Stadtrat

Stadt Winterthur

Protokollauszug vom 23.10.2019

Departement Finanzen / Informatikdienste IDW:
Informatikstrategie 2014: Genehmigung und Inkraftsetzung der Richtlinien zur Informatiksicherheit der Stadt Winterthur (Information Security Policy; ISP)
IDG-Status: öffentlich
SR.19.733-1

Der Stadtrat hat beschlossen:

1. Die Richtlinien zur Informatiksicherheit der Stadt Winterthur (Information Security Policy; ISP) werden gemäss Beilage 1 genehmigt und per 1. November 2019 in Kraft gesetzt. Sie werden im Intranet aufgeschaltet und in die interne Erlass-Sammlung aufgenommen.

2. Der/die Stelleninhaber/in «ICT Architektur & Sicherheit» bei den Informatikdiensten (IDW) wird als Informatiksicherheitsbeauftragte/r der Stadt Winterthur bezeichnet.

3. Die Departemente werden beauftragt, die Richtlinien in ihrem Zuständigkeitsbereich umzusetzen und einzuhalten.

4. Die Informatikbeauftragten (IB) werden beauftragt, die Mitarbeitenden ihrer Departemente über die Richtlinien zur Informatiksicherheit der Stadt Winterthur zu informieren.

5. Beilage 1 (Richtlinien zur Informatiksicherheit der Stadt Winterthur) wird veröffentlicht.

6. Mitteilung (mit Beilage 1) an: Alle Departemente; Stadtkanzlei; Informatik-Lenkungsausschuss ILA; Finanzamt; Finanzkontrolle; Datenschutzbeauftragter.

Vor dem Stadtrat
Der Stadtschreiber:

A. Simon

Begründung:

1. Ausgangslage

Die Informatikdienste (IDW) haben bereits im Jahre 2004 in Zusammenarbeit mit einer Beratungsfirma eine erste «Security Policy» erarbeitet. Im Hinblick auf die ISO-Zertifizierung 2009 wurde diese grundlegend überarbeitet und an die Strukturen der ISO-Norm 27001 angepasst. Die Informatik-Strategie 2014 (IT-Strategie) sowie die Organisationsentwicklungen in den Jahren 2012 und 2016 der IDW, die zur Schaffung der Stabsstelle «ICT Architektur & Sicherheit» führte, bilden nun die Voraussetzungen für eine neue «Information Security Policy», welche als «Richtlinien zur Informatiksicherheit der Stadt Winterthur» vom Stadtrat als Bestandteil der Informatik-Strategie 2014 erlassen werden.

Mit den vorliegenden Richtlinien werden die strategischen Ziele der Informatiksicherheit der Stadt Winterthur als Teilbereich der Informationssicherheit festgelegt. Sie richten sich nach übergeordneten Vorgaben (z.B. Gesetz und Verordnung über die Information und den Datenschutz; IDG und IDV vom 12.02.2007 und 28.05.2008, Personalstatut vom 01.01.2019) und bilden die Grundlage für die Ausführungsbestimmungen der IDW, welche im Management-Handbuch der IDW verankert sind und die Umsetzung der Informatiksicherheit in der Stadtverwaltung regeln.

2. Inhalt der Richtlinien zur Informatiksicherheit (Information Security Policy, ISP)

Die Richtlinien stellen die Corporate Governance und Compliance-Regelung der Stadt Winterthur im Bereich der Informatiksicherheit als Teilaspekt der Informationssicherheit dar, weshalb sie vom Stadtrat zu genehmigen und in Kraft zu setzen sind.

In den Allgemeinen Bestimmungen werden die Begriffe rund um die Informationssicherheit definiert. Von besonderer Bedeutung sind die Kapitel zu den Zielen, zur Umsetzung und zur Organisation der Informatiksicherheit in der Stadt Winterthur.

Eine wichtige Rolle kommt künftig dem oder der Informatiksicherheitsbeauftragten (ISB) zu. Er oder sie ist unter anderem für die Ausbildung der Mitarbeitenden zum Thema Informatiksicherheit sowie die Umsetzung und regelmässige Überprüfung von Sicherheitsmassnahmen zuständig. Ebenso ist er oder sie Ansprech- und Meldestelle bei Vorgängen oder Prozessen, die im Zusammenhang mit Informatiksicherheit oder Datenschutz stehen. Als Informatiksicherheitsbeauftragte/r wird der oder die Stelleninhaber/in «ICT Architektur & Sicherheit» ernannt.

Die «Information Security Policy» wurde im Informatik-Lenkungsausschuss (ILA) besprochen und den Mitgliedern in Vernehmlassung gegeben sowie gestützt auf deren Rückmeldungen überarbeitet.

3. Umsetzung der Richtlinien zur Informatiksicherheit in der Stadt Winterthur

Die Umsetzung der Richtlinien zur Informatiksicherheit wird hauptsächlich durch Aufgaben und Vorgaben der Informatikdienste (IDW) in Zusammenarbeit mit den Departementen erreicht.

In einzelnen Teilbereichen sind auch die Departemente bzw. Bereiche aufgefordert, die Vorgaben der ISP umzusetzen. Dies betrifft insbesondere jene Bestimmungen, die sich an die zuständigen Dateneigentümerinnen und Dateneigentümern richten, wie die Benutzerverwaltung (Kapitel 4.8.1), den Schutz von Informatikmitteln und Informationen (Kapitel 4.8.5) sowie die Beziehungen zu Dritten (Kapitel 4.4).

Sodann werden die Mitarbeitenden durch entsprechende Schulungsmassnahmen befähigt, Inhalt und Bedeutung der Informatiksicherheit zu kennen, um ihre Verantwortung wahrnehmen zu können. Dazu wird der oder die Informatiksicherheitsbeauftragte entsprechende E-Learning-Module entwickeln. Den diesbezüglichen Schulungsauftrag hat der Stadtrat den IDW bereits mit SR.18.877-2 vom 12.12.2018 erteilt.

4. Kommunikation

Da es sich um eine verwaltungsinterne Regelung handelt, ist keine Medienmitteilung vorgesehen.

Die interne Information der Mitarbeitenden obliegt dem oder der Informatikbeauftragen der Departement (IB). Zudem wird die ISP im Intranet und in der internen Erlass-Sammlung aufgeschaltet und ist damit allen Mitarbeitenden zugänglich.

Beilage:

1. Richtlinien zur Informatiksicherheit der Stadt Winterthur

Stadt Winterthur

Richtlinien zur Informatiksicherheit der Stadt Winterthur

(Information Security Policy; ISP)

IDG-Status	Öffentlich
Stand	Vom Stadtrat verabschiedet am 23. Oktober 2019 (SR.19.733-1)
In Kraft per	1. November 2019
Verfasser	IDW

1 Einleitung

Die Richtlinien zur Informatiksicherheit (Information Security Policy; ISP) sind Teil der Informatikstrategie 2014 der Stadt Winterthur. Sie sind vom Stadtrat verabschiedet und in Kraft gesetzt worden. Die Richtlinien sind für die ganze Stadtverwaltung verbindlich und öffentlich; Ausnahmen und Änderungen sind vom Stadtrat zu beschliessen.

In diesem Dokument werden die strategischen Vorgaben der Informatiksicherheit der Stadt Winterthur als Teilaspekt der Informationssicherheit definiert. Die darauf aufbauenden Ausführungsbestimmungen wurden im Rahmen der ISO 27001-Zertifizierung der Informatikdienste (IDW) in das Managementhandbuch der IDW aufgenommen und dienen den IDW für die Umsetzung der Informatiksicherheit in der Stadt Winterthur.

2 Allgemeine Bestimmungen

2.1 Definitionen

Die folgenden Begriffe spielen eine zentrale Rolle für das Verständnis der Informationssicherheit. Sie werden von der Stadt Winterthur wie folgt definiert:

2.1.1 Informationssicherheit

Unter Informationssicherheit versteht die Stadt Winterthur den Schutz sämtlicher in ihrer Verantwortung stehenden Informationen, ungeachtet der Art ihrer Darstellung (in Papier, elektronisch, mündlich), ihres Transfers und ihrer Speicherung sowie der damit verbundenen Infrastruktur.

Die Informationssicherheit basiert auf dem Informationssicherheits-Standard ISO 27001. Folgendes wird gewährleistet:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität.

Informationssicherheit wird erreicht, indem angemessene Massnahmen erlassen und umgesetzt werden, bestehend aus Regeln, Prozessen und organisatorischen Strukturen, welche die spezifischen Sicherheitsziele der einzelnen Organisationen der Stadtverwaltung berücksichtigen.

2.1.2 Informatiksicherheit

Informatiksicherheit der Stadt Winterthur bezieht sich auf jene Aspekte der Informationssicherheit, die mit der elektronischen Verarbeitung von Informationen zusammenhängen.

Ziel der Informatiksicherheit ist, bei der Verwendung und beim Betrieb der Informatikmittel in der Stadt Winterthur allen sicherheitstechnischen Anforderungen zu entsprechen und damit die in Kapitel 3 festgehaltenen Ziele zu erfüllen.

2.1.3 Datenschutz

Der Datenschutz beinhaltet den Schutz vor widerrechtlicher oder unverhältnismässiger Bearbeitung von Personendaten. Die rechtliche Grundlage bildet das Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 (LS 170.4) sowie die Verordnung über die Information und den Datenschutz (IDV) vom 28. Mai 2008 (LS 170.41).

2.2 Einordnung und Aufbau der Richtlinien zur Informatiksicherheit (ISP)

Die Richtlinien zur Informatiksicherheit basieren auf übergeordneten Vorgaben wie Gesetzen und Verordnungen des Bundes und des Kantons Zürich sowie Erlassen der Stadt Winterthur. Sie beinhalten die strategischen Vorgaben der Informatiksicherheit der Stadt Winterthur als Teilaspekt der Informationssicherheit und bilden die Grundlage für die Ausführungsbestimmungen, welche im Managementhandbuch der IDW enthalten sind und den IDW für die Umsetzung der Informatiksicherheit in der Stadtverwaltung dienen.

Übergeordnete Vorgaben: z.B. IDG und IDV[1], Personalstatut etc.

Richtlinien zur Informatiksicherheit (Information Security Policy; ISP): Strategische Vorgaben als Grundlage für die konkrete Umsetzung der Informatiksicherheit in der Stadt Winterthur.

Detailkonzepte: Definition von Standards, Umsetzungsrichtlinien und Massnahmen, enthalten im Managementhandbuch der Informatikdienste (IDW).

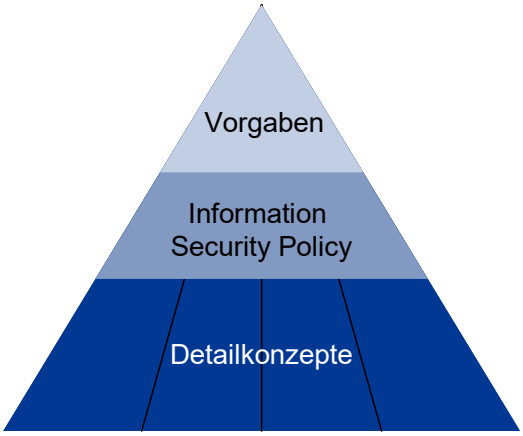

Abbildung 1: Einordnung der Richtlinien zur Informatiksicherheit

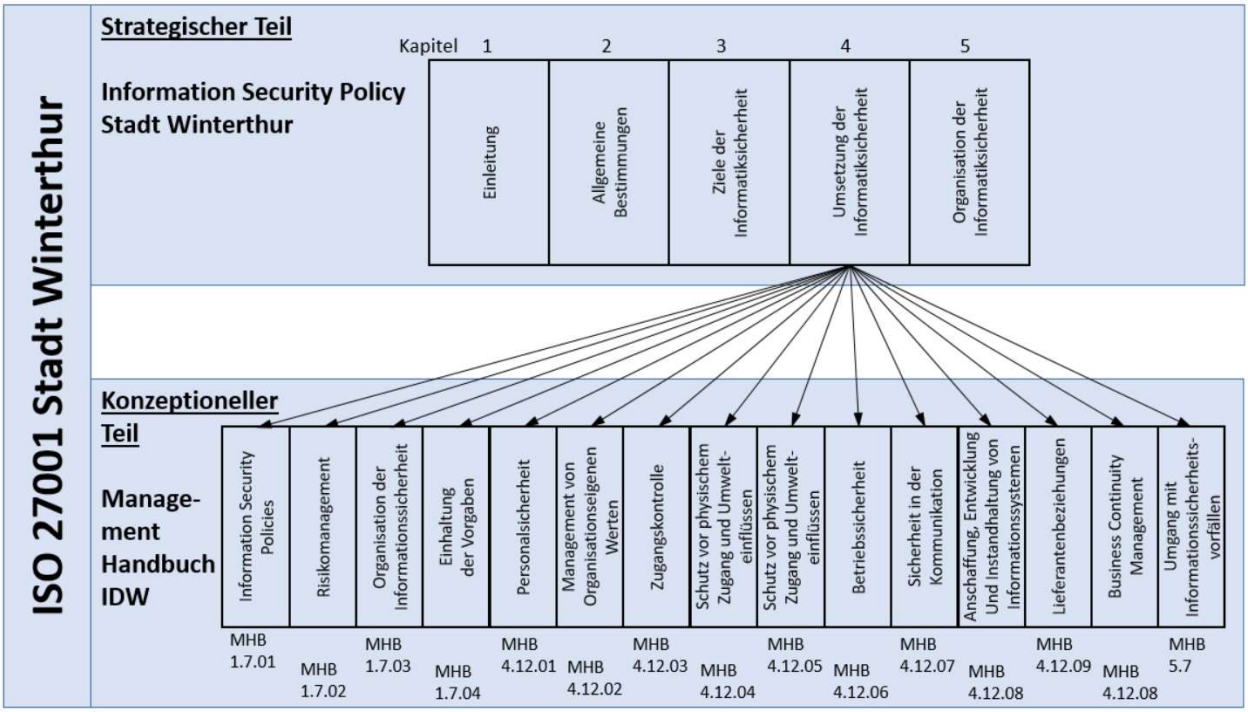

Abbildung 2: Dokumentaufbau der Informatiksicherheit der Stadt Winterthur

[1] Gesetz und Verordnung über die Information und den Datenschutz

2.3 Geltungsbereich

Die Richtlinien zur Informatiksicherheit gelten für alle Organisationseinheiten und Mitarbeitenden der Stadt Winterthur.

Ebenso werden die Vertragspartner und -partnerinnen der Stadt Winterthur im Rahmen ihrer Tätigkeit zur Einhaltung der jeweiligen Sicherheitsvorschriften verpflichtet.

2.4 Inkraftsetzung und Gültigkeitsdauer

Die Richtlinien zur Informatiksicherheit werden vom Stadtrat verabschiedet und in Kraft gesetzt und gelten bis zu deren Widerruf. Änderungen und Ausnahmen werden vom Stadtrat beschlossen.

2.5 Ausnahmen

Ausnahmen zu den vorliegenden Richtlinien sind gestützt auf einen entsprechenden Antrag des stadträtlichen Informatik-Ausschusses (SIA) vom Stadtrat zu genehmigen.

Alle vom Stadtrat genehmigten Ausnahmen werden in den Anhang 1 der Informatikstrategie 2014 der Stadt Winterthur (Ausnahmen zum Geltungsbereich) aufgenommen.

3 Ziele der Informatiksicherheit der Stadt Winterthur

Der Stadt Winterthur sind die Erfüllung eines festgelegten Sicherheitsstandards sowie darauf abgestimmte Aktivitäten wichtig. Daher werden folgende Sicherheitsziele festgesetzt:

- Informationen und Informatik-Mittel sind so zu betreiben und zu schützen, dass sie von allen Organisationseinheiten der Stadt Winterthur sowie deren Kunden und Kundinnen jederzeit genutzt werden können.
- Vertraulichkeit und Integrität der Daten sind in jedem Fall sicherzustellen.
- Die übergeordneten Regelungen für die Informationssicherheit und den Datenschutz sind einzuhalten.
- Der Schutz von Leben, Gesundheit und Integrität aller Mitarbeitenden, der Kundinnen und Kunden, der externen Vertragspartner und -partnerinnen sowie der Öffentlichkeit ist zu gewährleisten.
- Alle Mitarbeitenden kennen und setzen die Informationssicherheitsziele und Informationssicherheitsanforderungen der Stadt Winterthur um.

4 Umsetzung der Informatiksicherheit in der Stadt Winterthur

Im folgenden Kapitel werden die strategischen Vorgaben der Informatiksicherheit in der Stadt Winterthur als Teilaspekt der Informationssicherheit definiert. Die nachfolgend erwähnten Ausführungsbestimmungen für die konkrete Umsetzung der Informatiksicherheit wurden bzw. werden in das Management-Handbuch der IDW aufgenommen.

4.1 Informationssicherheits-Management (ISMS)

Die Informatikdienste der Stadt Winterthur betreiben ein Informationssicherheits-Managementsystem (ISMS).

Ziel des ISMS ist, die Verfügbarkeit, Vertraulichkeit und Integrität von elektronischen Informationen sicherzustellen, welche die Informatikdienste (IDW) zur Verfügung stellen,

bearbeiten und aufbewahren. Mit Anweisungen der Informatikdienste zu technischen und organisatorischen Massnahmen wird sichergestellt, dass die festgesetzten Sicherheitsziele erreicht werden.

4.2 Risikomanagement

Die Informatikdienste der Stadt Winterthur betreiben ein Risikomanagement. Dabei wird der Schutzbedarf von Informationen und Informatikmitteln erhoben. Das Risikomanagement umfasst die gesamte Verwaltung sowie auch Vertragspartner und -partnerinnen der Stadt Winterthur.

4.3 Sicherheitsorganisation

Es wird eine mit entsprechenden Kompetenzen ausgestattete Sicherheitsorganisation eingesetzt (vgl. Kapitel 5). Diese ist dafür verantwortlich, dass die in den vorliegenden Richtlinien festgelegten Ziele und Abläufe umgesetzt werden.

4.4 Beziehungen zu Dritten

Die Sicherheitsstandards der Stadt Winterthur werden von den Informatikdiensten definiert und gelten auch für alle externen Vertragspartner und -partnerinnen der Stadt, welche IT-Leistungen für die Stadt Winterthur erbringen. Die im konkreten Fall anwendbaren Sicherheitsstandards sind von den für den Vertragsabschluss zuständigen städtischen Organisationseinheiten in die jeweiligen IT-Verträge aufzunehmen.

Die Beziehungen zu Dritten werden von den zuständigen Organisationseinheiten in regelmässigen Abständen überprüft, bewertet und sind Teil des Risikomanagements.

4.5 Auskunftsbegehren

Die Stadt Winterthur regelt Zuständigkeiten und Verfahren im Zusammenhang mit Begehren zur Datenherausgabe und Datenbearbeitung auf der Grundlage des Gesetzes über die Information und den Datenschutz (IDG) und der zugehörigen Verordnung (IDV) sowie weiterer einschlägiger Bestimmungen.[2]

4.6 Schulungsmassnahmen

Die Stadt Winterthur trifft geeignete Massnahmen, um die Mitarbeitenden über den Datenschutz und die Informationssicherheit zu informieren und ihnen ihre Verantwortung im Umgang mit Informationen und Informatikmitteln bewusst zu machen. Dazu gehören Ausbildungsmodule, welche der oder die Informatiksicherheitsbeauftragte (ISB) zur Verfügung stellt und von den Mitarbeitenden der Stadtverwaltung mit städtischem IT-Arbeitsplatz zu absolvieren sind[3].

[2] Verordnung über die/den Datenschutzbeauftragte/n der Stadt Winterthur vom 30. August 2010 (WES 3.1-1)
Verordnung über die Bearbeitung von besonderen Personendaten vom 16. September 2013 (WES 3.1-2)

[3] Auftrag zur Durchführung einer obligatorischen Cyber-Schulung gemäss SR.18.877-2 vom 12.12.2018

4.7 Verwaltung von IT-Anlagen und Daten[4]

4.7.1 Sicherheitsstufen und Schutzziele

Die IT-Anlagen und Daten der Stadt Winterthur werden von den Informatikdiensten in Zusammenarbeit mit den zuständigen städtischen Stellen in Sicherheitsstufen eingeteilt. Dabei werden explizite Schutzziele[5] festgelegt.

4.7.2 Sicherheitsmassnahmen

Entsprechend den Sicherheitsstufen und Schutzzielen werden Sicherheitsmassnahmen festgesetzt und im Rahmen von IT-Projekten umgesetzt. Dabei wird zwischen Vorsorge- und Notfallmassnahmen unterschieden.

4.7.3 Überprüfung der Sicherheitsmassnahmen

Die Umsetzung und Angemessenheit der Sicherheitsmassnahmen unterliegt regelmässigen internen Prüfungen (Durchführung von Reviews und Audits etc.).

Für die Überprüfung der Sicherheitsmassnahmen ist der oder die Informatiksicherheitsbeauftragte (ISB) zuständig.

Im Weiteren sind der oder die Datenschutzbeauftragte sowie die Finanzkontrolle berechtigt, Kontrollen durchzuführen oder durchführen zu lassen.

4.8 Zugangskontrolle

4.8.1 Benutzerverwaltung

Die Dateneigentümer und -eigentümerinnen der Stadt Winterthur sind verpflichtet, verbindliche Abläufe für die Vergabe und Löschung der Zugriffsrechte auf Informationen und Informationssysteme zu definieren. Diese stellen sicher, dass die Zugriffsrechte nur für die erforderliche Zugriffsdauer gelten und auf den Zeitpunkt des Austritts der Nutzer und Nutzerinnen aus der Verwaltung oder einer Veränderung ihrer Aufgaben, die keinen Zugriff mehr erfordert, gelöscht werden.

4.8.2 Zugang zu Netzwerken

Der Zugriff auf interne und externe Netzwerke der Stadt Winterthur wird kontrolliert. Zu diesem Zweck werden von den Informatikdiensten zwischen dem Netzwerk der Stadt Winterthur und demjenigen Dritter angemessene Netzwerkkontrollen eingerichtet.

4.8.3 Informationelle Trennung

Die Informatikdienste der Stadt Winterthur stellen sicher, dass zwischen den einzelnen Dienststellen eine ausreichende Trennung des Informationsaustausches gewährleistet wird (Mandantenfähigkeit).

4.8.4 Verschlüsselung (Kryptographie)

Die Informatikdienste der Stadt Winterthur regeln den Einsatz von Verschlüsselungstechnologien. Dazu gehören auch Regeln zur Aufbewahrung von kryptographischen Schlüsseln sowie die Wiederherstellung von verschlüsselten Informationen.

---

[4] Management von organisationseigenen Werten gemäss ISO 27001

[5] Die Sicherheitsstufen und Schutzziele werden im Management-Handbuch der IDW definiert

4.8.5 Schutz der Informatikmittel und Informationen

Die Nutzerinnen und Nutzer treffen die notwendigen Massnahmen, um die städtischen Informatikmittel vor unberechtigten Zugriffen und Umwelteinflüssen zu schützen. Die Stadt Winterthur trifft entsprechende Schulungsmassnahmen[6].

Die elektronische Bearbeitung, Speicherung und Archivierung von heiklen Informationen erfolgt in angemessen gesicherten Räumen. Als Schutzmassnahmen dienen dem Risiko entsprechende Zugriffsbeschränkungen und -kontrollen sowie ausreichende bauliche Vorkehrungen, die Sicherheit gegen Einbruch und höhere Gewalt bieten. Ausnahmen bedürfen der schriftlichen Einwilligung des Dateneigentümers oder der -eigentümerin. Bei der Gewährung von Ausnahmen sind die Risiken von den Dateneigentümern oder -eigentümerinnen zu übernehmen.

4.9 Betriebssicherheit

Die Informatikdienste legen klare Verantwortlichkeiten und Prozesse für die Verwaltung und den Betrieb der Informatikmittel der Stadt Winterthur und den damit zusammenhängenden Dienstleistungen fest, inklusive Regelungen für allfällige Zwischenfälle, und sind für deren Durchsetzung besorgt.

4.10 Netzwerkzonen

Die Informatik-Systeme werden aufgrund ihres Schutzbedarfs in unterschiedliche Netzwerkzonen getrennt. Die Informatikdienste unterhalten zu diesem Zweck ein Netzwerkzonenkonzept.

4.11 Anschaffung, Entwicklung und Unterhalt von Informationssystemen

Die Informatikdienste stellen sicher, dass sämtliche Informatikmittel der Stadt Winterthur jederzeit den geltenden Anforderungen an die Informatiksicherheit genügen.

4.12 Vorsorge- und Notfallmassnahmen (Business Continuity Management)

4.12.1 Vorsorgemassnahmen

Der Schutzbedarf von Informationen und Anwendungen werden von den Informatikdiensten im Rahmen des Risikomanagements erhoben, und es werden die notwendigen Vorsorgemassnahmen definiert und umgesetzt.

4.12.2 Notfallmassnahmen

Die Stadt Winterthur betreibt eine Notfallorganisation, die für die Behandlung von betrieblichen und sicherheitstechnischen Vorfällen zuständig ist (vgl. Kapitel 5.3).

4.12.3 Umgang mit Sicherheitsvorfällen

Vorfälle im Zusammenhang mit Informatiksicherheit sind dem oder der Informatiksicherheitsbeauftragten (ISB) zu melden und werden von ihm bzw. ihr zentral erfasst.

Sicherheitsvorfälle sind mit dem ISB zu lösen; bei komplexen Fällen zieht er oder sie das Sicherheitsgremium der Informatikdienste und im Eskalationsfall den Notfall-Stab hinzu (vgl. Kapitel 5.3).

[6] Vgl. Fussnote 3 zu Kapitel 4.6.

5 Organisation der Informatiksicherheit

5.1 Führungsorgane

5.1.1 Stadträtlicher Informatik-Ausschuss (SIA)

Zusammensetzung: Drei Mitglieder des Stadtrates unter dem Vorsitz der Departementsvorsteherin oder des Departementsvorstehers Finanzen; der Bereichsleiter oder die Bereichsleiterin IDW / CIO hat beratende Stimme.

Aufgaben: Verantwortlich für eine aktuelle und zeitgemässe Informatiksicherheit in der Stadt Winterthur, die Vorberatung strategischer Entschiede im Zusammenhang mit der Informatiksicherheit und die Antragstellung bezüglich Ausnahmebewilligungen zuhanden des Stadtrates.

5.1.2 Informatik-Lenkungs-Ausschuss (ILA)

Zusammensetzung: Alle Informatikbeauftragten (IB) der Departemente und der Stadtkanzlei unter dem Vorsitz des Bereichsleiters oder der Bereichsleiterin IDW / CIO.

Aufgaben: Zuständig für die Einhaltung und Umsetzung der vorliegenden Richtlinien.

5.1.3 Informatiksicherheitsbeauftragte/r (ISB)

Die Stadt Winterthur bezeichnet einen Informatiksicherheitsbeauftragten oder eine Informatiksicherheitsbeauftragte für die gesamte Stadtverwaltung. Er oder sie

- ist für sämtliche Vorgaben und Geschäftsprozesse, welche die Informatiksicherheit betreffen, die zuständige Fachperson,
- unterstützt den SIA bei Fragen zur Informatiksicherheit,
- ist für die interne Überprüfung der Sicherheitsmassnahmen zuständig,
- stellt die erforderlichen Ausbildungsmodule zur Informatiksicherheit bereit,
- ist bei Sicherheitsvorfällen die zuständige Ansprech- und Meldestelle.

5.2 Datenschutzbeauftragte/r und Datenaufsicht

Für den Datenschutz in der Stadt Winterthur ist der oder die Datenschutzbeauftragte zuständig. Er oder sie ist zudem zur Überprüfung sämtlicher Massnahmen, welche die Informatiksicherheit betreffen, berechtigt.

5.3 Notfallorganisation

5.3.1 Sicherheitsgremium (Security Board)

Die Informatikdienste stellen ein Sicherheitsgremium, das für die langfristige Planung der Informatiksicherheit und die Behandlung von Sicherheitsvorfällen zuständig ist.

5.3.2 Notfall-Stab

Der Notfallstab wird von der Geschäftsleitung der Informatikdienste gestellt. Er ist für die Behandlung von Notfallmassnahmen zuständig und die Eskalationsstufe bei Sicherheitsvorfällen.