

Leitlinie zur Informationssicherheit

Diese Leitlinie hat den Zweck, die Gesamtverantwortung der Verbandsleitung für die Informationssicherheit zu verdeutlichen. Wichtig ist, dass die Behördenleitung sich zu dieser Leitlinie bekennt und deren Inhalt als hohes Organisationsziel definiert. Das Bekenntnis der Behördenleitung wird durch Unterschrift am Ende des Dokumentes besiegelt.



1. Verpflichtung und Verantwortung

Die Erhaltung der Informationssicherheit ist ein wichtiges Ziel für **den Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo M-V)**. Sie ist ferner Teil unserer Verpflichtung durch den Gesetzgeber und gegenüber den Mitgliedern und Bürgern. Mit der Leitlinie zur Informationssicherheit unterstreicht **der Zweckverband** die Bedeutung der Informationssicherheit für **seine** Aufgaben und verdeutlicht die besondere Wichtigkeit, jedem Beschäftigten das notwendige Sicherheitsbewusstsein zu vermitteln.

Der Zweckverband sieht sich als Koordinator und Partner auf dem Weg der Digitalisierung für **seine Mitglieder und Kunden**. Informationen, die durch bereitgestellte Dienste und Serviceleistungen gewonnen und verarbeitet werden, sind ein hohes Gut **für den Zweckverband**. Eine zuverlässig funktionierende Informationsverarbeitung ist für die Aufrechterhaltung des Betriebes unerlässlich. Vor diesem Hintergrund ist die Gewährleistung einer angemessenen Informationssicherheit ein hohes strategisches Ziel.

Der Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo M-V) ist daher bestrebt, Folgendes zu gewährleisten:

- Aufrechterhaltung und Weiterentwicklung organisatorischer Rahmenbedingungen zur Gewährleistung der Informationssicherheit,
- kontinuierliche Verbesserung des Informationssicherheitsmanagements,
- Fortschreibung abgestimmter Sicherheitsstandards einschließlich der Definition von Verantwortlichkeiten und Befugnissen,
- Standardisierung von Komponenten zur Steigerung der Informationssicherheit und Dokumentation aller Sicherheitsvorkehrungen und -maßnahmen.
- Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

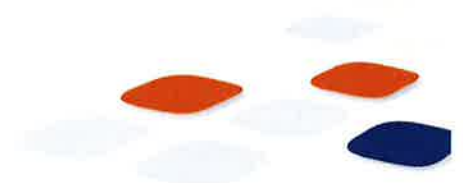
2. Geltungsbereich

Die Leitlinie Informationssicherheit sowie alle ihr untergeordneten Richtlinien, Handbücher und Arbeitsanweisungen gelten für die internen Bereiche des Zweckverbandes. Sie gelten nicht für Dienstleister und kommunale Partner, können aber von diesen übernommen werden.

3. Grundsätze der Informationssicherheit

Zur Aufrechterhaltung der Informationssicherheit verfolgt **der Zweckverband** den Schutz folgender Eigenschaften von Informationen und Informationsverarbeitenden Systemen:

- Vertraulichkeit:
Wir stellen sicher, dass schutzwürdige Informationen ausschließlich berechtigten Personen im Rahmen ihrer Aufgabenerfüllung zugänglich sind. Alle Beschäftigten wurden darüber hinaus auf die Vertraulichkeit nach **Art. 5 DS-GVO** verpflichtet. Im notwendigen Einzelfall werden die Mitarbeiter auch auf weitere Geheimschutzregeln verpflichtet.
- Integrität:



Korrekt und vollständig vorliegende Daten sind die Grundlage für eine ordnungsgemäße Aufgabenerfüllung. Wir schützen daher die von uns verarbeiteten Daten vor unbefugter Veränderung.

- **Verfügbarkeit:**

Es wird sichergestellt, dass die berechtigten Personen zeitnah Zugang zu allen benötigten Informationen und Diensten erhalten, damit der Service für die Mitglieder, Kunden und Bürger ohne unnötigen Zeitverzug erbracht werden können. Durch Archivierung relevanter Daten wird eine langfristige Informationsbewahrung sichergestellt.

Alle Daten und Anwendungen **des Zweckverbands** werden hinsichtlich ihres Schutzbedarfes klassifiziert und einer von drei Schutzbedarfsstufen (normaler, hoher oder sehr hoher Schutzbedarf) zugeordnet. In Abhängigkeit vom möglichen Potenzial und der Eintrittswahrscheinlichkeit eines Schadens werden diverse, vorbeugende organisatorische und technische Schutzmaßnahmen umgesetzt.

Durch geeignete Sensibilisierungsmaßnahmen (z.B. Schulungen oder interne Informationen) stellt **der Zweckverband** sicher, dass jeder Beschäftigte

- genaue Kenntnisse über die Erfordernisse der Informationssicherheit in seinem eigenen Verantwortungsbereich hat,
- ausreichende Kenntnisse über Gefährdungen und Risiken beim Umgang mit Informationen erlangt,
- die Fähigkeit besitzt, anvertraute Informationen sicher zu verarbeiten.

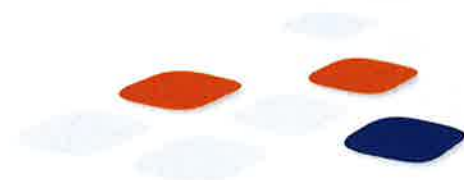
4. Anwendungsweise

Die Leitlinie Informationssicherheit beinhaltet die **vom Zweckverband** angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Sie manifestiert den Anspruch, dass das erforderliche Sicherheitsniveau auf allen Ebenen des **Zweckverbandes** erreicht werden soll.

Diese Richtlinie sowie alle darauf aufbauenden Regelwerke (Sicherheitskonzepte, Dienstregelungen, Handlungsleitfäden) sind vom ISMS Team und der Arbeitsgruppe Informationssicherheit (AG IS) erstellt worden und werden von ihr fortgeschrieben. Sie orientieren sich am den IT-Grundsatzkompodium des Bundesamts für Sicherheit in der Informationstechnik (BSI).

In Abwägung der Werte der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für Informationssicherheit wird für eingesetzte und geplante Geschäftsprozesse mit Informationsverarbeitung und die Informationstechnik (IT) beim **Zweckverband angemessenes Informationssicherheitsniveau** angestrebt. Hierfür werden IT-Sicherheitskonzepte nach der Vorgehensweise des IT-Grundsatz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellt und fortgeschrieben.

Beeinträchtigungen der IT-Nutzung sind zu akzeptieren, wenn dies der Informationssicherheit dient. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken durch den IT-Einsatz untragbar, ist an dieser Stelle auf die IT zu verzichten.



5. Ziele

Alle Beschäftigten gewährleisten die Informationssicherheit durch ihr verantwortliches Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

Für alle Geschäftsprozesse mit Informationsverarbeitung und für die IT sind die Sicherheitsziele Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu erreichen.

Alle Beschäftigten vermitteln den Mitgliedern, dass die durch wir zur Kenntnis erlangte Daten und Informationen

- vor Dritten geschützt sind (Vertraulichkeit),
- dass sie Service in Anspruch nehmen können, wenn sie ihn benötigen (Verfügbarkeit) und
- dass die Daten korrekt sind (Integrität).

6. Verantwortlichkeiten

Die Verantwortlichkeiten zur Aufrechterhaltung der Informationssicherheit sowie konkrete technische und organisatorische Maßnahmen werden in den intern verfügbaren IT-Sicherheitskonzepten dokumentiert.

7. Regelungsstruktur

Die Regelungsstruktur ist hierarchisch aufgebaut. Alle Dokumente bilden gemeinsam das **Informationssicherheitshandbuch**. Die vorliegende Leitlinie Informationssicherheit bildet die erste Ebene und gibt den strategischen Rahmen vor. Die zweite Ebene ist analytisch orientiert und beinhaltet die Schutzbedarfsfeststellung sowie das Sicherheitsmanagement verbunden mit der kontinuierlichen Verbesserung. In der dritten Ebene werden technische Einzelheiten und konkrete Umsetzungshinweise in Form von Sicherheitskonzepten beschrieben. Ferner werden hier konkrete Arbeitsanweisungen formuliert.

Bekanntgabe

Diese Informationssicherheitsleitlinie tritt am 01.09.2021 in Kraft.

Schwerin, 19.08.2021

Kuprat
Frau Kuprat, Verbandsvorsteherin

