**Informationssicherheitsleitlinie****der <Namen der Organisation>**

**Anwendungshinweis (Bitte vor Benutzung entfernen):**

Wir bitten Sie in Kenntnis zu nehmen, dass die vorliegende Richtlinie mit größter Sorgfalt erstellt und geprüft wurde, jedoch keinen Anspruch auf Vollständigkeit erhebt. Sie muss auf Ihre Organisation und auf deren Gegebenheiten individuell angepasst sowie zugeschnitten werden und dient hierfür als Hilfestellung und mögliches Beispiel.

**Hinweis für Kommunen:** Diese Mustervorlage ist explizit auf KRITIS-Betreiber zugeschnitten. Das LSI empfiehlt für die Zielgruppe der Kommunen die Verwendung folgender Vorlage:

* <https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf>
* [www.landkreistag.de/images/stories/themen/ITSicherheit/2024\_Handreichung\_IT-Sicherheit.pdf](http://www.landkreistag.de/images/stories/themen/ITSicherheit/2024_Handreichung_IT-Sicherheit.pdf)

Dokumenteneigenschaften

|  |  |
| --- | --- |
| **Titel** | Informationssicherheitsleitlinie |
| **Art** | Leitlinie |
| **Hauptverantwortlicher** | <Name der Organisationsleitung> |
| **E-Mail, Telefon** | <E-Mail-Adresse, Telefonnummer> |
| **Ansprechpartner** | <Name des Ansprechpartners der Richtlinie / ISB> |
| **E-Mail, Telefon** | <E-Mail-Adresse, Telefonnummer> |
| **Version** | <x.x> |
| **In Kraft seit** | <xx.xx.2022> |
| **In Kraft gesetzt durch** | <Name der Organisationsleitung / des Verantwortlichen> |
| **Überarbeitungsintervall** | <25 Monate> |
| **Nächste Überarbeitung** | <yy.yy.2023> |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Änderung** | **Datum** | **Autor** |
| v.1.0 | Initialerstellung | 01.01.2022 | LSI |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhalt**

[1. Einleitung 4](#_Toc95826433)

[2. Geltungsbereich 4](#_Toc95826434)

[3. Stellwert der Informationssicherheit 4](#_Toc95826435)

[4. Zweck der Leitlinie 4](#_Toc95826436)

[5. Sicherheitsziele 5](#_Toc95826437)

[6. Sicherheitsstrategie und Aufbauorganisation 6](#_Toc95826438)

[7. Grundsätze der Informationssicherheit 6](#_Toc95826439)

[8. Organisation 7](#_Toc95826440)

[9. Kontinuierliche Weiterentwicklung 8](#_Toc95826441)

[Inkrafttreten 8](#_Toc95826442)

# Einleitung

Informationssicherheit gewinnt mit zunehmender Digitalisierung fortlaufend an Bedeutung. Auch für Wasserversorger werden die Absicherung der Steuerungs- sowie der IT-Systeme gegenüber Ausfällen und der Schutz vor Cyberangriffen immer wichtiger. Wir haben deshalb beschlossen, das Thema Informationssicherheit im Kontext „Sichere Trinkwasserversorgung für unsere Kunden“ gezielt anzugehen. Bei dem folgenden Dokument handelt es sich um die Informationssicherheitsleitlinie der <Namen der Organisation>.

# Geltungsbereich

Diese Informationssicherheitsleitlinie gilt für den gesamten Bereich, in dem die <Namen der Organisation> tätig ist. Alle Mitarbeiter haben diese zu beachten und einzuhalten. Bei der Beauftragung von externen Dienstleistern sind diese über die Leitlinie in Kenntnis zu setzen und zur Einhaltung zu verpflichten.

# Stellwert der Informationssicherheit

Informationssicherheit stellt für Wasserversorger einen zentralen Baustein dar, um die Wasserversorgung der Bürgerinnen und Bürger ununterbrochen zu gewährleisten. Aufgrund fortschreitender Technisierung von Wasserwerken entstehen dadurch nicht nur neue Chancen, sondern auch zunehmend Risiken bezüglich der Informationssicherheit, welche unmittelbare Auswirkungen auf den reibungslosen Betrieb haben können.

Dabei können Gefahren sowohl von den eingesetzten technischen Systemen, als auch von organisatorischen Fehlern ausgehen.

Ziel ist es, das Werk hinsichtlich der Verfügbarkeit so abzusichern, dass es zu keinerlei Ausfällen oder Engpässen in der Versorgung kommt. Falls es Angreifern gelingt, die Kontrolle über die Anlagen zu erlangen, wäre eine Versorgung der Bevölkerung nicht mehr sichergestellt. Außerdem ist die Wahrung der Integrität der für den Betrieb notwendigen und schützenswerten Daten essenziell, um die Verfügbarkeit und somit auch die Versorgung zu garantieren, da bei der Übermittlung falscher Daten ein Ausfall der Versorgung droht. Gleiches gilt für die Vertraulichkeit. Kundendaten und vertrauliche Betriebsdaten dürfen Unberechtigten nicht zugänglich werden.

# Zweck der Leitlinie

Die IT-Sicherheitsleitlinie hat den Zweck, das gesamte Personal für ihren Stellenwert der Informationssicherheit zu sensibilisieren sowie nachhaltige Verbesserungsmaßnahmen anzustoßen. Sie dient dem Überblick über die Unternehmensziele und damit einhergehend auch über die Informationssicherheitsziele. Dabei wird auch beschrieben, wie diese Ziele erreicht werden können. Zudem hebt die Leitlinie die Verantwortlichen für Informationssicherheit hervor und konkretisiert deren Rollen beim Erhalt und der Weiterentwicklung von Informationssicherheit. Zusätzlich stellt die Informationssicherheitsleitlinie den ersten Schritt in Richtung Entwicklung eines Informationssicherheitsmanagementsystems dar.

# Sicherheitsziele

Sicherstellung der Wasserversorgung

Das wichtigste Ziel stellt die Sicherstellung der Wasserversorgung für die Bevölkerung dar. Ausfälle sind unbedingt zu vermeiden und entsprechend abzusichern. Für Notfälle sind deshalb entsprechende Notfallpläne auszuarbeiten.

Bewusstsein für Informationssicherheit

Für die Gewährleistung der Informationssicherheit sind angemessene organisatorische und technische Maßnahmen nötig. Diese Schritte sind nur dann wirksam, wenn alle Mitarbeiter die denkbaren Gefährdungen kennen und entsprechend verantwortlich handeln. Fortbildungen auf regelmäßiger Basis zur Informationssicherheit können hierbei unterstützend wirken.

Einhaltung von Gesetzen und Vorschriften

Auch sollen die Maßnahmen für die Informationssicherheit zur Einhaltung der für das Unternehmen relevanten Vorschriften, vertraglichen Verpflichtungen und Gesetze beitragen.

Wichtigste zu beachtenden Rahmenbedingungen:

* <Datenschutz-Grundverordnung (DSGVO)>
* <Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)>
* <GmbHG §41 Abs 1 GmbH-Gesetz (GmbHG)>
* <Betriebsverfassungsgesetz (BVerfG)>
* <…>

Verfügbarkeit der IT-Systeme

Auf IT-Systemen verwaltete Geschäftsdaten müssen hinreichend schnell wiederverfügbar sein. Ausfälle sind zu vermeiden.

Vermeidung materieller Schäden

Durch die Veränderung von Daten, einen Verlust der Vertraulichkeit schutzbedürftiger Daten oder einen Ausfall einer IT-Anwendung oder eines Systems können sowohl materielle als auch finanzielle Schäden entstehen.

Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

Vertraulichkeit und Integrität der Informationen, die für das Unternehmen wichtig sind, sind zu schützen, egal in welcher Form sie vorliegen. Den Geheimhaltungsanweisungen ist ebenso im Umgang mit elektronischen Informationen sowie Dokumenten strikt zu folgen.

# Sicherheitsstrategie und Aufbauorganisation

Diese Informationssicherheitslinie stellt dar, wie das Management der Informationssicherheit bei der <Name der Organisation> geplant ist. Ein adäquates Sicherheitsniveau wird angestrebt.

Die Organisationsleitung hat einen Informationssicherheitsbeauftragten ernannt, welcher als erster Ansprechpartner für Fragen bezüglich der Informationssicherheit zur Verfügung steht. Dieser ist der Organisationsleitung direkt unterstellt und berichtet ihr unmittelbar. Ebenso findet ein regelmäßiger Austausch mit der IT-Leitung statt.

Des Weiteren wird in regelmäßigen, zeitlichen Abständen geprüft, ob die getroffen Sicherheitsmaßnahmen noch ausreichend sind.

Falls ein Sicherheitsvorfall festgestellt wird, informiert der Informationssicherheitsbeauftragte die Organisationsleitung oder den Verfahrensverantwortlichen. Außerdem kooperiert er im Rahmen seiner Aufgabenerfüllung bei Notwendigkeit mit anderen Organisationen und staatlichen Einrichtungen.

Nicht zur <Name der Organisation> gehörende Personen und Unternehmen, die aber Leistungen für dieses erbringen, sind vertraglich zu der Einhaltung der festgelegten Informationssicherheitsziele zu verpflichten. Falls personenbezogene Daten verarbeitet werden, sind die Regelungen zur Auftragsverarbeitung (<Artikel 28 DSGVO>) zu beachten. Für das Erreichen eines angemessenen Informationssicherheitsniveaus bei der Arbeit mit schützenswerten Daten werden die erforderlichen Personal- und Finanzmittel zur Verfügung gestellt.

Für den Sicherheitsbeauftragten werden alle erforderlichen Ressourcen zur Verfügung gestellt. Um die Aufgaben zu erfüllen, werden ihm geeignete Qualifizierungsmaßnahmen ermöglicht. Um einen ständigen und durchgehenden Schutz zu erreichen, werden Mitarbeiter regelmäßig für die Belange der IT-Sicherheit sensibilisiert und geschult.

# Grundsätze der Informationssicherheit

Die nachfolgenden Grundsätze bilden das Fundament der Informationssicherheit des <Name der Organisation>. Sie sind unbedingt zu beachten und einzuhalten.

Dokumentation und Weiterentwicklung

Sämtliche Absicherungsmaßnahmen sind sorgfältig zu dokumentieren und bei Bedarf anzupassen, um ein stabiles Schutzniveau aufrecht zu erhalten. Die Überprüfung der Maßnahmen sollte dabei mindestens einmal jährlich erfolgen.

Minimalprinzip des Zugriffs

Grundsätzlich ist jeder Mitarbeiterin und jedem Mitarbeiter nur so viel Zugriff auf Systeme und sensible Daten zu gewähren, wie auch tatsächlich für die Erfüllung der Aufgaben notwendig ist. Diese Maßnahme verhindert unautorisierten Zugriff und schützt damit die entsprechenden IT-Systeme.

Maximalprinzip des Schutzes

Je nach Schutzbedarf sind andere Maßnahmen erforderlich, um den reibungslosen Betrieb sicherzustellen. Deshalb ist eine entsprechende Vorgehensweise bei der Benutzung festzulegen.

Sensibilisierung der Mitarbeiter

Von allen Mitarbeitern wird ein verantwortungsvoller Umgang mit schützenswerten Daten und Systemen erwartet. Das gesamte Personal muss den Informationssicherheitsprozess unterstützen. Führungskräfte müssen sich dabei ihrer Vorbildfunktion bewusst sein.

# Organisation

Die Verantwortlichkeiten des <Name Wasserversorger> sind wie folgt gruppiert:

Organisationsleitung

Die <Name der Organisationsleitung> trägt die Gesamtverantwortung für alle Belange der Informationssicherheit der <Name der Organisation>.

**Informationssicherheitsbeauftragter**

Der Informationssicherheitsbeauftragte ist dafür zuständig, die Organisationsleitung regelmäßig über den laufenden Betrieb sowie den Stand der umgesetzten Maßnahmen hinsichtlich der Informationssicherheit zu unterrichten. Er organisiert Awareness-Schulungen für das Personal und schafft dadurch ein Bewusstsein für Informationssicherheit.

Bei der Beschaffung neuer Systeme ist der Informationssicherheitsbeauftragte frühzeitig einzubinden. Dies gilt ebenso bei der Implementierung neuer Verfahren. Die Freigabe erfolgt in Abstimmung mit der Organisationsleitung. Bezüglich der Erfüllung seiner Aufgaben als Informationssicherheitsbeauftragter ist er alleine an Weisungen der Organisationsleitung gebunden.

Bei Fragen zur Informationssicherheit steht der Informationssicherheitsbeauftragte beratend zur Seite. Er untersucht und meldet informationssicherheitsrelevante Ereignisse an die notwendigen Stellen.

<Weitere Aufgaben ergänzen>

Mitarbeiter

Mitarbeiter sollen sich jederzeit ihrer Verantwortung im Umgang mit den Systemen und der darauf verarbeiteten Daten bewusst sein.

Bei Auffälligkeiten oder Unregelmäßigkeiten im Betrieb ist der Informationssicherheitsbeauftragte unverzüglich zu unterrichten, um frühzeitig reagieren zu können und Ausfällen vorzubeugen.

Entsprechende Awareness-Schulungen sind wahrzunehmen und Maßnahmen, welche der Informationssicherheit dienen, müssen eingehalten werden.

Weitere Verantwortlichkeiten

[Je nach Größe der Organisation]

# Kontinuierliche Weiterentwicklung

Der <Name der Organisation> verpflichtet sich zur kontinuierlichen Weiterentwicklung der Informationssicherheit.

# Inkrafttreten

Diese Informationssicherheitsrichtlinie tritt zum <tt.mm.jjjj> in Kraft und wird allen Mitarbeiterinnen und Mitarbeitern kenntlich gemacht.

|  |  |  |
| --- | --- | --- |
| Ort, Datum |  | Unterschrift Organisationsleitung |
|  |  |  |
|  |  |  |
|  |  |  |