Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 16. April 2025

438. Allgemeine Informationssicherheitsrichtlinie (Neuerlass, Stellenpläne)

1. Ausgangslage

Angesichts der zunehmenden Bedrohung durch Cyberangriffe ist es unerlässlich, angemessene und wirksame Massnahmen zum Schutz der Informationen und der damit verbundenen Werte zu ergreifen. Eine starke Informationssicherheit schützt nicht nur die Einwohnerinnen und Einwohner und ihre Daten, sondern stärkt auch das Vertrauen in die digitalen Dienstleistungen des Kantons. Sie ist für eine sichere und effiziente Verwaltung unerlässlich und fördert gleichzeitig Innovation und Wachstum im Kanton.

Gemäss § 7 Abs. 1 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (IDG; LS 170.4) sind die öffentlichen Organe verpflichtet, Informationen durch angemessene organisatorische und technische Massnahmen zu schützen. Diese Massnahmen dienen den Schutzzielen Vertraulichkeit, Unversehrtheit, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit (vgl. § 7 Abs. 2 IDG). Sie richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik (§ 7 Abs. 3 IDG). Zur Umsetzung dieser gesetzlichen Vorgaben erliess der Regierungsrat am 3. September 2019 (RRB Nr. 795/2019) die Allgemeine Informationssicherheitsrichtlinie (AISR). Die AISR legt in Anlehnung an international anerkannte Standards die Grundsätze zur Wahrung der Informationssicherheit in der kantonalen Verwaltung sowie die inhaltlichen Grundzüge der untergeordneten Regelungen fest. Sie regelt zudem den Aufbau des Informationssicherheits-Managementsystems und die Organisation der Informationssicherheit in der kantonalen Verwaltung.

2. Revisionsbedarf

Um weiterhin einen angemessenen und nachhaltigen Schutz zu gewährleisten, ist die AISR periodisch an die technologischen, gesellschaftlichen und politischen Entwicklungen anzupassen. Seit dem Erlass der AISR am 3. September 2019 wurden verschiedene Ereignisse identifiziert, die eine Anpassung erfordern. Dazu gehören Krisen wie die Covid-19-Pandemie, die Kriege in der Ukraine und im Nahen Osten, neue Technologien wie Künstliche Intelligenz, Cloud und Internet of Things, die

neu festgesetzte Cybersicherheitsstrategie (RRB Nr. 676/2022), überarbeitete Normen wie ISO/IEC 27001/2:2022, das Informationssicherheitsgesetz (SR 128) sowie die fortschreitende Zentralisierung der IKT-Grundversorgung.

Ergänzend zur Ausrichtung auf die Bedürfnisse und die Bedrohungslage des Kantons wurden weiterführende Optimierungspotenziale identifiziert, bewertet und entlang der geltenden Gesetze, Verordnungen und Beschlüsse in die vorliegende neue Fassung der AISR integriert.

3. Wesentliche Anpassungen

In der überarbeiteten Fassung der AISR wird die Vielfalt der Direktionen und der Staatskanzlei berücksichtigt, um eine bedarfsgerechte Umsetzung der Anforderungen an die Informationssicherheit in den verschiedenen Verwaltungseinheiten zu ermöglichen. Gleichzeitig regelt die AISR mit der «Gemeinsamen Basis» kantonale Vorgaben und Schnittstellen, fördert die Zusammenarbeit und nutzt Synergien optimal, z. B. durch kantonale Informationssicherheitsstandards und Informationssicherheitsservices.

Betont wird die Verantwortung der Vorsteherinnen und Vorsteher der Direktionen und der Staatskanzlei für die Umsetzung der Informationssicherheit in ihrer Direktion bzw. in der Staatskanzlei (§ 60 Abs. 1 lit. e Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung [LS 172.11] und § 7 Abs. 1 IDG, vgl. Ziff. 7.2.1 AISR). Die Entscheidungskompetenzen der Direktionen und der Staatskanzlei werden konkretisiert, und die Direktionen und die Staatskanzlei werden befähigt, die Anforderungen an die Informationssicherheit angemessen und wirksam umzusetzen.

Unterstützt werden diese Prozesse sowie die ganzheitliche Betrachtung der Informationssicherheit (aller Formen von Informationen und damit verbundenen Werten) durch die konsequente Orientierung an der international anerkannten Normenreihe ISO/IEC 27000.

Gleichzeitig können die Besonderen Informationssicherheitsrichtlinien (BISR) durch die stärkere Entkoppelung von der AISR eigenständig auf die Bedürfnisse der kantonalen Verwaltung ausgerichtet und ein kontinuierlicher Schutz gewährleistet werden.

Der Regierungsrat, die Direktionsvorsteherinnen und Direktionsvorsteher sowie die Staatsschreiberin oder der Staatsschreiber erhalten Hilfsmittel in Form von Kennzahlen sowie internen und externen Prüfergebnissen, die ihnen eine datengestützte Beurteilung und eine effiziente und effektive Steuerung der Informationssicherheit in ihrem Verantwortungsbereich ermöglichen sollen.

4. Rückmeldungen

Aus den Rückmeldungen zum Vorentwurf der AISR geht hervor, dass die Direktionen und die Staatskanzlei den Handlungsbedarf anerkennen und die Überarbeitung der geltenden AISR begrüssen. Dabei wurden mehrere Punkte positiv hervorgehoben, insbesondere

- die Orientierung an der aktuellen ISO/IEC-Norm,
- die Transparenz durch die Definition klarer Anforderungen und Verantwortlichkeiten,
- die Möglichkeit, die Informationssicherheit kontextspezifisch auszugestalten.

Gleichzeitig wurden auch Bedenken geäussert. Es wurde auf mögliche Konflikte bei der Umsetzung der Anforderungen hingewiesen, insbesondere in Bezug auf konkurrierende Ziele und Aufgaben sowie den damit verbundenen Mittelbedarf. Unsicherheiten resultierten auch aus der Entkopplung der BISR von der AISR. Zudem wurden vereinzelt die Objektivität und Vollständigkeit der Prüfaktivitäten hinterfragt.

Während allfällige Zielkonflikte sowie der damit einhergehende Mittelbedarf nachgelagert in den Informationssicherheitsstrategien der Direktionen und der Staatskanzlei zu klären sind (vgl. Abschnitt 5), wird den weiteren Bedenken wie folgt Rechnung getragen:

- Zur Gewährleistung qualitativ zuverlässiger Einhalteprüfungen in den Direktionen und der Staatskanzlei werden diese nach deren Abschluss durch eine zweite Instanz beurteilt. Ergänzend werden die externen Prüftätigkeiten von der individuellen Umsetzung in den Direktionen und der Staatskanzlei auf das kantonale Regelwerk bzw. die «Gemeinsame Basis» ausgeweitet.
- Die festgelegten Inhalte der BISR (93 Informationssicherheitsmassnahmen gemäss ISO/IEC 27001 Anhang A bzw. ISO/IEC 27002) werden transparent den einzelnen Richtlinien zugewiesen. Weiter soll das Gremium Steuerung Digitale Verwaltung und IKT (SDI) beim Erlass der BISR ausdrücklich auf deren Angemessenheit in Bezug auf die Vorgaben der AISR und den Bedarf der kantonalen Verwaltung achten.

5. Stellenbedarf

Mit RRB Nr. 1193/2020 wurden 7,0 unbefristete Stellen Informatikspezialist/in mbA (Informationssicherheitsbeauftragte/r der Direktion / der Staatskanzlei, ISID) bewilligt. Zweck dieser Stellen ist es, den Betrieb (Aufbau und Weiterentwicklung) des Informationssicherheits-Managementsystems (ISMS) in den Direktionen und der Staatskanzlei sicher-

zustellen. Zusätzlich wurde mit diesem Beschluss eine gebundene Ausgabe von rund 3,2 Mio. Franken bewilligt, um Rückstände im Bereich der Informationssicherheit innerhalb der Direktionen und der Staatskanzlei aufzuarbeiten.

Ein Benchmark (Gartner, IT Key Metrics Data 2025: IT Security Measures – Analysis, 5. Dezember 2024) zeigt auf, dass die kantonale Verwaltung über die notwendigen Strukturen und personellen Mittel verfügt, um die Governance und das Management der Informationssicherheit auf strategischer Ebene zu gewährleisten.

Im Gegensatz zur strategischen Ebene wurde bei der operativen Umsetzung der technischen und organisatorischen Massnahmen gemäss BISR eine unzureichende personelle Ausstattung festgestellt. In den Direktionen und der Staatskanzlei sollen deshalb entsprechend dem Verteilschlüssel von RRB Nr. 1193/2020 7,0 auf zwei Jahre befristete Stellen Informatikspezialist/in mbA (LK 21) geschaffen werden, die als Fachexpertinnen und -experten die Umsetzung der Anforderungen der BISR sicherstellen sollen. Die Direktionen und die Staatskanzlei sind für den optimalen Einsatz dieser Stellen zur Erhöhung der Resilienz verantwortlich. Die Einreihung der neu zu schaffenden Stellen erfolgt analog zu den mit RRB Nr. 1193/2020 geschaffenen Stellen. Es handelt sich mithin um Aufstockungen von in den Stellenplänen der Direktionen und der Staatskanzlei bereits bestehenden Stellen, weshalb sich eine erneute Einreihungsprüfung erübrigt.

Diese zusätzlichen, auf zwei Jahre befristeten personellen Mittel sollen dazu dienen, die operative Informationssicherheit an den neuen Richtlinien auszurichten. Dadurch soll die Resilienz innerhalb der Verwaltung weiter gestärkt werden, bis die Informationssicherheitsstrategien der Direktionen und der Staatskanzlei gemäss Ziff. 5.3 AISR erlassen sind und der tatsächliche Personalbedarf feststeht bzw. das geplante Budget in den Konsolidierten Entwicklungs- und Finanzplan (KEF) eingestellt worden ist.

Die zusätzlichen Personalkosten für die Jahre 2026 und 2027 werden jeweils zur Hälfte in der Leistungsgruppe Nr. 4620, Informationssicherheitsbeauftragter, sowie dezentral in den Direktionen und der Staatskanzlei in den KEF 2026–2029 eingestellt. Diese Kosten sind im KEF 2025–2028 nicht berücksichtigt und müssen deshalb als unabdingbare Mehrbelastungen in den KEF 2026–2029 aufgenommen werden.

6. Schlussfolgerung

Die digitale Transformation als strategischer Schwerpunkt des Regierungsrates setzt Informationssicherheit voraus. Deshalb hat der Regierungsrat eine Cybersicherheitsstrategie festgesetzt (RRB Nr. 676/2022)

und zum Legislaturziel «In einem vielfältigen sich rasch verändernden Umfeld Agilität der Verwaltung und Vertrauen in den Staat stärken» (RRZ 10) die Massnahme festgelegt, dass die Cybersicherheitsstrategie umzusetzen sowie der Datenschutz und die Informationssicherheit in die Verwaltungsprozesse zu integrieren sind (Massnahme RRZ 10g, vgl. RRB Nr. 871/2023).

Bei der vorliegenden Fassung der AISR handelt es sich um eine überarbeitete und an die aktuelle Bedrohungslage, die Legislaturziele (RRB Nr. 871/2023), die Cybersicherheitsstrategie (RRB Nr. 676/2022) und die Normen (ISO/IEC 27001/2:2022) ausgerichtete Neufassung der 2019 erlassenen Richtlinie. Mit dem Neuerlass der AISR wird die Verantwortung für die Gewährleistung der Informationssicherheit in der kantonalen Verwaltung fortgeführt und den veränderten Herausforderungen Rechnung getragen.

Das Gremium SDI hat den Entwurf der überarbeiteten AISR an seiner Sitzung vom 26. September 2024 vorberaten und zustimmend zur Kenntnis genommen.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Es wird eine Allgemeine Informationssicherheitsrichtlinie erlassen.

II. Die Allgemeine Informationssicherheitsrichtlinie wird auf den 1. Januar 2026 in Kraft gesetzt. Die Allgemeine Informationssicherheitsrichtlinie vom 3. September 2019 wird auf diesen Zeitpunkt aufgehoben.

III. Für die Umsetzung der technischen und organisatorischen Vorgaben der Besonderen Informationssicherheitsrichtlinien werden mit Wirkung ab 1. Januar 2026 folgende auf zwei Jahre befristete Stellen geschaffen:

Direktion	Stellen	Richtposition	Klasse VVO
Direktion der Justiz und des Innern	1,0	Informatikspezialist/in mbA	21
Sicherheitsdirektion	1,0	Informatikspezialist/in mbA	21
Finanzdirektion	0,6	Informatikspezialist/in mbA	21
Volkswirtschaftsdirektion	1,0	Informatikspezialist/in mbA	21
Gesundheitsdirektion	0,8	Informatikspezialist/in mbA	21
Bildungsdirektion	1,0	Informatikspezialist/in mbA	21
Baudirektion	1,0	Informatikspezialist/in mbA	21
Staatskanzlei	0,6	Informatikspezialist/in mbA	21

IV. Die Direktionen und die Staatskanzlei werden ermächtigt, 50% der Personalkosten in den Jahren 2026 und 2027 gemäss Ziff. 5 der Erwägungen mit Intercompany-Rechnungen (Sachkontogruppen 3910/4910 Personalleistungen) der Leistungsgruppe Nr. 4620, Informationssicherheitsbeauftragter, zu belasten.

V. Mitteilung an die Direktionen des Regierungsrates und die Staatskanzlei.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli