dsb
datenschutzbeauftragte
des kantons zürich

Anleitung

Aufbau und Organisationsstruktur Informationssicherheit in Gemeinden

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

Datenschutz mit Qualität

1 Einleitung

Die Organisation, die zur Planung, Um- und Durchsetzung sowie Aufrechterhaltung des Informationssicherheitsprozesses erforderlich ist, wird als Informationssicherheitsorganisation bezeichnet.

Dieses Dokument beschreibt den Aufbau einer Informationssicherheitsorganisation für Gemeinden ab 6000 Einwohnerinnen und Einwohner. Es zeigt, welche Dokumente dazu erstellt und wie diese angepasst werden müssen. Als Grundlage dient die durch die Gemeinde vorgängig verfasste Leitlinie zur Informationssicherheit.

Im Folgenden werden die zentralen Rollen des Informationssicherheitsprozesses beschrieben. Die Informatikverantwortlichen (IT-Verantwortliche), die insbesondere den geordneten Betrieb sicherstellen, werden ausgeklammert.

Die Anleitung «Aufbau und Organisationsstruktur Informationssicherheit» ist Teil einer Vorlagenreihe, die sämtliche relevanten Informationssicherheitsdokumente umfasst. Die empfohlene Vorgehensweise, die Hilfestellungen und die Erläuterungen zu den Vorlagen sind dem Leitfaden «Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000» zu entnehmen.

Der Leitfaden «Informationssicherheit in Gemeinden – Bevölkerungszahl < 6000», die Vorlagen und weitere Dokumente sind auf www.datenschutz.ch publiziert.

2 Zweck der Informationssicherheitsorganisation

Das von einer Gemeinde angestrebte Informationssicherheitsniveau kann nur erreicht werden, wenn der Informationssicherheitsprozess gemeindeweit umgesetzt wird. Dieser übergreifende Charakter des Informationssicherheitsprozesses macht es notwendig, Rollen fest-zulegen und diesen die entsprechenden Aufgaben zuzuweisen. Die Informationssicherheitsorganisation ermöglicht diesen Prozess und erlaubt der Gemeinde, das angestrebte Informationssicherheitsniveau zu erreichen und aufrechtzuerhalten.

3 Rollen

Im Rahmen der Informationssicherheitsorganisation sind die folgenden Rollen massgebend:

- die Gemeindeschreiberin / der Gemeindeschreiber
- die Datenschutzberaterin / der Datenschutzberater
- die / der Informationssicherheitsverantwortliche
- die Daten- und Anwendungsverantwortlichen
- die Mitarbeitenden und die Lernenden

3.1 Gemeindeschreiberin / Gemeindeschreiber

Diese tragen die Gesamtverantwortung für die Informationssicherheit in der Gemeinde. Sie werden regelmässig von den Informationssicherheitsverantwortlichen über den Stand der Informationssicherheit informiert.

3.1.1 Aufgaben

- Leitlinie zur Informationssicherheit festlegen
- Für die Informationssicherheit erforderliche Massnahmen und Mittel genehmigen

3.1.2 Anforderungen an die Unabhängigkeit

- Sollen nicht Informationssicherheitsverantwortliche sein
- Sollen nicht Datenschutzberaterin / Datenschutzberater sein

3.2 Datenschutzberaterin / Datenschutzberater

Der Datenschutz und die Informationssicherheit sind für alle Systeme und Prozesse, mit denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Es ist deshalb empfehlenswert, eine interne Spezialistin oder einen internen Spezialisten zu ernennen, der sich um Datenschutzfragen kümmert. Sie respektive er arbeitet in dieser Rolle eng mit den Informationssicherheitsverantwortlichen zusammen.

3.2.1 Aufgaben

- Transparenz in der Datenbearbeitung schaffen
- Mitarbeitende über die datenschutzrechtlichen Anforderungen instruieren
- Im Bereich des Datenschutzes beraten
- Ansprechpersonen für Betroffene (Auskunfts- und Löschbegehren) sein
- Interne und externe Ansprechpersonen bei Datenschutzfragen sein
- Notwendigkeit einer Vorabkontrolle durch die Datenschutzbeauftragte überprüfen

3.2.2 Anforderungen

- Gesetz (IDG, LS 170.4) und Verordnung (IDV, LS 170.41) über die Information und den Datenschutz kennen
- Wichtigste Fachausdrücke der Informationssicherheit kennen
- Prozesse und Abläufe in der Gemeinde kennen
- Fähigkeit haben, den Mitarbeitenden die datenschutzrechtlichen Voraussetzungen zu vermitteln
- Organisatorische Fähigkeiten haben, um datenschutzrelevante Massnahmen zu planen und umzusetzen

3.2.3 Anforderungen an die Unabhängigkeit

- Sollen nicht Gemeindeschreiberin oder Gemeindeschreiber sein
- Sollen nicht Informationssicherheitsverantwortliche sein

3.3 Informationssicherheitsverantwortliche / -verantwortlicher

Die Informationssicherheitsverantwortlichen tragen die Verantwortung für die Umsetzung der Leitlinie zur Informationssicherheit. Sie koordinieren sämtliche Aktivitäten im Bereich der Informationssicherheit.

3.3.1 Aufgaben

- Zuständigkeit für Initialisierung, Überwachung und Kontrolle der Leitlinie zur Informationssicherheit
- Sicherheitsvorgaben (Leitlinie zur Informationssicherheit, Informationssicherheitskonzept, Weisungen, Merkblätter usw.) erstellen, überarbeiten und überprüfen
- Abweichungen vom Sicherheitsstandard (evtl. in Absprache mit der Gemeindeschreiberin / dem Gemeindeschreiber) genehmigen und das Restrisiko dokumentieren
- Erste Ansprechpersonen der Gemeinde für Informationssicherheitsfragen sein
- Der Gemeindeschreiberin / dem Gemeindeschreiber über den Stand der Informationssicherheit berichten
- Mitarbeitende und Leitung in Fragen der Informationssicherheit beraten
- Projekte aus Sicht der Informationssicherheit begleiten und prüfen
- Die Gemeindeschreiberin / den Gemeindeschreiber über zu treffende, budgetrelevante Informationssicherheitsmassnahmen informieren und eine Entscheidung herbeiführen
- Den Fortschritt der Realisierung von Informationssicherheitsmassnahmen kontrollieren

- Kontrollen über die Wirksamkeit von Informationssicherheitsmassnahmen im laufenden Betrieb planen und durchführen (zum Beispiel Schwachstellenanalysen) und daraus Massnahmen ableiten
- Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit koordinieren
- Die Daten- und Anwendungsverantwortlichen bestimmen
- Sicherheitsrelevante Informationen beschaffen und bewerten
- Inventar über die Schutzobjekte führen

3.3.2 Anforderungen

- Einen Überblick über die Aufgaben und Ziele der Gemeinde haben
- Sich mit den Zielsetzungen der Informationssicherheit identifizieren
- Kooperations- und Teamfähigkeit
- Fähigkeit zum selbstständigen Arbeiten
- Durchsetzungsvermögen
- Erfahrungen im Projektmanagement

3.3.3 Anforderungen an die Unabhängigkeit

- Sollen nicht Gemeindeschreiberin / Gemeindeschreiber sein
- Sollen nicht IT-Verantwortliche / IT-Verantwortlicher sein

3.3.4 Geeignete Kandidatin / geeigneter Kandidat

- Abteilungsleiterin oder Abteilungsleiter

3.4 Daten- und Anwendungsverantwortliche

Für alle Informationen, Anwendungen und IT-Komponenten muss festgelegt werden, wer für deren Sicherheit verantwortlich ist. Hierfür ist je eine Person (inklusive Vertretung) zu bestimmen.

3.4.1 Aufgaben

- Sicherstellen, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt
- Verantwortlichkeit für den sicheren Betrieb der Anwendung (Vertraulichkeit und Integrität der Datensammlungen, Verfügbarkeit der Anwendung und Datensammlungen)
- Bestimmen, wer auf die Anwendung in welcher Form Zugriff hat
- Massnahmen für die Informationssicherheit und deren Kontrolle regeln
- Verantwortlichkeit für die Dokumentation der Sicherheitsvorkehrungen
- Informationssicherheitsverantwortliche über nicht behebbare Schwachstellen informieren
- Notfallpläne für längere Ausfälle erstellen
- Informationsstelle bezüglich der in ihrem Verantwortungsbereich liegenden Anwendung sein
- Informationsstelle bezüglich der in ihrem Verantwortungsbereich liegenden Datensammlung sein
- Inhalte der Datensammlung bestimmen
- Daten klassifizieren, die in ihrem Verantwortungsbereich bearbeitet werden (Vertraulichkeit, Integrität, Verfügbarkeit)
- Erfüllung der Datenschutz- und Informationssicherheitsbestimmungen kontrollieren
- Zugriffsrechte bezüglich der in ihrem Verantwortungsbereich liegenden Daten verwalten
- Verantwortlichkeit für die Bearbeitung (inklusive Bekannt- und Weitergabe), Archivierung oder Vernichtung der in ihrem Verantwortungsbereich liegenden Daten

3.4.2 Geeignete Kandidatin / geeigneter Kandidat

- Bei Hauptapplikationen: Abteilungsleiterin oder Abteilungsleiter
- Bei übergreifenden Applikationen: IT-Verantwortliche oder IT-Verantwortlicher

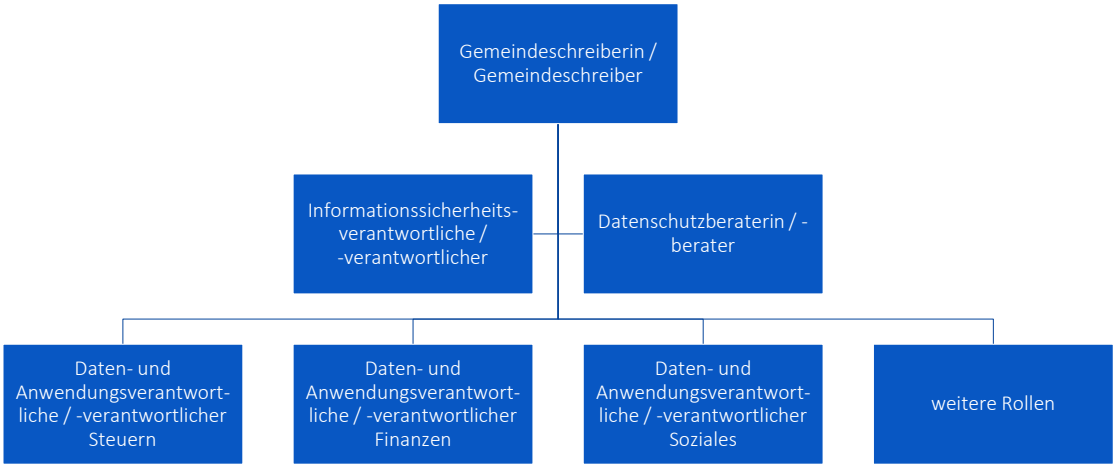
3.5 Mitarbeitende und Lernende

Informierte und geschulte Benutzerinnen sowie Benutzer sind Voraussetzung dafür, dass die Gemeinde die gesteckten Informationssicherheitsziele erreichen kann. Auf die Weiterbildung ist deshalb besonderes Gewicht zu legen.

3.5.1 Aufgaben

- Eine Kultur des sicheren Umgangs mit Informationen und IT-Mittel pflegen
- Regelungen und Anordnungen der Benutzerrichtlinien kennen und befolgen
- Vorfälle mit Auswirkung auf die Informationssicherheit unverzüglich den Informationssicherheits-verantwortlichen oder dem Helpdesk melden

4 Organigramm der Informationssicherheitsorganisation (Beispiel)



Die Struktur soll diejenige einer Stabsstelle sein, um den zentralen Rollenträgerinnen und Rollenträgern den direkten Zugang zu den Daten- und Anwendungsverantwortlichen zu gewährleisten.

5 Umsetzung der Informationssicherheitsorganisation

- Auswahl Kandidatinnen und Kandidaten

Für eine Rolle geeignete Mitarbeitende sind auszuwählen. Nur für eine Rolle qualifizierte Mitarbeitende gewährleisten eine optimale Aufgabenerfüllung.

- Dokumentation der Rollenzuteilung

Die Aufgaben der am Sicherheitsprozess beteiligten Mitarbeitenden sind dokumentiert. Idealerweise werden die Aufgaben in der Stellenbeschreibung festgehalten. Es ist ein Pensum festzulegen.

- Ausbildungsmassnahmen

Die Mitarbeitenden benötigen für ihre Aufgaben entsprechendes Fachwissen und müssen ausgebildet werden (zum Beispiel durch den Besuch von Weiterbildungsveranstaltungen).

6 Links

Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland

- ISMS.1.A6: Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
- ORP.1.A2: Zuweisung der Zuständigkeiten

V 4.2 / März 2021