Informationssicherheitspolitik der Stadt Zürich

1 Zweck

Die Informationssicherheitspolitik legt die Ziele und die Grundsätze der Informationssicherheit für die Stadt Zürich fest und definiert die Rollen bezüglich der Informationssicherheit und die damit verbundenen Verantwortungen. Sie bildet die verbindliche Grundlage für die Definition, Entwicklung, Implementierung und Überprüfung von Sicherheitsmassnahmen sowie für den Aufbau der Sicherheitsorganisation.

2 Geltungsbereich und Abgrenzung

Die Informationssicherheitspolitik kommt immer dann zur Anwendung, wenn im Sinne des IDG[1] § 3[2] Informationen zur Erfüllung einer öffentlichen Aufgabe bearbeitet werden. Sie dient der Umsetzung von IDG § 7[3].

Die Informationssicherheitspolitik gilt für die gesamte Stadtverwaltung. Darunter fallen:

- Gemeinderat und Stadtrat
- allgemeine Verwaltung der Stadt Zürich
- Departemente, Dienstabteilungen der Stadt Zürich
- die zur Stadt Zürich gehörenden Stiftungen, Behörden und selbständigen öffentlich-rechtlichen Anstalten

In der Folge Organisationseinheiten genannt.

Bei Zusammenarbeit mit Dritten, müssen die Verbindlichkeiten bezüglich der Informationssicherheit in schriftlicher Form geregelt werden. Dies gilt auch für alle anderen natürlichen und juristischen Personen, die die ICT-Infrastruktur der Stadtverwaltung benutzen.

3 Definition der Informationssicherheit

Informationssicherheit behandelt den Schutz von Informationen unabhängig davon, in welcher Form sie vorliegen (elektronisch, physisch, mündlich).

Informationen sind sicher, wenn gewährleistet ist, dass:

1. Informationen nur von den Personen eingesehen und bearbeitet werden können, für die sie bestimmt sind – **Vertraulichkeit**
2. die Informationen vollständig, korrekt und nicht verfälscht sind – **Integrität**
3. alle Informationen den Benutzenden und den Geschäftsprozessen zur richtigen Zeit und mit der vereinbarten Leistung zur Verfügung stehen – **Verfügbarkeit**
4. nachvollzogen und bei Bedarf nachgewiesen werden kann, wer wann welche Änderung an den Informationen vorgenommen hat –**Verbindlichkeit**

Die Stadtverwaltung definiert Informationssicherheit als einen Zustand, in dem alle relevanten und erkennbaren Risiken bezüglich der vorgenannten vier Kriterien auf ein akzeptables Mass reduziert sind.

---

[1] IDG: Gesetz über die Information und den Datenschutz (IDG), LS 170.4

[2] IDG §3: Informationen: Alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. Ausgenommen sind Aufzeichnungen, die nicht fertig gestellt oder die ausschliesslich zum persönlichen Gebrauch bestimmt sind.

[3] IDG § 7: Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.....

4 Ziele der Informationssicherheit

Die Stadt Zürich setzt sich bezüglich Informationssicherheit folgende übergeordnete Ziele:

- Hohe Verfügbarkeit und korrekte Funktionsweise aller informationsverarbeitenden Systeme und Anwendungen, die zum Schutz von Leib und Leben der Bevölkerung benötigt werden
- Sicherstellen der Handlungsfähigkeit der Stadtverwaltung durch adäquaten Schutz aller geschäftskritischen Informationen
- Gewährleistung der Einhaltung aller rechtlichen Anforderungen (Compliance) in Bezug auf Informationssicherheit, insbesondere Persönlichkeits- und Datenschutz
- Verhinderung von Datendiebstahl, Datenmanipulation oder Datenverlust und damit verbundenen Reputationsschäden

5 Grundsätze der Informationssicherheit

5.1 Flächendeckender Basisschutz

Der Basisschutz legt die verbindlichen personellen, organisatorischen und technischen Sicherheitsmassnahmen und –vorgaben für alle Informationen fest, die in und von der Stadtverwaltung Zürich bearbeitet werden.

Der Basisschutz wird im «Handbuch Informationssicherheit der Stadt Zürich» definiert und orientiert sich an den international anerkannten ISO/IEC-Standards 27001/27002.

Der Basisschutz ist in der Stadtverwaltung flächendeckend umzusetzen.

5.2 Verantwortung für Informationssicherheit

In der Stadtverwaltung ist jede Organisationseinheit in ihrem Verantwortungsbereich verantwortlich für die sichere Verarbeitung von Informationen.

Alle Mitarbeitenden der Stadtverwaltung haben die Aufgabe, für den Schutz der Informationen zu sorgen und sind verantwortlich für die Einhaltung und Umsetzung der Sicherheitsvorgaben in ihrem Verantwortungsbereich. Diese Verantwortung kann nicht delegiert werden.

5.3 Bewusstsein und Schulung für Informationssicherheit

Die Stadtverwaltung fördert eine Kultur des sicheren Umgangs mit Informationen. Prävention und Eigenverantwortung bilden die zentralen Stützen der Sicherheitskultur. Die Mitarbeitenden werden regelmässig und rollengerecht bezüglich der für sie relevanten Sicherheitsmassnahmen informiert und geschult.

5.4 Informationssicherheit in Vorhaben und Projekten

Bei Vorhaben und Projekten ist der Informationsschutz zu berücksichtigen, die finanziellen Aufwände für den Schutz von Informationen sind zu planen und zu budgetieren.

6 Rollen, Kompetenzen, Verantwortlichkeiten

6.1 Engagement des obersten Managements

Informationssicherheit fällt in die Verantwortung des Managements, welche von allen Mitgliedern des Stadtrates und den Geschäftsleitungen aller Organisationseinheiten wahrgenommen wird.

Der Stadtrat erlässt die stadtweit verbindlichen Leitlinien zur Informationssicherheit, insbesondere

- Die vorliegende Informationssicherheitspolitik, in der die strategische Ausrichtung der Infor-

mationssicherheit in der Stadtverwaltung Zürich festgelegt ist.
- Das Handbuch Informationssicherheit, welches den Basisschutz für die Stadtverwaltung formuliert.

Die in Ziff. 2 aufgeführten Einheiten haben mit geeigneten Massnahmen ihre Mitarbeitenden auf ihre Aufgaben und Pflichten bezüglich Informationssicherheit aufmerksam zu machen. Für diese Aufgaben kann die Fachstelle Informationssicherheit unterstützend beigezogen werden.

6.2 Verantwortlichkeiten

6.2.1 Stadtrat (beraten durch IT-Delegation)

- Beschluss der Informationssicherheitspolitik
- Sicherstellung der Umsetzung der Informationssicherheitspolitik
- Beschluss des «Handbuchs Informationssicherheit der Stadt Zürich»
- Erlass von Rechtsgrundlagen für den Bereich Informationssicherheit

6.2.2 Dienstchef/innen bzw. Departementssekretär/innen

- Sicherstellen des Schutzes der Informationen, welche in der eigenen Organisationseinheit bearbeitet oder die im Auftrag der Organisationseinheit erhoben werden
- Sicherstellung der Umsetzung der Informationssicherheitspolitik in der eigenen Organisationseinheit (organisatorische Belange)
- Bei Bedarf Benennen eines/r Informationssicherheitsbeauftragten und Betrauen mit Aufgaben in Belangen der Informationssicherheit
- Aktive Unterstützung der stadtweiten Informationssicherheitspolitik
- Sensibilisierung und Schulung der Mitarbeitenden bezüglich Informationssicherheit
- Fördern von verantwortungsvollem und sicherheitsbewusstem Umgang mit Informationen und ICT-Systemen in der Stadtverwaltung
- Verantwortung für die Einhaltung der Vorgaben aus dem „Handbuch Informationssicherheit der Stadt Zürich» und weiteren relevanten Rechtsgrundlagen in der eigenen Organisationseinheit
- Sicherstellen einer angemessenen Beachtung der Aspekte der Informationssicherheit in den relevanten Entscheidungsgremien der Organisationseinheit

6.2.3 Fachstelle Informationssicherheit

- Erarbeiten der «Informationssicherheitspolitik der Stadt Zürich»
- Definition eines durchgängigen, angemessenen Sicherheitsniveaus, und Gewährleistung, dass die verwendeten Standards, Methoden und Techniken aktuell sind und der gängigen Praxis entsprechen, insbesondere
  - Erarbeiten von stadtweit verbindlichen Richtlinien zur Informationssicherheit, wie das «Handbuch Informationssicherheit der Stadt Zürich»
  - Festlegen der ICT-Sicherheitsarchitektur und Erstellung von spezifischen weiterführenden Konzepten, Regelungen und Prozessen im Bereich Informationssicherheit
- Beratung und Unterstützung der Stadtverwaltung in allen Belangen der Informationssicherheit
- Kontrolle und Steuerung (Controlling) der Informationssicherheit der Stadtverwaltung Zürich, insbesondere durch:
  - Veranlassen von Prüfungen der Informationssicherheit
  - Formulieren von Auflagen und Kontrolle derer Umsetzung

  - Einfordern und Genehmigen von Informationssicherheits- und Datenschutz-Konzepten (ISDS-Konzepten)
  - Verfassen von Mitberichten und Kontrolle der Einhaltung derer Auflagen
  - Berichten über den Stand der Informationssicherheit und der Umsetzung der Informationssicherheitsvorgaben zuhanden der IT-Delegation
- Beurteilen von und Entscheiden über Abweichungen vom Basisschutz
- Bereitstellen und Durchführung von Informationssicherheitsschulungen und Sensibilisierungsmassnahmen
- Führen eines Prüfplans, in welchem festgelegt wird, welche Prüfungen der Informationssicherheit wann und in welchen Bereichen durchgeführt werden

6.2.4 Informationsverantwortliche/r

- Informationsverantwortliche (in der Regel Organisationseinheit (Def. → Kap. 2)) definieren des Schutzbedarfs derjenigen Informationen, welche er/sie selbst erstellt oder die in seinem/ihrem Auftrag erhoben werden
- Informationsverantwortliche (in der Regel Organisationseinheit (Def. → Kap. 2.5)) sind zuständig für die Informationsbestände, die sie selber erstellen oder die in ihrem Auftrag erhoben und verarbeitet werden. Sie definieren den Schutzbedarf dieser Informationen.
- Werden Informationen von mehreren Organisationseinheiten gemeinsam erhoben oder bearbeitet, ist die Hauptverantwortung für die Informationssicherheit und den Datenschutz zu regeln. Jede Organisationseinheit bleibt für ihre eigenen Informationsbearbeitungen verantwortlich (gemäss IDV § 27)
- Korrekte Klassierung der Informationen bei deren Beschaffung gemäss den gesetzlichen und geschäftspolitischen Anforderungen
- Bekanntgabe der Klassierung an die informationsverarbeitenden Stellen
- Sicherstellen der Inventarisierung der Informationsbestände und deren Klassierung
- Regelmässige Überprüfung der Zugriffsrestriktionen und der Klassierung
- Überprüfung einer Klassierung bei Informationszugangsgesuchen (Öffentlichkeitsprinzip)

6.2.5 Mitarbeitende

- Sind in ihrem Aufgabenbereich zuständig für die Einhaltung der Informationssicherheitsvorgaben und Weisungen
- Pflegen eine Kultur des sicheren Umganges mit Informationen
- Kennen und befolgen der Anordnungen der ICT-Benutzungsregelungen
- Melden sicherheitsrelevanter ICT-Vorfälle dem Service Desk oder der Fach-IT:

6.2.6 Weitere Rollen

In der Stadt Zürich sind weitere Rollen, welche eine Verantwortung bezüglich der Informationssicherheit haben, in den Organisationseinheiten bei Bedarf zu besetzen und einzelnen Fach- oder Linienfunktionen zuzuweisen. Eine Organisationseinheit muss nicht alle Rollen selber besetzen.

Informationssicherheitsbeauftragte/r

Die/der Informationssicherheitsbeauftragte ist zuständig für Anliegen der Informationssicherheit in seinem/ihrem Verantwortungsbereich. In diesem Zusammenhang arbeitet sie/er eng mit der Fachstelle Informationssicherheit zusammen.

ICT-Architekt/in

Der/die ICT-Architekt/in ist zuständig für die Definition der ICT-Architektur. Er/sie ist im Rahmen der ICT-Architekturen verantwortlich für die Umsetzung der Informationssicherheitsvorgaben.

Entwicklungsverantwortliche/r

Die/der Entwicklungsverantwortliche ist zuständig für die Entwicklung von neuen und Anpassungen von bestehenden ICT-Infrastrukturen und –Anwendungen. Dabei ist sie/er verantwortlich für die Umsetzung der Informationssicherheitsvorgaben.

Betriebsverantwortliche/r

Die/der Betriebsverantwortliche ist zuständig für die Sicherstellung des reibungslosen Betriebs von ICT-Infrastrukturen und –Anwendungen und deren Betreuung. Darunter fällt auch die Zuständigkeit, dass die Informationssicherheitsanforderungen im Betrieb eingehalten und umgesetzt werden.

Prozesseigner/in

Der/die Prozesseigner/in ist dafür zuständig, dass alle im Rahmen eines Prozesses definierten Aktivitäten durchgeführt und die Ziele der Prozessdefinition erfüllt werden. Darunter fällt auch die Zuständigkeit, dass die Informationssicherheitsanforderungen in den Prozessen eingehalten werden.

Projektleiter/in

Der/die Projektleiter/in ist zuständig für die Organisation und die Durchführung von Projekten. Er/sie ist dafür verantwortlich, dass die im Rahmen des Projektes erarbeitete und umgesetzte Lösung die Informationssicherheitsvorgaben einhält.

Service-Verantwortliche/r

Die/der Service-Verantwortliche ist gegenüber dem Kunden für die Initiierung, Überprüfung und fortlaufende Wartung und Unterstützung eines bestimmten Services verantwortlich. In diesem Rahmen sorgt sie/er dafür, dass der Service entsprechende Informationssicherheitsvorgaben einhält.

Personalverantwortliche/r

Die/der Personalverantwortliche ist zuständig für die Rekrutierung und die Betreuung des Personals. In diesem Rahmen ist sie/er dafür zuständig, dass die Informationssicherheits- und Datenschutzvorgaben eingehalten werden.

BCM-Verantwortliche/r

Die/der BCM[4]-Verantwortliche ist zuständig für die Entwicklung und Umsetzung von Strategien, Plänen und Handlungen, um die Fortführung der Geschäftstätigkeit unter Krisenbedingungen oder zumindest unvorhersehbar erschwerten Bedingungen zu sichern.

7 Steuerung der Informationssicherheit

7.1 Überprüfung der Informationssicherheit

Der Schutz der Informationen, ICT-Infrastrukturen und Applikationen und die angemessene Umsetzung der Anforderungen des Handbuchs Informationssicherheit werden regelmässig kontrolliert.

- Die Organisationseinheiten prüfen die Einhaltung der für sie relevanten Belange des «Handbuch Informationssicherheit der Stadt Zürich». Die «IKS[5]-Checkliste IT» kann sie dabei unter-

[4] BCM Business Continuity Management

[5] IKS - Internes Kontrollsystem

stützen.

- Die Fachstelle Informationssicherheit unterstützt die Organisationseinheiten dabei, die Regeln des Handbuchs Informationssicherheit einzuhalten, und ist befugt, die Einhaltung der Sicherheitsstandards in allen Organisationseinheiten zu überprüfen.
- Der Datenschutzbeauftragte der Stadt Zürich ist gemäss IDG[6] und Gemeindeordnung befugt, Audits einzufordern, um die Gewährleistung des Datenschutzes zu prüfen, bzw. prüfen zu lassen.

Stadtweit gültige Vorgaben zur Informationssicherheit und ihr Umsetzungsstand werden punktuell von unabhängiger Stelle geprüft.

7.2 Umgang mit Risiken

Die Kenntnis der Informationsrisiken ist Voraussetzung für die Bestimmung von angemessenen Sicherheitsmassnahmen.

Um die Sicherheitsziele zu erreichen, verfährt die Stadt Zürich nach einem kombinierten Ansatz:

- Der Basisschutz, definiert im Handbuch Informationssicherheit, wird für sämtliche Schutzobjekte (Informationen und davon abgeleitet Anwendungen, ICT-Systeme und Prozesse) angewendet, ungeachtet des Risikopotenzials.
- Für Schutzobjekte, für welche der Basisschutz nicht ausreicht, werden gestützt auf Risikoanalysen zusätzliche, über den Basisschutz hinausgehende Massnahmen implementiert und in einem ISDS[7]- Konzept festgehalten.

Je nach Ausmass fliessen die Informationsrisiken in das übergeordnete Chancen- und Risikomanagement der Stadt (RM) ein.

7.2.1 Informationsrisikomanagement

Das Management der ICT- und Informationsrisiken

- identifiziert die Gefahren, welche die Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit von Informationen, ICT-Infrastrukturen und -Anwendungen bedrohen, und
- bewertet die damit verbundenen Risiken systematisch gemäss einer einheitlichen Methodik und einem einheitlichen Prozess.

Zur Bewältigung wird jedem identifizierten Risiko eine der folgenden Behandlungsmethoden zugeordnet:

- Risikovermeidung durch das Untersagen von Aktivitäten, die das Risiko entstehen lassen können
- Risikoreduktion auf ein vertretbares Mass durch Anwendung angemessener personeller, organisatorischer und technischer Sicherheitsmassnahmen
- Risiko anderen Parteien übertragen, z.B. Versicherungen oder Lieferanten
- Risiko tragen: Restrisiken werden von der verantwortlichen Stelle aktiv übernommen.
  Dabei sind die Vorgaben der Organisation zur Risikoübernahme klar erfüllt.
  Die Methode, wie die Kontinuität des Geschäftes im Falle des Eintretens einer Bedrohung zu gewährleisten ist, ist aufgestellt und dokumentiert.

Ziel eines aktiven Risikomanagements und eines einheitlichen Vorgehens ist:

- Die Risiken sind bekannt, die Risikobehandlung ist definiert und dokumentiert
- Risikobehandlung und Restrisiken sind von der verantwortlichen Stelle akzeptiert.

[6] IDG – Gesetz über die Information und den Datenschutz

[7] ISDS – Informationssicherheit und Datenschutz

7.3 Umgang mit Ausnahmen

Der im «Handbuch Informationssicherheit der Stadt Zürich» definierte Basisschutz ist grundsätzlich verbindlich und im ganzen Geltungsbereich bei jeder Informationsbearbeitung einzuhalten.

7.3.1 Zusatzanforderungen zum Basisschutz

Die Vorsteherinnen bzw. Vorsteher der Departemente können in ihrem Verantwortungsbereich zusätzliche, über den Basisschutz hinausgehende Bestimmungen erlassen.

7.3.2 Unterschreiten des Basisschutzes

Muss im Einzelfall aus organisatorischen, technischen oder wirtschaftlichen Gründen vom Basisschutz im Sinne einer Unterschreitung abgewichen werden, liegt eine bewilligungspflichtige Ausnahme vor.

Bei einer Unterschreitung des Basisschutzes müssen die dadurch entstehenden Risiken identifiziert, quantifiziert und in einem Antrag der Fachstelle Informationssicherheit zur Beurteilung und Stellungnahme unterbreitet werden. Eskalationsinstanz ist die IT-Delegation.

Die Fachstelle Informationssicherheit informiert die IT-Delegation über die Ausnahmen.

Ausnahmen sollen in der Regel zeitlich befristet sein.

8 Dokumentenlenkung

Die stadtweit verbindlichen Leitlinien zur Informationssicherheit werden durch die Fachstelle Informationssicherheit erarbeitet und auf aktuellem Stand gehalten.

Die «Informationssicherheitspolitik der Stadt Zürich» und das «Handbuch Informationssicherheit der Stadt Zürich» werden regelmässig, mindestens alle 2 Jahre, durch die Fachstelle Informationssicherheit überprüft.

Kleinere Änderungen nimmt die Fachstelle Informationssicherheit in eigener Kompetenz vor und informiert die Adressaten in geeigneter Form. Dabei wird ein Änderungsnachweis geführt.

Grundlegende Änderungen bedürfen einer Bewilligung durch den Stadtrat (Stadtratsbeschluss).

9 Sanktionen

Bei Nichteinhalten der Informationssicherheitspolitik der Stadt Zürich können im Sinne der Anwendung bestehenden Rechts personal-, straf- und zivilrechtliche Konsequenzen zur Folge haben.

10 Inkrafttreten

Die Informationssicherheitspolitik tritt per 9. Juli 2014 in Kraft (STRB 634, vom 9. Juli 2014).

Zürich, 23. Juni 2014/ Version 1.0