Allgemeine Richtlinie für Informationssicherheit und Datenschutz der Gemeinde Langnau am Albis

vom 21. November 2023

Stand 21. November 2023

Inhaltsverzeichnis

1 Einleitung 3

2 Allgemeine Bestimmungen 3

2.1 Gegenstand und Zweck 3
2.2 Geltungsbereich 3
2.3 Grundlagen 3

3 Informationssicherheitsniveau 4

4 Informationssicherheitsziele 4

5 Informationssicherheitsorganisation 4

5.1 Gemeinderat 5
5.2 Gemeindeschreiber/in 5
5.3 Informationssicherheitsverantwortliche/r (ISV) 5
5.4 Anwendungs- und Datenverantwortliche/r 6
5.5 Datenschutzberater/in 6
5.6 Vorgesetzte 7
5.7 Mitarbeiterinnen und Mitarbeiter 7

6 Regelung von Ausnahmen 8

7 Kontinuierliche Verbesserung der Informationssicherheit 8

8 Informationssicherheitsmassnahmen 8

8.1 Mobiles Arbeiten und mobile Geräte 8
8.2 Personalsicherheit 8
8.3 Schulungsmassnahmen in Informationssicherheit 9
8.4 Verschlüsselungsmassnahmen 10
8.5 Verwaltung von organisationseigenen Werten 10
8.6 Informationshandhabung 10
8.7 Verwendung von Wechselmedien 11
8.8 Identitäts- und Zugriffskontrolle 11
8.9 Passwörter 11
8.10 Physische Sicherheit und Schutz vor Umwelteinflüssen 11
8.11 Sicherheit von Informationssystemen 13
8.12 Datensicherung und -wiederherstellung 14
8.13 Protokollierung 14
8.14 Verwaltung der Netzwerksicherheit 14
8.15 Sicherheit von Testdaten 14
8.16 Auslagerung von Datenbearbeitungen (Outsourcing) 15
8.17 Umgang mit Informationssicherheitsvorfällen 15
8.18 Drucker, Kopierer und Multifunktionsgeräte 16
8.19 Besprechungs- und Schulungsräume 16
8.20 Aufbewahrung und Archivierung 17
8.21 Risikoanalyse / Notfallplanung 17

9 Schlussbestimmungen 17

Der Gemeinderat erlässt, gestützt auf § 48 des Gemeindegesetzes vom 20. April 2015 und Art. 24 der Gemeindeordnung der Gemeinde Langnau am Albis vom 9. Februar 2020 folgende Richtlinie:

1 Einleitung

Die Gemeinde Langnau am Albis, zukünftig Gemeinde genannt, 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 nach § 7 Gesetz über die Information und den Datenschutz (IDG, LS 170.4) verabschiedet der Gemeinderat diese allgemeine Richtlinie. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Gemeinde angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Richtlinie eine Beschreibung der Informationssicherheitsorganisation.

2 Allgemeine Bestimmungen

2.1 Gegenstand und Zweck

Diese Richtlinie regelt die Ziele, die Organisation der Gemeinde und die allgemeinen Vorgaben in Bezug auf Datenschutz und Informationssicherheit sowie die Prozesse zu deren kontinuierlichen Verbesserung. Sie ist angelehnt an die Allgemeine sowie die Besonderen Informationssicherheitsrichtlinien des Kantons Zürich.

Ausnahmen zu den in dieser Richtlinie definierten Vorgaben sind durch die Gemeindeschreiberin / den Gemeindeschreiber bewilligen zu lassen.

2.2 Geltungsbereich

Die Allgemeine Richtlinie für Informationssicherheit und Datenschutz und die damit zusammenhängenden Dokumente (insbesondere die Weisung zur Informationssicherheit, das Rollen- und Berechtigungskonzept, die Massnahmen zur Sensibilisierung der Mitarbeitenden sowie das Notfallkonzept) gelten für alle Mitarbeiterinnen und Mitarbeiter sowie Behördenmitglieder.

Vertragspartner, die Daten bearbeiten, werden ebenfalls zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet. Zudem bildet die Informatiksicherheitsrichtlinie OBT Swiss Cloud (Kundenrichtlinien für die Nutzung der OBT-Informatikmittel) einen integrierenden Bestandteil für die detaillierte technische Umsetzung der in dieser Richtlinie formulierten Anforderungen.

2.3 Grundlagen

Die gesetzlichen Grundlagen für die Gemeinde sind:

- Gesetz über die Information und den Datenschutz (IDG, Z)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen zu beachten.

3 Informationssicherheitsniveau

Die Massnahmen der Gemeinde zur Sicherstellung von Datenschutz und Informationssicherheit sind auf einen erhöhten Schutzbedarf auszurichten. Diese Einstufung erfolgt aufgrund der Tatsache, dass die Gemeinde Daten bearbeitet, die einen erhöhten Schutz vor unberechtigten Zugriffen und vor unerlaubten Änderungen benötigen (Personendaten und besondere Personendaten bzw. Persönlichkeitsprofile), der Anzahl Einwohner/-innen, der betroffenen Personen der Gemeinde, der Unterstützung aller wesentlichen Funktionen und Aufgaben durch IT- und Netzwerksysteme, der Tatsache, dass ein Ausfall von IT- und Netzwerksystemen die Aufgabenerfüllung nicht wesentlich beeinträchtigen darf.

4 Informationssicherheitsziele

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele (§ 7 IDG):

Integrität	Informationen müssen richtig und vollständig sein
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
Verantwortung	Die politischen Behörden und die Mitarbeiterinnen und Mitarbeiter der Gemeinde 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.
Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

5 Informationssicherheitsorganisation

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.

Die Gemeindeschreiberin / der Gemeindeschreiber, die oder der Informationssicherheitsverantwortliche (nachfolgend ISV) und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht es der Gemeinde, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeiterinnen und Mitarbeiter sind die Voraussetzung dafür, dass die Gemeinde die gesteckten Informationssicherheitsziele erreichen kann. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.
Die Informationssicherheitsorganisation der Gemeinde geht aus der Dokumentation der Gemeindeführungsorganisation (GFO) hervor.

5.1 Gemeinderat

Der Gemeinderat trägt die Gesamtverantwortung für die Informationssicherheit in der Gemeinde. Er erlässt die Allgemeine Richtlinie für Informationssicherheit und Datenschutz, setzt diese in Kraft und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel.

5.2 Gemeindeschreiber/in

Die Gemeindeschreiberin / der Gemeindeschreiber trägt die operative Verantwortung für die Informationssicherheit in der Gemeinde. Er / sie bestimmt eine für Informationssicherheit und eine für Datenschutz verantwortliche Person oder übt diese Funktion(en) selbst aus. Sie / er stellt sicher, dass die Beschlüsse des Gemeinderats zur Informationssicherheit umgesetzt werden.

5.3 Informationssicherheitsverantwortliche/r (ISV)

Für die Umsetzung der Informationssicherheitsziele und der Überwachung der Einhaltung des angestrebten Sicherheitsniveaus ist die / der Informationssicherheitsverantwortliche (ISV) verantwortlich. Sie / Er ist für die Umsetzung der Sicherheitsrichtlinien und deren Kontrolle verantwortlich und berichtet in dieser Funktion direkt der ihr oder ihm vorgesetzten Stelle.

Der oder dem ISV werden ausreichende finanzielle und zeitliche Ressourcen für die Ausübung ihrer / seiner Tätigkeit zur Verfügung gestellt. Die Anwendungs- und Datenverantwortlichen 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.

Die / Der Informationssicherheitsverantwortliche entscheidet über sicherheitsrelevante Fragen und verwaltet allfällige Ausnahmen. Sie/er ist die Anlaufstelle für Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Aufgaben der/des Informationssicherheitsverantwortlichen (ISV) respektive Verantwortung:

- Betreuung der IKT-Umgebung der Gemeinde und Schnittstelle zu externen Betreibern
- Initialisieren, überwachen und kontrollieren der Richtlinien zur Informationssicherheit
- Führen des IT-Inventars
- Verwaltung von Domainnamen der Gemeinde, insbesondere rechtzeitige Verlängerung der Registrierung
- Verwaltung der digitalen Zertifikate (wo vorhanden) inklusive Überwachung der Gültigkeitsdauer
- Anpassen und Überprüfen der Sicherheitsvorgaben (allgemeine Informationssicherheitsrichtlinie und technische Richtlinie für den Betrieb von Informationssystemen, Weisung Informationssicherheit und Datenschutz, Rollen- und Berechtigungskonzept, Betriebsdokumentation usw.)

- Kontrollieren des Fortschritts der Umsetzung von Informationssicherheitsmassnahmen
- Information an die Gemeindeschreiberin / den Gemeindeschreiber über den Stand der Informationssicherheit
- Berichten an die Gemeindeschreiberin / den Gemeindeschreiber über zu treffende Informationssicherheitsmassnahmen und Herbeiführung von Entscheiden
- Erteilung von verbindlichen Anordnungen zur Abwehr von unmittelbar drohenden Gefahren bei Informationssicherheitsvorfällen
- Austausch mit internen und externen Stellen über Informationssicherheitsvorfälle im Bereich Informationssicherheit unter Wahrung der Informationsklassifizierung und Vertraulichkeit, wo nötig
- Beraten der Mitarbeiterinnen und Mitarbeiter sowie der Gemeindeschreiberin / des Gemeindeschreibers in Fragen der Informationssicherheit
- Umsetzung und Pflege des übergreifenden Rollen- und Berechtigungskonzepts
- Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit
- Bestimmen/Feststellen der Anwendungs- und Datenverantwortlichen
- Sicherstellen, dass alle Mitarbeiterinnen und Mitarbeiter über die allgemeinen Anforderungen an die Daten- und Informationssicherheit informiert sind und die Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit unterzeichnet haben

5.4 Anwendungs- und Datenverantwortliche/r

Für alle Prozesse, Daten, Anwendungen, IT- und Netzwerksysteme ernennt die / der zuständige Abteilungsleiter/in die verantwortlichen Personen (Anwendungs- und Datenverantwortliche/n) oder sie/er übt diese Funktion selbst aus.

Aufgaben der Anwendungs- und Datenverantwortlichen:
- Bestimmen, wer auf die Anwendung in welcher Form Zugriff hat
- Sicherstellen, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt
- 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
- Kontrollieren der Erfüllung der Datenschutzbestimmungen
- Mitarbeit beim Erstellen von Notfallplänen für längere Ausfälle
- Informationsstelle für die in ihrem Verantwortungsbereich liegenden Anwendungen und Datensammlungen
- Verantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe), Aufbewahrung und Archivierung oder Vernichtung der in ihrem Verantwortungsbereich liegenden Daten

5.5 Datenschutzberater/in

Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Die Gemeindeschreiberin / Der Gemeindeschreiber als oberstes Organ trägt die Gesamtverantwortung für den Datenschutz in der Gemeinde. Sie/Er weist die Rolle Funktion Datenschutzberaterin / Datenschutzberater einer verantwortlichen Person zu oder übt sie selbst

aus. Sie/Er arbeitet in dieser Rolle eng mit der bzw. dem ISV zusammen und ist interne Ansprechperson bei Datenschutzfragen.

Aufgaben der Datenschutzberaterin / des Datenschutzberaters:

- Ansprechperson für die Mitarbeiterinnen und Mitarbeiter sowie die Gemeindeschreiberin / den Gemeindeschreiber in Belangen des Datenschutzes
- Bindeglied zur kantonalen Datenschutzbeauftragten bei Fragen zum Datenschutz
- Zuständige Person für die Einhaltung der gesetzlichen Meldepflicht bei Datenschutzvorfällen
- Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
- Berichten an die Gemeindeschreiberin / den Gemeindeschreiber über den Stand des Datenschutzes
- Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Datenschutz

Bei einer kleinen Anzahl von Mitarbeiterinnen und Mitarbeiter (Richtwert 10 und kleiner) kann diese Funktion auch in Personalunion mit einer der anderen Funktionen ausgeübt werden, dabei sind jedoch wenn möglich Interessenskonflikte (z.B. zwischen Erstellung, Ausführung und Kontrolle) zu vermeiden.

5.6 Vorgesetzte

Die Vorgesetzten bilden eine wichtige Schnittstelle zwischen der obersten Leitung der Verwaltung und den Mitarbeiterinnen und Mitarbeitern und verfügen in ihrem Fachbereich über spezialisiertes Wissen.

Aufgaben der Vorgesetzten:

- Fungieren als Ansprechperson für die Mitarbeiterinnen und Mitarbeiter in Belangen des Datenschutzes
- Bilden eine Schnittstelle zu der obersten Leitung der Gemeinde
- Verfügen über spezialisiertes Wissen über datenschutzrelevante Vorschriften in ihrem Fachbereich und vermitteln dieses an ihre Mitarbeiterinnen und Mitarbeiter
- Informieren ihr Team über allfällige Vorfälle und Vorsichtsmassnahmen in Bezug auf Datenschutz und Informationssicherheit

5.7 Mitarbeiterinnen und Mitarbeiter

Den Mitarbeiterinnen und Mitarbeitern obliegt eine grosse Verantwortung, da sie durch ihr richtiges Handeln und im Kontakt mit den Betroffenen am meisten für die Sicherstellung des Datenschutzes und der Informationssicherheit beitragen können.

Aufgaben der Mitarbeiterinnen und Mitarbeiter:

- Teilnehmen an Sensibilisierungs- und Schulungsaktivitäten und Sicherstellung des Verständnisses
- Einhaltung der Gesetze sowie der vertraglichen Regelungen und internen Richtlinien und selbständige Information bei Unsicherheiten
- Unterstützung der Sicherheitsmassnahmen durch eine sicherheitsbewusste Arbeitsweise
- Aufrechterhalten des Risikobewusstseins und Rückfragen bei Unsicherheiten
- Melden von Informationssicherheitsvorfällen und Hinweisen auf Schwachstellen an die für die Informationssicherheit verantwortliche Person oder die oder den Vorgesetzten

6 Regelung von Ausnahmen

(In Anlehnung an die Besondere Informationssicherheitsrichtlinie 27 Amt für Informatik des Kantons Zürich)

Die oder der ISV entscheidet über Ausnahmen von den Richtlinien und Weisungen der Gemeinde. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail einzureichen und zur Nachvollziehbarkeit zu dokumentieren. Für jede Ausnahme ist ein Zeitpunkt, eine Dauer, der Antragsteller sowie ein Verantwortlicher zu definieren. Die bestehenden Ausnahmen sind periodisch zu überprüfen.

7 Kontinuierliche Verbesserung der Informationssicherheit

Die Gemeindeschreiberin / Der Gemeindeschreiber unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Er gibt mit der periodischen Überarbeitung dieser Richtlinie zur Informationssicherheit und den dazugehörigen Richtlinien und Weisungen die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung vor. Die Richtlinie wird alle 4 Jahre überprüft.

Die umgesetzten organisatorischen und technischen Massnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit werden regelmässig alle 2 Jahre sowie zusätzlich bei Projekten mit grossen Auswirkungen auf die Aktualität und die Wirksamkeit durch eine unabhängige Person / Stelle geprüft. Festgestellte Abweichungen sind innert nützlicher Frist zu beheben. Die zu ergreifenden Massnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards, die Umsetzung ist zu kontrollieren und zu protokollieren.

8 Informationssicherheitsmassnahmen

Aus der Definition der Informationssicherheitsziele ergeben sich die folgenden Massnahmen. Sie sind angelehnt an die Besondere Informationssicherheitsrichtlinien Amt für Informatik und Personalamt des Kantons Zürich.

8.1 Mobiles Arbeiten und mobile Geräte

Falls der Einsatz von mobilen Geräten inklusive die allfällige Verwendung von privaten Geräten (Bring Your Own Device) für dienstliche Zwecke durch die Mitarbeiterinnen und Mitarbeiter der Gemeinde zugelassen ist, sind die Voraussetzungen dafür geregelt und dokumentiert.

Die Telearbeit muss genehmigt werden, die entsprechenden arbeitsrechtlichen Bedingungen sind festgelegt. Verlust- und Reparaturprozess sowie Verkauf und Entsorgungen von mobilen Endgeräten sind geregelt.

Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.

Für dienstliche Zwecke werden nur durch die Gemeinde genehmigte Dienste und Produkte für Kommunikation und Datenaustausch verwendet.

8.2 Personalsicherheit

Mitarbeiterinnen und Mitarbeiter werden auf die Verpflichtungen in Bezug auf den Datenschutz und die Informationssicherheit hingewiesen:

- die Verantwortlichkeiten für die Klassifizierung und Umgang mit Informationen sowie dem Umgang mit organisationseigenen Werten
- die Verantwortlichkeiten im Umgang mit Informationen, die von anderen Organisationen erstellt wurden
- die Rechte und Pflichten von Mitarbeitenden, z.B. Urheberrecht oder Datenschutzgesetz
- die Massnahmen, die ergriffen werden, wenn Mitarbeitende sich nicht an die Bestimmungen halten

Die / Der Gemeindeschreiber/in muss sicherstellen, dass

- alle Mitarbeiterinnen und Mitarbeiter über ihre Verantwortlichkeiten bei klassifizierten Informationen orientiert werden,
- die Richtlinien und Weisungen jederzeit in der neusten Version abrufbar sind,
- die Richtlinien gelebt und eingehalten werden,
- das Bewusstsein für Datenschutz und Informationssicherheit geschaffen wird,
- die Fähigkeiten und Qualifikationen von Mitarbeiterinnen und Mitarbeitern mittels Schulungen gefördert werden.

8.3 Schulungsmassnahmen in Informationssicherheit

Alle Mitarbeiterinnen und Mitarbeiter werden regelmässig stufen- und funktionsgerecht auf Informationssicherheitsthemen sensibilisiert und geschult. Neu eintretende Mitarbeiterinnen und Mitarbeiter erhalten zeitnah eine Grundausbildung.

Schulungen zur Informationssicherheit finden regelmässig statt. Erstausbildung und Schulung gilt für Personen, die in neue Positionen oder Rollen mit wesentlich unterschiedlichen Informationssicherheitsanforderungen wechseln, und nicht nur für Neueinsteiger. Sie finden vor der Aufnahme der neuen Tätigkeit statt.

Die Sensibilisierungsmassnahmen können eine Reihe von Aktivitäten umfassen wie Kampagnen (z.B. einen «Tag der Informationssicherheit») oder Newsletter.

Das Bildungs- und Ausbildungsprogramm steht mit den Informationssicherheitsrichtlinien und relevanten Verfahren der Organisation in Einklang und berücksichtigt die zu schützenden Informationen der Organisation sowie die zum Schutz der Informationen durchgeführten Kontrollen. Das Programm berücksichtigt verschiedene Formen der allgemeinen und beruflichen Bildung, z.B. Vorlesungen oder Selbststudien.

Die Informationssicherheit und das Schutzniveau werden anhand der Aufgabe, Verantwortlichkeit und Empfehlungen vermittelt.

Die Schulungen werden nachvollziehbar dokumentiert.

Alle Mitarbeiterinnen und Mitarbeiter, die mobile IKT-Systeme nutzen, werden auf die spezifischen Risiken der Informationssicherheit sensibilisiert, z.B. mit Schulungen. Wenn die Richtlinie für mobile Geräte die Verwendung von mobilen Geräten in Privatbesitz erlaubt, sollten die Richtlinie und die zugehörigen Sicherheitsmassnahmen auch Folgendes berücksichtigen:

- Trennung der privaten und der geschäftlichen Nutzung der Geräte einschliesslich der Verwendung von Software zur Unterstützung einer solchen Trennung und zum Schutz von Geschäftsdaten auf einem privaten Gerät.
- Gewährung des Zugangs zu Geschäftsinformationen erst, nachdem die Benutzerinnen und Benutzer die Erklärung über die Nutzung von Internet und E-Mail sowie zur

Informationssicherheit unterschrieben haben, in der die Einhaltung entsprechender Schutzmassnahmen bestätigt wird (physischer Schutz, Software-Aktualisierung etc.).

Schulungen für Informationssicherheit beinhalten folgende Minimalanforderungen:

- Das Bekenntnis der Mitarbeiterinnen und Mitarbeiter zur Informationssicherheit der Gemeinde und angeschlossener Institutionen
- Die Notwendigkeit, sich mit der Thematik Informationssicherheit auseinander zu setzen (z.B. Weisung zur Informationssicherheit)
- Die persönliche Verantwortung für den Schutz von Informationen
- Die Abläufe der Informationssicherheit (z.B. Meldung von Informationssicherheitsvorfällen)
- Kontaktstellen für zusätzliche Informationen und Beratung zu Fragen der Informationssicherheit und weiterer Schulungsmöglichkeiten

Neue Mitarbeiterinnen und Mitarbeiter unterzeichnen bei Stellenantritt die Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit.

8.4 Verschlüsselungsmassnahmen

Bei Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt die Speicherung und Übermittlung verschlüsselt. Zur Anwendung kommen aktuelle Verschlüsselungsverfahren.

8.5 Verwaltung von organisationseigenen Werten

Sämtliche für den Betrieb notwendigen organisationseigenen Werte werden in einem aktuellen Inventar geführt (Informationen, Anwendungen, Systeme usw.). Die Verantwortlichkeiten werden ebenfalls im Inventar erfasst.

Die IKT-Umgebung ist dokumentiert, z.B. in Form einer Betriebsdokumentation.

8.6 Informationshandhabung

Informationen werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen. Die Vertraulichkeit ist jederzeit sicherzustellen. Musterbriefe für Auskunft, Informationszugang und Datensperre stehen auf der Website der Datenschutzbeauftragten des Kantons Zürich zur Verfügung.

Die Gemeinde bewertet bei einer beabsichtigten neuen Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen (Datenschutz-Folgenabschätzung). Sie unterbreitet eine solche vorab der Datenschutzbeauftragten zur Prüfung (Vorabkontrolle), wenn die Bearbeitung von Personendaten besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhält (§10 IDG).

Informationen werden nach Ablauf der vorab definierten Aufbewahrungsdauer dem zuständigen Archiv angeboten. Informationen, die das zuständige Archiv nicht übernimmt, werden sicher vernichtet.

8.7 Verwendung von Wechselmedien

Der Einsatz von Wechselmedien erfolgt kontrolliert, darauf enthaltene dienstliche Daten werden vor Zugriff von Dritten und Verlust geschützt.

8.8 Identitäts- und Zugriffskontrolle

Organisationseigene Werte werden mit geeigneten Massnahmen vor nicht autorisiertem Zugang und Zugriff geschützt. Dieser Schutz umfasst die Authentifizierung (Prüfung, ob die Nutzerin / der Nutzer derjenige ist, für den sie / er sich ausgibt) und Autorisierung (Prüfung, ob die Nutzerin / der Nutzer zugriffsberechtigt ist).

Es gelten die folgenden Grundsätze:

- Der Zugriff auf die Informationen ist durch ein Rollen- und Berechtigungskonzept geregelt.
- Berechtigungen werden nach einheitlichen Prozessen vergeben, angepasst und auch wieder gelöscht.
- Die Zugriffsberechtigungen für Behörden- und Kommissionsmitglieder, Mitarbeiterinnen und Mitarbeiter sowie für Lernende auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich.
- Bei der Einrichtung von Stellvertretungen, z.B. für Mailkonten, werden die jeweiligen Zugriffsrechte berücksichtigt.
- Technische Konten und Benutzerkonten sind einer verantwortlichen Person zugewiesen.
- Zugriffsrechte für Mitarbeitende werden mindestens jährlich geprüft. Administrative Zugriffsrechte werden mindestens halbjährlich geprüft.
- Bei Abteilungs- oder Aufgabenwechsel von Mitarbeitenden werden die Zugriffsrechte geprüft und wenn nötig angepasst.
- Bei Austritt von Mitarbeiterinnen und Mitarbeitern werden deren Zugriffsrechte umgehend entfernt bzw. deaktiviert. Verwaltungseigene Hardware wird spätestens bei Austritt zurückgenommen.
- Die Art und Stärke der Authentifizierung werden durch die Klassifizierung der Information und die Exponiertheit der Anwendung bestimmt, auf die der Zugriff erfolgen soll.
- Zugriffsrechte für administrative Zugriffe werden restriktiv und kontrolliert vergeben.
- Es ist jederzeit nachvollziehbar, wer welche Zugriffsrechte besitzt.

Bei der Berechtigungsvergabe gelten die allgemeinen Grundsätze:

- Need-to-know: Der Zugriff ist nur auf die Informationen gestattet, die zur Durchführung der Aufgabe benötigt werden.
- Least-privilege: Es sind nur die Berechtigungen zuzuweisen, die zur Durchführung der Aufgabe benötigt werden.
- Segregation of Duties: Zur Vermeidung von Interessenkonflikten ist die Funktionstrennung zu gewährleisten.

8.9 Passwörter

Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch persönliche Passwörter gesichert. Es wird eine ausreichende Qualität und Schutz der Passwörter sichergestellt.

8.10 Physische Sicherheit und Schutz vor Umwelteinflüssen

Zutritt

Gebäude und Räume sowie IT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem geschützt. Die Zutrittsberechtigungen werden verwaltet und restriktiv vergeben.

Physische Sicherheit
Gebäude und Räume sowie IT- und Netzwerksysteme werden mit angemessenen Massnahmen gegen Umwelteinflüsse wie Feuer, Wasser, Feuchtigkeit, Rauch, gegen Einbruch und Diebstahl sowie Stromausfall geschützt. Es sind entsprechende Alarmierungs- und Meldeanlagen vorhanden.

8.11 Sicherheit von Informationssystemen

Neue Informationssysteme werden im Inventar der Gemeinde nachgeführt, bei Bedarf werden die Auswirkungs- und Bedrohungsanalyse und die Schutzmassnahmen angepasst.

Auf Systemen der Gemeinde dürfen nur zugelassene, inventarisierte Anwendungen installiert werden.

Neue Informationssysteme werden vor ihrer Inbetriebnahme auf ihre Kompatibilität mit bestehenden Systemen geprüft, getestet und abgenommen. Vor der produktiven Inbetriebnahme liegt eine Dokumentation der Systeme vor.

Alle Informationssysteme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.

Bei der Evaluation und Beschaffung von Anwendungen werden deren Sicherheitsfunktionen berücksichtigt.

Die Informationssysteme werden nach der Beschaffung sicher installiert, konfiguriert und betrieben (gemäss anerkannten Sicherheitsstandards), mit einem Änderungsmanagement verwaltet und in einem geregelten Prozess ausser Betrieb genommen.

Die Verfügbarkeit und Qualität der Anwendungsdienste wird laufend überprüft. Sicherheitsrelevante Ereignisse werden aufgezeichnet und periodisch oder bei Verdacht ausgewertet.

Schwachstellen für Informationssysteme und Anwendungen werden laufend überprüft und gemäss ihrer Kritikalität behandelt, z.B. durch Updates oder Austausch.

Informationen zu Verwaltungstätigkeiten werden bei der elektronischen Übertragung und dem physischen Transport in Abhängigkeit ihrer Schutzstufe vor unbefugter Kenntnisnahme und Bearbeitung geschützt.

Beim Austausch von elektronischen oder physischen Informationen mit externen Organisationen und Personen werden die folgenden Anforderungen in Abhängigkeit von der Klassifizierung der auszutauschenden Informationen geprüft und, falls erforderlich, vertraglich geregelt:

- Verfahren zur Sicherstellung der Nachvollziehbarkeit
- Einsatz von kryptografischen Verfahren gemäss Kapitel 8.3
- Aufrechterhaltung einer Informationskette (z.B. Sendungsverfolgung, Empfangsbestätigung) während der elektronischen Übertragung
- Definierte Zugangskontrollen und Verfahren, die Informationen und physische Datenträger während des physischen Transports schützen

Falls für die Telefonie internetbasierte Systeme eingesetzt werden, so ist gewährleistet, dass diese den damit verbundenen Risiken entsprechend sicher eingerichtet und betrieben werden (z.B. Netztrennung, angemessene Zugriffsrechte, Ausfallsicherheit, Sicherheitskonfiguration, vertragliche Absicherungen).

Virenschutzprogramme werden auf allen IT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Die Ausserbetriebnahme und fachgerechte Entsorgung von Informationssystemen erfolgt nach einem dokumentierten Prozess. Bei der Ausserbetriebnahme oder einer Reparatur von Informationssystemen, insbesondere bei IKT-Systemen, die Speichermedien enthalten (z.B. mobile Endgeräte, Drucker, Kameras), müssen Informationen irreversibel gelöscht werden, bevor die Informationssysteme ausgetauscht, entsorgt oder wiederverwendet werden.

8.12 Datensicherung und -wiederherstellung

Datensicherungen werden regelmässig durchgeführt. Es ist sichergestellt, dass Datensicherungen geographisch abgetrennt von den produktiven Daten aufbewahrt und vor Zugriff geschützt werden.

Die Datensicherungen werden entsprechend den rechtlichen Anforderungen aufbewahrt (siehe Kapitel 8.20 Aufbewahrung und Archivierung).

Es ist gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.

8.13 Protokollierung

Aktivitäten der Benutzerinnen und Benutzer auf den IKT-Systemen der Gemeinde können aus Gründen der Nachvollziehbarkeitspflicht wie auch der Funktionsüberwachung, der Sicherheit, der Integrität und der Verfügbarkeit aufgezeichnet werden.

Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin respektive des Benutzers möglich.

8.14 Verwaltung der Netzwerksicherheit

Das Netzwerk wird in Sicherheitszonen unterteilt und alle Netzwerkzugänge werden mit Firewalls gesichert. Wo ausschliesslich eine LeuNet-Verbindung verwendet wird, kann auf eine zusätzliche Firewall verzichtet werden. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern.

Die Installation und der Betrieb von Netzwerkkomponenten erfolgen durch den Fulloutsourcing-Partner. Die Sicherheitsvorgaben für den Betrieb von Informationssystemen sind in den entsprechenden Verträgen geregelt.

Die Vorgaben des Kantons Zürich in Bezug auf den Anschluss an das übergeordnete Netzwerk (LEUnet) werden eingehalten.

8.15 Sicherheit von Testdaten

Für Testsysteme sind die gleichen Sicherheitsanforderungen umzusetzen, wie dies bei Produktivsystemen der Fall ist. Insbesondere gilt diese Anforderung, wenn auf Testsystemen mit Testdaten aus produktiven Systemen (Datenkopien) gearbeitet werden muss. Ist dies erforderlich, ist die Anzahl vertraulicher Daten auf ein Minimum zu beschränken. Nach durchgeführten Tests sind die Informationen zu löschen. Über die Verwendung von Tests mit Daten aus produktiven Systemen ist ein Protokoll zu führen. Wenn immer möglich sind Tests mit anonymisierten oder pseudonymisierten Daten durchzuführen.

8.16 Auslagerung von Datenbearbeitungen (Outsourcing)

Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.

Jeder Outsourcing-Vertrag enthält mindestens Regelungen zu folgenden Themen:

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich)
- Verfügungsmacht (immer beim öffentlichen Organ)
- Zweckbindung (Daten dürfen nur für Vertragszwecke bearbeitet werden)
- Bekanntgabe von Informationen (Voraussetzungen für Bekanntgabe an Dritte)
- Geheimhaltungsverpflichtungen (Hinweis auf Amtsgeheimnis)
- Rechte Betroffener (Umgang mit Auskunftsbegehren)
- Informationssicherheitsmassnahmen (organisatorisch/technisch)
- Kontrollmöglichkeit des öffentlichen Organs oder externer Prüfstellen
- Unterauftragsverhältnisse (Offenlegung, Änderung nur mit Bewilligung)
- Entwicklung und Wartung (Regelung für den Beizug Dritter)
- Orte der Datenbearbeitung (Schweiz, Ausland mit gleichwertigem Datenschutzniveau, ansonsten Schutz durch zusätzliche Massnahmen)
- Cloud Computing, wo angeboten (den zusätzlichen Risiken angepasste Massnahmen)
- Sanktionen (Konventionalstrafe für schwere Vertragsverletzungen)
- Vertragsdauer und Voraussetzungen der Vertragsauflösung
- Verhältnis zu Allgemeinen Vertragsbedingungen, soweit vorhanden (Vorrang des Vertrages)
- Anwendbares Recht (schweizerisches Recht)
- Gerichtsstand (schweizerischer Gerichtsstand im Kanton Zürich)

Für ausgelagerte Leistungen und Produkte werden Service Level Agreements abgeschlossen. Sie definieren und quantifizieren:

- Inbegriffene Leistungen und Produkte
- Mengengerüste, Kapazität, Anzahl Transaktionen etc.
- Betriebszeiten
- Maximale Ausfalldauer pro Vorfall (Recovery Time Objective RTO)
- Maximaler Datenverlust bei einem Ausfall (Recovery Point Objective RPO)
- Supportzeiten
- Reaktions- und Umsetzungszeiten
- Lösungszeiten
- Kommunikationspartner und Eskalationspfad
- Im Preis inbegriffene Leistungen, Verrechnungseinheiten, Preise für weitere Leistungen
- Kontrollmittel zur Überwachung der Leistungen
- Notfallszenarien und -massnahmen

8.17 Umgang mit Informationssicherheitsvorfällen

Bei Informationssicherheitsvorfällen erfolgt durch die bzw. den ISV eine Klassifizierung und wenn nötig sofortige Rapportierung an die Gemeindeschreiberin / den Gemeindeschreiber. Entsprechende interne Prozesse und Verfahren für Meldung, Aufnahme von Beweismitteln zwecks rechtlicher und/oder disziplinarischer Massnahmen sowie eine angemessene Eskalation sind geregelt (siehe dazu auch Notfallkonzept).

Mögliche Informationssicherheitsvorfälle sind (nicht abschliessend):

- Verlust, unberechtigte bzw. unbeabsichtigte Löschung oder Vernichtung von Daten, Kopien von Daten oder von Datenträgern
- Veränderung oder Manipulation von Informationen
- Unberechtigter Zugriff oder Bekanntgabe an Unbefugte
- Funktionalität eines oder mehrerer Informationssysteme gestört oder nicht mehr vorhanden

Bei meldepflichtigen Informationssicherheitsvorfällen (Gefährdung von Grundrechten durch die unbefugte Bearbeitung oder den Verlust von Personendaten) wird der Gemeindeschreiberin / dem Gemeindeschreiber unverzüglich nach Bekanntwerden des Vorfalls bei der Datenschutzbeauftragten Meldung erstattet (§12 IDG). Sofern nicht bereits erfolgt, ist mit der Datenschutzbeauftragen über den Einbezug der Kantonspolizei zu entscheiden. Bei Zweifeln über das Vorliegen einer Meldepflicht erfolgt eine unverzügliche Kontaktaufnahme mit der Datenschutzbeauftragten. Im Notfallkonzept sind mögliche Informationssicherheitsvorfälle und Massnahmen zu definieren.
Alle Informationssicherheitsvorfälle werden nachvollziehbar dokumentiert. Die Informationen sind als vertraulich zu betrachten.

8.18 Drucker, Kopierer und Multifunktionsgeräte

Drucker, Kopierer und Multifunktionsgeräte können eine Vielzahl von vertraulichen Daten speichern. Standort und Berechtigungen auf solchen Geräten werden daher entsprechend sorgfältig gewählt, so dass keine Daten durch Dritte eingesehen werden können.

Es ist sichergestellt, dass die Geräte einen möglichst hohen Sicherheitsstandard aufweisen bzw. so sicher wie möglich konfiguriert werden.

Mit den Lieferanten der Geräte werden Wartungsverträge und Datenschutzbestimmungen vereinbart.

Wenn Geräte die Räumlichkeiten der Gemeinde verlassen, wird sichergestellt, dass sich darauf keine Daten mehr befinden.

8.19 Besprechungs- und Schulungsräume

Bei der Benutzung von allgemeinen Räumen (z.B. Besprechungs-, Veranstaltungs- und Schulungsräumen) ist darauf zu achten, dass nach Verlassen darin keine vertraulichen Informationen zurückbleiben.

Besucher der Verwaltung sind jeweils ausserhalb der öffentlich zugänglichen Bereiche und der WC-Anlage zu begleiten und zu beaufsichtigen.

Schulungs- und Präsentationscomputer sind mit demselben Sicherheitsniveau aufzusetzen wie interne Systeme. Sie sind zudem speziell gegen Diebstahl zu sichern und bei jedem Verlassen zu sperren. Wenn möglich ist ein separates Netzwerksegment zu bilden.

Es ist speziell darauf zu achten, dass in solchen Räumen fremde Systeme nicht am internen Netzwerk angeschlossen werden können.

8.20 Aufbewahrung und Archivierung

Informationen, die für das Verwaltungshandeln nicht mehr benötigt werden, werden während höchstens zehn Jahren weiter aufbewahrt. Eine längere Aufbewahrungsdauer wird nur in Fällen angewendet, in denen abweichende gesetzliche Fristen zur Anwendung kommen. Die Begründung für die Wahl einer längeren Aufbewahrungsfrist wird dokumentiert.

Nach Ablauf der Aufbewahrungsfrist werden die Informationen dem zuständigen Archiv angeboten. Allen mit der Aufbewahrung von Informationen betrauten Mitarbeitenden ist bekannt, an welches Archiv die Informationen anzubieten sind.

Informationen, die vom zuständigen Archiv nicht übernommen werden, sind endgültig zu löschen bzw. ordnungsgemäss zu vernichten.

8.21 Risikoanalyse / Notfallplanung

Für die Gemeinde wird eine Auswirkungs- und Bedrohungsanalyse geführt. Es werden gemäss der Risikoabschätzung geeignete Massnahmen definiert und umgesetzt.

Die Risikoanalyse dient ebenfalls als Grundlage für das Notfallkonzept der Gemeinde. Das Notfallkonzept beschreibt die Notfallplanung für Geschäftsprozesse und/oder Ressourcen (Schutzobjekte), um die Aufrechterhaltung und Wiederherstellung der ordnungsmässigen Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.
Die Notfallmassnahmen sind regelmässig und bei veränderten Rahmenbedingungen zu überprüfen und zudem regelmässig zu testen.

Details sind im Notfallkonzept und der Auswirkungs- und Bedrohungsanalyse zu finden.

9 Schlussbestimmungen

Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und/oder personalrechtliche Konsequenzen haben.

Namens des Gemeinderates

Reto Grau	Adrian Hauser
Gemeindepräsident	Gemeindeschreiber

Vom Gemeinderat mit Beschluss vom 21. November 2023 auf den 1. Januar 2024 in Kraft gesetzt.