Stadt Affoltern am Albis

160.1

Leitlinie zur Informationssicherheit (Sicherheitsleitline)

vom 2. September 2025

In Kraft seit: 1. November 2025
(nachgeführt bis 1. November 2025)

Inhaltsverzeichnis

Art. 1 Einleitung

[1]Die Stadt Affoltern am Albis ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie (ICT-Systeme) abhängig. Zur Gewährleistung der Integrität, Vertraulichkeit, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme gemäss Gesetz über die Information und den Datenschutz (IDG), verabschiedet der Stadtrat diese Leitlinie zur Informationssicherheit.

[2]Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Stadt angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert.

[3]Diese Leitlinie beinhaltet eine Beschreibung der Informationssicherheitsorganisation und definiert die Rollen.

Art. 2 Geltungsbereich

Diese Sicherheitsleitlinie und die damit zusammenhängenden Dokumente gelten für Mitarbeitende, Behörden und Kommissionsmitglieder sowie alle Nutzende der ICT-Infrastruktur der Politischen Gemeinde Affoltern am Albis. Vertragspartnerinnen und Vertragspartner, welche Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

Art. 3 Informationssicherheitsniveau

Die Stadt strebt ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf an. Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

Art. 4 Informationssicherheitsziele

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele:

<u>Integrität</u>
Informationen müssen richtig und vollständig sein.

<u>Nachvollziehbarkeit</u>
Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

<u>Verantwortung</u>
Politische Behörden und die Mitarbeitenden der Stadt sind sich ihrer Verantwortung beim Umgang mit Informationen, ICT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.

<u>Verfügbarkeit</u>
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 zugeordnet werden können.

Art. 5 Massnahmen

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen:

Aktualisierungen (Updates)
Alle ICT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.

Archivierung / Löschung
Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht oder vernichtet.

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

Datenschutz
Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet.

Datensicherung (Backup)
Die Datensicherung wird regelmässig durchgeführt. Interne 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.

ICT-Systeme
Die ICT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannten Sicherheitsstandards) und betrieben, mittels eines Änderungsmanagements verwaltet und in einem geregelten Prozess ausser Betrieb genommen.

Mobile Geräte / Software
Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten sowie der Installation von Software auf Arbeitsplatzrechnern und Servern sind separat geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.

Monitoring
Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.

Netzwerk / Firewall
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 (z. B. Leunet) wird eingehalten.

Organisation
Die Organisation orientiert sich an der ordentlichen Organisationsstruktur gemäss Organisations- und Geschäftsreglement der Stadt Affoltern am Albis (OGR). Für alle Funktionen ist die Stellvertretung im OGR oder in den Stellenbeschrieben geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.

Outsourcing
Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet.

Passwörter
Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch persönliche Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt. Wenn immer möglich wird eine Zwei-Faktor-Authentifizierung eingerichtet.

Sensibilisierung / Schulung
Die Mitarbeitenden nehmen regelmässig an internen Sicherheitsschulungen teil. Sie werden über aktuelle Gefahren und zu treffende Massnahmen informiert.

Verschlüsselung
Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotentials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, wie z. B. von besonderen Personendaten, erfolgt über öffentliche Netze verschlüsselt.

Virenschutz / Internet
Viren-Schutzprogramme werden auf allen ICT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Weisungen
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
Gebäude und Räume sowie ICT-Systeme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.

Art. 6 Informationssicherheitsorganisation, Grundsatz

[1]Für die Abteilung Seewadel - Zentrum für Gesundheit und Alter liegt die Verantwortung für die Informationssicherheit bei der Geschäftsleiterin oder beim Geschäftsleiter Seewadel und für den pädagogischen Bereich der Abteilung Bildung bei der Schulpflege.

[2]Die zentralen Rollen in der Informationssicherheitsorganisation für die übrigen Abteilungen haben die Stadtschreiberin oder der Stadtschreiber, die Abteilungsleiterin oder der Abteilungsleiter Präsidiales, die Leiterin ICT oder der Leiter ICT und die für die einzelnen Abteilungen und Bereiche zuständigen Abteilungs- und Bereichsleitenden oder/und Fachapplikationsverantwortlichen inne.

Art. 7 Informationssicherheitsorganisation

[1]Der Stadtrat trägt die Gesamtverantwortung für die Informationssicherheit mit Ausnahme des pädagogischen Bereichs, wofür die Primarschulpflege verantwortlich ist. Er legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel.

[2]Die Stadtschreiberin oder der Stadtschreiber trägt die operative Verantwortung für die Informationssicherheit und ist interne Ansprechperson bei Datenschutzfragen und Anfragen nach IDG.

[3]Als Informationssicherheitsverantwortliche oder Informationssicherheitsverantwortlicher (ISV) wird die Abteilungsleiterin oder der Abteilungsleiter Präsidiales bezeichnet. Sie oder er ist in der Funktion als ISV für die Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus sowie für Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich. Für sicherheitsrelevante Fragen ist die oder der ISV weisungsberechtigt. Sie oder er ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen. Sie oder er wird in alle relevanten Projekte involviert, um frühzeitig die datenschutzrelevanten Aspekte einbringen zu können.

[4]Die Leiterin oder der Leiter ICT verantwortet alle ICT-Prozesse, ICT-Anwendungen, ICT- und Netzwerksysteme und bestimmt einen allfälligen Schutzbedarf in Zusammenarbeit mit der oder dem ISV sowie den Abteilungs- und Bereichsleitenden und den Fachapplikationsverantwortlichen. Die Leiterin oder der Leiter ICT vergibt die Zugriffsberechtigungen oder bezeichnet die dafür zuständigen Personen (z. B. Fachapplikationsverantwortliche). Die Leiterin oder der Leiter ICT wird in alle ICT-Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können. Sie oder er verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Art. 8 Kontinuierliche Verbesserung der Informationssicherheit

Der Stadtrat unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Er gibt mit der periodischen Überarbeitung dieser Sicherheitsrichtlinie die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung.

Art. 9 Inkrafttreten

Diese Leitlinie zur Informationssicherheit tritt per 1. November 2025 in Kraft. Gleichzeitig wird die ICT-Sicherheitsleitlinie vom 11. August 2015 aufgehoben.

Affoltern am Albis, 2. September 2025

Stadtrat Affoltern am Albis

Präsidentin	Schreiber
Eveline Fenner	Stefan Trottmann