Stadt Bülach

Allgemeine Richtlinie für Informationssicherheit und Datenschutz der Stadt Bülach

Inkraftsetzung: 1. März 2022

Version	Datum	Beschreibung, Bemerkung	Name
1.1	01.01.2022	Verabschiedung durch den SR	Wanner Markus

Inhaltsverzeichnis

1. Einleitung

Die Stadt Bülach 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 Stadtrat diese allgemeine Richtlinie. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Stadt Bülach angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Richtlinie eine Beschreibung der Informationssicherheitsorganisation. Die Geschäftsleitung regelt auf der Grundlage der «Allgemeinen Richtlinie für Informationssicherheit und Datenschutz» weitere Bestimmungen in der «Weisung zur Informationssicherheit und Datenschutz».

2. Allgemeine Bestimmungen

2.1 Gegenstand und Zweck

Diese Richtlinie regelt die Ziele, die Organisation und die allgemeinen Vorgaben in Bezug auf Datenschutz und Informationssicherheit sowie die Prozesse zu deren kontinuierlichen Verbesserung.

Sie ist angelehnt an die allgemeine und besondere Informationssicherheitsrichtlinie des Kantons Zürich sowie weitere Vorlagen und Dokumente, welche im Rahmen des Datenschutzreviews mit Selbstdeklaration durch die Datenschutzbeauftragte des Kanton Zürichs zur Verfügung gestellt wurden.

Ausnahmen zu den in dieser Richtlinie definierten Vorgaben sind durch die Geschäftsleitung bewilligen zu lassen.

2.2 Geltungsbereich

Die «Allgemeine Richtlinie für Informationssicherheit und Datenschutz» und die damit zusammenhängenden Dokumente gelten für alle Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung und der Primarschule der Stadt Bülach.

2.3 Grundlagen

Die gesetzlichen Grundlagen für die Stadt Bülach sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- 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 (insbesondere im Personalrecht) zu beachten.

3. Informationssicherheitsniveau

Die Massnahmen zur Sicherstellung von Datenschutz und Informationssicherheit sind auf einen erhöhten Schutzbedarf auszurichten. Diese Einstufung erfolgt aufgrund

- der Tatsache, dass die Stadt Bülach 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 Stadt Bülach
- der Unterstützung aller wesentlichen Funktionen und Aufgaben durch ICT- und Netzwerksysteme,
- der Tatsache, dass ein Ausfall von ICT- und Netzwerksystemen die Aufgabenerfüllung nicht 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 sind sich ihrer Verantwortung beim Umgang mit Informationen, ICT-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

5.1 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 Geschäftsleitung, die oder der Informationssicherheitsverantwortliche (nachfolgend ISV) und die für die einzelnen Bereiche zuständigen Anwendungs- und Datenverantwortliche (nachfolgend ADV) haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeiterinnen und Mitarbeiter sind die Voraussetzung dafür, dass die gesteckten Informationssicherheitsziele erreicht werden können. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.

Die Informationssicherheitsorganisation ist im Anhang A – Organigramm der Informationssicherheitsorganisation - definiert.

5.2 Stadtrat

Der Stadtrat trägt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz. Er nimmt die «Allgemeine Richtlinie für Informationssicherheit und Datenschutz» ab, setzt diese in Kraft und genehmigt die für die Informationssicherheit und Datenschutz erforderlichen Massnahmen und Mittel.

5.3 Geschäftsleitung

Die Geschäftsleitung trägt die operative Verantwortung für die Informationssicherheit. Sie bestimmt eine verantwortliche Person für die Informationssicherheit, Anwendungs- und Datenverantwortliche/r sowie eine/n Datenschutzberater/in und stellt sicher, dass die Beschlüsse des Stadtrats zur Informationssicherheit umgesetzt werden.

5.4 Informationssicherheitsverantwortliche/r (ISV)

Zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus wird durch die Geschäftsleitung eine Person bestimmt, die für die Informationssicherheit verantwortlich ist. Sie ist für die Umsetzung der Sicherheitsrichtlinien und deren Kontrolle verantwortlich und berichtet in dieser Funktion direkt der ihr oder ihm vorgesetzten Stelle und der Geschäftsleitung.

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 ICT-Benutzerinnen und ICT-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 ISV 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 und Verantwortung werden in der Weisung zur Informationssicherheit und zum Datenschutz festgelegt.

5.5 Anwendungs- und Datenverantwortliche/r (ADV)

Für alle Prozesse, Daten, Anwendungen, ICT- und Netzwerksysteme wird eine verantwortliche Person benannt. Diese definiert und setzt seine Verantwortlichkeiten in enger Absprache mit der/dem ISV um. Aufgaben und Verantwortung werden in der Weisung zur Informationssicherheit und zum Datenschutz festgelegt.

5.6 Datenschutzberater/in

Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Die Geschäftsleitung trägt die Gesamtverantwortung für den Datenschutz. Sie weist die Rolle Funktion Datenschutzberaterin / Datenschutzberater einer verantwortlichen Person zu. Diese arbeitet in ihrer Rolle eng mit der bzw. dem ISV zusammen und ist interne Ansprechperson bei Datenschutzfragen. Aufgaben und Verantwortung werden in der Weisung zur Informationssicherheit und zum Datenschutz festgelegt.

5.7 Vorgesetzte

Die Vorgesetzten bilden eine wichtige Schnittstelle zwischen der Geschäftsleitung und den Mitarbeiterinnen und Mitarbeitern und verfügen in ihrem Fachbereich über spezialisiertes Wissen. Aufgaben und Verantwortung werden in der Weisung zur Informationssicherheit und zum Datenschutz festgelegt.

5.8 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. Die Aufgaben werden in der Weisung zur Informationssicherheit und zum Datenschutz festgelegt.

6. Regelung von Ausnahmen

Die oder der ISV entscheidet über sicherheitsrelevante Fragen und Ausnahmen und verwaltet allfällige Ausnahmen.

7. Kontinuierliche Verbesserung der Informationssicherheit

Die Geschäftsleitung unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Er gibt mit der periodischen Überarbeitung dieser Richtlinie zur

Informationssicherheit und Datenschutz und den dazugehörigen Richtlinien und Weisungen die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung vor. Die Richtlinie wird alle 1 - 3 Jahre überprüft.

Die umgesetzten organisatorischen und technischen Massnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit werden regelmässig alle 1-2 Jahre sowie zusätzlich bei Projekten mit grosser Auswirkungen auf die Aktualität und die Wirksamkeit durch die zuständige interne Stelle geprüft. Bei Bedarf kann eine externe Stelle beigezogen werden. 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 eine Reihe von Massnahmen zu den Bereichen:

- Mobiles Arbeiten und mobile Geräte
- Personalsicherheit
- Schulungsmassnahmen in Informationssicherheit
- Verschlüsselungsmassnahmen
- Verwaltung von organisationseigenen Werten
- Informationshandhabung und Datenschutzfolgenabschätzung
- Identitäts-/Zugriffskontrollen und Passwörter
- Physische Sicherheit und Schutz vor Umwelteinflüssen
- Sicherheit von Informationssystemen
- Datensicherung und -wiederherstellung
- Protokollierung Verwaltung der Netzwerksicherheit
- Sicherheit von Testdaten
- Umgang mit Informationssicherheitsvorfällen
- Wechselmedien und Multifunktionsgeräte
- Allgemein zugängliche Räume
- Aufbewahrung und Archivierung
- Risikoanalyse / Notfallplanung

Für die Präzisierung und Umsetzung der Massnahmen ist die Geschäftsleitung verantwortlich.

9. 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.

Bei Cloud-Lösungen wird nach den Vorgaben der Datenschutzbeauftragten des Kantons Zürich vorgegangen.

10. Einhaltung der Richtlinie

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

11. Genehmigung und Inkraftsetzung

Diese Richtlinie wurde am 23. Februar 2022 von Stadtrat verabschiedet und tritt am 1. März 2022 in Kraft.

12. Anhang

Funktions-Organigramm der Informationssicherheitsorganisation: