3. Rahmendokumente

3.4 Sicherheitsleitlinie zur Gewährleistung der Informationssicherheit in der Stadt Neumarkt i.d.OPf.

Version:	1.1
Datum:	21.04.2020
Status:	veröffentlicht
Überprüfungsintervall:	jährlich
Verantwortlicher:	Ext. Informationssicherheitsbeauftragter Thomas Eberl
Verteiler:	alle Mitarbeiter öffentlich
Kategorisierung:	

Prüfung und Freigabe:

	Prüfung:	Freigabe:
Name:	Ext. ISB Thomas Eberl	OB T. Thumann
Datum:	23.04.20	30.4.20
Unterschrift:	Thomas Eberl	

Inhalt

1 Einleitung 3
2 Geltungsbereich 3
3 Grundsätze und Ziele der Informationssicherheit 3
3.1 Grundsätze 3
3.1.1 Begriffseinführung 3
3.1.2 Bedeutung der Informationssicherheit beim Einsatz von IT 4
3.1.3 Informationssicherheit als Leistungsmerkmal von IT-Verfahren 4
3.1.4 Informationssicherheit als Leistungsmerkmal der Organisation 4
3.1.5 Wirtschaftlichkeit 4
3.1.6 Regelungskompetenz 5
3.1.7 Sicherheit vor Verfügbarkeit 5
3.1.8 Prinzip des informierten Mitarbeiters 5
3.2 Informationssicherheitsziele 5
3.2.1 Verfügbarkeit 5
3.2.2 Vertraulichkeit 5
3.2.3 Integrität 6
4 Verantwortlichkeiten 6
4.1 Verantwortung der Behördenleitung 6
4.2 Verantwortung der Mitarbeiter 6
4.3 Verantwortung externer Leistungserbringer 7
5 Informationssicherheitsorganisation 7
5.1 Beauftragter für Informationssicherheit 7
5.2 Informationssicherheitsmanagement-Teams 8
6 Umsetzung 8
7 Sicherung und Verbesserung der Informationssicherheit 8

1 Einleitung

Die automatisierte Verarbeitung von Daten und Informationen spielt eine Schlüsselrolle bei der Aufgabenerfüllung der Stadt Neumarkt i.d.OPf. Alle wesentlichen Prozesse werden durch Informations- und Kommunikationstechnik maßgeblich unterstützt.

Mangelnde Informationssicherheit kann zu Störungen bei der Aufgabenerfüllung führen, die die Leistungsfähigkeit mindern und im Extremfall deren Geschäftsprozesse zum Erliegen bringen.

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit trägt die Behördenleitung der Stadt Neumarkt i.d.OPf.

Sie ist insbesondere verantwortlich für

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Informationssicherheits-Managements,
- die Umsetzung der vereinbarten Sicherheitsmaßnahmen einschließlich der Bereitstellung der erforderlichen Haushaltsmittel,
- eine hinreichende und geeignete Dokumentation der IT-Infrastruktur sowie aller Sicherheitsvorkehrungen und Sicherheitsmaßnahmen.

Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen und nachhaltigen Informationssicherheitsprozesses erforderlich sind.

2 Geltungsbereich

Diese Leitlinie gilt für die gesamte Stadtverwaltung der Stadt Neumarkt i.d.OPf. Dies ist sowohl räumlich, als auch organisatorisch für alle Aufgaben und Tätigkeiten der Stadtverwaltung zu verstehen.

Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Mitarbeitern zu beachten und einzuhalten.

3 Grundsätze und Ziele der Informationssicherheit

3.1 Grundsätze

3.1.1 Begriffseinführung

Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein akzeptierbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen. Dabei bedeuten:

- **Vertraulichkeit:** Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang (wer, wann, wie lange, mit wem etc.) sowie die Daten über den Sende- und Empfangsvorgang.

- **Integrität:** Der Begriff der Integrität bezieht sich sowohl auf Informationen, Daten als auch das gesamte IT-System. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Zum anderen bezieht sich der Begriff Integrität auch auf IT-Systeme, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann.
- **Verfügbarkeit:** Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

3.1.2 Bedeutung der Informationssicherheit beim Einsatz von IT

Erklärtes Ziel der Stadt Neumarkt i.d.OPf. ist es, dass alle Einrichtungen, die der Erstellung, Speicherung und Übertragung von Daten dienen, so ausgewählt, integriert und konfiguriert sind, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Dies gilt auch für die Orte zur Aufbewahrung der Medien zur Datensicherung.

3.1.3 Informationssicherheit als Leistungsmerkmal von IT-Verfahren

Die Informationssicherheit ist ein zu bewertendes und herbeizuführendes Leistungsmerkmal von IT-Verfahren. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist auf den IT-Einsatz zu verzichten. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Entwicklung und Einführung von IT-Verfahren,
- dem Betrieb und der Pflege von IT-Verfahren,
- der Beschaffung und Beseitigung/Entsorgung von IT-Produkten,
- der Nutzung von Diensten Dritter.

3.1.4 Informationssicherheit als Leistungsmerkmal der Organisation

Technische und organisatorische Sicherheitsmaßnahmen sind so zu gestalten, dass diese stets integraler Bestandteil aller Verwaltungsprozesse sind und nicht Erweiterungen, die über das Notwendige hinausgehen. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Gestaltung der Organisation,
- der Schaffung und Besetzung von Funktionen und Rollen,
- der Führung von Mitarbeitern,
- der Aus- und Weiterbildung,
- der Gestaltung von Arbeitsabläufen,
- der Zusammenarbeit mit anderen Behörden und Externen,
- der Auswahl und dem Einsatz von Hilfsmitteln.

3.1.5 Wirtschaftlichkeit

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser wird durch den Wert der zu schützenden Informationen und der IT-Systeme definiert. Zu bewerten sind dabei in der Regel die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Verwaltung und die Folgen von Gesetzesverstößen.

Für die Umsetzung der erforderlichen und angemessenen Sicherheitsmaßnahmen sind im Haushalt die notwendigen Ressourcen (Personal, Sach- und Investitionsmittel) bereit zu stellen.

3.1.6 Regelungskompetenz

Die Wahl der Mittel und die Formulierung von Anweisungen, mit denen die Sicherheitsziele erreicht werden sollen, obliegen untergeordneten Verwaltungsbereichen selbst. Sie können eigenständig angemessene Sicherheitsmaßnahmen planen und umsetzen.

3.1.7 Sicherheit vor Verfügbarkeit

Wenn Angriffe auf die Sicherheit der IT-Infrastruktur der Stadt Neumarkt i.d.OPf. drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, kann die Verfügbarkeit von IT-Anwendungen, Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Verwaltung ist der Schutz vor Schäden vorrangig. Vertretbare Einschränkungen in Bedienung und Komfort sind hinzunehmen. Dies gilt in besonderem Maße für die Übergänge zu anderen Netzwerken, insbesondere zum Internet.

3.1.8 Prinzip des informierten Mitarbeiters

Die Mitarbeiter sind im erforderlichen Umfang bezüglich der Informationssicherheit zu sensibilisieren und zu qualifizieren.

3.2 Informationssicherheitsziele

3.2.1 Verfügbarkeit

Für alle IT-Verfahren sind die Zeiten, in denen sie verfügbar sein sollen, festzulegen.

Betriebsunterbrechungen sind in diesen Zeiten weitgehend zu vermeiden, d. h. nach Zahl und Dauer zu begrenzen. Die Beschreibung der notwendigen Verfügbarkeit umfasst

- die regelmäßigen Betriebszeiten,
- die Zeiten mit erhöhter Verfügbarkeitsanforderung,
- die maximal tolerierbare Dauer einzelner Ausfälle.

Ebenfalls festzulegen sind regelmäßig geplante Auszeiten, insbesondere zu Wartungszwecken.

Bezogen auf die Bürger der Stadt bedeutet dies, dass die Services und Dienstleistungen der Stadtverwaltung zu den regelmäßigen Betriebszeiten erbracht werden können sollen. Ausfälle, welche durch mangelnde Verfügbarkeit von Informationsdiensten entstehen sollen vermieden werden.

3.2.2 Vertraulichkeit

Die in IT-Verfahren erhobenen, gespeicherten, verarbeiteten und weiter gegebenen Daten sind vertraulich zu behandeln und jederzeit vor unbefugtem Zugriff zu schützen. Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Mitarbeiter erhält eine Zugriffsberechtigung nur auf die Daten, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

Zur Erfüllung der Aufgaben und Dienste der Stadtverwaltung ist die Verarbeitung von Bürgerdaten unabdingbar. Daher muss es Ziel der ganzen Behörde sein, diese Daten vertrauensvoll zu

behandeln und nur denjenigen Personen zu offenbaren, die diese Informationen zur Erfüllung ihrer dienstlichen Aufgaben benötigen.

3.2.3 Integrität

Informationen sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Alle IT-Verfahren sollen stets aktuelle und vollständige Informationen liefern, eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren.

Da eine Verfälschung von Informationen direkte Auswirkungen auf das Wohlergehen der Bürger der Stadt Neumarkt haben kann muss es Ziel der Behörde sein, diese Informationen vor unberechtigter oder unbeabsichtigter Veränderung zu schützen.

4 Verantwortlichkeiten

4.1 Verantwortung der Behördenleitung

Die Behördenleitung erlässt verbindliche Regeln zur Informationssicherheit für die Verwaltung der Stadt Neumarkt i.d.OPf. und gibt sie den Mitarbeitern bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

4.2 Verantwortung der Mitarbeiter

Alle Mitarbeiter gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um.

Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden.

Mitarbeiter, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für die Verwaltung oder einen Dritten verursachen, können darüber hinaus nach den gesetzlichen Regelungen zum Schadenersatz herangezogen werden.

Als Straftaten kommen insbesondere in Betracht

- das unbefugte Verschaffen von Daten anderer, die nicht für den Mitarbeiter bestimmt und die gegen den unberechtigten Zugang besonders gesichert sind,
- das Schädigen fremden Vermögens durch unrichtiges Gestalten eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugtes Verwenden von Daten oder durch unbefugtes Einwirken auf den Ablauf eines Programms,
- das rechtswidrige Löschen, Verändern, Unterdrücken und Unbrauchbarmachen von Daten,
- das unbefugte Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers oder
- strafbewehrte Verstöße gegen das Bayerische Datenschutzgesetz oder das Bundesdatenschutzgesetz bzw. die EU-Datenschutzgrundverordnung.

Verstöße gegen die Informationssicherheit sind unverzüglich dem zuständigen Beauftragten für Informationssicherheit zu melden.

Als Verstöße gelten insbesondere Handlungen, die aufgrund einer Abweichung von dieser Leitlinie oder weiteren Richtlinien zur Informationssicherheit

- der Stadt Neumarkt i.d.OPf. materielle oder immaterielle Schäden zufügen,
- den unberechtigten Zugriff auf Informationen, deren Preisgabe und/oder Änderung zulassen,
- die Nutzung von Verwaltungsinformationen für illegale Zwecke beinhalten.

4.3 Verantwortung externer Leistungserbringer

Personen, Behörden und Unternehmen, die nicht zur Verwaltung der Stadt Neumarkt i.d.OPf. gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers 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 Informationssicherheitsorganisation

5.1 Beauftragter für Informationssicherheit

Als zentrale Sicherheitsinstanz der Verwaltung der Stadt Neumarkt i.d.OPf. ernennt die Behördenleitung einen Informationssicherheitsbeauftragten (ISB), der für alle operativen Belange und Fragen der Informationssicherheit zuständig ist. Der ISB ist als Stabsstelle in das Organigramm aufzunehmen und berichtet in dieser Funktion direkt an die Behördenleitung.

Es ist sicher zu stellen, dass diesem Beschäftigten ein angemessener Teil seiner Arbeitszeit für die Erledigung seiner Aufgaben als ISB zur Verfügung steht.

Die Funktion des ISB kann auch an einen geeigneten externen Dienstleister übertragen werden.

Im jeweiligen Zuständigkeitsbereich hat der ISB folgende Aufgaben:

- Steuerung des Informationssicherheitsprozesses und Mitwirkung bei allen damit zusammenhängenden Aufgaben,
- Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- Unterstützung bei der Erstellung, Fortschreibung und Umsetzung der sich aus dieser Leitlinie ableitenden weiteren Dokumente,
- Vorschlag von neuen Sicherheitsmaßnahmen und –strategien,
- Vertretung der Verwaltung der Stadt Neumarkt i.d.OPf. in allen Angelegenheiten der Informationssicherheit,
- Ansprechpartner für die Mitarbeiter in den Fragen der Informationssicherheit,
- Koordination von Sensibilisierungs- und Schulungsmaßnahmen,
- Meldung von besonders sicherheitsrelevanten Zwischenfällen im Rahmen seiner Berichtswege.

Der externe ISB wird in der Stadt Neumarkt durch einen internen Stellvertreter unterstützt. Dieser ist durch seine interne Position erste Anlaufstelle für die Mitarbeiter. Zudem nimmt er im Vertretungsfall alle oben genannten Aufgaben des ISB wahr. Hierzu wird er ebenfalls mit den selben Befugnissen ausgestattet.

Bei Gefahr im Verzug ist der ISB oder sein Stellvertreter berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Dies kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzzugängen führen.

Die Behördenleitung der Stadt Neumarkt i.d.OPf. ist hiervon unverzüglich zu unterrichten.

5.2 Informationssicherheitsmanagement-Teams

Zur Unterstützung des ISB bei der Erfüllung seiner Aufgaben können temporär Informationssicherheitsmanagement-Teams gebildet werden, um bei strategischen Entscheidungen oder Einzelmaßnahmen (z. B. bei Projekten entsprechender Größenordnung) die Belange der Informationssicherheit der Verwaltung der Stadt Neumarkt i.d.OPf. sicherzustellen.

Das Kernteam besteht aus dem ISB und dem IT-Leiter. Weitere Personen (Datenschutzbeauftragter, Beauftragter für Arbeitssicherheit, Personalrat, Geschäftsleitung) werden nach Bedarf einbezogen.

6 Umsetzung

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte und detaillierter Regelungen und Dienstanweisungen zur Informationssicherheit. Die Dienstanweisung für den Einsatz der Informationstechnik behält ihre Gültigkeit.

7 Sicherung und Verbesserung der Informationssicherheit

Der Informationssicherheitsprozess ist regelmäßig auf seine Aktualität und Wirksamkeit zu überprüfen. Insbesondere sind die Maßnahmen regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Mitarbeitern bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Die Behördenleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus.

Die Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen (1x jährlich) und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.