgt in:

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.2.5. Reparatur von IT-Komponenten und Systemen

Werden Systeme oder Komponenten, die vertrauliche Daten enthalten oder verarbeiten zur Reparatur oder Entsorgung gegeben, so ist die Wahrung der Vertraulichkeit sicherzustellen.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

## 4.3. Mitarbeiter und gegebenenfalls eingesetzte Subunternehmer

Neben den Einweisungen der Stadtwerke Völklingen Netz GmbH sind die Mitarbeiter des Dienstleisters und eventuellen Subunternehmern bzgl. grundsätzlicher Regelungen zur Informationssicherheit zu unterweisen und zu verpflichten. Dies ist nachzuweisen.

### 4.3.1. Vertraulichkeitsvereinbarung

Die Mitarbeiter sind durch ihren Arbeitsvertrag bzw. getrennte Verpflichtungserklärungen auf Vertraulichkeit und Einhaltung der informationssicherheitsspezifischen und datenschutzrechtlichen Bestimmungen auch über das Ende ihrer Beauftragung hinaus zu verpflichten.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

| |
|---|
| |

### 4.3.2. Sicherheitsunterweisung

Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen der IT-Ressourcen der Stadtwerke Völklingen Netz GmbH zu informieren. Das betrifft insbesondere die möglichen Risiken, adäquate Gegenmaßnahmen sowie die persönlichen Verantwortungen der Mitarbeiter im Rahmen ihrer Tätigkeiten. Zusätzlich sind die Mitarbeiter in Bezug auf Informationssicherheit regelmäßig durch entsprechende Schulungen oder Mitteilungen zu unterweisen. Hierzu gehören auch sicherheitsbezogene Informationen bei Einführung neuer Techniken und Verfahren. Die Sicherheitsunterweisungen sind zu belegen.

## 4.4. Netzwerksicherheit

Die Informationssicherheit im Netzwerk des Dienstleisters muss gewährleistet sein, da im Rahmen der Erbringung durch den Dienstleister in der Regel Informationen und Applikationen durch Netzkopplung oder anderweitige Einbringung in die leittechnischen Infrastrukturen der Stadtwerke Völklingen Netz GmbH gelangen bzw. übertragen werden.

### 4.4.1. Schutz des internen Netzwerks

Das interne IT-Netzwerk des Dienstleisters ist gegenüber externer Netzwerke am Netzübergang mindestens durch eine Paketfilter-Firewall zu schützen. Diese Firewall darf nur explizit benötigte und freigegebene Dienste erlauben.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

| |
|---|
| |

### 4.4.2. Erreichbare, externe Dienste und Remote-Access

Direkte Zugriffe aus dem Internet in das interne IT-Netzwerk der Stadtwerke Völklingen Netz GmbH sind nicht zulässig und müssen von der Firewall unterbunden werden. Sofern Remote-Access in das interne IT-Netzwerk erforderlich oder Dienste (z.B. Mailserver) von öffentlichen Netzwerken aus erreichbar sind, muss sichergestellt sein, dass dies die zum Zugriff oder zur Erbringung genutzten IT-Komponenten nicht schädigen oder beeinträchtigen kann. Einen Nachweis (bspw. Sicherheitsaudit) ist Stadtwerke Völklingen Netz GmbH auf Anfrage zur Verfügung zu stellen.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

## 4.5. Schutz vor Schadsoftware

Der Dienstleister muss ein wirksames Konzept zum Schutz der IT-Komponenten vor Schadsoftware im eigenen Haus umgesetzt haben. Dieses Konzept muss jeweils dem aktuellen Stand der Technik entsprechen und ggf. kontinuierlich der technischen Entwicklung angepasst werden.

### 4.5.1. Virenschutz

Der Dienstleister muss einen geeigneten Schutz vor Viren und sonstiger Schadsoftware auf allen seinen Arbeitsplatzrechnern betreiben. Dieser Schutz darf vom Benutzer nicht unterbunden werden können und muss kontinuierlich auf einem aktuellen Stand gehalten werden. Die eingesetzte Technologie muss eine Möglichkeit zum Überprüfen einzelner Dateien nach Benutzerwunsch aufweisen (bspw. zur Überprüfung von Dateien vor der Zustellung an die Stadtwerke Völklingen Netz GmbH). Weiterhin muss eine Überprüfung von Daten und Informationen im Netzwerk- und Serverbereich (z.B. Mail-Server, FTP) eingesetzt werden, um eine Verbreitung von Viren und anderer Schadsoftware vorzubeugen.

Erklärung der Umsetzung:

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.5.2. Zeitnahes Einspielen von Sicherheitsupdates

Für das eingesetzte Betriebssystem und die verwendeten Kommunikationsprogramme, sind Sicherheitsupdates nach deren Verfügbarkeit umgehend einzuspielen. Auch sind die Firewall und sämtliche öffentlich erreichbaren Server kontinuierlich auf dem aktuellen Stand zu halten. Sicherheitsupdates sind auf diesen Systemen ebenfalls einzuspielen.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

## 4.6. Wartungssysteme und Remotezugang

Wartungssysteme im Sinne dieser Richtlinie sind Systeme, welche zur Instandhaltung, Störungsanalyse, Fehler- und Störungsbehebung, Verbesserung, Anpassung usw. genutzt werden können. Komponenten und Netzwerke, die direkt mit den leittechnischen Infrastrukturen der Stadtwerke Völklingen Netz GmbH verbunden werden, sind besonders zu schützen. Insbesondere gilt dies für mobile Geräte, wie mobile Arbeits-PCs, Programmiergeräte und Speichermedien.

### 4.6.1. Allgemeines

Der Dienstleister darf nur über die zuvor von Stadtwerke Völklingen Netz GmbH genehmigten Remotezugänge zu Fernwartungszwecken auf die leittechnischen Infrastrukturen der Stadtwerke Völklingen Netz GmbH zugreifen. Die berechtigten Mitarbeiter des Dienstleisters werden zuvor den Stadtwerken Völklingen Netz GmbH benannt und ausreichend in der Benutzung der Remotezugangslösung geschult bzw. unterwiesen. Die Systeme auf Seiten des Dienstleisters sind speziell gesichert, sodass die Systeme nur über spezielle Zugriffs- und Zugangsberechtigungen aktiviert werden können. Automatisierte Abläufe des Dienstleisters dürfen keinen interaktiven Zugang zu den leittechnischen Infrastrukturen und Komponenten der Stadtwerke Völklingen Netz GmbH ermöglichen. Vor und nach Remotearbeiten ist das zuständige Personal der Stadtwerke Völklingen Netz GmbH zu kontaktieren.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.6.2. Physikalische Sicherheit

Die zum Zugriff benötigten Komponenten sind durch entsprechende Maßnahmen vor unberechtigtem physikalischem Zugriff zu sichern (bspw. durch getrennte Installation in verschlossenen Räumen mit angemessenem Zugangsschutz, verschlossene Schränke im Falle der Lagerung usw.).

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.6.3. Grundsicherung und Systemhärtung

Alle eingesetzten Systeme und Komponenten sind anhand anerkannter Best-Practice- Guides und nach aktuellem Stand der Technik zu härten und mit aktuellen Sicherheitspatches zu schützen. Nicht benötigte Benutzer, Dienste, Programme und Funktionen sind zu deinstallieren und gegen unbefugte Reaktivierung zu sichern. Diese Grundkonfiguration und Systemhärtung muss dokumentiert sein.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.6.4. Virenschutz

Insbesondere mobile Wartungssysteme müssen über einen Virenschutz und kontinuierlich aktualisierte Virenpattern verfügen. Vor einem Zugriff auf die leittechnischen Infrastrukturen ist die Aktualität zu überprüfen und auf Nachfrage Stadtwerke Völklingen Netz GmbH nachzuweisen. Der Virenschutz darf nicht vom Benutzer deaktiviert werden können.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

### 4.6.5. Wartungssysteme zur Vor-Ort-Wartung

Systeme die zur Vor-Ort-Wartung eingesetzt werden, dürfen bei der Benutzung an den leittechnischen Infrastrukturen der Stadtwerke Völklingen Netz GmbH nicht gleichzeitig mit öffentlichen oder nicht vertrauenswürdigen Netzwerken verbunden werden.

Umsetzungsgrad in %

0 % : ☐ 50 % : ☐ 100% : ☐ Nicht : ☐

Kommentar :

## 5. Bestätigung des Dienstleisters

Es wird versichert, dass die oben dokumentierten Angaben wahrheitsgemäß sind. Alle Abweichungen werden der Stadtwerke Völklingen Netz GmbH unverzüglich bekannt gemacht.

---

Datum, Stempel und Unterschrift des Dienstleisters

Abgabe mit Anhang : ☐ - falls Anhänge abgegeben werden – bitte hier Liste beifügen :

## 6. Bestätigung der Stadtwerke Völklingen Netz GmbH

Die Selbstauskunft wurde überprüft und die aufgeführten Sicherheitsmaßnahmen als ausreichend befunden.

_____

Datum, Stempel und Unterschrift des Informationssicherheitsbeauftragten der Stadtwerke Völklingen Netz GmbH