|  |  |
| --- | --- |
| HoP-01-01-03-22 Arbeitsanleitung Bereich ISMS:  Lieferanten Management | |
| **Dokumenten-ID** | Strom.V01.01.03.22 |
| **House of Policy** | Vorgabe auf Level 4 |
| **Dokumententyp** | Arbeitsanleitung |
| **Erlassen am** | xx.xx.2024 |
| **Erlassen durch** | STROM AG ISO (Information Security Officer) |
| **Genehmigung am** | xx.xx.2024 |
| **Genehmigung durch** | STROM AG CISO (Chief Information Security Officer) |
| **Inkrafttreten** | xx.xx.2024 |
| **Geltungsbereich** | Ganzes Unternehmen |
| **Thema** | Arbeitsanleitung Bereich ISMS für das Lieferanten Management in der Firma STROM AG |
| **Sachverantwortung** | Dylan Motivazione |
| **Verantwortliche Funktion** | ISO (Information Security Officer) |
| **Übergeordnetes Dokument** | Strom.V01.01.03: HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS |
| **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 |
| --- | --- |
| **Vermögensverwaltung (Asset Management) ID.AM:**  Die Daten, Mitarbeiter, Geräte, Systeme und Einrichtungen, die es der Organisation ermöglichen, ihre Geschäftsziele zu erreichen, werden entsprechend ihrer relativen Bedeutung für die Unternehmensziele und die Risikostrategie der Organisation identifiziert und verwaltet |  |
|  |  |
|  |  |
|  |  |

## 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 |