Leitlinie für

Informationssicherheit

des Zweckverbands Elektronische Verwaltung im Saarland – (eGo-Saar)

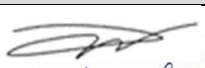
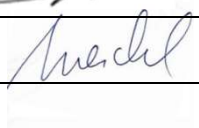
Version:	2.0
Version vom:	11.12.2024
Freigabe durch:	**Geschäftsführung**
Klassifizierung:	**intern**
Status:	Finale Version

I Dokumentinformationen

Dokumentinformationen

Beschreibung	Leitlinie für Informationssicherheit
Empfänger / Nutzer / Zielgruppe	Intern
Elektronische Dokumentenablage	Alle Dokumente werden in der nextcloud abgelegt.
Revision	Januar 2026

Verantwortlichkeit

Rolle	Name	Abteilung	Funktion	Datum	Unterschrift
Autor	William Dube		ISB	28.02.2024	
Prüfer	Daniel Merckel	FBL	ZIB	11.12.2024	

Änderungsnachweis

Version	Status	durch	gültig ab
0.9	Entwurf	Andreas Storb	19.07.2023
1.0	Final	William Dube	28.02.2024
1.1	Überarbeitung	William Dube	04.03.2024
2.0	Überarbeitung	William Dube	18.11.2024
2.0	Final	Geschäftsführung	11.12.2024

II Inhaltsverzeichnis

1. Einleitung

Die digitale Transformation und der zunehmende Einsatz moderner Technologien bringen erhebliche Chancen, aber auch neue Herausforderungen für die Informationssicherheit mit sich. Als kommunale IT-Dienstleister trägt der Zweckverband Elektronische Verwaltung im Saarland (eGo-Saar) eine besondere Verantwortung, den Schutz sensibler Daten, die Verfügbarkeit von IT-Systemen und die Integrität von Informationen sicherzustellen.

Diese Leitlinie zur Informationssicherheit legt die grundlegenden Prinzipien, Verantwortlichkeiten und Maßnahmen fest, die erforderlich sind, um ein angemessenes Sicherheitsniveau zu gewährleisten. Sie dient als Orientierung für alle Mitarbeitenden, Partner und externen Dienstleister, um ein gemeinsames Verständnis für den sicheren Umgang mit Informationen und IT-Systemen zu schaffen.

Das Ziel dieser Leitlinie ist es, Risiken zu minimieren, gesetzliche und regulatorische Anforderungen zu erfüllen und das Vertrauen in die IT-Dienstleistungen des eGo-Saar zu stärken. Eine wirksame Informationssicherheit erfordert dabei das Engagement aller Beteiligten.

Diese Leitlinie zur Informationssicherheit definiert die grundlegenden Ziele der Informationssicherheit für den eGo-Saar. Sie legt folgende Aspekte fest:

- den Geltungsbereich,
- die Sicherheitsorganisation,
- den Stellenwert der Informationssicherheit,
- das Bekenntnis der Geschäftsführung zur Verantwortung für die Informationssicherheit,
- die Sicherheitsstrategie,
- die allgemeinen Sicherheitsziele,
- die Verpflichtung zur kontinuierlichen Fortschreibung des Regelwerks zur Informationssicherheit sowie
- den Rahmen zur Inkraftsetzung und Veröffentlichung der Leitlinie.

2. Geltungsbereich

Diese Leitlinie zur Informationssicherheit ist das übergeordnete Regelwerk für das Informationssicherheitsmanagement und Informationssicherheitskonzept.
Sie gilt für den gesamten Geschäftsbereich des Zweckverbandes eGo-Saar, insbesondere für den Bereich des zentralen IT-Betriebs und die vom eGo-Saar angebotenen Dienstleistungen innerhalb des Zweckverbandes und gegenüber seinen Mitgliedern.

3. Informationssicherheits-Organisation

Der Zweckverband Elektronische Verwaltung im Saarland (eGo-Saar) ist das Kompetenzzentrum für die Digitalisierung der kommunalen Verwaltungen und Verbände im Saarland. Als Dienstleister und Berater unterstützt er seine Mitglieder in allen Fragen des eGovernments sowie in der Bereitstellung sicherer und moderner IT-Lösungen. Von der strategischen Planung über die Entwicklung und Implementierung von Online-Diensten bis hin zu Prozessberatung, Datenschutz und IT-Support begleitet der eGo-Saar die Digitalisierung der Kommunalverwaltungen.

Im Rahmen seiner Aufgaben bietet der Zweckverband den Kommunen sichere Basisinfrastrukturen sowie gemeinsame Fachverfahren an, um Verwaltungsmodernisierung nachhaltig zu gestalten und Arbeitsabläufe effizient zu unterstützen. Ziel ist es, Bürgerinnen und Bürgern sowie Unternehmen einen sicheren, rechtssicheren und zeitlich unabhängigen digitalen Zugang zu Verwaltungsleistungen zu ermöglichen.

Zusätzlich koordiniert der eGo-Saar den digitalen Wandel gemeinsam mit seinen Mitgliedern und dem Land. Er schafft Synergieeffekte, indem er Kommunen miteinander vernetzt, Anforderungen bündelt und gemeinsame Standards für IT-Lösungen und Prozesse entwickelt. Als Projektträger engagiert sich der eGo-Saar zudem für innovative Digitalisierungsprojekte wie den „Gigapakt Schulen Saar“, durch den alle saarländischen Schulen mit Glasfaseranschlüssen ausgestattet werden.

Die Informationssicherheit ist eine zentrale Grundlage für die erfolgreiche Erfüllung dieser Aufgaben. Der eGo-Saar betreibt und entwickelt kontinuierlich Informationstechnologien, die sowohl für interne Abläufe als auch für seine Mitglieder von entscheidender Bedeutung sind. Um den Schutz dieser Systeme zu gewährleisten, werden Sicherheitskonzepte entwickelt, die den Schutzbedarf für jede Leistung und Aufgabe aus fachlicher Perspektive bestimmen. Anschließend wird dieser Schutzbedarf auf die technischen Systeme und die IT-Infrastruktur übertragen, um sicherzustellen, dass alle relevanten Prozesse angemessen geschützt sind.

Die festgelegten Sicherheitsmaßnahmen müssen konsequent umgesetzt werden, auch wenn sie gegebenenfalls zu Anpassungen oder Einschränkungen im Betrieb führen. Falls Risiken bestehen bleiben, die als nicht tragbar eingestuft werden, ist zu prüfen, ob der Einsatz der betroffenen Informationstechnik weiterhin vertretbar ist.

Jede verantwortliche Person im eGo-Saar ist dazu verpflichtet, bei Verstößen oder Sicherheitsbeeinträchtigungen unverzüglich geeignete Maßnahmen zu ergreifen, um die

Aufrechterhaltung des Betriebs und die Integrität der Systeme zu gewährleisten. Unabhängig davon, ob und in welcher Weise einzelne Aufgaben delegiert werden, bleibt die Gesamtverantwortung für die Informationssicherheit stets bei der Geschäftsführung des eGo-Saar.

Die nachstehende Abbildung verdeutlicht die Organisationsstruktur des eGo-Saar:

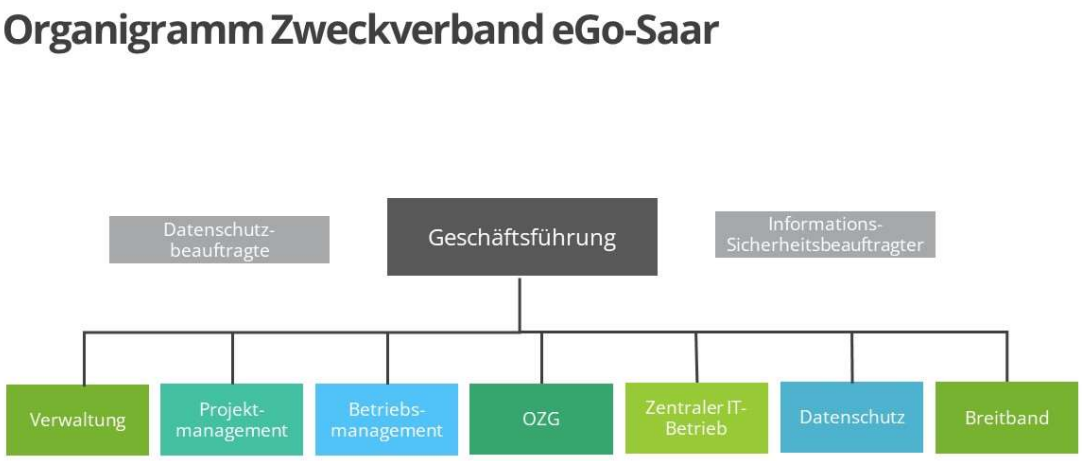


Abbildung 1: Organisationsstruktur

3.1. Geschäftsführung

Die Geschäftsführung trägt die oberste Verantwortung für die Informationssicherheit innerhalb des eGo-Saar. Sie stellt sicher, dass die notwendigen Rahmenbedingungen geschaffen werden, um ein hohes Sicherheitsniveau aufrechtzuerhalten. Dazu gehören die Bereitstellung personeller Ressourcen, technischer Mittel sowie finanzieller Investitionen, die erforderlich sind, um Sicherheitsmaßnahmen konsequent umzusetzen.

Ein zentraler Bestandteil der Verantwortung der Geschäftsführung ist die Verabschiedung der Leitlinie zur Informationssicherheit. Zudem ernennt sie eine verantwortliche Person für die Informationssicherheit und stellt sicher, dass regelmäßige Berichte über den aktuellen Sicherheitsstatus eingeholt werden. Die Geschäftsführung verpflichtet sich, sich aktiv an der Weiterentwicklung der Sicherheitsstrategie zu beteiligen und eine kontinuierliche Verbesserung der Maßnahmen zu unterstützen.

3.2. Informationssicherheitsbeauftragte/r (ISB)

Die oder der Informationssicherheitsbeauftragte (ISB) ist die zentrale Ansprechperson für alle Belange der Informationssicherheit und berichtet direkt an die Geschäftsführung. Sie oder er

trägt die Verantwortung für die Entwicklung und Pflege des Informationssicherheitsmanagementsystems (ISMS) und führt regelmäßig Schutzbedarfsanalysen sowie Risikobewertungen durch.

Darüber hinaus obliegt dem ISB die Koordination der Sicherheitsmaßnahmen innerhalb des eGo-Saar. Dies umfasst die Erstellung von Richtlinien, die Umsetzung technischer und organisatorischer Schutzmaßnahmen sowie die Sensibilisierung der Mitarbeitenden für sicherheitsrelevante Themen. Der ISB wird frühzeitig in geplante organisatorische und technische Veränderungen eingebunden, um mögliche Risiken bereits in der Planungsphase zu identifizieren. In sicherheitskritischen Fällen verfügt der ISB über ein Vetorecht, um untragbare Risiken abzuwenden.

Um die Informationssicherheitsstrategie weiterzuentwickeln und zu optimieren, leitet der ISB eine Arbeitsgruppe (ISMS-Team) für Informationssicherheit. Gemeinsam mit dieser Gruppe wird die Weiterentwicklung der Informationssicherheitsleitlinie und der IT-Sicherheitskonzepte vorangetrieben.

3.3. ISMS-Team

Das Informationssicherheits-Management-System-Team (ISMS-Team) ist für die operative Umsetzung und Weiterentwicklung des Informationssicherheitsmanagementsystems verantwortlich. Es arbeitet eng mit dem ISB zusammen und unterstützt ihn bei der Identifikation und Bewertung von Sicherheitsrisiken sowie bei der Umsetzung der definierten Maßnahmen.

Das ISMS-Team ist zudem für die regelmäßige Überprüfung und Anpassung der Sicherheitsstrategie zuständig. Es analysiert sicherheitsrelevante Vorfälle, entwickelt Handlungsempfehlungen und sorgt dafür, dass die Informationssicherheit in alle relevanten Prozesse des eGo-Saar integriert wird. Darüber hinaus ist es eng in die Zusammenarbeit mit dem Fachbereichsleiter – Zentral IT-Betrieb eingebunden, um sicherzustellen, dass technische Sicherheitsstandards eingehalten werden.

3.4. Fachbereichsleiter – Zentral IT-Betrieb

Der Fachbereichsleiter – Zentral IT-Betrieb trägt die technische Verantwortung für die Sicherheit der IT-Systeme des eGo-Saar. In enger Abstimmung mit dem ISB und dem ISMS-Team stellt er sicher, dass die IT-Infrastruktur den aktuellen Sicherheitsanforderungen entspricht und zuverlässig funktioniert.

Zu seinen Aufgaben gehört die Sicherstellung der Systemverfügbarkeit und Netzwerksicherheit sowie die Umsetzung technischer Schutzmaßnahmen wie Firewalls, Zugriffskontrollen und Verschlüsselung. Um potenzielle Schwachstellen frühzeitig zu erkennen, führt er regelmäßige Sicherheitsaudits und Penetrationstests durch.

Ein weiterer zentraler Aspekt seiner Verantwortung besteht in der Dokumentation und Überwachung sicherheitsrelevanter Ereignisse sowie in der Entwicklung von Notfallplänen für

den Umgang mit sicherheitskritischen Vorfällen. Er arbeitet zudem daran, neue IT-Systeme sicher zu integrieren und gewährleistet, dass die Anforderungen der Informationssicherheit bereits in der Planungsphase berücksichtigt werden.

3.5. Mitarbeitende

Informationssicherheit kann nur dann auf einem hohen Niveau gewährleistet werden, wenn alle Mitarbeitenden sich ihrer Verantwortung bewusst sind. Deshalb ist Informationssicherheit eine grundlegende Dienstpflicht aller Beschäftigten.

Jede Mitarbeiterin und jeder Mitarbeiter ist dazu verpflichtet, die geltenden IT-Sicherheitsrichtlinien zu beachten und sensible Informationen vertraulich zu behandeln. Dies schließt den sorgfältigen Umgang mit Passwörtern, die Nutzung sicherer Authentifizierungsmechanismen und die Einhaltung von Datenschutzvorgaben ein.

Zudem müssen alle Mitarbeitenden sicherheitsrelevante Vorfälle unverzüglich an die ZIB oder den melden, um Risiken frühzeitig zu minimieren. Die Teilnahme an Schulungen und Sensibilisierungsmaßnahmen ist ein wichtiger Bestandteil der Sicherheitsstrategie, da nur durch kontinuierliche Weiterbildung ein angemessenes Sicherheitsbewusstsein geschaffen werden kann.

3.6. Weitere Verantwortlichkeiten

Neben der Geschäftsführung, dem ISB, dem ISMS-Team, dem Fachbereichsleiter – Zentral IT-Betrieb und den Mitarbeitenden gibt es weitere Akteure mit spezifischen Aufgaben in der Informationssicherheitsorganisation.

Die Fachbereichsverantwortlichen unterstützen den ISB bei der Identifikation und Analyse sicherheitskritischer Prozesse in ihren jeweiligen Bereichen. Sie tragen dazu bei, dass spezifische Sicherheitsmaßnahmen innerhalb ihrer Abteilungen umgesetzt werden und als Multiplikatoren für Sicherheitsrichtlinien dienen.

Die oder der Datenschutzbeauftragte bildet die Schnittstelle zwischen Datenschutz und Informationssicherheit. Sie oder er überwacht die Einhaltung der datenschutzrechtlichen Vorgaben und stellt sicher, dass die IT-Sicherheitsmaßnahmen den gesetzlichen Anforderungen entsprechen.

Auch externe Dienstleister und Partner müssen sich an die Sicherheitsrichtlinien des eGo-Saar halten. Durch regelmäßige Überprüfungen und Vertragsprüfungen wird sichergestellt, dass Sicherheitsanforderungen auch bei externen Partnern eingehalten werden.

4. Stellenwert der Informationssicherheit und der zu schützenden Objekte

Der Zweckverband übernimmt als IT-Dienstleister eine zentrale Rolle in der digitalen Verwaltung und stellt für seine Mitglieder sichere und zuverlässige IT-Infrastrukturen bereit. Informationssicherheit ist dabei ein unverzichtbarer Grundwert, da moderne Verwaltungsprozesse zunehmend auf digitale Lösungen angewiesen sind.

Der Stellenwert der Informationssicherheit bemisst sich an der Bedeutung der Verfügbarkeit, Integrität und Vertraulichkeit gespeicherter, verarbeiteter und übertragener Informationen. Die Informationstechnik bildet in vielen Bereichen der Verwaltung die führende – teils sogar ausschließliche – Kommunikations- und Arbeitsinfrastruktur. Die Sicherstellung dieser Grundwerte ist entscheidend, um den Schutz sensibler Informationen zu gewährleisten, rechtliche Vorgaben einzuhalten und die vertrauenswürdige Erbringung digitaler Dienstleistungen sicherzustellen.

Vernetzte IT-Infrastrukturen sind heute verstärkt Bedrohungen ausgesetzt, insbesondere durch Cyberangriffe, Schadsoftware oder technische Ausfälle. Die fortschreitende Digitalisierung erhöht zudem die Abhängigkeit von stabilen und sicheren IT-Systemen. Daher müssen alle verarbeiteten und übertragenen Informationen durch angemessene technische und organisatorische Maßnahmen geschützt werden.

Die Informationssicherheit ist für den Zweckverband und ihre Mitglieder ausfolgenden Gründen von essenzieller Bedeutung:

- **Einhaltung gesetzlicher Vorschriften**, insbesondere der Datenschutzgesetze und IT-Sicherheitsvorgaben,
- **Wahrung von Dienstgeheimnissen** und Schutz sensibler Verwaltungsdaten,
- **Sichere und vertrauenswürdige Bereitstellung von Online-Diensten** für Bürgerinnen und Bürger, Unternehmen und Verwaltungen,
- **Minimierung von Schadensauswirkungen** durch präventive Schutzmaßnahmen,
- **Erhaltung investierter Werte** in Technik, Informationen, Arbeitsprozesse und Know-how,
- **Aufrechterhaltung der Arbeitsfähigkeit des eGo-Saar und seine Mitglieder**, um den reibungslosen Betrieb sicherzustellen,
- **Vermeidung von Ansehens- und Vertrauensverlusten** durch Sicherheitsvorfälle oder Datenschutzverletzungen.

Ein Ausfall der IT-Systeme könnte schwerwiegende Konsequenzen für die Verwaltungstätigkeit haben und die Funktionsfähigkeit der kommunalen IT-Infrastruktur erheblich beeinträchtigen. Daher ist ein systematisches Informationssicherheitsmanagement notwendig, das kontinuierlich angepasst und verbessert wird.

5. Sicherheitsziele

Ziel der Informationssicherheit beim eGo-Saar ist es, die Schutzbedürfnisse der verarbeiteten Informationen zu wahren und die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit in angemessener Weise sicherzustellen.

Jede wesentlich relevante Leistung oder jeder wesentliche Prozess wird entsprechend seines Schutzbedarfs eingestuft. Die Klassifizierung erfolgt gemäß „D-020 Schutzbedarfsfeststellung“, um geeignete Sicherheitsmaßnahmen festzulegen.

Die Schutzmaßnahmen müssen sowohl den rechtlichen Anforderungen entsprechen als auch wirtschaftlich sinnvoll sein. Daher ist es unabdingbar, den individuellen Schutzbedarf von Informationen und Systemen zu kennen und darauf abgestimmte Maßnahmen zu ergreifen. Neben den Informationen selbst sind auch folgende Schutzobjekte zu berücksichtigen:

- **IT-Systeme und Netzwerkinfrastrukturen**, die für den Betrieb des eGo-Saar essenziell sind,
- **Kommunikationskanäle und Schnittstellen**, die für den Austausch sensibler Daten genutzt werden,
- **physische und digitale Speichermedien**, die vertrauliche Informationen enthalten,
- **Zugriffs- und Berechtigungsmanagement**, um unbefugte Nutzung zu verhindern.

Durch eine kontinuierliche Weiterentwicklung der Informationssicherheitsstrategie stellt der eGo-Saar sicher, dass alle digitalen Verwaltungsprozesse langfristig geschützt und an neue Herausforderungen angepasst werden.

5.1. Festlegung von Sicherheitszielen

Zur Abbildung des hohen Stellenwertes der Informationssicherheit werden für den eGo-Saar die nachstehenden Sicherheitsziele festgelegt:

- **Verfügbarkeit**
  Die Verfügbarkeit von Informationen, IT-Systemen und Diensten muss sichergestellt werden, damit berechtigte Nutzer jederzeit auf notwendige Daten und Anwendungen zugreifen können. Maßnahmen wie Redundanz, Notfallvorsorge und Ausfallsicherheit tragen dazu bei, Betriebsunterbrechungen zu minimieren.
- **Integrität**
  Die Integrität von Informationen stellt sicher, dass Daten unverändert, konsistent und zuverlässig bleiben. Unautorisierte Änderungen, Manipulationen oder unbeabsichtigte Verfälschungen müssen durch geeignete Sicherheitsmaßnahmen erkannt oder verhindert werden.
- **Vertraulichkeit**
  Die Vertraulichkeit garantiert, dass Informationen nur von autorisierten Personen eingesehen oder verarbeitet werden dürfen. Zugriffskontrollen, Verschlüsselung und

andere Sicherheitsmaßnahmen gewährleisten den Schutz sensibler Daten vor unbefugtem Zugriff.

Zusätzlich zu diesen Grundwerten berücksichtigt den eGo-Saar weitere Datenschutz- und Sicherheitsziele, um den gestiegenen Anforderungen an den Schutz personenbezogener und geschäftskritischer Daten gerecht zu werden:

- **Authentizität** – Personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.
- **Revisionsfähigkeit** – Es muss nachvollziehbar sein, wer, wann, welche Daten in welcher Weise verarbeitet hat.
- **Transparenz** – Sämtliche Prozesse bei der Planung, Einführung und dem Betrieb von IT-Verfahren müssen dokumentiert sein und geeigneten Kontrollmechanismen unterliegen.

Diese Ziele werden in einem separaten Zieleplan operationalisiert, regelmäßig überprüft und fortgeschrieben, um den aktuellen Herausforderungen der Informationssicherheit gerecht zu werden.

5.2. Bezug der Informationssicherheit zu den Geschäftszielen und Aufgaben des eGo-Saar

Die Informationssicherheit ist für den eGo-Saar nicht nur eine technische Anforderung, sondern eine strategische Notwendigkeit. Sie steht im direkten Zusammenhang mit der Aufgabenerfüllung und der Qualität der IT-und Digitalisierungsdienstleistungen.

Sowohl bei der Erbringung von Pflichtaufgaben als auch bei freiwilligen Leistungen werden Informationen verarbeitet, deren Schutz höchste Priorität hat. Dazu gehören:

- **Personenbezogene und verwaltungsrelevante Daten**, die gesetzlichen Datenschutzvorgaben unterliegen,
- **Geschäfts- und Betriebsgeheimnisse**, die den Mitgliedskommunen und Unternehmen anvertraut wurden,
- **Kritische Infrastrukturen**, deren Schutz für die Funktionsfähigkeit der kommunalen Verwaltung essenziell ist.

Eine ganzheitliche Betrachtung der IT-Systeme, Fachverfahren, Aufgaben und Kommunikationskanäle ist erforderlich, um ein hohes Sicherheitsniveau aufrechtzuerhalten. Informationssicherheit umfasst daher alle organisatorischen, personellen und technischen Maßnahmen, die für den Schutz der digitalen Verwaltungsprozesse erforderlich sind.

6. Kernelemente der Sicherheitsstrategie

Um eine durchgängige Sicherheitsstrategie zu etablieren, erlässt der eGo-Saar nach Bedarf zusätzliche Richtlinien zur Aufrechterhaltung der Informationssicherheit. In diesem Zusammenhang führt die Organisation regelmäßig eine Bedarfsermittlung durch und legt Mindestsicherheitsstandards für ihre Verfahren fest. Bei Verfahren, die über verschiedene Verwaltungsebenen hinweg genutzt werden, sind die entsprechenden Regelungen und Vorgaben des Bundes oder des Landes zu berücksichtigen und umzusetzen.

Zur strukturierten Umsetzung der Sicherheitsstrategie wird das etablierte ISMS kontinuierlich weiterentwickelt. In regelmäßigen Abständen wird überprüft, ob die bestehenden Sicherheitsmaßnahmen weiterhin den aktuellen Anforderungen entsprechen oder angepasst werden müssen. Der ISB leitet das IS-Management-Team und entwickelt die notwendigen Maßnahmen kontinuierlich weiter, um das Sicherheitsniveau auf einem hohen Stand zu halten.

Die Sicherheitsstrategie umfasst die gesamte Informationsverarbeitung innerhalb des eGo-Saar. Das Informationssicherheits-Managementsystem (ISMS) wird durch den ISB in Abstimmung mit der Geschäftsführung koordiniert. Das ISMS hat die Aufgabe, dem jeweiligen Schutzzweck angemessene Sicherheitsmaßnahmen zu definieren und deren wirtschaftliche Umsetzung sicherzustellen. Dabei ist es entscheidend, dass das erforderliche Sicherheitsniveau erreicht wird, ohne den Ablauf von Geschäftsprozessen unnötig zu beeinträchtigen.

Als zentrale Sicherheitsinstanz ernennt die Geschäftsführung einen Informationssicherheitsbeauftragten (ISB) sowie eine Stellvertretung. Diese Personen sind für alle Belange der Informationssicherheit zuständig und dienen als direkte Ansprechpersonen für die Geschäftsführung, Fachabteilungen und externe Partner. Um eine unabhängige Entscheidungsfindung zu ermöglichen, agiert der ISB weisungsfrei und ist ausschließlich der Geschäftsführung unterstellt. Die Berichtswege und Verantwortlichkeiten sind dabei klar festzulegen.

Ein regelmäßiger Austausch zwischen dem ISB und der Leitung des Fachbereichs Zentral IT-Betrieb ist essenziell, um sicherzustellen, dass aktuelle Bedrohungslagen erkannt und angemessene Maßnahmen ergriffen werden. Darüber hinaus müssen dem ISB geeignete Qualifizierungsmaßnahmen ermöglicht werden, damit er seine Verantwortung fachlich fundiert und effizient wahrnehmen kann.

Bei akuten Bedrohungen oder Gefahr im Verzug ist der ISB oder seine Stellvertretung berechtigt, im Namen der Geschäftsführung kurzfristig notwendige Sicherheitsmaßnahmen anzuordnen und durchzusetzen. Dies kann im Ernstfall bis zur vorübergehenden Sperrung bestimmter Anwendungen oder Netzübergänge führen, um kritische Sicherheitsvorfälle zu verhindern oder einzudämmen.

Sämtliche externen Personen oder Unternehmen, die Dienstleistungen für den eGo-Saar erbringen, sind verpflichtet, die geltenden Informationssicherheitsrichtlinien einzuhalten. Der eGo-Saar als Auftraggeber informiert die beauftragten Unternehmen über die geltenden

Sicherheitsvorgaben und stellt sicher, dass diese vertraglich zur Einhaltung der Informationssicherheitsziele verpflichtet werden. Darüber hinaus sind gesetzliche und vertragliche Sicherheitsanforderungen stets zu berücksichtigen und stellen den Mindeststandard für die internen Sicherheitsmaßnahmen des eGo-Saar dar.

Zur weiteren Stärkung der Sicherheitsstrategie werden gemeinsame Basiskomponenten innerhalb der Organisation genutzt, um die Zusammenarbeit zwischen verschiedenen Verwaltungsebenen zu vereinfachen und Synergieeffekte bei der Sicherheitsumsetzung zu nutzen. Die regelmäßige Sensibilisierung und Schulung aller Mitarbeitenden stellt dabei einen essenziellen Bestandteil der Sicherheitsstrategie dar.

Die Sicherheitsstrategie des eGo-Saar basiert auf einer Reihe zentraler Grundsätze, die sicherstellen, dass Sicherheitsmaßnahmen zielgerichtet und effizient umgesetzt werden:

- **Sicherheit für nachhaltige Verfügbarkeit**: Um eine langfristige Verfügbarkeit zu gewährleisten, können kurzfristige Einschränkungen bei Funktionalität und Komfort akzeptabel sein.
- **Prinzip des Schutzbedarfs**: Der Schutzbedarf eines IT-Systems wird durch den Schutzbedarf der darauf verarbeiteten, gespeicherten oder übertragenen Daten bestimmt.
- **Minimalprinzip des Zugriffs**: Der Zugriff auf IT-Systeme und Daten wird auf die notwendigen Personen und Systeme beschränkt, um unbefugten Zugriff zu minimieren.
- **Restriktives Nutzungsprinzip**: Jede Person erhält nur die Zugriffsrechte, die für die Erfüllung der jeweiligen Aufgaben erforderlich sind.
- **Einbindung aller Beschäftigten**: Die Mitarbeitenden werden aktiv in den Sicherheitsmanagementprozess eingebunden und regelmäßig für die Bedeutung der Informationssicherheit sensibilisiert.
- **Zentrale Rolle der Informationssicherheit**: Sicherheitsaspekte müssen bereits bei der Planung von Änderungen und Neuerungen berücksichtigt werden. Der ISB ist in allen Fragen zur Informationssicherheit zu unterstützen.
- **Verhältnismäßigkeit der Sicherheitsmaßnahmen**: Der Aufwand für Sicherheitsmaßnahmen muss in einem angemessenen Verhältnis zum erwarteten Nutzen und zu den Risiken stehen.
- **Bereitstellung ausreichender Ressourcen**: Um ein angemessenes Maß an Informationssicherheit aufrechtzuerhalten, sind ausreichend finanzielle und personelle Ressourcen sowie zeitliche Freiräume für Sicherheitsaufgaben bereitzustellen.

7. Umsetzung der Sicherheitsstrategie

Die Sicherheitsstrategie des eGo-Saar verfolgt das Ziel, mit wirtschaftlichem Ressourceneinsatz ein höchstmögliches Maß an Sicherheit zu erreichen und verbleibende Restrisiken auf ein Minimum zu reduzieren.

Dieser kontinuierliche Prozess wird durch die Einführung eines Informationssicherheits-Managementsystems (ISMS) realisiert, das sich an der ISO 27001 auf der Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert.

Da ein ISMS ein sich wiederholender und dynamischer Prozess ist, wird dieser kontinuierlich weiterentwickelt und an aktuelle Bedrohungslagen angepasst. Zur strukturierten Einführung wurde das Verfahren "Compliance und Informationssicherheit in 12 Schritten" (CISIS12) herangezogen, das speziell für kleine und mittlere Organisationen entwickelt wurde.

CISIS12 beschreibt ein Verfahren, das bei der Einführung des ISMS unterstützt. Die Umsetzung erfolgt durch Ablauf der 12 Schritte des CISIS12-Vorgehensmodells, die in die folgenden Phasen unterteilt sind:

Initialisierungsphase (Schritte 0-2) umfasst das Projektstartup, die Erstellung dieser Leitlinie sowie die Sensibilisierung der Beschäftigten.
Festlegung der Aufbau- und Ablauforganisation (Schritte 3-5) beinhaltet den Aufbau eines Informationssicherheitsteams sowie die Festlegung der Dokumentationsstruktur und die Einführung eines IT-Service-Managementprozesses, in dem Abläufe und Zuständigkeiten bei Wartung, Änderung bzw. Störungsbeseitigung von bzw. an IT-Systemen beschrieben werden.
Entwicklung und Umsetzung (Schritte 6-12): In dieser Phase werden nach Identifikation der kritischen Applikationen Sicherheitsmaßnahmen entwickelt und umgesetzt. Das ISMS wird festgeschrieben und regelmäßig überprüft (Audits).

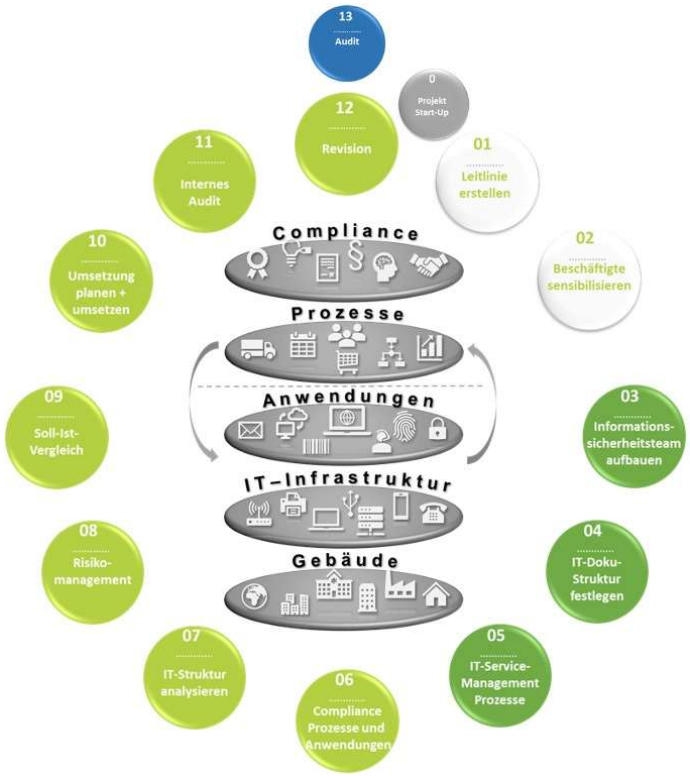


Abbildung 2: Vorgehensmodell CISIS12

Die Umsetzung dieser Sicherheitsstrategie erfolgt schrittweise durch folgende Maßnahmen:

1. **Etablierung eines ISMS**, das eine durchgängige Steuerung der Sicherheitsmaßnahmen ermöglicht.
2. **Verankerung der Informationssicherheit in der Organisation** durch klare Richtlinien und Zuständigkeiten.
3. **Integration von Sicherheitsaspekten in alle relevanten Prozesse**, um Sicherheitsmaßnahmen frühzeitig zu berücksichtigen.
4. **Regelmäßige Sensibilisierung und Schulung der Mitarbeitenden**, um ein dauerhaftes Sicherheitsbewusstsein zu schaffen.
5. **Absicherung der IT-Infrastruktur** durch geeignete technische Maßnahmen und regelmäßige Sicherheitsprüfungen.
6. **Orientierung an anerkannten Standards und Best Practices**, um den Schutz der IT-Systeme kontinuierlich zu verbessern.

Durch diese strukturierte Vorgehensweise wird sichergestellt, dass die Informationssicherheit des eGo-Saar langfristig stabil, effektiv und anpassungsfähig bleibt.

Informationssicherheit ist ein fortlaufender Prozess, der sich ständig an neue Bedrohungen und Herausforderungen anpassen muss. Der eGo-Saar verpflichtet sich daher, die Sicherheitsstrategie regelmäßig zu überprüfen, weiterzuentwickeln und an veränderte Rahmenbedingungen anzupassen

Das ISMS wird durch den ISB in Abstimmung mit der Geschäftsführung koordiniert.

Die Sicherheitsstrategie umfasst die gesamte Informationsverarbeitung im eGo-Saar. Das ISMS soll dem jeweiligen Schutzzweck angemessene Sicherheitsmaßnahmen definieren und für deren wirtschaftliche Umsetzung sorgen. Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass das erforderliche Sicherheitsniveau erreicht wird, ohne den Ablauf von Geschäftsprozessen unnötig zu beeinträchtigen.

8. Verpflichtung zur Umsetzung und Compliance

Die konsequente Umsetzung der Informationssicherheitsstrategie ist eine grundlegende Verpflichtung aller Beteiligten im eGo-Saar. Die Sicherstellung der Einhaltung interner Vorgaben sowie externer gesetzlicher und regulatorischer Anforderungen ist essenziell, um das Vertrauen der Mitgliedskommunen, Bürgerinnen und Bürger sowie Unternehmen in die digitalen Verwaltungsprozesse zu gewährleisten.

Die Verpflichtung zur Umsetzung umfasst die praktische Durchführung der Sicherheitsmaßnahmen durch alle verantwortlichen Akteure, während der Compliance-Bereich sicherstellt, dass alle relevanten Gesetze, Vorschriften und Standards eingehalten werden. Diese sind im Rechtskataster beschrieben.

Der Compliance-Beauftragte erarbeitet ein Compliance-Konzept, das sicherstellt, dass alle gesetzlichen und regulatorischen Anforderungen erfüllt werden. Dazu gehört die Erstellung eines Rechtskatasters, das alle relevanten Gesetze, Verordnungen und internen Richtlinien dokumentiert und regelmäßig aktualisiert.

9. Verpflichtung zur kontinuierlichen Verbesserung

Informationssicherheit ist kein statischer Zustand, sondern ein kontinuierlicher Prozess, der sich an neue Bedrohungen, gesetzliche Vorgaben und technische Entwicklungen anpassen muss. Deshalb verpflichtet sich die Geschäftsführung zur regelmäßigen Überprüfung und Optimierung der Sicherheitsmaßnahmen.

Der ISB wird in enger Zusammenarbeit mit dem ISMS-Team und dem Fachbereichsleiter – Zentral IT-Betrieb sicherstellen, dass die definierten Maßnahmen wirksam sind und sich nahtlos in den Arbeitsalltag des eGo-Saar integrieren. Sicherheitslücken oder Optimierungsmöglichkeiten werden regelmäßig evaluiert und zeitnah umgesetzt.

Die Informationssicherheitsstrategie wird kontinuierlich weiterentwickelt, um neuen Herausforderungen gerecht zu werden und ein hohes Maß an Schutz und Stabilität zu gewährleisten.

10. Awareness-Strategie

Informationssicherheit betrifft ohne Ausnahme alle Beschäftigten. Jede und jeder Einzelne muss durch verantwortungs- und sicherheitsbewusstes Handeln dazu beitragen, Schäden zu

vermeiden. Sensibilisierung für Informationssicherheit und fachliche Schulung der Beschäftigten sind daher eine Grundvoraussetzung für Informationssicherheit.
Die Beschäftigten werden über den Sinn von Sicherheitsmaßnahmen aufgeklärt. Dies ist insbesondere dann erforderlich, wenn diese Komfort- und/oder Funktionseinbußen zur Folge haben. Die Sicherheitsmaßnahmen sollten für den Anwender transparent und verständlich sein, sofern dadurch kein Sicherheitsrisiko entsteht.

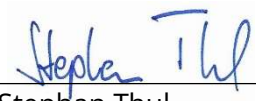
11. Verstöße und Sanktionen

Jeder Beschäftigte wird zu einem sorgfältigen Umgang mit den Daten, Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen verpflichtet. Beabsichtigte oder grob fahrlässige Verletzungen der Informationssicherheit, zum Beispiel der Missbrauch von Daten, der unberechtigte Zugriff auf Informationen oder ihre Änderung und unbefugte Übermittlung, die illegale Nutzung von Informationen, die Gefährdung der Informationssicherheit Dritter kann arbeits- und dienstrechtliche Folgen nach sich ziehen.

12. Schlussbestimmungen

Diese Leitlinie zur Informationssicherheit tritt mit Unterzeichnung durch die Geschäftsführung in Kraft. Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie zur Informationssicherheit nach spätestens 12 Monaten auf ihre Aktualität hin überprüft und ggf. aktualisiert.

Saarbrücken, den 11.12.2024



Stephan Thul
Geschäftsführer

Christophe Boutter
Geschäftsführer