Stadt Vilsbiburg

Leitlinie zur Informations-sicherheit

Leitlinie zur Informationssicherheit der Stadt Vilsbiburg

1 Einleitung

Die Stadt Vilsbiburg ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie abhängig. Zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme beschließt das Informationssicherheitsteam diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Stadt Vilsbiburg angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Maßnahmen definiert. Weiter beinhaltet die Leitlinie eine kurze Beschreibung der Informationssicherheitsorganisation.

2 Geltungsbereich

Die Leitlinie zur Informationssicherheit und die damit zusammenhängenden Dokumente (insbesondere das Sicherheitskonzept, das Berechtigungskonzept, die Informationssicherheitsorganisation, die Dienstanweisung zur Informationssicherheit und der Bildschirmarbeitsplätze, die Datenschutzdienstanweisung, sowie der Schulungsplan zur Sensibilisierung der Mitarbeitenden) gelten für alle Mitarbeitenden der Stadt Vilsbiburg mit Ausnahme der Stadtwerke Vilsbiburg und der Schulen ohne den Hausmeistern. Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

3 Informationssicherheitsniveau

Alle wesentlichen Funktionen und Aufgaben der Stadt Vilsbiburg werden durch IT- und Netzwerksysteme unterstützt. Ein Ausfall von IT- und Netzwerksystemen darf die Aufgabenerfüllung nicht beeinträchtigen. Die Stadt Vilsbiburg bearbeitet auch Daten, die einen erhöhten Schutz vor unberechtigten Zugriffen und von unerlaubten Änderungen benötigt.

4 Informationssicherheitsziele

Die Stadt Vilsbiburg legt folgende Informationssicherheitsziele fest:

Authentizität	Informationsbearbeitungen müssen einer Person zugerechnet werden können.
Integrität	Informationen müssen richtig und vollständig sein.
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
Verantwortung	Die politischen Behörden und die Mitarbeitenden der Stadt Vilsbiburg sind sich ihrer Verantwortung beim Umgang mit Informationen, IT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.
Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Verwaltungsbetrieb haben.
Vertraulichkeit	Informationen dürfen nicht unrechtmäßig zur Kenntnis gelangen.

5 Informationssicherheitsmaßnahmen

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Maßnahmen:

Aktualisierungen / Updates	Alle IT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmäßig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.
Archivierung / Löschung	Alle Daten werden gemäß den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.
Berechtigungskonzept	Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen für Behördenmitglieder, für Mitarbeitende sowie für Lernende auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich.
Datenschutz	Alle Daten werden gemäß den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.
Datensicherung (Back-up)	Die Datensicherung wird regelmäßig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.
IT-Systeme	Die IT-Systeme werden nach der Beschaffung sicher installiert (gemäß anerkannten Sicherheitsstandards) und betrieben, mittels eines Änderungsmanagements verwaltet und in einem geregelten Prozess außer Betrieb genommen.
Mobile Geräte / Software	Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive die Verwendung von privaten Geräten (Bring Your Own Device) sowie die Installation von Software auf Arbeitsplatzrechnern und Servern sind im Detail geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Maßnahmen ergriffen.
Monitoring / Überwachung	Die Verfügbarkeit und Qualität der Anwendungsdienste wird laufend überprüft.
Netzwerk / Firewall	Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern.
Organisation	Die relevanten Funktionen der Organisation sind festgelegt und in einem Organigramm dokumentiert. Für alle Funktionen ist die Stellvertretung geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe

	erfüllen können.
Outsourcing	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Datensicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmaßnahmen vereinbart werden.
Passwörter	Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.
Sensibilisierung	Die Mitarbeiterinnen und Mitarbeiter nehmen mindestens jährlich an einer internen Sicherheitsschulung der für die Informationssicherheit verantwortlichen Person teil. Sie werden regelmäßig über aktuelle Gefahren und zu treffende Maßnahmen informiert.
Verschlüsselung	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netze.
Virenschutz / Internet	Virenschutzprogramme werden auf allen IT-Systemen eingesetzt. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.
Weisungen	Die Mitarbeiterinnen und Mitarbeiter werden angewiesen, die Gesetze sowie die vertraglichen Regelungen und internen Richtlinien einzuhalten. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmaßnahmen. Informationssicherheitsfragen und Hinweise auf Schwachstellen werden an die für die Informationssicherheit verantwortliche Person gerichtet.
Zutritt	Gebäude und Räume sowie IT- und Netzwerksysteme werden durch ein ausreichendes Schließsystem und weitere Maßnahmen für die physische Sicherheit angemessen geschützt.

6 Informationssicherheitsorganisation

Der Erste Bürgermeister, der Geschäftsleiter, der Informationssicherheitsbeauftragte, der Datenschutzbeauftragte, ein Verantwortlicher aus dem Sachgebiet IuK, sowie ein Personalvertreter aus dem Personalrat, bilden das Informationssicherheitsteam.
Zusätzlich werden für die einzelnen Bereiche zuständige Daten- und Anwendungsverantwortliche bestimmt. Auch sie haben eine zentrale Rolle in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht es, der Stadt Vilsbiburg, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeitende sind die Voraussetzung dafür, dass die Stadt Vilsbiburg die gesteckten Informationssicherheitsziele erreichen können. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.

6.1 Informationssicherheitsverantwortung

Informationssicherheitsteam
Das Informationssicherheitsteam gibt die erforderlichen Leitplanken für die Informationssicherheit der Stadt Vilsbiburg. Es legt die Leitlinie zur Informationssicherheit fest und aktualisiert diese in regelmäßigen Zeitabständen.

Stadtrat
Der Stadtrat oder sein jeweils zuständiges Entscheidungsgremium bestellt eine für Informationssicherheit und eine für Datenschutz verantwortliche Person und genehmigt soweit erforderlich, die für die Informationssicherheit erforderlichen Maßnahmen und Mittel.

Erster Bürgermeister/ in
Der/ Die Erste Bürgermeister/ in trägt die Gesamtverantwortung für die Informationssicherheit der Stadt Vilsbiburg und stellt sicher, dass die Leitlinie des Informationssicherheitsteams durch geeignete Maßnahmen umgesetzt wird.

Der/ Die Informationssicherheitsbeauftragte
Zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus wird eine Person bestimmt, die für die Informationssicherheit verantwortlich ist. Sie ist für die Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich und berichtet in dieser Funktion direkt der ihr / ihm vorgesetzten Stelle.

Der oder dem Informationssicherheitsbeauftragten werden ausreichende finanzielle und zeitliche Ressourcen für die Ausübung ihrer Tätigkeit zur Verfügung gestellt. Die IT- und Anwendungsverantwortlichen sowie die IT-Benutzerinnen und IT-Benutzer unterstützen sie / ihn in ihrer / seiner Tätigkeit. Sie / er wird in alle Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.
Für sicherheitsrelevante Fragen ist die / der Informationssicherheitsbeauftragte weisungsberechtigt. Sie/ Er ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Aufgaben der / des Informationssicherheitsbeauftragten:

- Initialisieren, überwachen und kontrollieren der Leitlinie zur Informationssicherheit
- Führen des Inventars über die Schutzobjekte
- Erstellen, überarbeiten und überprüfen der Sicherheitsvorgaben (Leitlinie zur Informationssicherheit, Informationssicherheitskonzept, Weisungen, Merkblätter usw.)
- Kontrollieren des Fortschritts der Umsetzung von Informationssicherheitsmaßnahmen
- Berichten an den/ die Ersten Bürgermeister/ in über den Stand der Informationssicherheit
- Berichten an den/ die Ersten Bürgermeister/ in über zu treffende Informationssicherheitsmaßnahmen und Herbeiführen einer Entscheidung
- Beraten der Mitarbeitenden und die den/ die Ersten Bürgermeister/ in Fragen der Informationssicherheit
- Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit
- Bestimmen der Daten- und Anwendungsverantwortlichen

Anwendungs- und Datenverantwortliche
Für alle Prozesse, Daten, Anwendungen, IT- und Netzwerksysteme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Zugriffsberechtigungen vergibt.

Aufgaben der Anwendungs- und Datenverantwortlichen:

- Sicherstellen, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt
- Bestimmen, wer auf die Anwendung in welcher Form Zugriff hat
- Klassifizieren der Daten, die in ihrem Verantwortungsbereich bearbeitet werden (Vertraulichkeit, Integrität, Verfügbarkeit)
- Verantwortung für den sicheren Betrieb ihrer Anwendung (Vertraulichkeit und Integrität der Datensammlungen, Verfügbarkeit der Anwendung und Datensammlungen)
- Regeln der Maßnahmen für die Informationssicherheit sowie deren Kontrolle und Verantwortung für die Dokumentation der Sicherheitsvorkehrungen
- Kontrollieren der Erfüllung der Datenschutz- und Informationssicherheitsbestimmungen
- Erstellen von Notfallplänen für längere Ausfälle
- Informationsstelle für die in ihrem Verantwortungsbereich liegenden Anwendungen und Datensammlungen
- Verantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe), Archivierung oder Vernichtung der in ihrem Verantwortungsbereich liegenden Daten

Datenschutzbeauftragte/ Datenschutzbeauftragter
Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Zur Umsetzung des Datenschutzes wird eine Person bestimmt, die für den Datenschutz verantwortlich ist. Die Datenschutzbeauftragte/ Datenschutzbeauftragter arbeitet in dieser Rolle eng mit den Informationssicherheitsbeauftragten zusammen und ist interne Ansprechperson bei Datenschutzfragen.

Aufgaben der Datenschutzbeauftragte/ Datenschutzbeauftragter:

- Beraten der Mitarbeitenden und des/ der Ersten Bürgermeister/ in Fragen des Datenschutzes
- Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
- Berichten an den/ die Ersten Bürgermeister/ in über den Stand des Datenschutzes
- Planen, koordinieren und Umsetzen von Sensibilisierungs- und Schulungsmaßnahmen zum Thema Datenschutz

6.2 Kontinuierliche Verbesserung der Informationssicherheit

Das Informationssicherheitsteam unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Es gibt mit der periodischen Überarbeitung dieser Leitlinie zur Informationssicherheit die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung. Die Leitlinie wird alle 3 Jahre von der oder dem

Informationssicherheitsbeauftragten überprüft, ggf. angepasst und dem Informationssicherheitsteam erneut zur Überprüfung und Information vorgelegt.

Das Informationssicherheitskonzept wird regelmäßig alle 2 Jahre sowie zusätzlich bei Projekten mit große Auswirkungen auf den Datenschutz und Informationssicherheit auf die Aktualität und die Wirksamkeit geprüft. Festgestellte Abweichungen werden innert nützlicher Frist behoben. Die zu ergreifenden Maßnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards.

Erstellt und beschlossen vom Informationssicherheitsteam.

Vilsbiburg, den 31.10.2019

Tizian Karasz
Informationssicherheitsbeauftragter

Helmut Haider
Erster Bürgermeister

Sebastian Stelzer
Geschäftsleiter

Wolfgang Braumann
Leiter IuK

Georg Lechner
Personalratsvorsitzender

Wolfgang Oberndorfer
Datenschutzbeauftragter