dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Datenschutzreview mit Selbst-deklaration für Gemeinden und Städte

Inhalt

1 Einleitung 3

2 Übersicht Ablauf 3

3 Phasen des Datenschutzreviews mit Selbstdeklaration 4

3.1 Begrüssung 4
3.2 Informationsveranstaltung 4
3.3 Selbstdeklaration bearbeiten 4
3.4 Dokumente senden 4
3.5 Erhalt bestätigen 4
3.6 Dokumente prüfen 4
3.7 Abgabe Bericht 4
3.8 Umsetzung der Massnahmen 4
3.9 Umsetzung neuer Anforderungen 4
3.10 Periodische Überprüfung und Bestätigung 5

4 Dokumente und Vorlagen 5

4.1 Leitfaden Datenschutzreview mit Selbstdeklaration (dieses Dokument) 5
4.2 Vorlage Leitlinie zur Informationssicherheit 6
4.3 Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz 6
4.4 Vorlage Technische Richtlinie für den Betrieb von Informationssystemen 6
4.5 Vorlage Weisung zur Informationssicherheit und zum Datenschutz 7
4.6 Vorlage Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit 7
4.7 Vorlage Rollen- und Berechtigungskonzept 7
4.8 Vorlage Sensibilisierung Informationssicherheit und Datenschutz 8
4.9 Vorlage Betriebsdokumentation 8
4.10 Vorlage Notfallkonzept 8
4.11 Vorlage Bedrohungsanalyse 9
4.12 Vorlage Schutzbedarfsanalyse 9
4.12.1 Anwendungs-/Systemverantwortliche bestimmen 9

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

4.12.2 Schutzstufe zuteilen 9
4.13 Vorlage Umsetzungsbestätigung 10

5 Hilfsmittel Massnahmenplanung und -umsetzung 10

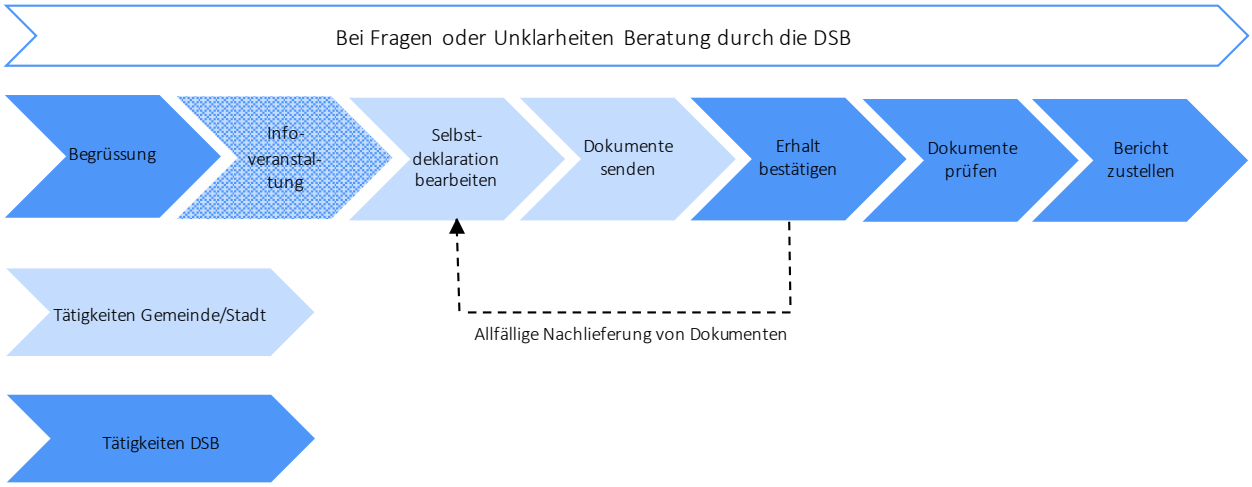
5.1.1 Verantwortliche zuweisen 10
5.1.2 Basis-Sicherheitscheck durchführen 10
5.1.3 Umsetzung planen 11
5.1.4 Revision planen 11

1 Einleitung

Dieser Leitfaden richtet sich an Gemeinden und Städte des Kantons Zürich und hilft bei der Einführung, Umsetzung und Pflege eines nachhaltigen Datenschutzes und der Informationssicherheit. Weiter werden die von der Datenschutzbeauftragten (DSB) zur Verfügung gestellten Anleitungen und Vorlagen erläutert.
Die Digitalisierung durchdringt sämtliche Lebensbereiche und eine Informationsbearbeitung ohne IKT-Unterstützung ist nicht mehr denkbar. Die Risiken nehmen zu und Angriffe auf Systeme häufen sich. Die Themen Datenschutz und Informationssicherheit müssen deshalb bewusst und strukturiert angegangen werden. Ein Risikomanagement, klare Weisungen und effektive Schutzmassnahmen helfen, die Risiken zu mindern.
Die umfassenden Anleitungen und Vorlagen der DSB unterstützen die Städte und Gemeinden bei der Umsetzung der notwendigen Massnahmen unterstützen. Nach der Umsetzung der Massnahmen können die Gemeinden und Städte dies der DSB als Selbstdeklaration melden.
Damit ist gewährleistet, dass die Gemeinden und Städte die Anforderungen des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) einhalten können. Die DSB hat den gesetzlichen Auftrag, die Umsetzung zu kontrollieren.
Das Vorgehen, die Massnahmen und die Empfehlungen richten sich nach den Vorgaben der Allgemeinen und der Besonderen Informationssicherheitsrichtlinien des Kantons Zürich sowie dem international anerkannten Standard des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

2 Übersicht Ablauf

Die Grafik stellt den Ablauf des Datenschutzreviews mit Selbstdeklaration dar. Die einzelnen Schritte werden in diesem Leitfaden erklärt.



3 Phasen des Datenschutzreviews mit Selbstdeklaration

3.1 Begrüssung

Die DSB lädt die Gemeinde/Stadt für den Datenschutzreview mit Selbstdeklaration ein. Die zu prüfenden Organe werden nach verschiedenen, objektiven Kriterien ausgewählt. Die Gemeinden/Städte können sich auch freiwillig für einen Datenschutzreview mit Selbstdeklaration bei der DSB melden.

3.2 Informationsveranstaltung

Die DSB stellt der Gemeinde/Stadt alle erforderlichen Dokumente und Vorlagen zu.
Anschliessend wird in einer Informationsveranstaltung mit Vertreterinnen und Vertretern der Gemeinde/Stadt sowie der DSB das Vorgehen erläutert.
Nach der Informationsveranstaltung eruiert und analysiert die Gemeinde/Stadt die Massnahmen, die umzusetzen sind, um eine vollständige Erfüllung der Anforderungen in den Bereichen Datenschutz und Informationssicherheit zu erreichen. Sie schätzt den erforderlichen Zeitaufwand und meldet der DSB den voraussichtlichen Termin der vollständigen Umsetzung.

3.3 Selbstdeklaration bearbeiten

Die Gemeinde/Stadt setzt die Massnahmen unter Verwendung der Vorlagen um. Die Umsetzung richtet sich nach dem Betriebsmodell der Gemeinde/Stadt und kann auch die Beiziehung von externen Partnern erfordern. Bei Fragen oder Unklarheiten steht die DSB den Gemeinden/Städten zur Verfügung.

3.4 Dokumente senden

Die Gemeinde/Stadt sendet nach der Umsetzung der Massnahmen und Vervollständigung der Vorlagen die Dokumente der DSB zu. Die Betriebsdokumentation und der Massnahmenkatalog müssen nicht eingereicht werden.

3.5 Erhalt bestätigen

Die DSB bestätigt der Gemeinde/Stadt den Erhalt der Dokumente. Fehlende Dokumente werden von der DSB nachgefordert.

3.6 Dokumente prüfen

Die DSB prüft die Dokumente auf Basis von Stichproben.

3.7 Abgabe Bericht

Die DSB erstellt einen Berichtsentwurf. Dieser enthält das Ergebnis, den Umfang und den Inhalt der Überprüfung der Selbstdeklaration sowie, falls nötig, priorisierte Massnahmen. Die Gemeinde/Stadt erhält Gelegenheit, den Inhalt zu überprüfen. Bei Bedarf wird die DSB den Bericht mit der Gemeinde/Stadt besprechen. Danach wird je ein Exemplar des finalen Berichts der Gemeinde/Stadt und dem Bezirksrat zugestellt.

3.8 Umsetzung der Massnahmen

Die Gemeinde/Stadt informiert die DSB zeitnah über die Umsetzung der mit einer Frist versehenen Massnahmen.

3.9 Umsetzung neuer Anforderungen

Die Einhaltung der eingeführten Massnahmen muss von der Gemeinde/Stadt periodisch überprüft werden. Bei Änderungen der Risiken müssen die Massnahmen angepasst werden, beispielsweise infolge neuer Aufgaben der Verwaltung, Änderungen der IKT-Umgebung, des IKT-Betriebs oder der Baulichkeiten. Dies hat durch die Gemeinde/Stadt selbstständig zu erfolgen. Die DSB steht unterstützend zur Verfügung.

3.10 Periodische Überprüfung und Bestätigung

Die DSB kann die Umsetzung der Massnahmen und deren regelmässige Überprüfung durch die Gemeinde/Stadt einer Neuprüfung unterziehen.

4 Dokumente und Vorlagen

Für eine umfassende und integrale Informationssicherheit müssen die erforderlichen Informationssicherheitsdokumente auf der strategischen, taktischen und operativen Ebene erstellt werden. Die nachfolgende Pyramide zeigt die entsprechende Gliederung und Zuweisung der Dokumente in den verschiedenen Ebenen. Idealerweise werden die Dokumente im Top-Down-Ansatz (von oben nach unten) erstellt.

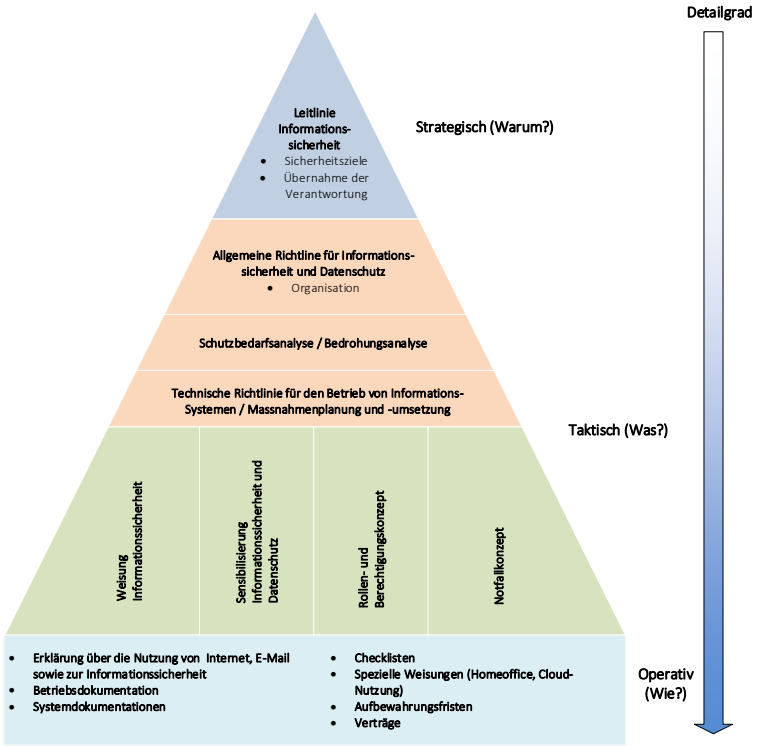


Abbildung 1: Sicherheitspyramide Übersicht Dokumente Informationssicherheit

4.1 Leitfaden Datenschutzreview mit Selbstdeklaration (dieses Dokument)

Der Leitfaden veranschaulicht das Prüfmodell und führt die Gemeinden/Städte durch den Prozess.

Was ist zu tun:

1. Leitfaden durcharbeiten
2. Anforderungen der Schritte und Dokumente umsetzen und bei Unklarheiten die DSB beiziehen

4.2 Vorlage Leitlinie zur Informationssicherheit

Die Sicherheitsstrategie, das angestrebte Sicherheitsniveau sowie die für die Gemeinde/Stadt gültigen Sicherheitsziele müssen definiert und festgehalten werden. Sie bildet das Hauptdokument, das durch die weiteren Vorlagen ergänzt wird.

Was ist zu tun:

1. Layout der Vorlage Leitlinie zur Informationssicherheit an das eigene Corporate Design anpassen
2. Inhalt an die Gegebenheiten der Gemeinde/Stadt anpassen
3. Änderungskontrolle nachführen
4. Leitlinie durch einen Beschluss des Gemeinderats/Stadtrats in Kraft setzen
5. Leitlinie allen Mitarbeitenden kommunizieren und an einem intern zugänglichen Ort publizieren

4.3 Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz

Die Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz enthält die Organisation (Rollen und Verantwortlichkeiten) sowie allgemeine Regelungen der Informationssicherheit und Datenschutz der Gemeinde/Stadt.

Was ist zu tun:

1. Layout der Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz an das eigene Corporate Design anpassen
2. Inhalt an die Gegebenheiten der Gemeinde/Stadt anpassen
3. Änderungskontrolle nachführen
4. Allgemeine Richtlinie für Informationssicherheit und Datenschutz durch die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber genehmigen und in Kraft setzen lassen
5. Anforderungen in Verbindung mit den übrigen Dokumenten der Vorlagenreihe umsetzen

4.4 Vorlage Technische Richtlinie für den Betrieb von Informationssystemen

Die Vorlage Technische Richtlinie für den Betrieb von Informationssystemen enthält die technischen Vorgaben für den Betrieb der IKT-Umgebung. Diese können durch die Gemeinde/Stadt selbst umgesetzt werden oder in Zusammenarbeit mit externen Dienstleistern. Sie sind aus diesem Grund von der Allgemeinen Richtlinie losgelöst.

Was ist zu tun:

1. Layout der Vorlage Technische Richtlinie für den Betrieb von Informationssystemen an das eigene Corporate Design anpassen
2. Inhalt an die Gegebenheiten der Gemeinde/Stadt anpassen
3. Änderungskontrolle nachführen
4. Technische Richtlinie für den Betrieb von Informationssystemen durch die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber genehmigen und in Kraft setzen lassen
5. Anforderungen auf den bestehenden Systemen umsetzen bzw. einen Auftrag für die Umsetzung durch einen oder mehrere IKT-Dienstleister erteilen

4.5 Vorlage Weisung zur Informationssicherheit und zum Datenschutz

Die Vorlage Weisung zur Informationssicherheit und zum Datenschutz richtet sich an die Mitarbeitenden der Gemeinde/Stadt. Sie enthält die Regelungen bezüglich Informationssicherheit und Datenschutz, die bei der Arbeit zu beachten sind.

Was ist zu tun:

1. Layout der Vorlage Weisung zur Informationssicherheit und zum Datenschutz an das eigene Corporate Design anpassen
2. Inhalt an die Gegebenheiten der Gemeinde/Stadt anpassen
3. Änderungskontrolle nachführen
4. Weisung zur Informationssicherheit und zum Datenschutz durch die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber genehmigen und in Kraft setzen lassen
5. Weisung an die Mitarbeitenden bekanntmachen bzw. abgeben
6. Weisung zugänglich machen, z.B. im Intranet

4.6 Vorlage Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit

Mit der Vorlage Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit können sich alle Mitarbeitenden der Gemeinde/Stadt zur Einhaltung der darin aufgeführten Verhaltensregeln verpflichten und dies per Unterschrift bestätigen.

Was ist zu tun:

1. Layout der Vorlage Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit an das eigene Corporate Design anpassen
2. Inhalt an die Gegebenheiten der Gemeinde/Stadt anpassen
3. Änderungskontrolle nachführen
4. Mitarbeitende bezüglich der einzelnen Regelungen instruieren
5. An alle Mitarbeitenden zur Unterschrift verteilen sowie sicherstellen, dass dies bei neu eintretendem Personal ebenfalls erfolgt
6. Erklärungen in den Personaldossiers ablegen
7. Vorlage Erklärung zugänglich machen, z.B. im Intranet

4.7 Vorlage Rollen- und Berechtigungskonzept

Die Vorlage Rollen- und Berechtigungskonzept dient zur Beschreibung und Dokumentation der Berechtigungen von Mitarbeitenden der Gemeinde/Stadt auf die Dateiablage sowie die Anwendungen. Sie stellt sicher, dass die Berechtigungen nach klaren Vorgaben und beschränkt auf die notwendigen Rechte erfolgen.

Was ist zu tun:

1. Layout der Vorlage Rollen- und Berechtigungskonzept an das eigene Corporate Design anpassen
2. Funktionen und Verantwortlichkeiten gemäss Vorlage zuweisen
3. Zugriffsmatrix definieren (Rollen, Gruppen und Zuweisungen)
4. Prozesse für Beantragung, Prüfung, Zuweisung, Kontrolle und Löschung von Berechtigungen und Passwörtern festlegen
5. Änderungskontrolle nachführen
6. Rollen- und Berechtigungskonzept durch die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber genehmigen und in Kraft setzen lassen

4.8 Vorlage Sensibilisierung Informationssicherheit und Datenschutz

Die Vorlage Sensibilisierung Informationssicherheit und Datenschutz enthält verschiedene Module zur Sensibilisierung und Schulung der Mitarbeitenden. Sie sind unterteilt in einen obligatorischen und einen optionalen Teil und setzt sich aus Inhalten für die erstmalige Grundausbildung sowie wiederkehrenden kurzen Ausbildungsblöcke zusammen.

Was ist zu tun:

1. Layout der Vorlage Sensibilisierung Informationssicherheit und Datenschutz an das eigene Corporate Design anpassen
2. Inhalt an die Gegebenheiten der Gemeinde/Stadt anpassen
3. Zielgruppen und Kursleitende für Ausbildungsmodule bestimmen
4. Planung sowie Ausbildungskontrolle für obligatorische und optionale Ausbildungsmodule erstellen
5. Änderungskontrolle nachführen
6. Obligatorische Ausbildungsmodule durchführen
7. Eventuell optionale Ausbildungsmodule durchführen
8. Ausbildungskontrolle nachführen
9. Ausbildungsmodule periodisch prüfen und durchführen, z.B. für neu eintretende Mitarbeitende

4.9 Vorlage Betriebsdokumentation

Die Vorlage Betriebsdokumentation enthält ein Musterinhaltsverzeichnis für die vollständige Dokumentation der IKT-Umgebung. Die Betriebsdokumentation dient der Gemeinde/Stadt und dem Betreiber der IKT-Umgebung zur Übersicht und Kontrolle der Infrastruktur. Sie hilft, die Reaktionszeit bei Ausfällen oder Problemen zu verringern, und ermöglicht es der Gemeinde/Stadt, bei Notfällen oder beim Wechsel des Betreibers unabhängig zu handeln. Die Vorlage Betriebsdokumentation kann als Checkliste zur Prüfung auf Vollständigkeit der bestehenden Betriebsdokumentation verwendet werden. Falls keine Betriebsdokumentation besteht, kann daraus eine Betriebsdokumentation erstellt werden.

4.10 Vorlage Notfallkonzept

Mit der Vorlage Notfallkonzept werden die Bedrohungen/Risiken, welche die Gemeinde/Stadt gefährden können, aufgenommen und bewertet sowie Schutzmassnahmen definiert. Sie enthält Vorgaben für das Vorgehen im Notfall sowie die dazu notwendige Organisation.

Was ist zu tun:

1. Layout der Vorlage Notfallkonzept an das eigene Corporate Design anpassen
2. Notfallorganisation, Funktionen und Kontaktinformationen aufnehmen
3. Notfallinfrastruktur definieren
4. Bedrohungen aufnehmen und bewerten (siehe auch Vorlage Bedrohungsanalyse)
5. Plan für Schutzmassnahmen erstellen
6. Schutzmassnahmen umsetzen und Risiken erneut bewerten
7. Notfallprozesse definieren
8. Kommunikationsplan erstellen
9. Änderungskontrolle nachführen
10. Notfallkonzept den Mitarbeitenden vorstellen
11. Notfalltests und -übungen planen und durchführen
12. Notfallkonzept an verschiedenen Orten (auch physisch) aufbewahren, um im Notfall darauf zugreifen zu können

4.11 Vorlage Bedrohungsanalyse

Die Vorlage Bedrohungsanalyse ist ein Hilfsdokument des Notfallkonzepts. Sie enthält einen vorgegebenen Katalog von Bedrohungen, die im Hinblick auf ihre Eintrittswahrscheinlichkeit sowie Auswirkungen auf die Gemeinde/Stadt beurteilt werden. Aufgrund der Analyse werden geeignete Massnahmen zu deren Verminderung oder Verhinderung definiert.

Was ist zu tun:

1. Bedrohungen gemäss Katalog auf Eintrittswahrscheinlichkeit und Auswirkung beurteilen und Risikostufe festlegen
2. Massnahmen definieren, mit jeweiligen Risiken verknüpfen und Risikostufe nach Massnahme bewerten
3. Massnahmen zur Umsetzung planen und Fortschritt dokumentieren
4. Kommunikationsmatrix erstellen (als Ergänzung zum Notfallkonzept)
5. Änderungskontrolle nachführen
6. Periodische Wiederholung der obigen Schritte, um neue oder veränderte Ausgangslagen zu erkennen

4.12 Vorlage Schutzbedarfsanalyse

Ziel der Schutzbedarfsanalyse ist es, die in Bezug auf das Risiko angemessenen Sicherheitsmassnahmen festzulegen.
Für die Schutzbedarfsanalyse sind alle Anwendungen und IKT-Systeme zu erheben, welche die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen. Zusätzlich zur Auflistung der Anwendungen sind die zugehörigen bearbeiteten Datenarten zu vermerken.

Nr	Funktion / Zweck	Anwendung	Bearbeitete Datenart
A.1	Baugesuchsverwaltung	CMI Bau	Nur Sachdaten
A.2	Scanning Steuererklärungen	ARTS	Personendaten
A.3	Office-Anwendungen	Office 2019	Besondere Personendaten

Abbildung 2: Beispiel Inventar Anwendungen

4.12.1 Anwendungs-/Systemverantwortliche bestimmen

Für alle Anwendungen/Systeme beziehungsweise Daten muss festgelegt werden, wer für ihre Sicherheit verantwortlich ist. Die Aufgaben der Anwendungsverantwortlichen sind in der Allgemeinen Richtlinie für Informationssicherheit und Datenschutz definiert. Die Anwendungsverantwortlichen sind im Register Anwendungen zu hinterlegen.

4.12.2 Schutzstufe zuteilen

Um den Schutzbedarf jeder Anwendung beziehungsweise jedes IKT-Systems und der bearbeiteten Datenarten (Sachdaten, Personendaten, besondere Personendaten) zu beurteilen, sollte die Schutzstufe zugeteilt werden. Die Schutzstufe setzt sich aus den Schutzzielen der Daten (Vertraulichkeit, Integrität, Verfügbarkeit) zusammen.

Schutzstufe		
Vertraulichkeit	Integrität	Verfügbarkeit
Hoch	Normal	Hoch
Normal	Normal	Normal
Sehr hoch	Normal	Sehr hoch

Abbildung 3: Schutzstufen

Im Register Schutzstufenzuteilung wird vorerst die Datenart sowie die Zuordnung (Normal, Hoch, Sehr hoch) überprüft und gegebenenfalls angepasst. Anschliessend wird pro Anwendung und je Schutzziel die

Schutzstufe (Normal, Hoch, Sehr hoch) im Register Anwendungen zugeteilt. Danach sind die restlichen Informationen (z.B. Hersteller, Betrieb durch und Datenstandort) zu ergänzen.

4.13 Vorlage Umsetzungsbestätigung

Mit der Vorlage Umsetzungsbestätigung wird der DSB die Umsetzung der Massnahmen gemeldet, die in den verschiedenen Vorlagen beschrieben sind. Allfällige Ausnahmen sind im Formular mit einer Begründung anzugeben.

Was ist zu tun:

1. Layout der Vorlage Umsetzungsbestätigung an das eigene Corporate Design anpassen
2. Formular ausfüllen, allenfalls Angabe von Ausnahmen und einer Begründung
3. Formular unterschreiben lassen durch Gemeindeschreiber/in oder Stadtschreiber/in
4. Formular und sämtliche aufgeführten Dokumente der Umsetzungsbestätigung sind an die DSB des Kantons Zürich zustellen

5 Hilfsmittel Massnahmenplanung und -umsetzung

Zur Planung von Sicherheitsmassnahmen stellt die DSB für Gemeinden/Städte mit mehr als 6000 Einwohnerinnen und Einwohner den Massnahmenkatalog zur Verfügung. Für Gemeinden mit weniger als 6000 Einwohnerinnen und Einwohner steht der Minimummassnahmenkatalog zur Verfügung. Diese basieren auf dem IT-Grundschutzkatalog des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Der Massnahmenkatalog beziehungsweise der Minimummassnahmenkatalog unterstützt die Gemeinde/Stadt bei der Umsetzung und Kontrolle der Informationssicherheitsmassnahmen.

Jeder Massnahme ist eine eindeutige Nummer zugeordnet (z.B. ISMS.1.A1). Die vollständige Beschreibung der Massnahme kann über das BSI abgerufen werden.

5.1.1 Verantwortliche zuweisen

Die DSB empfiehlt Gemeinden/Städten mit mehr als 6000 Einwohnerinnen und Einwohner die Massnahmen der Schutzstufe 2 umzusetzen. Diese sind im Massnahmenkatalog in der Spalte Niveau S2 mit einer «2» gekennzeichnet.
Für Gemeinden mit weniger als 6000 Einwohnerinnen und Einwohner empfiehlt die DSB die Massnahmen der Schutzstufe 1 umzusetzen. Diese sind im Minimummassnahmenkatalog in der Spalte Niveau S1 mit einer «1» gekennzeichnet.

Sicherheitsmassnahmen werden nur plangemäss umgesetzt, wenn die Verantwortlichkeiten festgelegt sind. Diese können in der Spalte Verantwortung dokumentiert werden.

Was ist zu tun:

1. Massnahmenkatalog/Minimummassnahmenkatalog nach Niveau S2 beziehungsweise Niveau S1 filtern
2. Für jede Sicherheitsmassnahme die oder der umsetzungsverantwortliche Mitarbeitende beziehungsweise Auftragnehmende eintragen

5.1.2 Basis-Sicherheitscheck durchführen

Beim Basis-Sicherheitscheck wird geprüft, ob die Massnahmen gemäss Niveau S2 beziehungsweise Niveau S1 bereits umgesetzt wurden oder ob Sicherheitsmassnahmen fehlen. Dieser Check wird anhand von Unterlagen, Gesprächen mit Verantwortlichen sowie stichprobenartigen Überprüfungen vor Ort ermittelt. Werden Dienstleistungen durch externe Auftragnehmende erbracht, ist die Gemeinde/Stadt dafür verantwortlich, dass die erforderlichen Sicherheitsmassnahmen umgesetzt sind.

Im Massnahmenkatalog stehen vier Möglichkeiten zur Verfügung, um den Umsetzungsgrad der Massnahmen in der Spalte Umsetzung zu dokumentieren:

- Ja – wenn alle in der Massnahme genannten Anforderungen vollständig umgesetzt sind.
- Teilweise – wenn einige, aber nicht alle Anforderungen umgesetzt sind.
- Nein – wenn keine oder nahezu keine der Anforderungen umgesetzt sind.
- Entbehrlich – wenn die Massnahme nicht benötigt wird, weil mindestens gleichwertige alternative Massnahmen umgesetzt wurden oder weil das Objekt nicht vorhanden ist, das durch die Massnahme geschützt werden soll.

Was ist zu tun:

1. Status der Massnahmen bestimmen und in der Spalte Umsetzung dokumentieren. Wird bei einer Massnahme der Status Entbehrlich gewählt, so ist dies im Feld Bemerkung zu begründen.
2. Bei einer umgesetzten Massnahme ist die Spalte Nachweisdokument auszufüllen. Darin ist auf das Dokument zu verweisen, das die umgesetzte Massnahme beschreibt.
3. In der Spalte Betroffene IKT-Systeme sind die Systeme zu dokumentieren, die für die Massnahme anwendbar sind.
4. Bei Bedarf die restlichen Spalten nachführen
5. Massnahmenumsetzung bei den Verantwortlichen in Auftrag geben

5.1.3 Umsetzung planen

Die Umsetzung der noch nicht vorhandenen Massnahmen (Umsetzung: Teilweise/Nein) muss geplant werden. Dabei ist die Spalte Umsetzungstermin abzufüllen. Bei Bedarf sind zusätzlich die Priorität und Kosten einzutragen.

5.1.4 Revision planen

Bei der Durchführung von Revisionen kann der Massnahmenkatalog/Minimummassnahmenkatalog zur Unterstützung beigezogen werden. Bei jeder Massnahme kann der Termin der letzten und der nächsten Revision sowie die verantwortliche Revisorin beziehungsweise der verantwortliche Revisor dokumentiert werden. Der Status aller Massnahmen sollte mindestens alle drei Jahre überprüft werden.

V 2.1 / Dezember 2023