Leitlinie zur Informationssicherheit der Stadtverwaltung Naumburg (Saale)

Dokumenteneigenschaften

Verantwortung	Fachbereichsleiter I (FBL 1) – Olaf Ehrhardt
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	Januar 2026

Dokumentenstatus und Freigabe

Status	Version	Datum	Name und Abteilung/Firma
Erstellt	1.0	18.10.2024	

Dokumentenhistorie

Version	Änderung	Datum	Autor
1.0		18.10.2024	

Inhaltsverzeichnis

1 Kontext

1.1 Einleitung

Die Stadtverwaltung Naumburg (Saale) etabliert ein Managementsystem für Informationssicherheit (ISMS), das dem Regelwerk „IT-Grundschutz" des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügen soll. Zentraler Bestandteil eines ISMS ist u.a. die Leitlinie zur Informationssicherheit.

Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der Stadtverwaltung Naumburg (Saale). Die detaillierten Regelungen erfolgen im Rahmen des ISMS für die einzelnen Teilbereiche per entsprechender Dienstanweisungen, Dienstvereinbarungen, Konzepte, Pläne und Regelungen für die jeweiligen Module der Informationssicherheit (z.B. Dienstanweisung IT-Nutzung, Datensicherungs-Konzept, Notfallkonzept, Business-Continuity-Concept, etc.).

1.2 Geltungsbereich

Der Geltungsbereich dieser Leitlinie ist der Geltungsbereich des ISMS, wie in der Strukturanalyse beschrieben.

Die Richtlinie gilt für alle Mitarbeiter, externe Gremienmitglieder und externe Nutzer der IT-Infrastruktur der Stadtverwaltung Naumburg (Saale) im Geltungsbereich.

1.3 Ansprechpartner

Ihr Ansprechpartner zu allen Fragen dieser Richtlinie: FBL I – Olaf Ehrhardt.

1.4 Verantwortlichkeiten

Diese Leitlinie hat die Verwaltungsleitung der Stadtverwaltung Naumburg (Saale) freigegeben.

2 Stellenwert der Informationstechnologie und Informationssicherheit

Informationssicherheit stellt für die Stadtverwaltung Naumburg (Saale) ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da alle wesentlichen strategischen und operativen Prozesse in der Verwaltung durch Informationstechnologie (IT) maßgeblich unterstützt werden.

Ziel der Verwaltung ist es, die Daten und IT-Systeme in allen technikabhängigen Bereichen in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Stillstandzeiten und der maximale Datenverlust toleriert werden können. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Daten und personenbezogenen Daten in ausreichender Weise zu garantieren; hierzu gehören Personaldaten ebenso wie verwaltungstechnische Unterlagen. Schadensfälle mit hohen finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für die Stadtverwaltung sowie Schäden für die Bürger müssen verhindert werden.

Beeinträchtigungen hinsichtlich der Verfügbarkeit der verwaltungseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen. Die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, Anwendungen und IT-Systeme werden nicht nur durch Externe bedroht, sondern können auch durch interne Schwachstellen gefährdet werden.

Ferner werden der Informationssicherheit im Hinblick auf Ausschreibungen Vorteile am Markt eingeräumt.

3 Ziele

Die Verwaltungsleitung der Stadtverwaltung Naumburg (Saale) hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Dies bedeutet im Einzelnen:

Bewusstsein für Informationssicherheit:

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten, externe Gremienmitglieder und externe Nutzer der IT-Infrastruktur der Stadtverwaltung Naumburg (Saale) die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit unterstützen hierbei zusätzlich.

Einhaltung von Gesetzen oder Vorschriften:

Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für die Stadtverwaltung Naumburg (Saale) relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden.

Als wichtigste zu beachtende Rahmenbedingungen gelten dabei:

- Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- NIS2-Richtlinie (EU-weite Gesetzgebung zur Cybersicherheit)
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- ergänzende Anforderungen durch externe Einrichtungen und Partner

Informationssicherheit unterstützt damit auch die Einhaltung von Gesetzen und Vorschriften.

Funktionale Aufgabenerledigung:

IT-Systeme, Anwendungen und Daten müssen den Berechtigten stets wie vorgesehen zur Aufgabenerfüllung zur Verfügung stehen. Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Verwaltungsbetrieb haben.

Informationssicherheit unterstützt damit auch eine funktionale Aufgabenerledigung.

Vermeidung materieller Schäden:

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines Systems entstehen.

Informationssicherheit wirkt damit auch materiellen Schäden entgegen.

Wahrung von Persönlichkeitsrechten und Verwaltungsgeheimnissen:

Vertraulichkeit und Integrität der für die Stadtverwaltung Naumburg (Saale) wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

Vermeidung von Ansehensverlust bzw. Imageschaden:

Finanzielle Schäden und ein negatives Image für die Stadtverwaltung Naumburg (Saale), seine Gremien und seine Partner müssen verhindert werden.

Informationssicherheit vermeidet damit Ansehensverlust und Imageschäden.

Kontinuierliche Verbesserung:

Und ferner strebt die Stadtverwaltung Naumburg (Saale) die kontinuierliche Verbesserung seiner Prozesse rund um die Informationssicherheit an.

4 Organisation des Managementsystems für Informationssicherheit

Grundsätzlich sind folgende Verantwortlichkeiten innerhalb des ISMS definiert:

4.1 Oberbürgermeister

Der Oberbürgermeister trägt die Gesamtverantwortung für die Informationssicherheit. Er verabschiedet in Zusammenarbeit mit dem Gemeinderat auf Vorschlag der Informationssicherheitsbeauftragten diese Informationssicherheitsleitlinie.

Der Oberbürgermeister ist dafür verantwortlich, sicherzustellen, dass das ISMS entsprechend dieser Richtlinie umgesetzt und aktualisiert wird und dass die notwendigen Ressourcen verfügbar sind. Den IT-Beauftragten und dem Informationssicherheitsbeauftragten werden vom Oberbürgermeister ausreichende finanzielle, technische, personelle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die von der Verwaltungsleitung festgelegten Sicherheitsziele zu erreichen.

Der Oberbürgermeister muss das ISMS mindestens einmal jährlich überprüfen (bzw. immer im Falle von erheblichen Änderungen) und freigeben. Zweck dieser Überprüfung durch den Oberbürgermeister ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.

Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) verbleibt beim Oberbürgermeister.

4.2 Vertretung / Gemeinderat

Der Gemeinderat oder sein jeweils zuständiges Entscheidungsgremium genehmigt die für die Informationssicherheit erforderlichen Mittel.

4.3 IT-Beauftragung

Die zentrale Instanz für die operative IT-Sicherheit ist die IT-Beauftragung im SG Organisation und Digitalisierung. Sie ist für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich. In Zusammenarbeit mit dem Datenschutzbeauftragten und

dem Informationssicherheitsbeauftragten bringt sie die für die Informationssicherheit spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig.

Die IT-Beauftragung stellt sicher, dass alle Beteiligten frühzeitig in alle IT-Projekte eingebunden werden.

4.3.1 Informationssicherheitsbeauftragter (ISB)

Der Informationssicherheitsbeauftragte wird durch den Oberbürgermeister benannt. Er steuert und koordiniert den Sicherheitsprozess und ist für die Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich und berichtet in dieser Funktion an den Oberbürgermeister. Er ist Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten. Der Informationssicherheitsbeauftragte agiert weisungsfrei und hat die Möglichkeit, dem Oberbürgermeister bei Bedarf direkt zu berichten und jederzeit Vor-Ort-Kontrollen durchzuführen. In Abstimmung mit dem Datenschutzbeauftragten, prüft er ob die Maßnahmen zur Sicherstellung der Informationssicherheit im Einklang mit den datenschutzrechtlichen Bestimmungen stehen. Er wird in neue Projekte involviert und muss neue Fachverfahren freigeben. Der ISB berichtet dem Oberbürgermeister jährlich und bedarfsweise über den Umsetzungsstand des ISMS sowie aktuelle Risiken.

4.3.2 Datenschutzbeauftragter (DSB)

Der Datenschutzbeauftragte wird durch den Oberbürgermeister benannt. Die Aufgaben ergeben sich aus § 20 DSAG-LSA. Der Datenschutzbeauftragte führt das Verzeichnis der Verarbeitungstätigkeiten, nimmt Vorabkontrollen vor und wirkt auf die Einhaltung des Datenschutzes hin. Der Datenschutzbeauftragte wirkt bei der Einhaltung der Meldepflicht von sicherheitsrelevanten Vorfällen bei der Verarbeitung von personenbezogenen Daten mit und ist in dem Prozess zu beteiligen. Der Datenschutzbeauftragte agiert weisungsfrei und hat die Möglichkeit, dem Oberbürgermeister bei Bedarf direkt zu berichten und jederzeit Vor-Ort-Kontrollen durchzuführen. Der DSB berichtet dem Oberbürgermeister jährlich und bedarfsweise über den Umsetzungsstand des DSMS sowie aktuelle Risiken.

4.4 IS-Management-Team (ISMS-Team)

Das IS-Management-Team setzt sich aus dem Datenschutzbeauftragten, dem Informationssicherheitsbeauftragten sowie fachkundigen Mitarbeitern für die Administration und für den Betrieb zusammen. Das IS-Management-Team hält regelmäßige Treffen ab.

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

4.5 Mitarbeiter

Die Mitarbeiter sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Geheimnissen achten.

Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Werten unterliegt der Verantwortung der Eigentümer der jeweiligen Werte.

Bei Unregelmäßigkeiten müssen die Mitarbeiter unverzüglich die IT-Beauftragung und ihre Vorgesetzten informieren. Es wird erwartet, dass jeder Nutzer von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennt und beachtet.

4.6 Gremien und externe Nutzer

Die Mitglieder in Gremien und externe Nutzer der IT-Infrastruktur der Stadtverwaltung Naumburg (Saale) sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten, sowie mit den per Cloud-Lösungen zur Verfügung gestellten und extern gespeicherten Daten umgehen und auf die Wahrung von Geheimnissen achten.

Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Werten unterliegt der Verantwortung der Eigentümer der jeweiligen Werte.

Bei Unregelmäßigkeiten müssen die Mitglieder in Gremien und externe Nutzer der IT-Infrastruktur der Stadtverwaltung Naumburg (Saale) unverzüglich die IT-Beauftragung und ihre Vorgesetzten informieren. Es wird erwartet, dass jeder Nutzer von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennt und beachtet.

4.7 Weitere Verantwortlichkeiten

Für alle Informationen, Prozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Informations-, Prozess- und Systemeigentümer, Eigentümer von Zielobjekten) benannt. Diese sind dafür zuständig, die Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeiter 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 Kooperationspartnern die Vorgaben der Stadtverwaltung Naumburg (Saale) zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

5 Folgen von Zuwiderhandlungen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Bürger schädigen oder den Ruf der Stadtverwaltung Naumburg (Saale) gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

6 Weitere Maßnahmen

Ausgehend von der IT-Grundschutz-Methodik zur Einführung und Aufrechterhaltung eines Managementsystems für Informationssicherheit wurden diverse weiterführende Regelungen geschaffen, die dieses ISMS konkretisieren und gleichfalls gültig sind.

7 Inkrafttreten

Die Richtlinie tritt zum 01.11.2024 in Kraft.

Freigegeben durch: Verwaltungsleitung

Naumburg (Saale), 01.11.2024

Armin Müller
Oberbürgermeister