Leitlinie Informationssicherheit

der Organisation XYZ

Auf Basis des BSI IT-Grundschutz

Typ	Strategisches Dokument
Vertraulichkeitsstatus	Intern
Verantwortlicher	_____
Ablageort	_____
Gültig ab	_____

1. Geltungsbereich / Zertifizierungsbereich

Diese Leitlinie gilt für alle Einrichtungen der Organisation XYZ inklusive Home-Offices. Ein Testat wird angestrebt. Der Testat-Bereich ist identisch mit dem Geltungsbereich.

2. Stellenwert der Informationssicherheit

Die Organisation XYZ besitzt eine große Aufgabenvielfalt, die permanenten Änderungen unterliegt. Eine wirtschaftliche, zeitnahe Aufgabenerfüllung stützt sich dabei zunehmend auf die Möglichkeiten der Informationstechnologie und ist für die Organisation XYZ unabdingbar. Sie eröffnet völlig neue Möglichkeiten, die auch die Organisation XYZ aktiv nutzt. In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen, den Anforderungen von Auftraggebern und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen.

Durch diese Informationssicherheitsleitlinie (ISL) wird die Übernahme der Gesamtverantwortung durch die Organisationsleitung zum Ausdruck gebracht. Informationssicherheit umfasst neben IT-Systemen auch Papierunterlagen in Form von Akten und sonstigen Unterlagen sowie Daten im allgemeinen Sinn. Sie umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um die Informationssicherheit zu gewährleisten.

Modernes Arbeiten erfordert den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung im Sinne der Bürgerinnen und Bürger, Unternehmen und Partner effizient und effektiv zu gestalten. Die Informationssicherheit ist eine unverzichtbare Grundlage für das Handeln der Organisation, dem alle Partner ihr Vertrauen schenken können.

3. Bezug der Informationssicherheit zu den Geschäftszielen und Aufgaben

Es ist notwendig, das Zusammenspiel der Informationen, IT-Fachverfahren, Anwendungen, Aufgaben und Produkte sowie der Infrastruktur und Kommunikationskanäle ganzheitlich zu betrachten. Bei allen Tätigkeiten werden Informationen erhoben und verarbeitet, deren **Vertraulichkeit, Integrität und Verfügbarkeit** ein hohes Gut darstellen. Hierbei handelt es sich um Daten, die entsprechend den gesetzlichen Anforderungen geschützt werden müssen, oder auch um eigene schützenswerte Informationen, die Unberechtigten nicht bekannt werden dürfen.

4. Ziele der Informationssicherheit

Die Ziele orientieren sich an der zuverlässigen Aufgabenerfüllung und dem Schutz der Informationen vor unbefugten Zugriffen oder Verlusten. Die Einführung und der Betrieb eines ISMS sind zudem durch gesetzliche Vorgaben wie das Bayerische Digitalgesetz oder auch Art. 32 DSGVO untermauert.

Um die Erreichung der Informationssicherheitsziele zu überprüfen, werden geeignete Kennzahlen (Key Performance Indicators) definiert. Die Wirksamkeit des ISMS wird regelmäßig anhand dieser Messgrößen bewertet, um einen objektiven Nachweis über das erreichte Sicherheitsniveau zu führen.

Hinweis: *Hier können organisationsspezifische Ziele aus dem Projekthandbuch oder der Strategie ergänzt werden.*

Sicherheitsanforderungen von übergeordnetem Interesse, für deren Umsetzung eine vertragliche oder gesetzliche Verpflichtung besteht, sind in jedem Fall zu erfüllen. Entsprechende Vorschriften und Maßnahmen stellen den Mindeststandard bei der Formulierung organisationsinterner Vorgaben und Maßnahmen dar.

5. Kernelemente der Sicherheitsstrategie und Verantwortlichkeiten

Informationssicherheit ist kein in sich abgeschlossenes Projekt, sondern ein kontinuierlicher Verbesserungsprozess. Als zentrale Sicherheitsinstanz benennt die Organisationsleitung eine/n Informationssicherheitsbeauftragte/n (ISB) sowie eine Stellvertretung.

Sowohl der/die ISB als auch die Stellvertretung sind für alle Belange und Fragen der Informationssicherheit zuständig und in dieser Rolle der Organisationsleitung direkt unterstellt. Beiden Rollen ist ein direktes und jederzeitiges Vortrags- und Berichtsrecht bei der Organisationsleitung eingeräumt. Um ihre Verantwortung fachlich und zeitlich erfüllen zu können, werden dem/der ISB und der Stellvertretung geeignete Qualifizierungs- und

Weiterbildungsmaßnahmen ermöglicht. Dem/Der ISB wird ein Team Informationssicherheit zur Seite gestellt.

Ein Informationssicherheitsmanagementsystem (ISMS) auf Basis des Standards BSI IT-Grundschutz ist zu etablieren und im Rahmen der Angemessenheit und Verhältnismäßigkeit kontinuierlich zu verbessern. In regelmäßigen Abständen ist zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind.

Für alle betriebene und geplante Informationstechnik ist im Zuge der ISMS-Einführung und des Betriebs eine Sicherheitskonzeption zu erstellen. Die sich daraus ergebenden Maßnahmen sind auch dann umzusetzen, wenn sich Beeinträchtigungen für die Nutzung ergeben – gemäß dem Grundsatz „Sicherheit vor Komfort“.

5.1 Verankerung in der Organisation

Die Organisation XYZ verankert das Thema Informationssicherheit über folgende Bausteine:

- Eine geeignete Informationssicherheitsorganisation, die das Thema aktiv betreibt
- Einführung und kontinuierlichen Betrieb eines ISMS auf Basis des Standards BSI IT-Grundschutz
- Klar formulierte Sicherheitsvorgaben in Form von Richtlinien und Anweisungen, die für alle Mitarbeitenden (inklusive der Führungskräfte) verbindlich sind
- Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse
- Kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Mitarbeitenden
- Absicherung der IT-Infrastruktur durch Umsetzung geeigneter Sicherheitsmaßnahmen auf Infrastruktur-Ebene

Können Sicherheitsvorgaben in begründeten Einzelfällen (z. B. aus technischen oder betrieblichen Gründen) vorübergehend nicht eingehalten werden, ist ein strukturierter Ausnahmeantrag zu stellen. Diese Ausnahmen müssen dokumentiert, zeitlich befristet und durch die Organisationsleitung oder eine von ihr autorisierte Stelle unter Akzeptanz des Restrisikos freigegeben werden.

5.2 Rollen und Verantwortlichkeiten

Rolle	Aufgaben und Verantwortlichkeiten (nicht abschließend)
Organisationsleitung (Bürgermeister / Landrat)	Trägt die Gesamtverantwortung für den sachgemäßen Umgang mit Informationen. Stellt die benötigten finanziellen und zeitlichen Ressourcen bereit und nimmt eine Vorbildfunktion wahr, indem sie die Wichtigkeit der Informationssicherheit authentisch vorlebt. Sie lässt sich regelmäßig über den Stand der Informationssicherheit berichten und passt bei Bedarf Strategie und Ziele der Organisation zur Informationssicherheit dem Risiko angemessen an.

Rolle	Aufgaben und Verantwortlichkeiten (nicht abschließend)
ISB und Stellvertretung	Zuständig für alle Belange der Informationssicherheit. Direkt der Organisationsleitung unterstellt. Haben direktes Vortrags- und Berichtsrecht. Erhalten geeignete Qualifizierungs- und Weiterbildungsmaßnahmen.
Fachbereichsleitung und Führungskräfte	Sorgen für ein sicheres Arbeitsumfeld der unterstellten Mitarbeitenden, vermitteln und kontrollieren Sicherheitsregelungen, erfassen den Ist-Zustand, setzen auf ihren Verantwortungsbereich zutreffende Schutzmaßnahmen um und binden den / die ISB frühzeitig in Änderungen ein. Für alle wesentlichen Informationen und IT-Anwendungen sind Verantwortliche (Asset Owner) zu benennen. Diese sind insbesondere für die Einstufung des Schutzbedarfs (Vertraulichkeit, Integrität, Verfügbarkeit) sowie für die Freigabe von Zugriffsberechtigungen in ihrem Zuständigkeitsbereich verantwortlich.
Mitarbeitende	Jede/r Mitarbeitende ist für die Informationssicherheit an ihrem/seinem Arbeitsplatz verantwortlich. Verpflichtet zur Teilnahme an Sensibilisierungsmaßnahmen und zur unverzüglichen Meldung von Sicherheitsverstößen.
IT-Leitung	Ergreift technische Maßnahmen zur Erhöhung der Informationssicherheit und sichert die IT-Infrastruktur bestmöglich ab. Ist ständiges Mitglied im Team Informationssicherheit.
DSB und Stellvertretung	Überwacht die Einhaltung der datenschutzrechtlichen Vorgaben (DSGVO, BayDSG). Berät die Organisationsleitung und den ISB bei der Auswahl technisch-organisatorischer Maßnahmen, sofern personenbezogene Daten verarbeitet werden. Er/Sie wird bei Datenschutz-Folgenabschätzungen und Sicherheitsvorfällen mit Personenbezug zwingend beteiligt.

5.3 Externe Auftragnehmer und Dritte

Personen und Unternehmen, die nicht zur Organisation XYZ gehören, jedoch für diese Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser ISL einzuhalten. Die Organisation XYZ informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung, beispielsweise im Rahmen einer Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO oder durch Geheimhaltungsvereinbarungen.

6. Verpflichtung zur Umsetzung und kontinuierlichen Verbesserung

Der / Die Unterzeichner tragen die Gesamtverantwortung und stellen die benötigten Ressourcen bereit. Die sich aus der Sicherheitskonzeption ergebenden Maßnahmen sind auch dann umzusetzen, wenn sich Beeinträchtigungen für die Nutzung ergeben – gemäß dem Grundsatz „Sicherheit vor Komfort“.

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Einflüssen ab, wie z. B. neuen Bedrohungen, neuen Gesetzen oder der Entwicklung neuer technischer Lösungen, denen kontinuierlich Rechnung getragen werden muss. Aus diesem Grund ist Informationssicherheit ein fortlaufender Prozess und kein in sich abgeschlossenes Projekt.

Der/die ISB ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig und eigeninitiativ einzubinden. Die Organisationsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeitende sind angehalten, mögliche Verbesserungen oder Schwachstellen an den/die ISB weiterzugeben.

Die Angemessenheit und Wirksamkeit des ISMS wird in geplanten Abständen durch unabhängige interne Audits oder Revisionen überprüft. Die Ergebnisse dieser Prüfungen werden der Organisationsleitung vorgelegt und dienen als Basis für die weitere Optimierung der Sicherheitsmaßnahmen.

7. Verstöße und Sanktionen

Jede/r Mitarbeitende der Organisation XYZ wird zu einem sorgfältigen Umgang mit den Daten, Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen verpflichtet. Beabsichtigte oder grob fahrlässige Verletzungen der Informationssicherheit können arbeits- oder dienstrechtliche Folgen nach sich ziehen. Dazu zählen insbesondere:

- 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

8. Aktualisierung und Inkraftsetzung

Das Sicherheitskonzept und die ISL werden von dem/der ISB jährlich auf Aktualität und Wirksamkeit geprüft und bei Bedarf angepasst. Abweichungen werden analysiert, um die Sicherheitssituation kontinuierlich zu verbessern. Die Leitlinie tritt mit Unterzeichnung in Kraft und wird allen Mitarbeitenden im Rahmen von Sensibilisierungsmaßnahmen umgehend zur Kenntnis gebracht.

Ort,	Datum:	Ort,	Datum:
_____		_____	
_____		_____	
gez. Organisationsleitung I		*gez. Organisationsleitung II*	

ANHANG: Optionale Formulierungsvorschläge

Die nachfolgenden Abschnitte sind als Ergänzungsoptionen zu verstehen. Sie können bei Bedarf in die Leitlinie übernommen werden, sind aber nicht zwingend erforderlich.

Option 1: Meldepflichten bei Sicherheitsvorfällen

Empfohlener Einfügeort: Abschnitt 5 (Kernelemente), als eigener Unterabschnitt 5.4

Alle Mitarbeitenden sind verpflichtet, Sicherheitsvorfälle, Auffälligkeiten oder Schwachstellen unverzüglich dem/der ISB oder dem Team Informationssicherheit zu melden. Die Organisation XYZ stellt hierfür geeignete Meldewege bereit. Vorfälle, die eine Meldepflicht gegenüber Behörden auslösen können (z. B. gegenüber dem BSI gemäß BSIG oder gegenüber der Datenschutzaufsichtsbehörde gemäß Art. 33 DSGVO), sind über den/die ISB und / oder DSB zu koordinieren. Jeder gemeldete Vorfall wird dokumentiert und ausgewertet, um das Sicherheitsniveau kontinuierlich zu verbessern.

Option 2: Notfallmanagement und Business Continuity

Empfohlener Einfügeort: Abschnitt 6 (Verpflichtung zur Umsetzung), als zusätzlicher Absatz

Die Verfügbarkeit kritischer Geschäftsprozesse und IT-Systeme ist ein zentrales Ziel der Informationssicherheit. Die Organisation XYZ erarbeitet und pflegt ein Notfallkonzept, das den Fortbestand oder die schnelle Wiederherstellung wesentlicher Funktionen im Schadensfall sicherstellt. Die Verantwortlichen ergreifen bei Betriebsstörungen und Sicherheitsvorfällen die zur Aufrechterhaltung des Betriebes geeigneten und angemessenen Maßnahmen. Notfallpläne werden regelmäßig getestet und aktualisiert.

Option 3: Verhältnis von Informationssicherheit und Datenschutz

Empfohlener Einfügeort: Abschnitt 3 (Bezug zu Geschäftszielen) oder Abschnitt 4 (Ziele)

Informationssicherheit und Datenschutz ergänzen einander. Während der Datenschutz den Schutz personenbezogener Daten nach der DSGVO sowie nationalen Rechtsvorschriften sicherstellt, zielt die Informationssicherheit auf den umfassenden Schutz aller Informationswerte der Organisation ab. ISB und Datenschutzbeauftragte/r (DSB) stimmen sich regelmäßig ab und arbeiten eng zusammen, um Überschneidungen zu nutzen und Widersprüche zu vermeiden.

Option 4: Risikomanagement als Grundlage der Maßnahmenauswahl

Empfohlener Einfügeort: Abschnitt 5.1 (Verankerung in der Organisation), zusätzlicher Spiegelstrich

Die Auswahl von Sicherheitsmaßnahmen basiert auf einer systematischen Risikoanalyse. Im Rahmen der Strukturanalyse, Schutzbedarfsfeststellung und Risikobeurteilung nach BSI IT-Grundschutz werden Gefährdungen bewertet und angemessene Maßnahmen abgeleitet. Erkannte Risiken, die nicht vollständig durch Maßnahmen adressiert werden können, sind zu dokumentieren und der Organisationsleitung zur Kenntnis und Entscheidung vorzulegen.

Option 5: Awareness-Maßnahmen mit Nachweispflicht

Empfohlener Einfügeort: Abschnitt 5.2 (Rollen), bei den Pflichten der Mitarbeitenden

Die Teilnahme an Informationssicherheits-Sensibilisierungsmaßnahmen ist für alle Mitarbeitenden (inklusive der Führungskräfte) verpflichtend. Die Durchführung und Teilnahme werden dokumentiert, um den Nachweis im Rahmen von Audits und Zertifizierungsverfahren erbringen zu können. Schulungen werden mindestens einmal jährlich angeboten und bei wesentlichen Änderungen der Sicherheitslage oder der Vorgaben aktualisiert.

Option 6: Hinweis zur gendergerechten Sprache

Hinweis zur redaktionellen Anpassung des gesamten Dokuments

Dieses Dokument verwendet durchgängig die Form „Mitarbeitende“ sowie geschlechtsneutrale Konstruktionen (z. B. „der/die ISB“). Organisationen, die eine andere Sprachregelung bevorzugen, sollten die Terminologie vor Inkraftsetzung einheitlich anpassen. Eine konsistente Sprachregelung im gesamten Dokument erhöht die Leser-freundlichkeit und entspricht modernen Anforderungen an öffentliche Dokumente.

Versionsverlauf

Version	Datum	Änderungen	Autor	Status	Freigabe
1.0		Erstfassung		Entwurf	