Leitlinie Informationssicherheit

Gemeinde Oberau

Dokumenteninformationen

Dokumenteneigentümer	Behördenleitung
Freigabeberechtigter	1. Bürgermeister
Autor(en)	actago GmbH, Gemeinde Oberau
Datum	10.03.2021
Version	1.1
Status	Freigegeben
Klassifizierung	Öffentlich

Hinweis:
Ein Ausdruck dieses Dokuments könnte aufgrund notwendiger Aktualisierungen bereits veraltet sein. Bitte überprüfen Sie immer die Aktualität und Gültigkeit des Ihnen vorliegenden Dokuments.

Versionshistorie

Version	Datum	Anmerkung	Bearbeiter
1.0	18.02.2021	Initiale Erstellung	actago GmbH
1.1	10.03.2021	Inhaltliche Modifikationen	Gemeinde Oberau

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Behördenleitung der Gemeinde Oberau verabschiedet folgende Leitlinie zur Informationssicherheit - *nachfolgend Leitlinie genannt*- als zentralen Bestandteil ihrer Informationssicherheitspolitik.

In dieser Leitlinie werden die grundlegenden Ziele, Anforderungen, Verpflichtungen und Verantwortlichkeiten der Informationssicherheit für die Gemeinde Oberau festgelegt. Weiterhin wird in übersichtlicher Form dargestellt und für die betroffenen Personen verständlich beschrieben, in welchem organisatorischen Rahmen diese umgesetzt werden sollen.

Die Leitlinie muss allen betroffenen Personen bekannt gegeben und kontinuierlich aktualisiert werden.

2 Stellenwert der Informationssicherheit

Die Informationssicherheit ist umfassend mit der allgemeinen Aufgabenerfüllung in der Gemeinde Oberau verbunden. Die Umsetzung der Informationssicherheit nimmt in Zeiten der fortschreitenden Digitalisierung und zunehmenden Vernetzung sowie der steigenden Bedrohung durch Angriffe einen immer höheren Stellenwert in der öffentlichen Verwaltung ein.

Zeitgemäßes Verwaltungshandeln erfordert deshalb den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung der Kommunalverwaltung im Sinne der Bürgerinnen und Bürger sowie weiterer Partner und betroffener Dritter zuverlässig, effizient und effektiv zu gestalten.

Die Gemeinde Oberau erhebt, verarbeitet und speichert eine Vielzahl von analogen und digitalen Daten (auch personenbezogen) und besitzt zudem eine enorme Aufgabenvielfalt. Von der Daseinsfürsorge bis hin zu Dienstleistungen für Bürgerinnen und Bürger, die zusätzlich einen erhöhten Schutzbedarf aufweisen. Deren Daten sind vor unberechtigter Kenntnisnahme durch Dritte besonders zu schützen.

Die Informationssicherheit ist für die Gemeinde Oberau zur Erfüllung der Verwaltungsaufgaben ein unverzichtbarer Grundwert und gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

3 Sicherheitsziele

Zur Abbildung des hohen Stellenwertes der Informationssicherheit werden für die Gemeinde Oberau die nachstehenden Sicherheitsziele festgelegt:

- **Vertraulichkeit**
  Informationen dürfen ausschließlich dem berechtigten Personenkreis zur Verfügung stehen.
- **Integrität**
  Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten muss jederzeit gewahrt sein. Dieses umfasst auch die unberechtigte Erstellung oder Änderung von Informationen.
- **Verfügbarkeit**
  Systeme, Anwendungen und Daten müssen den Berechtigten in jeder Situation wie vorgesehen zeitgerecht zur Verfügung stehen.

Im Bereich der Informationsverarbeitung und Kommunikation müssen deshalb Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten und übertragenen Informationen durch angemessene technische und organisatorische Maßnahmen gewährleistet werden.

Hierbei sind rechtliche Bestimmungen zu berücksichtigen. Zur Erreichung dieser Ziele ist die Verhältnismäßigkeit der eingesetzten Mittel zur Wahrung der schützenswerten Güter zu beachten.

4 Geltungsbereich

Die Leitlinie ist das zentrale Dokument für die gesamte Informationssicherheit. Sie bildet die Grundlage für die Informationssicherheitspolitik sowie Informationssicherheitsziele im eigenen Wirkungskreis. Sie gilt für alle Personen der unmittelbaren Verwaltung sowie für alle Personen der an sie angeschlossenen Einrichtungen und ist von diesen entsprechend ihrer Aufgabenverantwortung umzusetzen.

Personen, Behörden und Unternehmen, die nicht der Behördenleitung (Auftraggeber) der Gemeinde Oberau unterstehen, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten.

Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört auch, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

5 Verantwortung der Leitung

Die allgemeine Verantwortung bis zu einer Delegation trägt zunächst der 1. Bürgermeister.

Er trägt die Gesamtverantwortung für die Informationssicherheit zur Gewährleistung einer ordnungsgemäßen und sicheren Aufgabenerledigung im Rahmen der in Artikel 8 Abs. 1 und Art. 11 Abs. 1 BayEGovG aufgeführten gesetzlichen Grundlagen.

Er verantwortet die Umsetzung von angemessenen Sicherheitsmaßnahmen sowie eine geeignete Dokumentation innerhalb seines Verantwortungsbereiches. Er benennt einen Informationssicherheitsbeauftragten - *nachfolgend ISB genannt* - für die Gemeinde Oberau und stellt ausreichende Ressourcen zur Verfügung, um die erforderlichen personellen, infrastrukturellen, technischen und organisatorischen Maßnahmen umsetzen zu können. Des Weiteren ist die Behördenleitung verantwortlich für eine angemessene Aus- und Weiterbildung des Personals in Bezug auf Informationssicherheit und für die Durchführung von Informationssicherheits-Sensibilisierungsmaßnahmen der Nutzerinnen und Nutzer.

Die Umsetzung dieser Leitlinie sowie die daraus resultierenden Sicherheitsmaßnahmen unterliegen einer ständigen Überprüfung mit dem Ziel der Weiterentwicklung des Informationssicherheitsmanagementsystems - *nachfolgend ISMS genannt.*

6 Informationssicherheitsstrategie

Die Informationssicherheitsstrategie der Gemeinde Oberau hat das Ziel, mit wirtschaftlichem Ressourceneinsatz ein angemessenes Maß an Sicherheit zu erreichen und verbleibende Restrisiken zu minimieren. Die Informationssicherheitsstrategie wird durch die Einführung eines ISMS realisiert, welches sich an der VdS 10000 orientiert und als kontinuierlicher Prozess gestaltet wird. Dieser Prozess hat das Ziel, ein ISMS zu etablieren, aufrechtzuerhalten und kontinuierlich zu verbessern und umfasst folgende Schritte:

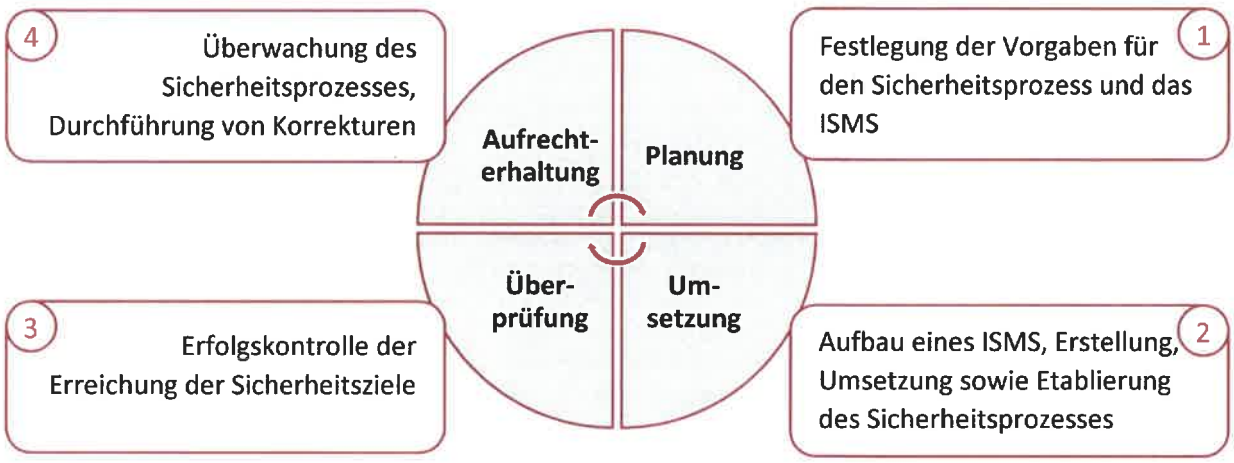

Abbildung 1: PDCA-Zyklus

Die Informationssicherheitsstrategie gilt für die gesamte Informationsverarbeitung in der Gemeinde Oberau. Das ISMS soll für den 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 die Verwaltungstätigkeiten nennenswert zu beeinträchtigen.

Die Informationssicherheitsstrategie soll von folgenden Grundsätzen der Informationssicherheit geprägt sein:

- **Zentrale Rolle der Informationssicherheit:** Die Informationssicherheit wird im Änderungsmanagement von Beginn an mitberücksichtigt. Der ISB ist bei allen Fragen zur Informationssicherheit zu beteiligen.
- **Verhältnismäßigkeit der Sicherheitsmaßnahmen:** Aufwand und Ergebnis müssen in einem angemessenen Verhältnis zueinanderstehen.
- **Bereitstellung von ausreichenden Ressourcen:** Um ein angemessenes Maß an Informationssicherheit zu erreichen und aufrecht zu erhalten, sind ausreichende finanzielle und personelle Ressourcen bereitzustellen.
- **Einbindung aller Bediensteten:** Alle Bediensteten werden in das ISMS eingebunden und hinsichtlich der Informationssicherheit sensibilisiert.
- **Restriktives Nutzungsprinzip:** Jeder Nutzer erhält nur die Zugriffsrechte, die er zur Erfüllung seiner Aufgaben benötigt.
- **Minimalprinzip des Zugriffs:** Der Zugriff auf IT-Systeme und Informationen wird auf die notwendigen Personen, Systeme und Dienste beschränkt.
- **Schutzbedarfsprinzip:** Der Schutzbedarf von IT-Systemen und - Anwendungen wird vom Schutzbedarf der darauf verarbeiteten, gespeicherten, übertragenen Informationen bestimmt.
- **Nachhaltige Betriebssicherheit:** Um die festgelegten Sicherheitsziele zu erreichen, ist eine angemessene Einschränkung hinsichtlich Funktionalität und Komfort vertretbar.

7 Struktur der dokumentierten Informationen

Wesentlicher Bestandteil eines funktionierenden ISMS sind dokumentierte Informationen wie Leitlinien, Richtlinien, Verfahrens- und Prozessbeschreibungen sowie Aufzeichnungen und Nachweise, mit denen die Informationssicherheit in der Behörde nachvollziehbar und transparent dargestellt wird.

Die Gesamtheit der dokumentierten Informationen wird übersichtlich in einer pyramidalen Struktur wie folgt abgebildet:

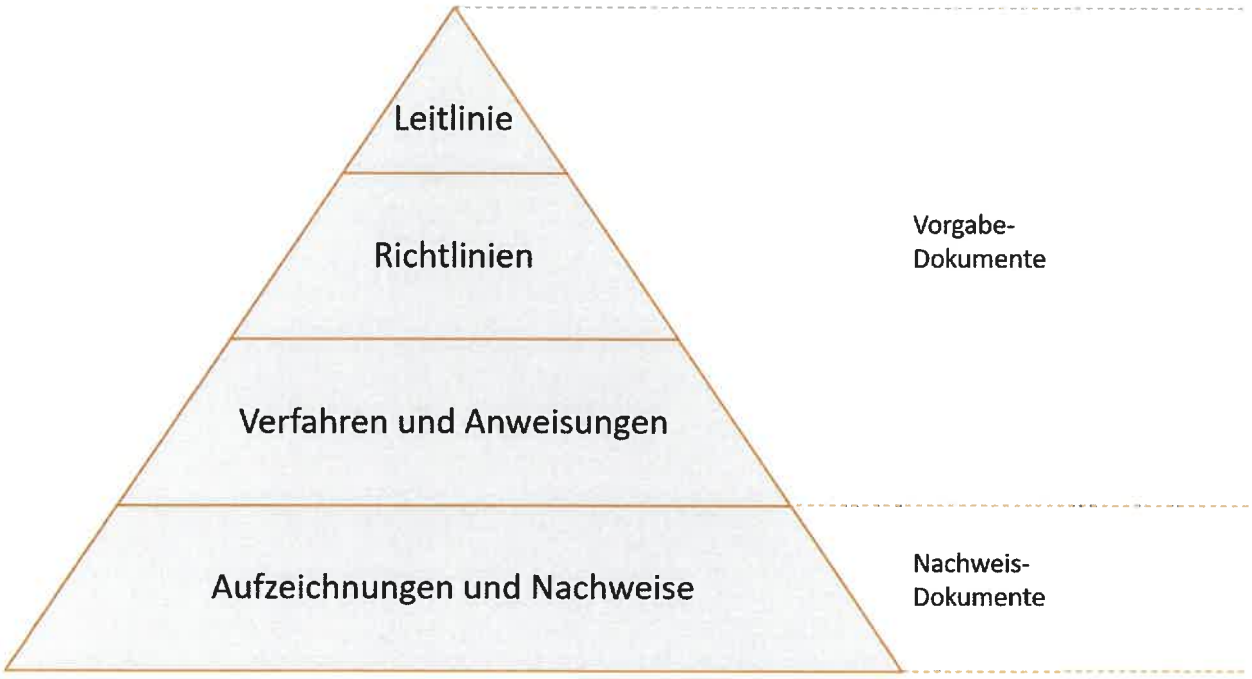

Abbildung 2: Dokumenten-Pyramide

Dabei gliedern sich die Dokumente nach dem Top-Down Prinzip:

- **Leitlinie:** Die Leitlinie steht an der Spitze der dokumentierten Informationen und beschreibt das „Warum" in Form von Strategien, Zielen und Verantwortlichkeiten der Behörde.
- **Richtlinien:** Die Richtlinien beschreiben das „Was" und konkretisieren und beschreiben einzelne Themen wie z.B. den Einsatz mobiler Endgeräte oder die Datensicherung.
- **Verfahren und Anweisungen:** Die Verfahren beschreiben das „Wie" anhand konkreter Vorgaben und Vorgehensweisen wie z.B. das Einspielen von Patches oder den Prozess bei Eintritt oder Ausscheiden von Bediensteten.
- **Aufzeichnungen und Nachweise:** Die Aufzeichnungen und Nachweise stellen die unterste Ebene der Dokumenten-Pyramide dar. Hier wird in Form von Aufzeichnungen und Nachweisen dokumentiert, wie die Vorgaben umgesetzt wurden. Dies können z.B. Protokolle oder Audit-Berichte sein, die einen Status zu einem festen Zeitpunkt widerspiegeln. Sie sind somit in die Vergangenheit gerichtet und nicht mehr änderbar.

8 Organisation der Informationssicherheit

Bei der Besetzung der Rollen wird darauf geachtet, dass die Personen fachlich und persönlich für die ihnen zugewiesene Aufgabe qualifiziert sind. Die für die Organisationsstruktur notwendigen Ressourcen werden mit geeigneten Vertreterregelungen zur Verfügung gestellt.

Bei der Verteilung der Verantwortlichkeiten muss das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten dürfen nicht von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

Die Organisationsstruktur für die Informationssicherheit der Gemeinde Oberau setzt sich aus nachfolgenden Rollen zusammen.

8.1 Behördenleitung

Die Behördenleitung beschließt die Leitlinie, überträgt die Umsetzung in die steuernde Verantwortung der Geschäftsleitung und schafft dadurch die Rahmenbedingungen für die Informationssicherheit. Auf dieser Grundlage entscheidet die Geschäftsleitung über Richtlinien und Regelungen zur Informationssicherheit.

Die Behördenleitung zeichnet gesamtverantwortlich für den Informationssicherheitsprozess und das Einbetten der Informationssicherheit in die Strukturen, Hierarchien und Arbeitsabläufe.

8.2 Informationssicherheitsteam (IST)

Das IST definiert den erforderlichen Rahmen für die Informationssicherheit in der Behörde und unterstützt den ISB in allen Belangen der Informationssicherheit.

Zu seinen Aufgaben gehört es,

- neue Bedrohungen und Schwachstellen zu erkennen und zu bewerten,
- Maßnahmen zur Informationssicherheit zu entwickeln und zu bewerten,
- Maßnahmen zur Informationssicherheit zu steuern und zu koordinieren.

Das IST informiert und unterstützt den ISB in Fragen der Informationssicherheit. Insbesondere bei der verwaltungsweiten Koordinierung und Lenkung der Informationssicherheitsmaßnahmen und beim Erkennen neuer Gefährdungen.

8.3 Informationssicherheitsbeauftragter (ISB)

8.3.1 Zuständigkeiten und Aufgaben

Der ISB ist für alle Fragen rund um die Informationssicherheit in der Gemeinde Oberau zuständig. Zu seinen Aufgaben gehört es,

- den Sicherheitsprozess zu planen, zu steuern, zu koordinieren und weiterzuentwickeln,
- die Leitung bei der Erstellung der Sicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts (Leitlinie) und zugehöriger Teilkonzepte sowie Richtlinien zu koordinieren,
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung zu initiieren und zu überprüfen,
- der Behördenleitung und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen, sowie
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren.

8.3.2 Rechte und Befugnisse

Während der Dauer der Bestellung hat der ISB unter Berücksichtigung der geltenden Datenschutzvorschiften auf alle betroffenen IT-Systeme der Behörde Zugriff, um Kontroll- und Beratungsaufgaben wahrzunehmen. Zu seinen Rechten und Befugnissen zählen,

- über alle für die Informationssicherheit relevanten Themen informiert zu werden (sowohl auf Nachfrage als auch unaufgefordert),
- über Vorhaben und Änderungen, die die Informationssicherheit berühren können (z.B. neue IT-Projekte, Änderungen der IT-Infrastruktur oder Änderungen von Rahmenbedingungen mit Auswirkungen auf die Informationssicherheit) informiert zu werden,
- das Zutrittsrecht zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhängende Daten verarbeitet werden und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden,
- die Durchführung von Prüfungen im Themenbereich der Informationssicherheit bzw. Veranlassung von Prüfungen durch unabhängige Dritte zur Überprüfung des aktuellen Informationssicherheitsniveaus.

9 IT-Verantwortlicher

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.

10 Datenschutzbeauftragter (DSB)

Der DSB wirkt auf den gesetzeskonformen Umgang mit personenbezogenen Daten im Bereich der Informationssicherheit hin. Er wird bei der Umsetzung von Maßnahmen zur Informationssicherheit in die Planungen mit einbezogen und achtet auf die Einhaltung datenschutzrechtlicher Vorgaben.

Weitere Rollen und Gremien können bei Bedarf in die Organisationsstruktur eingebunden werden.

11 Verpflichtung zur kontinuierlichen Verbesserung

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Begebenheiten und Einflüssen, wie z. B. neuen Bedrohungen, neuen Gesetzen oder auch der Entwicklung neuer technischer Lösungen ab.

Diesen Entwicklungen muss sich ein agiles ISMS stellen. Aus diesem Grund muss dafür Sorge getragen werden, dass die Sicherheitsstrategie der Gemeinde Oberau kontinuierlich weiterentwickelt wird.

Die Behördenleitung verpflichtet sich deshalb, sich an der Optimierung der Informationssicherheit zu beteiligen. Sie ist regelmäßig bzw. im Einzelfall akut über den aktuellen Sicherheitszustand durch den ISB zu informieren und ist für die Absicherung der Kontinuität des Sicherheitsprozesses verantwortlich.

Zur Umsetzung dieser Leitlinie sind durch das IST Sicherheitsmaßnahmen zur Erreichung und Aufrechterhaltung der Informationssicherheitsziele zu erarbeiten.

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

Die Sicherheitsmaßnahmen umfassen sowohl technische als auch organisatorische Maßnahmen.

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.

Der ISB ist bei allen organisatorischen und technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig einzubinden. Er hat ein Vetorecht.

12 Mitgeltende Dokumente und Aufzeichnungen

- Dienstanweisung für die Nutzung informationstechnischer Systeme
- Informationssicherheitsrichtline „Mobile IT-Systeme“
- Informationssicherheitsrichtline „Mobile Datenträger“
- Informationssicherheitsrichtline „IT-Outsourcing und Cloud Computing“
- Informationssicherheitsrichtline „Datensicherung“
- Informationssicherheitsrichtline „Archivierung“
- Informationssicherheitsrichtline „Störungen und Ausfälle“
- Informationssicherheitsrichtline „Sicherheitsvorfälle“
- Informationssicherheitsrichtline „Passwörter“

13 Änderungen und Erweiterungen

Änderungen und Abweichungen der Inhalte dieser Leitlinie sind grundsätzlich zulässig, bedürfen aber der schriftlichen Genehmigung der Behördenleitung.

Nebenvereinbarungen zu dieser Leitlinie sind nicht vorhanden. Notwendige Änderungen oder Erweiterungen zu dieser Leitlinie bedürfen der Neufassung mit anschließender erneuter Vorlage und Genehmigung der vereinbarenden Parteien.

14 Unwirksamkeit bzw. Undurchführbarkeit

Sollten einzelne Bestimmungen dieser Leitlinie unwirksam oder undurchführbar sein, oder nach Schluss derselbigen unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Leitlinie im Übrigen unberührt.

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen bzw. organisatorischen Zielsetzung am nächsten kommt, die die vereinbarenden Parteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben.

Die vorstehenden Bestimmungen gelten sinngemäß für den Fall, dass sich die Leitlinie als lückenhaft erweist, damit jedoch ihre Gültigkeit behält.

15 Konsequenzen bei Nichtbeachtung

Verhalten, das den Grundsätzen dieser Leitlinie widerspricht, die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, 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 und die Gefährdung der Informationssicherheit Dritter, kann disziplinare oder arbeitsrechtliche Folgen nach sich ziehen.

Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden.

Verstöße gegen die Informationssicherheit sind unverzüglich dem zuständigen ISB und der Behördenleitung der Gemeinde Oberau zu melden.

16 Schlussbestimmungen

Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie spätestens zwei Jahre nach Inkraftsetzung auf ihre Aktualität hin überprüft und ggf. aktualisiert.

17 Inkraftsetzung

Diese Leitlinie gilt für die gesamte Gemeinde Oberau.

Diese Leitlinie tritt mit Unterschrift der Behördenleitung in Kraft und wird allen Beschäftigten nach Unterzeichnung und Freigabe umgehend zur Kenntnis gebracht.

Bereits bestehende Leitlinien verlieren hiermit ihre Gültigkeit.

Unterschrift
Datum: 10.03.2021
(Imminger) 1. Bürgermeister