wetzikon

Leitlinie

für die Informationssicherheit an der Schule Wetzikon

vom 23. Juni 2026

Genehmigungsinstanz:
Schulpflege

Inkraftsetzung:
23. Juni 2026

Stand:
28. Mai 2026

SR.-Nr.:
163.2

Version:
V1

STADTKANZLEI · WETZIKON ZH ·

2026.07.03 07:21:28
+02'00'

Inhaltsverzeichnis

I. Einleitung

Rechtsgrundlagen

Art. 1

Gestützt auf die Bestimmungen des Gesetzes über die Information und den Datenschutz IDG, der Verordnung über die Information und den Datenschutz IDV und der Verordnung über die Informationsverwaltung und -sicherheit IVSV erlässt die Schulpflege eine Leitlinie "für die Informationssicherheit an der Schule Wetzikon".

Geltungsbereich

Art. 2

Die Leitlinie und die damit zusammenhängenden Dokumente gelten für alle Mitarbeitenden der Schule Wetzikon sowie Behördenmitglieder – nachfolgend "Mitarbeitende" genannt.

Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

Zweck

Art. 3

Die Schule Wetzikon ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie abhängig. Diese haben die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität gemäss den Bestimmungen des IDG zu erfüllen.

Die Leitlinie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Schule Wetzikon angestrebte allgemeine Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Leitlinie eine Beschreibung der Informationssicherheitsorganisation.

II. Informationssicherheitsstandards

Sicherheitsniveau

Art. 4

Für die generelle Informationssicherheit wird ein angemessenes Sicherheitsniveau mit einem normalen Schutzbedarf angestrebt.

Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

III. Informationssicherheitsziele

Integrität

Art. 5

Informationen müssen richtig und vollständig sein.

Nachvollziehbarkeit

Art. 6

Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

Verantwortung

Art. 7

Die Mitarbeitenden sind sich ihrer Verantwortung im Umgang mit Informationen, Informations- und Kommunikationstechnologie IKT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele der Schule Wetzikon.

Verfügbarkeit

Art. 8

Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Betrieb haben.

Vertraulichkeit

Art. 9

Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.

Zurechenbarkeit

Art. 10

Informationsbearbeitungen müssen einer Person zugerechnet werden können.

IV. Informationssicherheitsmassnahmen

Anforderungen

Art. 11

Die Auswahl der technischen und organisatorischen Massnahmen erfolgt anhand der Anforderungen der ISO/IEC 27001 und den Standards des deutschen Bundesamts für Sicherheit in der Informationstechnik BSI.

Aktualisierungen

Art. 12

Alle IKT-Systeme werden regelmässig aktualisiert und mit den aktuellen Sicherheitsupdates versorgt.

Archivierung / Löschung

Art. 13

Für die Aufbewahrung von Informationen und Daten ist das kantonale Archivgesetz massgebend. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.

Berechtigungskonzept

Art. 14

Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen der Mitarbeitenden auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben erforderlich und geeignet.

Datenschutz

Art. 15

Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.

Datensicherung

Art. 16

Die Datensicherung wird regelmässig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.

IKT-Systeme

Art. 17

Die IKT-Systeme werden nach der Beschaffung gemäss anerkannten Sicherheitsstandards installiert und betrieben, mit einem Änderungsmanagement verwaltet und in einem geregelten Prozess ausser Betrieb genommen.

Mobile Geräte / Software

Art. 18

Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie die Installation von Software auf Arbeitsplatzrechnern und Servern sind im Detail geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.

Überwachung

Art. 19

Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.

Netzwerk / Firewall

Art. 20

Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern. Die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (Leunet) wird eingehalten.

Organisation

Art. 21

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.

Outsourcing

Art. 22

Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.

Zugangssicherung

Art. 23

Die Zugänge zu allen Systemen, Daten und Anwendungen sind gemäss den aktuellen technischen Erkenntnissen (Passwörter, 2-Faktoren-Authentifizierung, Biometrie, etc.) gesichert.

Sensibilisierung

Art. 24

Die Mitarbeitenden nehmen mindestens jährlich an einer internen Sicherheitsschulung der für die Informationssicherheit verantwortlichen Person teil. Sie werden regelmässig über aktuelle Gefahren und über zu treffende Massnahmen informiert.

Verschlüsselung

Art. 25

Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netze.

Virenschutz / Internet

Art. 26

Virenschutzprogramme werden auf allen IKT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Weisungen

Art. 27

Die Mitarbeitenden werden angewiesen, die Gesetze sowie die vertraglichen Regelungen und internen Richtlinien einzuhalten. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmassnahmen. Informationssicherheitsfragen und Hinweise auf Schwachstellen werden an die für die Informationssicherheit verantwortliche Person gerichtet.

Zutritt

Art. 28

Gebäude und Räume sowie IKT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.

Physische Sicherheit

Art. 29

Brandschutzmassnahmen, Zutrittskontrolle usw. sind angemessen geregelt.

V. Informationssicherheitsorganisation

Allgemein

Art. 30

Zur Erreichung des angestrebten Informationssicherheitsniveaus sowie der festgelegten Informationssicherheitsziele wird eine Informationssicherheitsorganisation (Anhang) aufgebaut.

Ressourcen

Art. 31

Für den Aufbau und den Betrieb der Informationssicherheitsorganisation werden ausreichende finanzielle und personelle Ressourcen zur Verfügung gestellt.

Funktionen

Art. 32

Die zentralen Funktionen in der Informationssicherheitsorganisation sind:

- Die Schulpflege
- Die Geschäftsleitung Bildung
- Die/der Chief Information Security Officer CISO
- Die Informationssicherheitsverantwortlichen der Geschäftsbereiche ISV
- Der/die Datenschutzberater/in
- Die Daten- und Anwendungsverantwortlichen der Geschäftsbereiche DAV

Schulpflege

Art. 33

Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit. Sie legt die Leitlinie "Informationssicherheit an der Schule Wetzikon" fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel.

Geschäftsleitung Bildung

Art. 34

Die Geschäftsleitung Bildung trägt die operative Verantwortung für die Informationssicherheit.

Sie bestimmt

- eine/n CISO;
- eine/n DB;

Sie weist diesen Funktionen in ihren Stellenbeschreibungen ihre Rollen und Aufgaben zu.

Sie stellt sicher, dass die Beschlüsse der Schulpflege zur Informationssicherheit umgesetzt werden.

Chief Information Security Officer CISO

Art. 35

Der/die CISO ist zuständig für die Erreichung und Überwachung des angestrebten Sicherheitsniveaus, der Einhaltung der Informationssicherheitsziele und die Umsetzung der Informationssicherheitsmassnahmen an der Schule Wetzikon:

- Er/Sie trägt die Verantwortung für die Umsetzung der Leitlinie sowie der damit zusammenhängenden Dokumente.
- Er/Sie koordiniert sämtliche Aktivitäten im Bereich der Informationssicherheit.
- Er/Sie ist verantwortlich für die Ausarbeitung und Umsetzung eines Sicherheitskonzepts.
- Der/Die CISO ist der/dem Stadtschreiber/in unterstellt.
- Er/Sie berichtet regelmässig in der Geschäftsleitung Bildung über seine/ihre Arbeit und den Stand der Umsetzung.

Informationssicherheitsverantwortliche/r ISV

Art. 36

Der/Die Informationssicherheitsverantwortliche/r ISV unterstützt den/die CISO bei seiner/ihrer Arbeit, stellt die Schnittstelle zu den Schulen sicher und trägt die Verantwortung für die Umsetzung der Leitlinie sowie der damit zusammenhängenden Dokumente im Schulbetrieb. Er/Sie koordiniert in Absprache mit dem/der CISO sämtliche informationssicherheitsrelevanten Aktivitäten in den Schulen.

Daten- und Anwendungsverantwortliche DAV

Art. 37

Für alle Prozesse, Daten, Anwendungen, IKT- und Netzwerksysteme wird eine verantwortliche Person bestimmt, die in Absprache mit dem/der CISO den jeweiligen Schutzbedarf klassifiziert und die Zugriffsberechtigungen vergibt.

Datenschutzberater/in DB

Art. 38

Zur Sicherstellung und Umsetzung des Datenschutzes in der Schule Wetzikon wird ein/eine Datenschutzberater/in bestimmt. Er/Sie arbeitet in dieser Rolle eng mit dem/der CISO und dem ISV zusammen und ist seine/ihre interne Ansprechperson bei Datenschutzfragen.

Sicherstellung von Sicherheitsmassnahmen

Art. 39

Der/Die CISO ist in alle Projekte zu involvieren, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

Für sicherheitsrelevante Fragen sind der/die CISO, sowie der/die ISV in ihren Geschäftsbereichen weisungsberechtigt.

Sie sind die Anlaufstellen für Informationssicherheitsfragen und Hinweise auf Schwachstellen.

Schulung der Mitarbeitenden

Art. 40

Der/die CISO legt besonderes Gewicht auf eine angemessene Sensibilisierung und ausreichende Weiterbildung der Mitarbeitenden.

Sicherheitsüberprüfung

Art. 41

Das Informationssicherheitskonzept inkl. aller Dokumentationen wird regelmässig auf die Aktualität und die Wirksamkeit geprüft. Die Überprüfung orientiert sich am jeweils aktuellen Stand der Technik sowie an nationalen und internationalen Standards.

Umsetzung

Art. 42

Die Geschäftsleitung Bildung wird mit der Umsetzung dieser Leitlinie beauftragt.

VI. Schlussbestimmungen

Inkraftsetzung

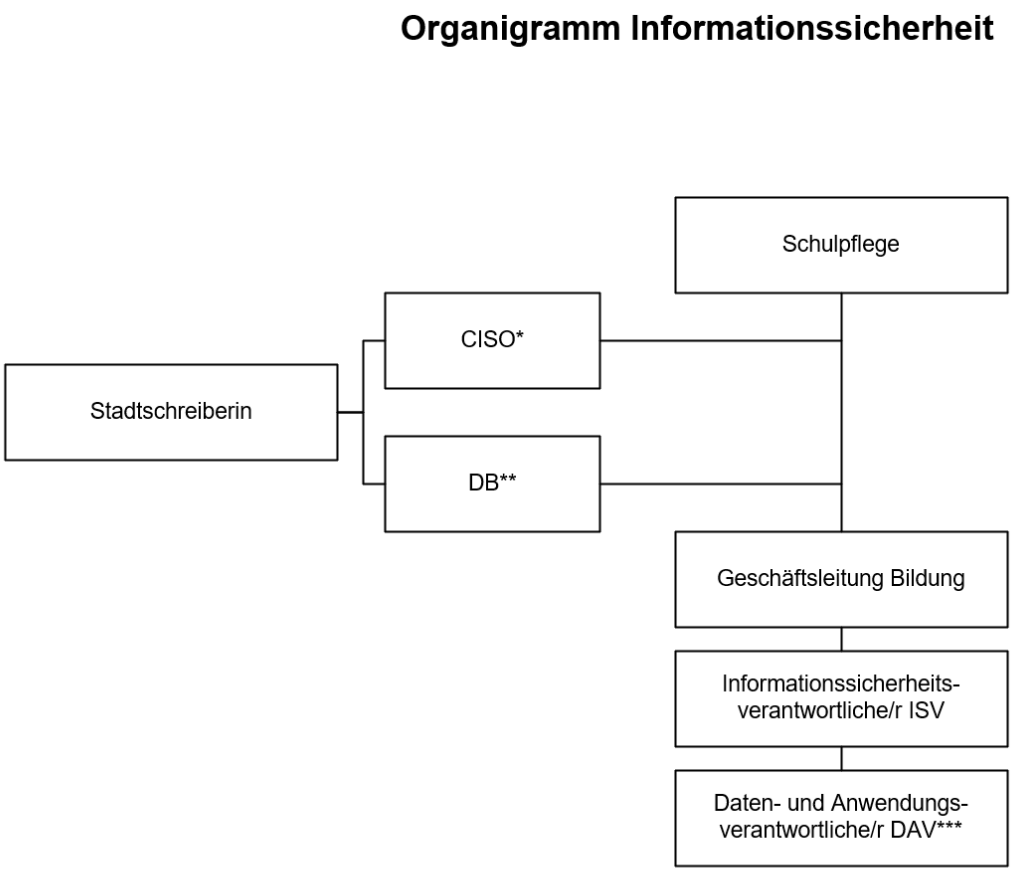
Art. 43

Die Leitlinie für die Informationssicherheit an der Schule Wetzikon wird von der Schulpflege am 23. Juni 2026 genehmigt und per sofort in Kraft gesetzt.

Artikel	Änderungsbeschrieb	Version	Beschluss (Behörde / Nr. / Datum)

Anhang

Organigramm Informationssicherheit



*Chief Information Security Officer / ** Datenschutzberater/in / ***eine oder mehrerer Personen pro Schule