



Informationssicherheitsleitlinie

vom 01. Januar 2024

Diese Leitlinie ist in männlicher Form verfasst. Es wird ausdrücklich darauf hingewiesen, dass alle Geschlechter gleichberechtigt gemeint sind und nur zur besseren Lesbarkeit die männliche Form verwendet wird.

Inhaltsverzeichnis

1. Zielsetzung	2
2. Geltungsbereich	3
3. Sicherheitsgrundsätze	3
4. Sicherheitsstrategie	4
5. Sicherheitsorganisation	4
6. Pflichten und Berichtswege	5
7. Umsetzungsplan	6
8. Notfallmanagement	6
9. Inkrafttreten	6

1. Zielsetzung

Durch die stetige Zunahme der Informationstechnik (IT) bei der Aufgabenerledigung in der Stadtverwaltung Tauberbischofsheim ist die IT zu einem unverzichtbaren Arbeitsfaktor geworden. Eine Aufgabenerledigung ohne IT ist heute kaum mehr vorstellbar, bzw. schlicht nicht möglich. Mit der zunehmenden Abhängigkeit von einer funktionierenden IT ist auch das Risiko eines Ausfalls oder der Beeinträchtigung durch technisches Versagen oder gar durch gezielte Angriffe entsprechend zu bewerten. Für die Stadtverwaltung ist eine sichere Informations- und Kommunikationstechnik von höchster Bedeutung. Sie resultiert aus der Verpflichtung gegenüber den Bürgern und der Wirtschaft, verantwortungsvoll bei der Erhebung, Speicherung, Übermittlung und Nutzung von Daten, insbesondere von personenbezogenen Daten vorzugehen.

Diese Informationssicherheitsleitlinie legt die Ziele, Grundsätze, Organisationsstrukturen und Maßnahmen fest, die für die Etablierung eines ganzheitlichen Informationssicherheitsprozesses in der Stadtverwaltung erforderlich sind. Die Vorgehensweise orientiert sich am IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem Grundschutz-Kompendium in der jeweils aktuellen Fassung sowie den Standards der ISO 2700x-Reihe.

Anstelle des in der Literatur oft synonym verwendeten Begriffs „IT-Sicherheit“ wird hier die weitergehende Formulierung „Informationssicherheit“ verwendet.

Entsprechend der Empfehlung gemäß BSI-Standard wird Informationssicherheit umfassend und ganzheitlich verstanden, sie umfasst auch die Begriffe „Informations- und Kommunikationstechnik“ und „Informations- und Telekommunikationstechnik“ und bezieht sich auf den Schutz von Informationen jeglicher Art und Herkunft, unabhängig davon, ob diese in technischen Systemen, auf Papier oder in Köpfen gespeichert sind.

Die Ziele im Einzelnen sind:

- Hohe Verlässlichkeit beim Umgang mit Informationen,
- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen,
- Vermeidung von Datenverlust,
- Sicherung der Qualität der Informationen,
- Gewährleistung der Einhaltung der gesetzlichen Anforderungen,
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Stadtverwaltung Tauberbischofsheim und in der Zusammenarbeit mit anderen Stellen,
- Investitionsschutz, das heißt Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Reduzierung der im Schadensfall entstehenden Kosten sowie
- Vermeidung von Reputationsschäden.

2. Geltungsbereich

- 2.1 Wer Informationen, informationsverarbeitende Einrichtungen oder Infrastruktur der Stadtverwaltung Tauberbischofsheim nutzt, unterliegt dieser Informationssicherheitsleitlinie. Sie gilt insbesondere für alle Mitarbeiter der Stadt Tauberbischofsheim.
- 2.2 Sie gilt durch gesonderte Verpflichtung auch für Dritte, die als Auftragnehmer für die unter Nummer 2.1 genannten Leistungen erbringen.
- 2.3 Sofern sich aus anderen Regelungen weitergehende Anforderungen an die Informationssicherheit ergeben, bleiben diese unberührt.

3. Sicherheitsgrundsätze

- 3.1 Die Stadtverwaltung Tauberbischofsheim hat die Umsetzung der Informationssicherheit gemäß IT-Grundschutz nach BSI-Standards zum Ziel.
- 3.2 Für die Stadtverwaltung wird ein Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an die internationalen Standards (ISO = International Standardization Organization) unter Berücksichtigung des nationalen BSI-Standards eingeführt. Dieses ISMS umfasst Ressourcen, Prozesse und Konzepte für die Informationssicherheit.
- 3.3 Die Stadtverwaltung setzt Informationssicherheit zunächst nach dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ um. Das IT-Grundschutz-Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind. Das IT-Grundschutz-Profil wurde von der Arbeitsgruppe kommunale Basis-Absicherung (AG koBa) der Kommunalen Spitzenverbände erstellt. Es umfasst eine Untermenge der Forderungen der IT-Grundschutz-Kataloge und der ISO/IEC 27001 und soll es auf diese Weise den Kommunalverwaltungen einfacher machen, Informationssicherheit systematisch herzustellen.
- 3.4 Die ebenenübergreifende Zusammenarbeit zwischen Bund, Ländern und Kommunen wird berücksichtigt.
- 3.5 Die Notfallvorsorge und -bewältigung erfolgt gemäß den Vorgaben aus dem BSI-Standard zum Notfallmanagement.
- 3.6 Informationssicherheit erfordert personelle, organisatorische, rechtliche und technische Maßnahmen.
- 3.7 Informationssicherheit ist als kontinuierlicher Prozess zu gestalten. Der Prozess umfasst insbesondere die mindestens jährlich dokumentierte Überprüfung der Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen und gegebenenfalls erforderliche Anpassungen.
- 3.8 Der Zugriff auf IT-Systeme, -Anwendungen, Daten und Informationen ist unter Abwägung des Schutzbedarfs und der Wirtschaftlichkeit auf den unbedingt erforderlichen Personenkreis zu beschränken. Beschäftigte und Bedienstete erhalten nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die zur Erfüllung der jeweiligen dienstlichen Aufgaben erforderlich sind.

- 3.9 Beim Einsatz von Informations- und Kommunikationstechnik sind Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu erreichen. Dazu sind angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu ergreifen.
- 3.10 Notwendige Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die Nutzung von IT-Systemen ergeben.
- 3.11 Die angemessene Sicherheit der in der Stadtverwaltung eingesetzten IT-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.
- 3.12 Die jeweils für IT-Verfahren Verantwortlichen sorgen dafür, dass verfahrens- bzw. anwendungsbezogene Sicherheitskonzepte erstellt und regelmäßig bedarfsgerecht fortgeschrieben werden. Soweit für einzelne Verfahren keine Sicherheitskonzepte erforderlich sind, wird dies jeweils aktenkundig begründet. Das Ziel ist, dass die Stadtverwaltung und damit alle unter Nummer 2.1 Genannten jeweils alle ihre Verfahren und Anwendungen, die damit verarbeiteten Daten und deren Schutzbedarf und die mit der Verarbeitung verbundenen Risiken sowie die zugehörigen Rechtsgrundlagen kennen und darüber auskunftsfähig sind. Diese Anforderung ergibt sich insbesondere aus der EU-Datenschutz-Grundverordnung

4. Sicherheitsstrategie

Die Sicherheitsstrategie der Stadtverwaltung Tauberbischofsheim ist es, das jeweils notwendige Sicherheitsniveau mit wirtschaftlichem Ressourceneinsatz zu erreichen und zu halten. Hierzu wird durch die Einführung eines ISMS ein kontinuierlicher Prozess etabliert, der sicherstellt, dass das Sicherheitsniveau den jeweiligen Anforderungen jederzeit bedarfsgerecht angepasst und fortgeschrieben wird. Wesentliche Elemente dieses ISMS sind Planung, Umsetzung, Überprüfung und Aufrechterhaltung des Prozesses. Dabei kann anstelle der Umsetzung aller Maßnahmen des IT-Grundschatzes auch ein risikobasierter Ansatz gewählt werden. Dabei werden die Risiken klassifiziert und bewertet und in der Folge genau diejenigen Maßnahmen ergriffen, die notwendig sind, um das Risiko auf ein tragbares Maß zu reduzieren.

5. Sicherheitsorganisation

- 5.1 Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung und damit auch für die Informationssicherheit verbleibt bei der Verwaltungsleitung (Bürgermeister). Dazu gehört auch die Verantwortung für eine angemessene Aus- und Weiterbildung und für die Sensibilisierung für Sicherheitsthemen (Security-Awareness).

5.2 Die Grundsätze der Sicherheitsorganisation sind:

- 5.2.1 Für die Stadtverwaltung Tauberbischofsheim wird ein Informationssicherheitsbeauftragter (ISB) bestellt. Der ISB berichtet direkt an die Verwaltungsleitung.
- 5.2.2 Informationssicherheitsbeauftragte können Informationssicherheits-Management-Teams gemäß aktuellem BSI Standard bilden. Dieses Informationssicherheits-Team unterstützt den ISB bei seinen Aufgaben.
- 5.2.3 Die für die Sicherheitsprozesse erforderlichen Ressourcen (Personal- und Sachmittel sowie angemessene zeitliche Freistellung) werden im notwendigen Umfang durch die jeweils verantwortlichen Organisationseinheiten bereitgestellt.

5.3 Zu den Aufgaben des ISB gehören insbesondere:

- 5.3.1 Allgemeingültige Richtlinien und Grundsätze für Maßnahmen in der Informationssicherheit in der Stadtverwaltung Tauberbischofsheim in Abstimmung mit der Verwaltungsleitung zu erarbeiten und fortzuschreiben.
- 5.3.2 Die Verwaltungsleitung, Amtsleitungen und deren Mitarbeiter bei deren Aufgabewahrnehmung bezüglich der Informationssicherheit zu beraten und bei der Umsetzung zu unterstützen, um damit ein angemessenes und dem Stand der Technik entsprechendes Informationssicherheitsniveau der Stadtverwaltung Tauberbischofsheim zu erreichen und zu halten.
- 5.3.3 Einen jährlichen Sicherheitsbericht zur Vorlage an die Verwaltungsleitung zu erstellen. Dieser enthält Angaben zum Stand der Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen und der gegebenenfalls erforderlichen Erstellung und Fortschreibung der jeweiligen Dokumente und Sicherheitskonzepte. Dabei unterstützt das jeweils zuständige Sachgebiet durch Zulieferung von Beiträgen.

6. Pflichten und Berichtswege

- 6.1 Der Bürgermeister und die Amtsleitungen wirken darauf hin, dass diese Informationssicherheitsleitlinie umgesetzt wird.
- 6.2 Alle unter 2.1 Genannten haben Sicherheitsvorfälle möglichst zu vermeiden und sicherheitsrelevante Ereignisse, soweit diese für sie erkennbar sind, unverzüglich über die bekannt gegebenen Wege zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können. Ein Sicherheitsvorfall liegt vor, wenn eines oder mehrere der unter Nummer 1 genannten Ziele verletzt werden. Ein sicherheitsrelevantes Ereignis liegt vor, wenn die in Nummer 1 genannten Ziele gefährdet erscheinen.
- 6.3 Sicherheitshinweise und -handlungsanleitungen sind unverzüglich an alle Betroffenen im eigenen Zuständigkeitsbereich weiterzuleiten.
- 6.4 Die jeweils verantwortlichen Organisationseinheiten sensibilisieren die Beschäftigten für das Thema Informationssicherheit.

- 6.5 Bei Beeinträchtigungen der Informationssicherheit ergreifen die jeweils Verantwortlichen unverzüglich die zur Aufrechterhaltung bzw. Wiederherstellung des IT-Betriebs und der Informationssicherheit geeigneten und angemessenen Maßnahmen.
- 6.6 Soweit Dritte als Auftragnehmer für die unter Nr. 2.1 genannten Leistungen erbringen, sind diese bei der Auftragserteilung auf die Vorgaben dieser Informationssicherheitsleitlinie im notwendigen Umfang zu verpflichten. Dies ist über einzelvertragliche Regelungen oder Rahmenverträge sicherzustellen und vom Auftraggeber zu kontrollieren.

7. Umsetzungsplan

Der ISB erstellt den Umsetzungsplan für die Informationssicherheitsleitlinie. Der Umsetzungsplan beschreibt die zur Einrichtung und Aufrechterhaltung des ISMS erforderlichen Maßnahmen und einen Zeitplan für die Umsetzung. Er enthält auch eine Abschätzung der damit verbundenen Aufwände und Kosten. Der Umsetzungsplan wird bedarfsgerecht fortgeschrieben.

8. Notfallmanagement

Zur Bewältigung von Notfällen und Krisen werden im Geltungsbereich dieser Informationssicherheitsleitlinie angemessene Notfallmanagement-Prozesse gemäß dem IT-Grundschutzstandard des BSI in der jeweils aktuellen Fassung etabliert. Geeignete Präventivmaßnahmen sollen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen, den Schaden beim Ausfall dieser Prozesse reduzieren und ein schnelles und zielgerichtetes Handeln im Notfall oder bei einer Krise ermöglichen.

9. Inkrafttreten

Diese ISLL gilt für die gesamte Stadtverwaltung und tritt mit Unterschrift des Bürgermeisters in Kraft.

Tauberbischofsheim, 01.01.2024

Anette Schmidt
Bürgermeisterin