LEITLINIE FÜR INFORMATIONSSICHERHEIT - GEMEINDE GROSSROSSELN

ÄNDERUNGSHISTORIE

Version	Ausgabedatum	Veranlassung, Art & Stelle der Änderung	Status	Bearbeiter
0.2	21.08.2023	Grundlegende Erstanpassung	In Bearbeitung	Céline Schwindling
0.3	12.09.2023	Kleinere Anpassungen	In Bearbeitung	Céline Schwindling
1.0	12.09.2023	Freigabe	freigegeben	Dominik Jochum
1.1	24.04.2024	Kleine Anpassung (Geschäftsbereich)	In Bearbeitung	Céline Schwindling
1.2	23.05.2024	Freigabe	freigegeben	William Dube, Dominik Jochum
1.3	21.03.2025	Anpassung des Geltungsbereichs	In Bearbeitung	Eileen Ohene
1.4	27.03.2025	Überarbeitung	In Bearbeitung	William Dube, Céline Schwindling
2.0	07.05.2025	Freigabe	freigegeben	William Dube, Dominik Jochum
2.1	05.03.2026	Anpassung des Geltungsbereichs	In Bearbeitung	Yannick Halfmann
2.2	05.03.2026	Freigabe	freigegeben	William Dube, Dominik Jochum

Tabelle 1: Änderungshistorie

INHALTSVERZEICHNIS

1 Einleitung

Geschäftsprozesse, Informationstechnik, Bedrohungsszenarien und Sicherheitstechnik unterliegen einem kontinuierlichen Wandel. Externe Rahmenbedingungen, wie z. B. Gesetze und Verordnungen, spielen hier eine wesentliche Rolle. Das Informationssicherheitsmanagement ist daher ein wesentlicher Prozess, dessen Angemessenheit und Wirksamkeit als Schlüsselrolle für eine Behörde angesehen werden kann.

Die Informationssicherheit ist eine unverzichtbare Grundlage für ein Verwaltungshandeln, dem die Bürgerinnen und Bürger, die Unternehmen und alle unsere Partner ihr Vertrauen schenken können. Ziel der vorliegenden Leitlinie ist es, die Leitaussagen zur Informationssicherheitsstrategie zusammenzufassen und die zu verfolgenden Informationssicherheitsziele und das angestrebte Sicherheitsniveau zu dokumentieren.

Für die Gemeinde Großrosseln, mit ihrer dezentralen Verwaltungsstruktur und der Nähe zur Bevölkerung, ist ein hohes Maß an Vertraulichkeit, Integrität und Verfügbarkeit von Informationen essenziell. Gerade in einer grenznahen Lage und mit vielfältiger digitaler Infrastruktur – von der zentralen Verwaltung bis zu Schulen und kommunalen Einrichtungen – gewinnt ein systematisches Informationssicherheitsmanagement nach dem CISIS12-Standard an Bedeutung.

Im Rahmen ihrer Digitalisierungsstrategie strebt die Gemeinde Großrosseln nicht nur eine effiziente und bürgernahe Verwaltung an, sondern auch einen proaktiven Schutz vor Cyberbedrohungen. Die kontinuierliche Sensibilisierung der Mitarbeitenden, die klare Festlegung von Verantwortlichkeiten sowie die technische und organisatorische Absicherung aller Informationswerte sind dabei zentrale Ziele.

Mit dem vorliegenden Sicherheitsleitlinie bekennt sich die Behördenleitung der Gemeinde Großrosseln mitsamt Ihrer Eigenbetriebe zu ihrer Verantwortung für Informationssicherheit. Der Informationssicherheitsbeauftragte pflegt diese Leitlinie im Auftrag der Gemeinde.

2 Geltungsbereich

In nahezu allen Bereichen der Gemeinde werden Daten und Informationen elektronisch verarbeitet, gespeichert und übermittelt. In allen Fachbereichen spielt die Informationsverarbeitung eine tragende Rolle.

Diese Leitlinie gilt für alle Dienststellen der Gemeinde Großrosseln, die im Geschäftsverteilungsplan der Gemeinde Großrosseln genannt sind. Der Geltungsbereich des Informationssicherheitsmanagement bezieht sich zunächst auf das Rathaus sowie auf das Bauamt. Das Rathaus und das Bauamt umfassen das Wesen der Verwaltung, weshalb diese Stellen zuerst betrachtet werden. Die restlichen Stellen (bspw. Schule, Feuerwehr etc.) werden aufgrund von Zuständigkeiten der Systeme vor Ort nur sukzessive betrachtet. Im Klostergebäude des Rathauses befinden sich Räumlichkeiten, die von anderen Dienstleistern verwendet werden. Diese werden aus dem Geltungsbereich ausgeschlossen.

3 Stellenwert der Informationssicherheit

Die Gemeinde Großrosseln misst der Informationssicherheit eine zentrale Bedeutung bei. Sie ist Grundvoraussetzung für eine moderne, effiziente und vertrauenswürdige Verwaltungsarbeit – sowohl im digitalen Raum als auch bei klassischen Verwaltungsprozessen. Die fortschreitende Digitalisierung macht ein strukturiertes und nachhaltiges Informationssicherheitsmanagementsystem (ISMS) unverzichtbar.

Mit dieser Informationssicherheitsleitlinie definiert die Gemeindeverwaltung verbindliche Grundsätze und Regelungen zum Schutz der ihr anvertrauten Informationen in allen Fachbereichen.

Informationssicherheit wird dabei ganzheitlich verstanden. Sie bezieht sich auf:

- die gesamte Informations- und Kommunikationstechnik (IKT),
- analoge Informationen (z. B. Papierakten),
- interne und externe Kommunikationswege,
- gesprochene und gedachte Informationen im dienstlichen Kontext.

Moderne Verwaltungsprozesse sind in nahezu allen Bereichen auf digitale Werkzeuge und vernetzte IT-Infrastrukturen angewiesen. Daraus ergeben sich neue Risiken: technische Ausfälle, Schadsoftware, Cyberangriffe oder menschliches Fehlverhalten können schwerwiegende Auswirkungen auf die Handlungsfähigkeit der Verwaltung haben. Gleichzeitig steigen die Erwartungen von Bürger*innen, Unternehmen und Behördenpartnern an eine zuverlässige und sichere digitale Verwaltung.

4 Schutzziele der Informationssicherheit

Die Gemeinde Großrosseln verfolgt mit dem Betrieb des ISMS klare Schutzziele. Diese orientieren sich an den drei Grundwerten der Informationssicherheit:

- **Vertraulichkeit**
  Informationen dürfen nur von befugten Personen eingesehen, verarbeitet und weitergegeben werden.

  Beispiel: Der Zugriff auf Personalakten ist auf berechtigte Personen beschränkt.

- **Integrität**
  Informationen müssen vollständig und unverfälscht sein. Unautorisierte Änderungen sind zu verhindern.

  Beispiel: Einträge in Personalakten dürfen nicht durch unbefugte Mitarbeitende geändert werden.

- **Verfügbarkeit**
  Informationen und IT-Systeme müssen für berechtigte Nutzer*innen zuverlässig zugänglich sein.

  Beispiel: Der Zugriff auf wichtige Unterlagen darf nicht durch Systemausfälle verhindert werden.

Die Sicherheit der Informationsverarbeitung ist damit ein zentrales Anliegen der Gemeinde und beruht auf dem Zusammenspiel von:

- bewusstem, sicherheitsgerechtem Verhalten,
- organisatorischen Vorgaben und Regelungen,
- zeitgemäßen technischen Schutzmaßnahmen.

Ziel ist es, Informationen und Systeme so abzusichern, dass:

- zu erwartende Ausfallzeiten tolerierbar bleiben,
- der Verlust von Informationen kompensierbar ist,
- die Vertraulichkeit sensibler Daten, z. B. von Personaldaten oder technischen Dokumentationen, geschützt wird,
- finanzielle Schäden und Imageschäden durch Sicherheitsvorfälle vermieden werden.

Nicht nur externe Bedrohungen gefährden die Informationssicherheit – auch interne Schwachstellen, Nachlässigkeiten oder Fehlkonfigurationen können zu schwerwiegenden Problemen führen. Daher ist es notwendig, systematisch und kontinuierlich Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit aller Informationen, Anwendungen und IT-Systeme zu ergreifen.

5 Sicherheitsziele der Gemeinde Großrosseln

Informationssicherheit ist kein Selbstzweck, sondern dient der Erreichung konkreter strategischer und operativer Ziele. Die Gemeinde Großrosseln verfolgt im Rahmen ihres Informationssicherheitsmanagementsystems (ISMS) definierte Sicherheitsziele, die zur Sicherstellung eines verlässlichen, rechtskonformen und leistungsfähigen Verwaltungshandelns beitragen.

Diese Sicherheitsziele orientieren sich an den Schutzzielen der Informationssicherheit und bilden die Grundlage für konkrete Maßnahmen, Regelungen und Prozesse innerhalb der Organisation. Sie unterstützen die kontinuierliche Verbesserung des ISMS und dienen als Maßstab für die Bewertung seiner Wirksamkeit.

Die Sicherheitsziele der Gemeinde Großrosseln sind:

- **Förderung des Sicherheitsbewusstseins bei allen Mitarbeitenden:**

  Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihrem Aufgabenbereich entsprechend verantwortungsvoll handeln. Regelmäßige verpflichtende Fortbildungen aller Mitarbeitenden und Sensibilisierung müssen hier unterstützen.

- **Einhaltung gesetzlicher und regulatorischer Anforderungen:**

  Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für die Gemeindeverwaltung relevanten Gesetze, Vorschriften und vertraglichen Verpflichtungen eingehalten werden (siehe Rechtskataster der Gemeinde Großrosseln).

- **Vermeidung und Reduktion sicherheitsrelevanter Vorfälle:**

  durch präventive Schutzmaßnahmen, Risikomanagement und strukturierte Reaktion auf Störungen und Schwachstellen.

- **Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen:**

  Vertraulichkeit und Integrität wichtiger Informationen sind zu schützen, unabhängig davon in welcher Form sie vorliegen. Geheimhaltungsanweisungen sind im Umgang mit Dokumenten und Informationen sowohl in elektronischer als auch in analoger (Papier) Form Folge zu leisten.

- **Vermeidung von Ansehensverlust bzw. Imageschaden:**

  Finanzielle Schäden und ein negatives Image müssen verhindert werden

- **Schutz sensibler und vertraulicher Informationen.**

  wie z. B. Personal-, Finanz-, Sozial- oder Bauverwaltungsdaten sowie Daten mit Sicherheits- oder Geheimhaltungsrelevanz.

- **Sicherstellung der Verfügbarkeit kritischer IT-Systeme und Fachverfahren** um den ordnungsgemäßen Ablauf der Verwaltungsprozesse auch im Störungsfall zu gewährleisten.

- **Transparenz in sicherheitsrelevanten Entscheidungen und Prozessen** durch Dokumentation, Freigabeverfahren und einheitliche Richtlinien.

- **Kontinuierliche Verbesserung des ISMS**

  durch interne Audits, Managementbewertungen, Anpassung an neue Risiken und technische Entwicklungen.

6 Informationssicherheits-Organisation

Die Informationssicherheit in der Gemeinde Großrosseln wird systematisch, zielgerichtet und verantwortungsbewusst organisiert. Hierfür wurde ein Informationssicherheitsmanagementsystem (ISMS) auf Basis von CISIS12 eingeführt, das eine klare Rollen- und Aufgabenverteilung sowie definierte Prozesse zur Sicherstellung und Weiterentwicklung der Informationssicherheit vorsieht.

Die Verantwortung für die Informationssicherheit liegt bei der Verwaltungsleitung. Sie trägt die Gesamtverantwortung für den Schutz der Informationswerte der Gemeinde und stellt sicher, dass die notwendigen organisatorischen und personellen Ressourcen zur Verfügung stehen.

Zur operativen Umsetzung wurde ein Informationssicherheitsbeauftragter (ISB) bestellt. Diese Person ist zentraler Ansprechpartner in allen Belangen der Informationssicherheit und koordiniert die Umsetzung der Maßnahmen im Rahmen des ISMS. Der ISB berichtet direkt an die Verwaltungsleitung und arbeitet eng mit der IT-Abteilung, dem Datenschutzbeauftragten, dem Personalbereich sowie allen Fachbereichen zusammen.

Die Fachbereiche der Verwaltung sind verantwortlich für die Informationssicherheit in ihrem jeweiligen Zuständigkeitsbereich. Sie stellen sicher, dass Schutzmaßnahmen umgesetzt und Mitarbeitende für den sicheren Umgang mit Informationen sensibilisiert werden.

Grundsätzlich sind folgende Verantwortlichkeiten innerhalb des ISMS definiert:

- **Behördenleitung**

Die Behördenleitung ist das oberste Entscheidungsgremium. Sie verabschiedet auf Vorschlag des Informationssicherheitsbeauftragten diese Informationssicherheitsleitlinie.

Die Behördenleitung ist dafür verantwortlich, sicherzustellen, dass das ISMS entsprechend dieser Richtlinie umgesetzt und aktualisiert wird und die notwendigen Ressourcen verfügbar sind.

Den involvierten Mitarbeitenden werden ausreichend finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die festgelegten Sicherheitsziele zu erreichen.

Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) verbleibt bei der Behördenleitung.

- **IT-Leitung**

Die zentrale Instanz für die operative IT-Sicherheit ist die IT-Leitung. Sie ist für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich.

- **Informationssicherheitsbeauftragter**

Der Informationssicherheitsbeauftragte, ist für die Koordination des Betriebs des ISMS verantwortlich, sowie für die Berichterstattung über dessen Leistungsfähigkeit. Er ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für Mitarbeitende verantwortlich.

Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch den Informationssicherheitsbeauftragten. Dabei muss besonderes Augenmerk darauf gerichtet werden, dass durch den Einsatz der neuen Komponenten und Verfahren Risiken hinsichtlich Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) nicht erhöht werden.

Der Informationssicherheitsbeauftragte berät die Behördenleitung und die Fachbereiche in Fragen der Informationssicherheit. Er beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt notwendige Maßnahmen vor. Des Weiteren ist er frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen zu können.

- **ISMS-Management-Team**

Das ISMS-Management-Team setzt sich aus dem Informationssicherheitsbeauftragten, der IT-Leitung, der Projektleitung, der Behördenleitung, der Vertreterin des Personalrates, der Datenschutzbeauftragte und bei Bedarf aus der Personalvertretung zusammen.

Das ISMS-Management-Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit. Weiterhin werden im ISMS-Management-Team Audits geplant und Sicherheitsvorfälle besprochen. Im ISMS-Management-Team werden auch die Dokumente des ISMS laufend überprüft und überarbeitet. Planungen und Änderungen im Anwendungsbereich sind stets im ISMS-Management-Team abzustimmen.

- **Mitarbeitende**

Die Mitarbeitenden tragen eine zentrale Verantwortung für die Informationssicherheit in der Gemeinde. Sie sind verpflichtet, sich regelmäßig mit den Inhalten der Informationssicherheitsleitlinie sowie weiteren relevanten Regelungen vertraut zu machen und an angebotenen Schulungen und Sensibilisierungsmaßnahmen teilzunehmen. Ziel ist es, das Bewusstsein für Risiken im Umgang mit Informationen und IT-Systemen zu schärfen und ein sicherheitsgerechtes Verhalten im Arbeitsalltag zu fördern. Ein verantwortungsvoller Umgang mit den eingesetzten Informationssystemen sowie den darin gespeicherten und verarbeiteten Daten ist unerlässlich. Dabei sind insbesondere Betriebs- und Geschäftsgeheimnisse vertraulich zu behandeln und vor unbefugtem Zugriff zu schützen. Jeder Mitarbeitende ist verpflichtet, Unregelmäßigkeiten oder sicherheitsrelevante Vorkommnisse unverzüglich dem Informationssicherheitsbeauftragten sowie der jeweiligen Führungskraft zu melden. Es wird erwartet, dass alle Nutzenden von IT-Systemen die Informationssicherheitsleitlinie kennen, verstehen und deren Vorgaben im täglichen Handeln umsetzen. Die Verantwortung für den Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Informationen liegt grundsätzlich bei den jeweiligen Eigentümerinnen der Informationen; die Mitarbeitenden unterstützen diesen Schutz aktiv im Rahmen ihrer Aufgaben.

- **Weitere Verantwortlichkeiten**

Für alle Informationen, Geschäftsprozesse, sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Projektkoordinatorin, Informations-, Prozess-, und Systemeigentümer) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeitenden dieser Bedeutung entsprechend handeln. Sie

verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber der Leitung rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartner die Vorgaben der Stadtverwaltung zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

7 Kernelemente der Sicherheitsstrategie

Die Informationssicherheitsstrategie der Gemeinde Großrosseln verfolgt einen systematischen, risikobasierten und an den tatsächlichen Bedürfnissen orientierten Ansatz. Ziel ist es, ein angemessenes und wirtschaftlich tragfähiges Sicherheitsniveau zu schaffen, das sowohl gesetzlichen Anforderungen genügt als auch die digitale Handlungsfähigkeit der Verwaltung nachhaltig sichert.

Die Strategie basiert auf dem Managementsystemansatz von CISIS12 und verbindet organisatorische, technische und personelle Maßnahmen zu einem ganzheitlichen Schutzkonzept.

Die zentralen Elemente der Sicherheitsstrategie sind:

- **Verbindliche Sicherheitsleitlinie**

  Die Informationssicherheitsleitlinie definiert grundlegende Prinzipien und Regelungen. Sie wird durch die Behördenleitung beschlossen, regelmäßig überprüft und bei Bedarf angepasst.

- **Rollenbasierte Verantwortung**

  Klare Zuständigkeiten auf allen Ebenen: von der Behördenleitung über den Informationssicherheitsbeauftragten (ISB) bis hin zu allen Mitarbeitenden.

  Ziel: Jeder kennt seine Aufgaben und Pflichten im Kontext der Informationssicherheit.

- **Gefährdungs- und Risikoanalyse**

  Schutzmaßnahmen werden auf Basis identifizierter Risiken geplant und umgesetzt.

  Grundsatz: Nur wer Risiken kennt, kann diese wirksam begrenzen.

- **Schutzbedarfsgerechte Maßnahmenplanung**

  Technische und organisatorische Maßnahmen richten sich nach dem Schutzbedarf der jeweiligen Informationen und Prozesse (Vertraulichkeit, Integrität, Verfügbarkeit).

- **Awareness und Schulung**

  Regelmäßige Sensibilisierung und Fortbildung aller Mitarbeitenden zur Förderung eines sicherheitsbewussten Verhaltens.

- **Notfallvorsorge und Wiederanlaufplanung**

  Entwicklung von Notfallkonzepten für kritische Prozesse und Systeme zur Sicherstellung der Handlungsfähigkeit im Ernstfall.

- **Kontinuierliche Verbesserung**

  Das ISMS wird regelmäßig evaluiert, durch interne Audits geprüft und im Rahmen des PDCA-Zyklus (Plan – Do – Check – Act) weiterentwickelt.

- **Dokumentation und Nachvollziehbarkeit**

  Alle sicherheitsrelevanten Prozesse, Maßnahmen und Entscheidungen werden nachvollziehbar dokumentiert.

- **Einbindung externer Partner**

  Dienstleister und externe Partner werden vertraglich zur Einhaltung definierter Sicherheitsstandards verpflichtet.

8 Verpflichtung zur Umsetzung

Interne und externe Vorschriften

Die konsequente Umsetzung der Informationssicherheitsstrategie ist eine grundlegende Verpflichtung aller Beteiligten der Gemeinde Großrosseln. Die Sicherstellung der Einhaltung interner Vorgaben sowie externer gesetzlicher und regulatorischer Anforderungen ist essenziell, um das Vertrauen der 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 Personalbereich sicherstellt, dass alle relevanten Gesetze, Vorschriften und Standards eingehalten werden.

Diese sind im Rechtskataster beschrieben.

9 Verpflichtung zur kontinuierlichen Verbesserung

Die Gemeinde Großrosseln strebt die kontinuierliche Verbesserung ihrer Prozesse rund um die Informationssicherheit an.

Die Identifizierung und Steuerung von Informationssicherheitsrisiken und die dadurch entstehende Transparenz vorhandener Risiken haben eine hohe Bedeutung.

10 Verstöße und Sanktionen

Alle Mitarbeiter/-innen der Gemeinde Großrosseln sind zu einem sorgfältigen Umgang mit den Daten, Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen verpflichtet. Vorsätzliche 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

können dienstrechtliche und strafrechtliche Folgen nach sich ziehen.

11 Inkraftsetzung

Die Informationssicherheitsleitlinie tritt mit Unterzeichnung in Kraft und wird allen Mitarbeiter/-innen nach Unterschrift umgehend zur Kenntnis gebracht.

Großrosseln, 12.03.2026

[Behördenleitung] [ISB]