Reglement über die Informationssicherheit der Gemeinde Riehen (Informationssicherheitsreglement)

Vom 6. Juli 2021 (Stand 1. August 2021)

Der Gemeinderat Riehen,

gestützt auf § 8 Abs. 4 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 [1)] und auf § 24 Abs. 3 lit. f und g der Gemeindeordnung der Einwohnergemeinde Riehen vom 27. Februar 2002 [2)],

beschliesst:

I. Allgemeines

§ 1 *Gegenstand*

[1] Dieses Reglement regelt unter Berücksichtigung des übergeordneten kantonalen Rechts sowie kantonaler Vorgaben die Umsetzung der Informationssicherheit in der Gemeinde Riehen, insbesondere die Zuständigkeiten, die Sicherheitsprozesse sowie die Sicherstellung des Geschäftsbetriebs.

§ 2 *Zweck der Informationssicherheit*

[1] Die Informationssicherheit bezweckt:

a) die Gewährleistung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Informationen, die zur Ausübung der geschäftlichen Tätigkeit der Gemeinde verwendet werden, ungeachtet der Art ihrer Darstellung und Speicherung;
b) die Zurechenbarkeit und Nachvollziehbarkeit der Informationsbearbeitungen durch angemessene Massnahmen;
c) die Sicherheit von IT-Systemen bei der Bearbeitung, Speicherung und Übermittlung von elektronischen Informationen und
d) den Einsatz datenschutzfreundlicher Technologien.

§ 3 *Geltungsbereich*

[1] Dieses Reglement gilt für alle Organisationseinheiten der Gemeinde Riehen im Sinne von § 3 Abs. 1 IDG und für alle Informationen gemäss § 3 Abs. 2 IDG.
[2] Die Regelungen betreffen alle Informationen und IT-Systeme im Zusammenhang mit der Aufgabenerfüllung der Gemeinde Riehen.
[3] Ziehen Organisationseinheiten externe Leistungserbringende für ihre Aufgabenerfüllung bei, stellen die Organisationseinheiten vertraglich sicher, dass die externen Leistungserbringenden die Anforderungen dieses Reglements ebenfalls erfüllen.

§ 4 *Umgang mit Informationen*

[1] Die Organisationseinheiten schützen Informationen durch angemessene organisatorische und technische Massnahmen. Die Schutzziele richten sich nach § 2.
[2] Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

1) SG 153.260
2) RiE 111.100

§ 5 *Umgang mit Informatiksystemen*

[1] Es dürfen für die Aufgabenerfüllung der Gemeinde Riehen nur die von der Leitung Informatikbetrieb bereitgestellten oder freigegebenen IT-Systeme benutzt werden.
[2] Vorbehalten bleibt der Einsatz externer IT-Systeme, der von der Leitung Informatikbetrieb bewilligt wurde.

II. Zuständigkeiten und Aufgaben

§ 6 *Gemeinderat*

[1] Der Gemeinderat trägt die Gesamtverantwortung für die Informationssicherheit und sorgt für ein entsprechendes Informationssicherheitsmanagementsystem, welches auch ein Risikomanagementsystem betreffend Informationssicherheit umfasst. Er stellt die notwendigen Ressourcen sicher.
[2] Er definiert die strategischen Vorgaben zur Informationssicherheit, zur digitalen Transformation der Verwaltung und zum Umgang mit den damit verbundenen Risiken.
[3] Er steuert die Umsetzung der jeweiligen Strategien mit dem Informationssicherheitsmanagementsystem.

§ 7 *Verwaltungsleiterin oder Verwaltungsleiter*

[1] Die Verwaltungsleiterin oder der Verwaltungsleiter stellt die operative Umsetzung der Informationssicherheit und der Anforderungen der digitalen Transformation mit angemessenen Massnahmen sicher.
[2] Sie oder er:

a) stellt die Führung und zeitgerechte Anpassung des Informationssicherheits- und des Risikomanagementsystems an veränderte Verhältnisse sicher;
b) setzt einen beratenden Fachausschuss ein;
c) erlässt den übergeordneten Massnahmenplan und genehmigt die Massnahmen- und Notfallpläne der Organisationseinheiten;
d) genehmigt die Klassifizierung der Informationen, das Schutzobjektinventar und das Register der Datensammlungen;
e) entscheidet über das Vorgehen betreffend die Übernahme von Risiken, schwerwiegender Sicherheits- und Datenschutzvorfälle und Verstösse gegen Sicherheitsvorgaben;
f) erlässt die notwendigen Richtlinien und Weisungen zur Informationssicherheit.

§ 8 *Generalsekretariat, Abteilungen, Fachbereiche*

[1] Die Generalsekretärin oder der Generalsekretär, die Abteilungsleitungen und die Fachbereichsleitungen sind in ihren Zuständigkeitsbereichen für die Sicherstellung der Informationssicherheit gemäss den Richtlinien und Weisungen Informationssicherheit verantwortlich.

§ 9 *Leitung Informatikbetrieb*

[1] Die Leitung Informatikbetrieb ist für die Entwicklung, Beschaffung, Bereitstellung und den Unterhalt der IT-Systeme sowie für deren sicheren Betrieb verantwortlich.
[2] Sie unterstützt die Organisationseinheiten beim sicheren Betrieb ihrer Fachanwendungen und der Umsetzung und Kontrolle der Sicherheitsmassnahmen.

§ 10 *Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter*

[1] Die oder der Informationssicherheitsbeauftragte ist die Anlaufstelle für den Bereich Informationssicherheit und hat insbesondere folgende Aufgaben:

a) Beratung und Unterstützung bei der strategischen Planung und operativen Umsetzung der Informationssicherheit;

b) Beobachten von Entwicklungen und Risiken im Bereich der Informationssicherheit;
c) Koordination der Umsetzung der Informationssicherheit;
d) Führung und Überprüfung des Informationssicherheitsmanagementsystems und des Schutzobjektinventars;
e) Mitarbeit in Projekten, die für die Informationssicherheit relevant sind;
f) Durchführung von Risikoanalysen und jährliche Überprüfung der organisatorischen und technischen Sicherheitsmassnahmen;
g) Analyse, Behandlung und Dokumentation von Sicherheitsvorfällen;
h) Erarbeitung der notwendigen Richtlinien und Weisungen sowie technischer Vorgaben;
i) Ausarbeitung von Empfehlungen zu risikomindernden Massnahmen;
j) Sensibilisierung und Schulung der Mitarbeitenden.

§ 11 *Eignerinnen und Eigner, Anwendungsverantwortliche*

[1] Alle Schutzobjekte, insbesondere IT-Systeme, Informationen, Gebäude usw. werden einer Objekteignerin oder einem Objekteigner zugeordnet. Sie sind verantwortlich für die Inventarisierung, Klassifizierung und die Sicherheit ihrer Schutzobjekte in Zusammenarbeit mit der oder dem Informationssicherheitsbeauftragten und überprüfen diese regelmässig.
[2] Die Dateneignerinnen und -eigner tragen die Verantwortung für die Sicherheit der Informationen sowie für deren korrekten Umgang und den rechtmässigen Zugriff auf die Informationen.
[3] Die Anwendungsverantwortlichen sind für ihre Applikationen und damit auch für die Sicherheit der darauf bearbeiteten Informationen verantwortlich.
[4] Die Systemeignerinnen und -eigner sind für den ordnungsgemässen Betrieb ihrer Systeme zuständig. Sie tragen die Betriebsverantwortung für die Systeme.
[5] Jedem Informationssicherheitsrisiko wird eine Risikoeignerin oder ein Risikoeigner im Sinne des Internen Kontrollsystems zugeordnet.
[6] Die Aufgaben der Eignerinnen und Eigner sowie der Anwendungsverantwortlichen werden in einer Richtlinie zur Informationssicherheit geregelt.

III. Sicherheitsprozesse

§ 12 *Schutzkatalog und Schutzbedarfsanalyse*

[1] Die oder der Informationssicherheitsbeauftragte definiert in einem Schutzkatalog die Schutzziele gemäss § 2.
[2] Die Schutzbedarfsanalyse bildet die Grundlage für die Festlegung und Umsetzung der Schutzmassnahmen.
[3] Besteht ein erhöhter oder sehr hoher Schutzbedarf, müssen die Dateneignerinnen und -eigner eine Risikoanalyse durchführen.

§ 13 *Schutzobjektinventar*

[1] Die Objekteignerinnen und -eigner analysieren und klassifizieren ihre Daten bzw. Objekte mittels Schutzbedarfsanalyse gemäss dem Schutzkatalog und den Richtlinien und Weisungen Informationssicherheit, erfassen sie im Schutzobjektinventar und überprüfen dies mindestens einmal jährlich.

§ 14 *Risikoregister Informationssicherheit*

[1] Risiken der Informationssicherheit werden im Rahmen des Risikomanagements einheitlich bewertet, im Risikoregister dokumentiert und einer Risikoeignerin oder einem Risikoeigner zugewiesen. Das Risikoregister Informationssicherheit ist Teil des Risikomanagementsystems der Gemeinde Riehen und wird von der oder vom Informationssicherheitsbeauftragten periodisch überprüft.
[2] Ist eine Risikoelimination nicht möglich oder wirtschaftlich nicht tragbar, sind die entstehenden Restrisiken auszuweisen.

§ 15 *Massnahmenpläne*

[1] Die oder der Informationssicherheitsbeauftragte definiert in einem übergeordneten Massnahmenplan, wie die gesetzlichen und internen Vorgaben innerhalb der Gemeindeverwaltung umzusetzen sind. Dieser wird von der Verwaltungsleiterin oder dem Verwaltungsleiter erlassen.
[2] Die Generalsekretärin oder der Generalsekretär, die Abteilungsleitungen und die Fachbereichsleitungen sind für die Erarbeitung der abteilungsspezifischen Massnahmenpläne in ihren Zuständigkeitsbereichen verantwortlich, welche von der Verwaltungsleiterin oder vom Verwaltungsleiter genehmigt werden.

§ 16 *Zugriffs-, Berechtigungs-, Aufbewahrungs- und Löschkonzept*

[1] Die oder der Informationssicherheitsbeauftragte führt und überprüft regelmässig das übergeordnete Zugriffs- und Berechtigungskonzept sowie das übergeordnete Aufbewahrungs- und Löschkonzept, welche den Zugriff auf Personendaten sowie deren Aufbewahrung und Löschung definieren.
[2] Sie oder er wird von den Dateneignerinnen und -eignern, den Anwendungsverantwortlichen und Fachstelle Records Management unterstützt.

§ 17 *Nichteinhalten von Sicherheitsmassnahmen*

[1] Wenn aus berechtigten Gründen einzelne Sicherheitsmassnahmen nicht umgesetzt werden können, muss das damit verbundene Risiko beurteilt, dokumentiert und durch die Risikoeignerin oder den Risikoeigner erfasst werden.
[2] Diese Risiken müssen der Verwaltungsleiterin oder dem Verwaltungsleiter gemeldet werden. Sie oder er informiert den Gemeinderat über das weitere Vorgehen.
[3] Abweichungen gegenüber Vorgaben der Informationssicherheit sind gemäss den Richtlinien Informationssicherheit zu melden.

§ 18 *Sicherheitsvorfälle*

[1] Als Sicherheitsvorfälle gelten Verstösse gegen Sicherheitsvorgaben und sicherheitsrelevante Ereignisse, die effektiv einen Schaden verursacht haben oder einen solchen beinahe verursacht hätten, sowie vermutete oder tatsächliche Verstösse gegen den Datenschutz oder die Datenschutzbestimmungen.
[2] Eine Datenschutzverletzung liegt vor, wenn durch eine Verletzung der Informationssicherheit bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder wenn Unbefugte Zugang zu solchen Personendaten erhalten. Datenschutzverletzungen sind gemäss den Vorgaben des IDG zu melden.
[3] Solche Vorfälle sind zudem umgehend den zuständigen Abteilungsleitungen und der oder dem Informationssicherheitsbeauftragten zu melden, damit die notwendigen Massnahmen eingeleitet werden können. Bei schweren Fällen sind die Verwaltungsleiterin oder der Verwaltungsleiter sowie der Gemeinderat zu informieren.
[4] Die externen Leistungserbringenden informieren die auftraggebende Organisationseinheit unverzüglich über eine Datenschutzverletzung.
[5] Sicherheitsvorfälle werden von der oder vom Informationssicherheitsbeauftragten dokumentiert und ausgewertet.

IV. Sicherstellung des Geschäftsbetriebs und Berichterstattung

§ 19 *Notfallkonzepte*

[1] Für Geschäftsprozesse, deren Ausfall oder Beeinträchtigung negative Folgen für die Gemeindeverwaltung Riehen oder die Einwohnerinnen und Einwohner der Gemeinde haben können, entwickeln die Generalsekretärin oder der Generalsekretär, die Abteilungsleitungen und die Fachbereichsleitungen entsprechende Notfallkonzepte.
[2] Die Leitung Informatikbetrieb entwickelt einen Notfallplan für den Informatikbetrieb.

[3] Im Notfallkonzept wird das Verfahren festgelegt, welches eine schnelle, wirksame und planmässige Reaktion auf sicherheitsrelevante Ereignisse, insbesondere Betriebsausfälle, ermöglicht. Es definiert die Rahmenbedingungen für die einzelnen Notfallpläne.

§ 20 *Berichterstattung zur Informationssicherheit*

[1] In einem jährlichen Bericht fasst die oder der Informationssicherheitsbeauftragte wichtige Vorkommnisse wie Sicherheitsvorfälle, Auditergebnisse, Risiken und Projekte im Bereich der Informationssicherheit zu Handen des Gemeinderats und der Verwaltungsleiterin oder des Verwaltungsleiters zusammen.
[2] Sie oder er wird bei der Berichterstellung von der Generalsekretärin oder vom Generalsekretär, den Abteilungsleitungen, den Fachbereichsleitungen und der Leitung Informatikbetrieb unterstützt.

V. Übergangs- und Schlussbestimmungen

§ 21

[1] Bisherige IT-Systeme, Applikationen und Datensammlungen sind bis zum 31. Dezember 2022 an die Vorgaben dieses Reglements anzupassen.

Schlussbestimmung

Dieses Reglement ist zu publizieren; es tritt am 1. August 2021 in Kraft.