LANDKREIS
FREYUNG-GRAFENAU

FRG
Landkreis
Freyung
Grafenau

MEHR RAUM
UND ZEIT.

Leitlinie für Informationssicherheit

Version: 2025-02

Inhaltsverzeichnis

1. Dokumentenschutz

Name	Servername	Pfad
Öffentlich	-	Webseite

2. Stellenwert der Informationssicherheit

Das Landratsamt Freyung-Grafenau ist als öffentliche Verwaltung auf eine funktionierende und verlässliche Informationsverarbeitung angewiesen. Ein Großteil der Daten der Verwaltung sind personenbezogene Daten. Das Landratsamt Freyung-Grafenau ist aufgrund von gesetzlichen Vorgaben dazu verpflichtet, die angemessene Sicherheit seiner Informationen und seiner Informationsverarbeitung sicher zu stellen.

Die gesetzliche Grundlage ergibt sich u.a. aus:

- Informationssicherheitsgesetz (ISiG)
- Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG)
- Datenschutz-Grundverordnung (DSGVO)
- Bayerisches Datenschutzgesetz (BayDSG)
- Bayerisches Digitalgesetz Gesetz (BayDiG)
- dem Grundsatz des rechtmäßigen Verwaltungshandels (Rechtsstaatsprinzip Art. 20 Abs. 3 Grundgesetz

Im Landratsamt Freyung-Grafenau sind bei Vorfällen in der Informationssicherheit verschiedene Stakeholder betroffen. Zu den wichtigsten gehören:

- Mitarbeiter
- Leitung der Behörde
- Bürger
- externe Partner
- Aufsichtsbehörden

Die zunehmende Digitalisierung stellt die Verwaltung des Landratsamtes Freyung-Grafenau vor vielfältige zukünftige Herausforderungen. Dazu gehören die flexible Nutzung von Heimarbeitsplätzen, die Integration von Cloud-Diensten, die Einführung einer elektronischen Aktenführung (E-Akte) sowie die Bereitstellung von Online-Bürgerdiensten im Rahmen des Onlinezugangsgesetzes (OZG).

In diesem Kontext spielt der KI-Einsatz eine entscheidende Rolle. Künstliche Intelligenz (KI) bietet sowohl für Bürger als auch für Verwaltungsmitarbeiter enormes Potenzial, die Effizienz zu steigern, die Qualität der Dienstleistungen zu verbessern und die Verwaltung zukunftsorientiert auszurichten.

Die Grundlage dafür ist ein Bekenntnis der Behördenleitung zur Informationssicherheit. Dieses Bekenntnis und damit auch die Übernahme der Gesamtverantwortung durch den Unterzeichner, wird durch diese Informationssicherheitsleitlinie (ISL) zum Ausdruck gebracht.

3. Geltungsbereich

Die Leitlinien verpflichten alle internen und externen Mitarbeiter zu gesetzeskonformem und verantwortungsbewusstem Umgang mit der IT-Infrastruktur und den Informationen, die im Landratsamt Freyung-Grafenau verarbeitet, gespeichert und übertragen werden. Die Leitlinien werden allen

internen und externen Mitarbeitern in geeigneter Weise bekannt gegeben und zugänglich gemacht. Diese Leitlinie gilt grundsätzlich für alle Bereiche der Verwaltung, insbesondere für die Prozesse, die die Informationen und Daten elektronisch verarbeiten, übermitteln oder speichern.

Der Geltungsbereich umfasst die gesamte IT-Infrastruktur im Verwaltungsnetzwerk des Landratsamtes Freyung-Grafenau inkl. aller Außenstellen.

4. Sicherheitsziele

Das Landratsamt Freyung-Grafenau schützt durch die Gewährleistung einer angemessenen Informationssicherheit seine Interessen.

Folgende Ziele sollen in Bezug auf die Informationssicherheit konkret erreicht werden:

- Sensibilisierung aller Mitarbeiter und Vermittlung der erforderlichen Kenntnisse im Umgang mit Daten, IT-Systemen und Kommunikationsmedien
- Aktualität und Aufrechterhaltung der Einsatzbereitschaft der IT-Systeme (Arbeitsplätze, Server, Netzwerkinfrastruktur, Anwendungen)
- Vermeidung von IT-Sicherheitsvorfällen und negativen Auswirkungen auf die Verwaltung (Kosten, Reputation, Datenverlust)
- Einhaltung der gesetzlichen Vorschriften
- Schaffung eines hohen Vertrauensniveaus für alle Beteiligten

Die gesetzten Ziele werden anhand geeigneter Maßnahmen und von messbaren Zielen (interne Audits, Begehungen, Mitarbeitergespräche, Checklisten, Auswertung von Protokollen usw.) kontrolliert und in regelmäßigen Abständen der Behördenleitung berichtet.

5. Kernelemente der Sicherheitsstrategie

Die Informations- und Datensicherheit ist für das Landratsamt Freyung-Grafenau sehr wichtig. Die Sicherheitsstrategie ist deshalb wie folgt aufgebaut:

- Das Landratsamt Freyung-Grafenau etabliert ein geeignetes Informationssicherheitsmanagementsystem (ISMS) und orientiert sich dabei am BSI-Grundschutz.
- Als zentrale Sicherheitsinstanz ernennt der Landrat einen Informationssicherheitsbeauftragten (ISB) und einen Stellvertreter, der für alle Belange und Fragen der Informationssicherheit zuständig ist. Er ist unabhängig und weisungsfrei sowie der Behördenleitung in dieser Rolle direkt unterstellt. Dem ISB sind ausreichend Ressourcen zur Verfügung zu stellen und geeignete Qualifizierungsmaßnahmen zu ermöglichen.
- Zur Unterstützung des ISBs wird ein Informationssicherheitsteam gebildet, das sich in regelmäßigen Abständen zu Besprechungen trifft. Das Team besteht aus dem ISB, Vertretern der Leitungsebene, dem IT-Leiter, Personalrat und dem Datenschutzbeauftragten.
- Das Landratsamt Freyung-Grafenau verankert das Thema Informationssicherheit in der gesamten Organisation durch klar formulierte Richtlinien und Sicherheitsvorgaben, die für alle

Beschäftigten verbindlich sind.
- Für die Mitarbeiter gibt es fortlaufende Schulungs- und Sensibilisierungsmaßnahmen.
- Die umgesetzten Sicherheitsmaßnahmen werden einer regelmäßigen Kontrolle unterzogen (z.B. durch Begehungen oder interne Audits) und das Ergebnis wird der Behördenleitung mitgeteilt.
- Das eingeführte Informationssicherheitsmanagementsystem und die damit verbundenen Maßnahmen werden regelmäßig aktualisiert und weiterentwickelt.
- Das Landratsamt Freyung-Grafenau orientiert sich bei allen Aktivitäten zur Informationssicherheit an aktuellen Standards und bewährten Methoden aus der Praxis.

6. Maßnahmen

Die Maßnahmen umfassen sowohl technische und organisatorische Vorkehrungen, als auch verbindliche Regeln und Vorgaben für alle Mitarbeiter. Diese Regeln und Vorgaben werden in Form von Dienstanweisungen, Richtlinien, Verfahrensanweisungen und ggf. Betriebshandbüchern hinterlegt. Sie sind zu befolgen.

Bei der Umsetzung der erforderlichen Maßnahmen werden Anforderungen wie Bedienkomfort, Zugriffsgeschwindigkeit und Wirtschaftlichkeit gemäß den jeweiligen Umständen entsprechend bestmöglich berücksichtigt. Jedoch gilt folgender Grundsatz:
Sicherheit vor Verfügbarkeit vor Funktionalität.

7. Umsetzung

Um die Erreichung und Aufrechterhaltung der Informationssicherheitsziele sicherzustellen, wird ein dauerhafter, sich zyklisch wiederholender Informationssicherheitsmanagementprozess etabliert.

Ausgerichtet an den Zielen werden Maßnahmen identifiziert und dahingehend überprüft, ob zur Einhaltung der Informationssicherheit entsprechende Vorbeuge- bzw. Korrekturmaßnahmen ergriffen werden müssen. Unter Abwägung des Kosten-Nutzen-Verhältnisses wird eine entsprechende Priorisierung und Umsetzung geplant und deren Umsetzung überwacht.

Der ISB ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig zu informieren und einzubinden.

8. Schulung und Sensibilisierung der Mitarbeiter

Damit allen Mitarbeitern bekannt ist, was von Ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollen, werden regelmäßig Schulungs- und Sensibilisierungsmaßnahmen durchgeführt.

Hierzu werden folgende Maßnahmen vorbereitet und durchgeführt:

- Jeder Mitarbeiter nimmt an einer Schulung zu den Grundlagen der Informationssicherheit teil.
- Durch weitere Schulungen wird den Mitarbeitern die notwendige Kompetenz zur Informationssicherheit vermittelt, die sie bei der Ausführung ihrer Fachaufgaben benötigen.
- Bei konkretem Informationsbedarf erhalten die Mitarbeiter Newsletter oder individuelle Nachrichten vom Informationssicherheitsbeauftragten.

9. Verantwortlichkeiten

Das Erreichen und Erhalten eines angemessenen Sicherheitsniveaus erfordert ein kontinuierliches Engagement all jener, die an der Informationsverarbeitung und deren Planung und Administration beteiligt sind.

- Die Leitungsebene übernimmt die Gesamtverantwortung für die Informationssicherheit und den Informationssicherheitsprozess. Sie stellt die dafür notwendigen technischen, finanziellen und personellen Ressourcen zur Verfügung und sorgt dafür, dass der Informationssicherheitsprozess in die Strukturen, Hierarchien und Arbeitsabläufe der Verwaltung eingebettet werden.
- Der Informationssicherheitsbeauftragte (ISB) initiiert, plant und setzt den Informationssicherheitsprozess um, steuert diesen und nimmt die Rolle des zentralen Ansprechpartners für Informationssicherheit wahr.
- Das Informationssicherheitsteam (IST) unterstützt den ISB, insbesondere bei der verwaltungsweiten Koordinierung und Lenkung der Informationssicherheitsmaßnahmen und beim Erkennen neuer Gefährdungen.
- Der IT-Verantwortliche setzt die Richtlinien in seinem Verantwortungsbereich durch entsprechende technische und organisatorische Maßnahmen um und stimmt jene Maßnahmen mit dem ISB ab, die aus seiner Sicht zur Verbesserung und Erhaltung der Informationssicherheit in seinem Verantwortungsbereich ergriffen werden müssen.
- Die Administratoren implementieren technische Maßnahmen in Abstimmung mit dem IT-Verantwortlichen und erstellen Vorschläge für die Verbesserung der Informationssicherheit.
- Die Vorgesetzten mit Personalverantwortung stellen sicher, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter bzw. die in ihrem Verantwortungsbereich tätigen Nutzer umgesetzt werden.
- Jeder Mitarbeiter trägt durch sein Verhalten zur Gewährleistung der Informationssicherheit bei. Jeder Mitarbeiter ist verpflichtet, die ihn oder seine Tätigkeit betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten und umzusetzen, sowie Störungen und Sicherheitsvorfälle zu melden.
- Projektverantwortliche müssen den ISB bei allen Projekten mit Auswirkung auf die Informationsverarbeitung konsultieren, um sicherzustellen, dass sicherheitsrelevante Aspekte ausreichend beachtet werden.
- Lieferanten und sonstige Auftragnehmer werden verpflichtet, die sie betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten bzw. umzusetzen, sofern sie Zugriff auf schützenswerte Informationen oder schützenswerte Teile der Informationsverarbeitung der Verwaltung besitzen.

10. Verstöße und Sanktionen

Jeder Beschäftigte der Verwaltung 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 dienst- und strafrechtliche Folgen nach sich ziehen. Die Mitarbeiter sind angehalten, mögliche Schwachstellen oder Sicherheitsverstöße umgehend zu melden. Die Verantwortlichen prüfen bei Verstößen oder bei Nichteinhaltung von Regeln geeignete und angemessenen disziplinarische Maßnahmen zu ergreifen (z.B. Ermahnung, Abmahnung).

11. Inkraftsetzung

Die Informationssicherheitsleitlinie Version 2025-02 tritt mit Wirkung vom 27.02.2025 in Kraft.

Freyung, 27.02.2025	Herr Sebastian Gruber (Landrat)
Freyung, 27.02.2025	Frau Monika Eichinger (Leitung Hauptverwaltung)
Freyung, 27.02.2025	Herr Tomas Kudej (Informationssicherheitsbeauftragter)
Freyung, 27.02.2025	Herr Alexander Bertelshofer (Personalratsvorsitzender)