|  |  |
| --- | --- |
| HoP-01-01 Direktive zur Informationssicherheit & Informationssicherheitsmanagement ISM | |
| **Dokumenten-ID** | Strom.V01.01 |
| **House of Policy** | Vorgabe auf Level 1 |
| **Dokumententyp** | Direktive |
| **Erlassen am** | xx.xx.2024 |
| **Erlassen durch** | STROM AG CIO (Chief Information Officer) |
| **Genehmigung am** | xx.xx.2024 |
| **Genehmigung durch** | STROM AG CEO (Chief Executive Officer) |
| **Inkrafttreten** | xx.xx.2024 |
| **Geltungsbereich** | Ganzes Unternehmen |
| **Thema** | Direktive zur Informationssicherheit & Informationssicherheits-management ISM in der Firma STROM AG |
| **Sachverantwortung** | Mike Information |
| **Verantwortliche Funktion** | CIO (Chief Information Officer) |
| **Übergeordnetes Dokument** | Strom.V01.00: HoP-01-00 Weisung zur Geschäftsführung |
| **Ersetzt** | - |
| **Mitgeltende Dokumente** | - |
| **Gültigkeit** | bis auf Widerruf |
| **Nächste Überprüfung** | xx.xx.2026 |
| **Publikation** | STROM AG Insider |
| **Klassifizierung** | Intern |
| **Archiv** | Archivierungssystem STROM AG |
| **Sprachen** | Deutsch und Englisch |
| **Formate** | docx Original; .pdf |
| **Bemerkungen** | - |

Inhaltsverzeichnis

[A. Ziel und Zweck 3](#_Toc158444606)

[B. Geltungsbereich 3](#_Toc158444607)

[C. Verantwortlichkeiten 3](#_Toc158444608)

[D. Anwendbare Checkpoints 3](#_Toc158444609)

[Checkpoints nach NIST Cyber Security Framework CSF 1.1 3](#_Toc158444610)

[Checkpoints nach ISO/IEC 27001:2022 3](#_Toc158444611)

[Checkpoints nach … 3](#_Toc158444612)

[E. Inhalt 4](#_Toc158444613)

[1. … 4](#_Toc158444614)

[2. … 4](#_Toc158444615)

[F. Sanktionen 5](#_Toc158444616)

[G. Inkrafttreten 5](#_Toc158444617)

[H. Änderungsverzeichnis 5](#_Toc158444618)

[I. Referenzierte Dokumente, Anhänge. Weiterführende Informationen 5](#_Toc158444619)

[Referenzierte Dokumente: 5](#_Toc158444620)

[Anhänge 5](#_Toc158444621)

[Weiterführende Dokumente 6](#_Toc158444622)

[J. Verweise auf weitere Frameworks, Normen und Standards 6](#_Toc158444623)

[{Titel} 6](#_Toc158444624)

[K. Glossar und Abkürzungen 6](#_Toc158444625)

[Glossar 6](#_Toc158444626)

[Abkürzungen 6](#_Toc158444627)

Abbildungsverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

# Ziel und Zweck

{Beschreibung Ziel und Zweck des Dokumentes}

# Geltungsbereich

{Definition des Geltungsbereiches: Konzern, Unternehmen, Organisation, Bereich, Abteilung}

# Verantwortlichkeiten

{Definition des Geltungsbereiches: Konzern, Unternehmen, Organisation, Bereich, Abteilung}

# Anwendbare Checkpoints

## Checkpoints nach NIST Cyber Security Framework CSF 1.1

| Checkpoint (Funktion, Kategorie, Subkategorie) | Bemerkungen / Abgrenzung |
| --- | --- |
| **Funktion IDENTIFY (ID):**  Mit der Funktion "IDENTIFY" (ID) des NIST Cybersecurity Framework (CSF) 1.1 werden die Ressourcen, Daten, Systemen und möglichen Bedrohungen im Unternehmen und den Organisationseinheiten identifiziert. Sie dient dazu, das Verständnis für die gesamte Cybersicherheitslage zu verbessern, einschliesslich der internen und externen Faktoren, die die Sicherheit beeinflussen können. Durch eine umfassende Identifizierung werden potentielle Risiken frühzeitig erkannt und entsprechende Massnahmen ergriffen, um die Cybersicherheitslage zu stärken. Dies umfasst die Identifizierung von Assets, Schwachstellen, Bedrohungen und den Kontext, in welchem das Unternehmen und die Organisationseinheiten tätig sind. |  |
| **Funktion PROTECT (PR):**  Mit der Funktion "PROTECT" (PR) im NIST Cybersecurity Framework (CSF) 1.1 werden angemessene Schutzmassnahmen implementiert, um die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Systemen zu gewährleisten. Dies beinhaltet die Implementierung von Sicherheitskontrollen und -verfahren, um potentielle Schwachstellen zu minimieren und Angriffe abzuwehren. Durch präventive Massnahmen wie Zugriffssteuerung, Datensicherung, Sicherheitsbewusstseinstraining und Schutz vor Schadsoftware schütz das Unternehmen und die Organisationseinheiten ihre Systeme vor Bedrohungen und minimieren das Risiko von Sicherheitsvorfällen. |  |
| **Funktion DETECT (DE):**  Mit der Funktion "DETECT" (DE) im NIST Cybersecurity Framework (CSF) 1.1 müssen Massnahmen getroffen werden, um potentielle Sicherheitsvorfälle frühzeitig zu erkennen und darauf zu reagieren. Dies beinhaltet die Implementierung von Mechanismen zur kontinuierlichen Überwachung, Erkennung und Analyse von Sicherheitsereignissen in Echtzeit. Durch die Nutzung von Sicherheitsüberwachungssystemen, Protokollierung, Anomalie Erkennung und Bedrohungsdatenanalyse kann das Unternehmen und die Organisationseinheiten verdächtige Aktivitäten identifizieren, Schwachstellen aufdecken und potentielle Angriffe erkennen. Auf diese Weise kann schnell auf Sicherheitsvorfälle reagiert und Gegenmaßnahmen eingeleitet werden, um die Auswirkungen von Sicherheitsverletzungen minimieren. |  |
| **Funktion RESPOND (RS):**  Mit der Funktion "RESPOND" (RS) im NIST Cybersecurity Framework (CSF) 1.1werden Massnahmen umgesetzt, um angemessen auf Sicherheitsvorfälle zu reagieren, um Schaden zu begrenzen und die Wiederherstellung zu unterstützen. Es müssen Massnahmen zur effektiven Bewältigung von Sicherheitsvorfällen, einschliesslich der Erstellung von Notfallplänen, der Koordination von Reaktionsteams und der Kommunikation mit relevanten Parteien, implementiert und umgesetzt werden. Durch eine schnelle und koordinierte Reaktion kann das Unternehmen und können die Organisationseinheiten die Ausbreitung von Sicherheitsverletzungen eindämmen, den Betrieb wiederherstellen und potentielle Schäden minimieren. |  |
| **Funktion RECOVER (RE):**  Mit der Funktion "RECOVER" (RE) im NIST Cybersecurity Framework (CSF) 1.1 müssen Massnahmen definiert und umgesetzt werden, um nach einem Sicherheitsvorfall die Geschäftstätigkeit wiederherzustellen und die Widerstandsfähigkeit der Organisation zu stärken. Sie beinhaltet die Implementierung von Massnahmen zur schnellen Wiederherstellung von Systemen, Daten und Diensten sowie die Überprüfung und Anpassung von Prozessen und Richtlinien, um künftige Sicherheitsvorfälle zu verhindern oder ihre Auswirkungen zu minimieren. Durch einen effektiven Wiederherstellungsprozess kann das Unternehmen und können Organisationseinheiten die Betriebsunterbrechung reduzieren und die Kontinuität ihrer Geschäftstätigkeit sicherstellen. |  |

## Checkpoints nach ISO/IEC 27001:2022

| Kapitel / Annex | Bemerkungen / Abgrenzung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

## Checkpoints nach …

| … | Bemerkungen / Abgrenzung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

# Inhalt

## …

{hier wird der eigentliche Inhalt des Dokumentes beschrieben

## …

# Sanktionen

{Beschreibung von eventuellen Sanktionen, wenn der Inhalt des Dokumente nicht angewendet wirdd}.

# Inkrafttreten

Das vorliegende {Weisung, Richtlinie usw.} tritt auf den 01. Januar 2023 in Kraft

{Wenn nötig mit Namen und Funktionsbezeichnung inkl. Unterschrift}

# Änderungsverzeichnis

| Datum |  | Version | Bearbeitet durch | Dokument / Details |
| --- | --- | --- | --- | --- |
| xx.xx.20xx |  | 0.1 | Stefan Mattmann | Erster Entwurf |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Referenzierte Dokumente, Anhänge. Weiterführende Informationen

## Referenzierte Dokumente:

| Referenz / Dokument ID | Dokumentbeschreibung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

## Anhänge

| Anhang / Dokument ID | Dokumentbeschreibung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

## Weiterführende Dokumente

| Dokument | Dokumentbeschreibung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

# Verweise auf weitere Frameworks, Normen und Standards

## {Titel}

| … | Bemerkungen / Abgrenzung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

# Glossar und Abkürzungen

## Glossar

| Begriff | Beschreibung |
| --- | --- |
| ISM | Informations Sicherheit Management bezieht sich auf die Planung, Umsetzung und Überwachung von Maßnahmen zum Schutz von Informationen und IT-Systemen vor unbefugtem Zugriff, Manipulation oder Zerstörung. Ein effektives ISM beinhaltet die Identifizierung von Risiken, die Entwicklung von Sicherheitsrichtlinien, Schulungen für Mitarbeiter, die Implementierung von Sicherheitslösungen und regelmäßige Überprüfungen, um sicherzustellen, dass die Sicherheitsmaßnahmen auf dem neuesten Stand sind. |
| ISMS | Ein Informationssicherheitsmanagementsystem (ISMS) ist ein strukturierter Ansatz zur Verwaltung und zum Schutz von Informationen in einer Organisation. Es umfasst Richtlinien, Prozesse, Technologien und Maßnahmen, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen. Ein ISMS berücksichtigt potentielle Bedrohungen für die Informationssicherheit und entwickelt Strategien, um diesen Bedrohungen entgegenzuwirken. |

## Abkürzungen

| Abkürzung | Beschreibung |
| --- | --- |
| CISO | Chief Information Security Officer |
| CSO | Cyber Security Officer |
| CTO | Chief Technology Officer |
| ISM | Informations Sicherheit Management |
| ISMS | Informations Sicherheit Management System |
| ISO | Information Security Officer |
| ISO/IEC | International Organization for Standardization / International Electrotechnical Commission |
| IT | Information Technology |
| NIST | US National Institute of Standards and Technology (NIST) |
| OT | Operational Technology |