

# Informationssicherheitspolitik

## Plusnet GmbH und verbundene Unternehmen

Autor	Dr. Katja Siegemund
Dokumenten-Owner	Team Quality & Information Security Management
Abnahme/Freigabe Plusnet GmbH	Ulrich Hoffmann
Status	Freigegeben am (siehe Dok.ende)
Version	4.0
Geltungsbereich	Plusnet GmbH und verbundene Unternehmen
Dokumentenkategorie	Leitlinie
Klassifizierung	streng vertraulich   vertraulich   intern   <u>öffentlich</u>

# Informationssicherheitspolitik

## 1. Einleitung

Die Informationssicherheitspolitik umfasst die Pflichten, Verantwortlichkeiten und Kontrollen für den Umgang mit Informationssicherheit der Plusnet GmbH. Sie orientiert sich an den geltenden Richtlinien und Standards im EnBW-Konzern (s.a. KRL-025). Die Einführung eines ISMS und die Zertifizierung des gesamten Unternehmens nach ISO 27001 ist eine strategische Entscheidung für die Plusnet GmbH.

Zum Schutz der Informationen sowohl der Plusnet GmbH als auch der Kunden sowie zur Gewährleistung der Verfügbarkeit aller Informationen und deren Verarbeitungssysteme, hat die Geschäftsführung diese Informationssicherheitspolitik erlassen. Die vorliegende Informationssicherheitspolitik definiert das Informationssicherheitsniveau, auf dem die Aufgaben durch die Plusnet GmbH erfüllt werden. Die Plusnet GmbH ist bestrebt, dieses Sicherheitsniveau durch geeignete Maßnahmen und Strategien einzuhalten.

## 2. Definition Informationssicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

## 3. Geltungsbereich

Die Informationssicherheitspolitik formuliert Ziele und Leitgedanken der Informationssicherheit für die Plusnet GmbH und verbundene Unternehmen. Sie gilt für alle Standorte, Mitarbeiterinnen und Mitarbeiter<sup>1</sup> sowie Dritte, die IT-Systeme und IT-Verfahren der Plusnet GmbH benutzen oder betreiben.

## 4. Ziele der Informationssicherheit

Die Konzernrichtlinie KRL-025 formuliert die Informationssicherheitsziele für den gesamten EnBW Konzern. Sie sind die strategische Grundlage aller Aktivitäten im Bereich der Informationssicherheit und spiegeln auch die Bedeutung der Informationsverarbeitung für die Plusnet GmbH wider. Da die strategische und operative Bedeutung der Informationsverarbeitung für die Plusnet GmbH und ihre Aufgaben groß ist, wird bei der Bearbeitung von Informationen und der Erbringung von Dienstleistungen ein hohes Sicherheitsniveau angestrebt.

Daraus ergeben sich folgende Informationssicherheitsziele für die Plusnet:

Nr.	Beschreibung
Ziel 1	Wir gewährleisten eine hohe Verfügbarkeit und Integrität kritischer IT-Systeme zur Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Plusnet GmbH.

<sup>1</sup> Im nachfolgenden Dokument wird aus Gründen der verbesserten Lesbarkeit nur noch der Begriff des Mitarbeiters verwendet. Dies schließt Personen jeden Geschlechts ein.

# Informationssicherheitspolitik

Ziel 2	Wir gewährleisten eine zuverlässige Erbringung von Dienstleistungen gegenüber Kunden und anderen Firmen.
Ziel 3	Wir halten den Aufbau eines angemessenen Sicherheitsstandards aufrecht.
Ziel 4	Wir halten eine kontinuierliche und gesamtheitliche Informationssicherheitsstrategie ein und integrieren Informationssicherheit in Unternehmensprozesse.
Ziel 5	Wir schützen Informationen sowohl von Kunden als auch der Plusnet GmbH.
Ziel 6	Wir identifizieren Risiken bzw. schädigende Ereignisse und reduzieren diese in Häufigkeit und Auswirkung auf ein vertretbares Maß.
Ziel 7	Wir gewährleisten die aus gesetzlichen oder regulatorischen Vorgaben resultierenden Anforderungen.
Ziel 8	Das Gesamtunternehmen wird nach ISO 27001 zertifiziert.

Tabelle 1: Informationssicherheitsziele

## 5. Grundsätze der Informationssicherheit

Im Sinne dieser Politik wird eine Kultur des sicheren Umgangs mit Informationen, Anwendungen und IT-Systemen gefördert. Dabei setzen wir im Sinne einer Vertrauenskultur Eigenverantwortung über Kontrolle und Überwachung der Mitarbeiter.

Folgende Grundsätze gelten für die Informationssicherheit der Plusnet GmbH und verbundenen Unternehmen:

- Die vorrangigen Kriterien für geeignete Sicherheitsmaßnahmen sind deren Wirksamkeit im Hinblick auf das zu tragende Restrisiko, die wirtschaftliche Angemessenheit sowie eventuelle Chancen.
- Informationen werden entsprechend ihres Schutzbedarfs angemessen und sicher verarbeitet sowie vor unberechtigten Zugriffen geschützt.
- IT-Systeme werden in einer angemessenen sicheren Weise und Umgebung betrieben.
- Alle Mitarbeiter haben ein Grundverständnis für Belange der Informationssicherheit und sind zu einer zweckmäßigen und verantwortungsvollen Nutzung der Informationstechnik angehalten.
- Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft und dokumentiert.

## 6. Verantwortlichkeiten und Rollen

### 6.1 Verpflichtung des obersten Managements

Die Führung der Plusnet GmbH trägt die Verantwortung für die Informationssicherheit der ihr untergeordneten Systeme, Anwendungen und Informationen. Diese Verantwortung kann nicht delegiert werden. Die Mitarbeiter sind verantwortlich für die Einhaltung und Umsetzung der Informationssicherheitsvorgaben in ihren jeweiligen Tätigkeitsbereichen.

# Informationssicherheitspolitik

## 6.2 Chief Information Security Officer (CISO)

Der CISO und die Geschäftsführung benennen den ISMS Beauftragten und übertragen diesem die Aufgabe, innerhalb der gesamten Plusnet GmbH die Informationssicherheit gemäß den definierten Vorgaben umzusetzen, zu koordinieren und zu kontrollieren.

## 6.3 ISMS Beauftragter

Der ISMS Beauftragte wird von der Geschäftsführung und dem CISO mit der Implementierung, Umsetzung und dem Betrieb des ISMS (Umsetzungsverantwortung) innerhalb der gesamten Plusnet GmbH beauftragt. Er berichtet direkt an die Geschäftsführung der Plusnet. Durch die Einbettung des Unternehmens in das EnBW Informationssicherheitsmanagement existiert ein weiterer Berichtsweg des ISMS Beauftragten zum CISO der EnBW.

## 6.4 Mitarbeiter

Die Plusnet GmbH stellt sicher, dass das Personal, dem die im ISMS definierten Verantwortlichkeiten zugewiesen werden, die erforderlichen Kompetenzen für die entsprechenden Aufgaben besitzen, indem sie:

- die notwendigen Fähigkeiten des Personals ermittelt, das ISMS-relevante Tätigkeiten ausübt,
- für Schulungen sorgt oder andere Maßnahmen ergreift,
- die Wirksamkeit der ergriffenen Maßnahmen bewertet und
- Aufzeichnungen über Ausbildung, Schulung, Fertigkeiten, Erfahrung und Qualifikationen führt.

Die Plusnet GmbH stellt weiterhin durch geeignete Maßnahmen sicher, dass das gesamte betreffende Personal sich der Relevanz und Wichtigkeit seiner Tätigkeiten in der Informationssicherheit bewusst ist und weiß, wie es zum Erreichen der Ziele des ISMS beitragen kann.

## 7. Abweichungen und Ausnahmen

Abweichungen von dieser Politik sind schriftlich zu begründen und werden in einer ersten Instanz durch den ISMS Beauftragte angenommen oder verworfen. Die Geschäftsführung behält sich bei Zuwiderhandlungen vor, angemessene Sanktionen umzusetzen.

## 8. Verbindlichkeitserklärung

Die Geschäftsführung der Plusnet GmbH definiert in der vorliegenden Informationssicherheitspolitik Grundsätze, die allen Entscheidungen und Maßnahmen in IT-Belangen im Unternehmen zugrunde zu legen sind. Die Plusnet GmbH verpflichtet sich, die vorliegende Informationssicherheitspolitik zu verwirklichen, aufrechtzuerhalten und deren Wirksamkeit ständig zu verbessern.

06.11.2023

Datum



Ulrich Hoffmann (CEO)