Netz- und Informationssystemsicherheitsgesetz 2026 – NISG 2026
Rahmenkonzept gemäß § 32 Abs. 4 NISG 2026 (Risikomanagementmaßnahmen)

Gemeindeverband für Abfallwirtschaft und Abgabeneinhebung im Verwaltungsbezirk BADEN („GVA Baden")

Informationssicherheitskonzept

§ 32 Abs 4 a NISG 2026

Erstellt von: DI Kurt Berthold / CleverData GmbH

Letzte Bearbeitung und Freigabe durch: Mathias Fransche

Freigegeben am: 7. September 2026

In Kraft gesetzt durch: Obmann Dr. Christian Macho

Einleitung

Mit dem vorliegenden Dokument wird das Informationssicherheitskonzept des GVA Baden im geltenden Anwendungsbereich beschrieben.

Die Richtlinie ist eine bindende Richtungsvorgabe und Unterstützung durch die oberste Leitung unserer Einrichtung und legt in Übereinstimmung mit den Geschäftsanforderungen sowie geltenden Gesetzen und Regelungen den geltenden Ansatz zur Sicherung der Informationssicherheitsziele dar. Dieses Informationssicherheitskonzept bildet das übergeordnete Rahmendokument für die Umsetzung von Risikomanagementmaßnahmen gemäß § 32 NISG 2026. Die konkreten organisatorischen, technischen und operativen Maßnahmen werden in ergänzenden themenspezifischen Richtlinien und Konzepten geregelt.

Die oberste Leitung des GVA Baden bekennt und engagiert sich für die Informationssicherheit durch die Bekanntmachung dieses Informationssicherheitskonzepts bei den Beschäftigten sowie relevanten externen Parteien, dessen Umsetzung, Aufrechterhaltung und laufende Pflege.

Alle Beschäftigten sowie relevanten externen Parteien, denen diese Richtlinie zur Kenntnis gebracht wird, sind verpflichtet, den Anforderungen der Netz- und Informationssystemsicherheit entsprechend diesem Konzept sowie der themenspezifischen Konzepte der Einrichtung nachzukommen.

Überblick

Der GVA Baden wurde im Jahr 1990 gegründet, hat seinen Sitz am Schulweg 6, 2441 Mitterndorf/Fischa und betreut mit rund 30 Mitarbeitern insgesamt 32 Gemeinden, das sind mittlerweile fast 170.000 Einwohner inkl. Nebenwohnsitze des Bezirkes Baden in den Bereichen Abfallwirtschaft und Abgabenerhebung.

Bei der Umsetzung dieser Aufgaben stellen IKT-Geräte und Prozesse einen bedeutenden Faktor dar: sie sind erforderlich, um die internen und externen Abläufe unserer Tätigkeiten zeitgerecht, kosteneffizient und mit der notwendigen Qualität zu gewährleisten.

Der GVA Baden ist somit in hohem Maße von einer sicheren und stets verfügbaren Informationsverarbeitung abhängig. Die Vertraulichkeit, Verfügbarkeit und Integrität unserer Daten sind dabei durch technische Fehler, technisches oder menschliches Fehlverhalten, Sabotage und Spionage gefährdet. Damit verknüpfte Folgen können Imageverlust, wirtschaftliche Schäden und sogar Gefährdung von Umwelt und Menschen sein.

Die Risikomanagementmaßnahmen des GVA Baden beruhen auf einem gefahrenübergreifenden Ansatz („All-Hazards-Ansatz"), der sowohl cyberbezogene als auch physische Bedrohungen und Risiken für Netz- und Informationssysteme berücksichtigt. Ziel ist der umfassende Schutz der Systeme sowie ihrer physischen Komponenten vor Cybersicherheitsvorfällen.

Informationssicherheit hat somit für den GVA Baden einen sehr hohen Stellenwert.

Die Kontaktpersonen des GVA Baden sind vornehmlich Gemeindebürger, für welche die Themen Datensicherheit und Datenschutz immer wichtiger werden: das Vertrauen der Bürger in die Sicherheit unserer Dienstleistungen ist für uns von besonderer Wichtigkeit. Dies umfasst alle Daten und Informationen, die zum sicheren Betrieb der Büroumgebung und der Außenstellen benötigt werden. Betroffen sind hierbei auch personenbezogene Daten, welche ein erhöhtes Schutzniveau erfordern. Zum Schutz dieser Daten treffen wir alle notwendigen und wirtschaftlich vertretbaren Maßnahmen, um diese gemäß dem Stand der Technik zu schützen.

Informationssicherheit bedeutet für den GVA Baden, dass in allen technischen (und nichttechnischen) Systemen, die für die Informationsverarbeitung eingesetzt werden, folgende Grundwerte gesichert sein müssen:

- **Vertraulichkeit:** der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.
- **Integrität:** die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
- **Verfügbarkeit** von Dienstleistungen, Funktionen der IT-Systeme, -Anwendungen oder -Netzen. Diese sollen von den Anwendern stets wie vorgesehen genutzt werden können.

Informationssicherheitsziele

Der GVA Baden bewegt sich in einem hochtechnisierten Umfeld. Deshalb ist es erforderlich, dass wir uns laufend mit den neuesten Technologien auseinandersetzen. Demgemäß verfolgen wir im Rahmen des Informationssicherheitsmanagements die folgenden Sicherheitsziele:

- Das Image des GVA Baden hängt in hohem Maße von der Zuverlässigkeit der übertragenen Aufgabenerfüllung und dem Vertrauen der Gemeinden und Bürger ab. In diesem Sinne ist auf größte Sorgfalt hinsichtlich des bestimmungsgemäßen Gebrauchs der Informationsverarbeitung zu achten, um das Vertrauen und das gute Image aufrecht zu erhalten.
- Informationen und Systeme werden im Hinblick auf ihre Verfügbarkeit so gesichert, dass allenfalls auftretende Ausfallzeiten im Rahmen tolerierbarer Grenzen liegen.
- Die Anforderungen an Integrität und Vertraulichkeit orientieren sich an gesetzlichen Vorgaben und den Anforderungen der Bürger.
- Die Erfordernisse des Datenschutzes müssen bei der Bearbeitung personenbezogener Daten uneingeschränkt erfüllt werden.
- Sämtliche Maßnahmen der Informationssicherheit müssen in einem sinnvollen und auch wirtschaftlich zu verstehenden Verhältnis zum Wert der zu schützenden Informationen stehen. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen müssen jedenfalls verhindert werden.
- Der Zugriff auf Informationen muss durch ein Berechtigungskonzept geregelt sein.
- Auf den angemessenen Schutz unserer gesamten IT-Infrastruktur und Räumlichkeiten ist stets zu achten.
- Für den Zugriff auf Informationssysteme werden dem Stand der Technik entsprechende Authentifizierungsverfahren eingesetzt. Insbesondere werden für kritische Systeme Mehrfaktor-Authentifizierungsverfahren vorgesehen.
- Die Kommunikation (z.B. E-Mail, Sprache, Videokommunikation) ist entsprechend dem Schutzbedarf durch geeignete Sicherheitsmaßnahmen (z.B. Verschlüsselung) abgesichert.

Informationssicherheitsstrategie

Qualitätsanspruch: Im Hinblick auf die Erreichung der Informationssicherheitsziele und eine kontinuierliche Verbesserung des Sicherheitsniveaus orientiert sich der GVA Baden an einschlägigen Normen.

Rechtmäßigkeit: Wir haben uns verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) den Anforderungen des NISG 2026 entsprechend zu verwirklichen, aufrechtzuerhalten

und fortlaufend zu verbessern. Der GVA Baden versteht die Informationssicherheit als kontinuierlichen Prozess, welcher laufend umgesetzt wird.

Awareness: Da die schwächsten Glieder im System die wahrscheinlichsten Angriffsziele darstellen, richten wir unsere Risikomanagementprozesse dahingehend aus, ein möglichst hohes Sicherheitsniveau zu erreichen. Jeder einzelne kann dazu beitragen, das Sicherheitsniveau zu verbessern - Sicherheit kann auch von kleinen Handlungen und/oder Entscheidungen abhängen.

Portfolio: Die Umsetzung der Informationssicherheitsstrategie erfolgt durch ein verbindliches Richtlinien- und Maßnahmenportfolio.
Diese Richtlinien decken die Mindestinhalte gemäß § 32 Abs. 4 NISG 2026 ab und stellen sicher, dass ein angemessenes Cybersicherheitsniveau entsprechend dem Stand der Technik umgesetzt und aufrechterhalten wird.

Verantwortungen

Alle Mitarbeiter haben die gemeinsame Verpflichtung, für ein angemessenes Sicherheitsniveau zu sorgen. Diese Mitverantwortung für die Informationssicherheit gilt unabhängig von Stellung und Aufgabenbereich. Es wird von jedem erwartet, im Falle von erkannten Sicherheitsproblemen selbständig und ohne Aufforderung aktiv zu werden. Demgemäß sind alle Mitarbeiter verpflichtet, Risiken zu identifizieren und bei der Risikobehandlung mitzuwirken. Ansprechpartner für Sicherheitsbelange und auch für Verbesserungsvorschläge ist der Informationssicherheitsbeauftragte.

Zur Aufrechterhaltung und Weiterentwicklung des Sicherheitsbewusstseins werden daher entsprechende Unterstützungen in Form von Schulungen und Trainings geleistet. Mitarbeiter und Führungskräfte sind angehalten, an diesen Trainings teilzunehmen und sich aktiv einzubringen.

Alle bestehenden und zukünftigen Vorgaben zur Erreichung der Sicherheitsziele sind zu beachten und umzusetzen.

Die Einhaltung der Informationssicherheitsmaßnahmen wird aktiv kontrolliert. Sollten Mitarbeiter die Informationssicherheitsmaßnahmen nicht ausreichend beachten, werden die zuständigen Leitungsorgane diese Mitarbeiter bezüglich ihrer Verpflichtungen anleiten. Gegebenenfalls wird Missachtung sanktioniert.

Für jede themenspezifische Richtlinie ist ein Prozessverantwortlicher festzulegen. Dieser ist für die Erstellung, Aktualisierung, Umsetzung und Überwachung der jeweiligen Richtlinie zuständig.

Die Einhaltung der Richtlinien wird durch den Informationssicherheitsbeauftragten regelmäßig überprüft und der obersten Leitung berichtet.

Verpflichtung der obersten Leitung

Die oberste Leitung hat die Einhaltung der Risikomanagementmaßnahmen sicherzustellen. Sie verpflichtet sich zur Bereitstellung dafür ausreichender Ressourcen. Dazu gehören finanzielle Mittel sowie Personal, Verfahren, Instrumente, Technologien, Material, Räumlichkeiten, Ausstattung, Schulungen und zeitliche Kapazitäten.

Die oberste Leitung legt mit dem vorliegenden Informationssicherheitskonzept Grundsätze und Maßnahmen der Informationssicherheit fest. Das Konzept ist wesentlicher Bestandteil der Umsetzung der IT-Strategie. Die oberste Leitung verpflichtet sich, das vorliegende Informationssicherheitskonzept umzusetzen und dessen Wirksamkeit ständig zu verbessern, insbesondere auch durch regelmäßige Überprüfung und Aktualisierung.

Geltungsbereich des Dokuments

Die Inhalte dieses Dokuments gelten für alle Mitarbeiter, Auftragnehmer und sonstigen Partner des GVA Baden, soweit diese vertraglich, gesetzlich oder durch gesonderte Verpflichtung zur Einhaltung der Informationssicherheitsvorgaben verpflichtet wurden.

Alle o.e. werden hiermit darauf hingewiesen, diese Leitlinie zur Kenntnis zu nehmen. Sollte ein Punkt Unklarheiten oder Missverständnisse hervorrufen, sind sie dazu aufgefordert, sich umgehend mit uns in Verbindung zu setzen.

Inkraftsetzung und Kommunikation

Die fachlich inhaltliche Freigabe dieses Dokuments erfolgt durch den Informationssicherheitsbeauftragten, die Genehmigung und Inkraftsetzung durch die oberste Leitung. Dieses Dokument tritt nach Bekanntgabe in Kraft, gilt in der jeweils aktuellen veröffentlichten Form und ist verpflichtend anzuwenden.

Klassifizierung und Zugriff

Dieses Dokument ist **öffentlich** und unter https://gvabaden.at/ abrufbar.

Überprüfung der Richtlinie

Die nächste Überprüfung dieser Richtlinie durch den Informationssicherheitsbeauftragten findet bis zum 30.06.2027 statt. Die Überprüfung findet zumindest jährlich statt und umfasst auch die Einbeziehung der obersten Leitung in das Ergebnis der Überprüfung.

Darüber hinaus wird die Wirksamkeit der Informationssicherheitsmaßnahmen regelmäßig anhand geeigneter Methoden überprüft. Dazu zählen insbesondere interne Audits, Kontrollen, Kennzahlen (KPIs), Tests sowie Managementbewertungen. Die Ergebnisse fließen in die kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems ein.

Gender-Disclaimer

Aus Gründen der besseren Lesbarkeit wurde bei Personenbezeichnungen und personenbezogenen Hauptwörtern auf dieser Webseite die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform dient ausschließlich der besseren Lesbarkeit und beinhaltet keinerlei Wertung.

Dokumentenstruktur des ISMS

Das vorliegende Informationssicherheitskonzept bildet die oberste Ebene der ISMS-Dokumentation. Darauf aufbauend bestehen themenspezifische Richtlinien, Prozessbeschreibungen sowie operative Anweisungen.

Diese Dokumente sind miteinander verknüpft und bilden gemeinsam das Informationssicherheitsmanagementsystem des GVA Baden.

Dr. Christian Macho
Obmann des GVA Baden

Mathias Fransche
Informationssicherheitsbeauftragter
des GVA Baden