Kanton Zürich
Regierungsrat

Allgemeine Informationssicherheitsrichtlinie

des Regierungsrates für die kantonale Verwaltung

vom 3. September 2019

Abkürzungen

AFI	Amt für Informatik
CB	Compliancebeauftragte/r
FAGIS	Fachgruppe IKT-Sicherheit
BD	Baudirektion
IKT	Informations- und Kommunikationstechnologie
IMA	Immobilienamt
ISID	IKT-Sicherheitsbeauftragte/r der Direktion oder Staatskanzlei
ISIK	IKT-Sicherheitsbeauftragte/r des Kantons Zürich
ISMS	Informationssicherheits-Managementsystem
IVAD	Informatikverantwortliche/r der Direktion oder Staatskanzlei
KAPO	Kantonspolizei
PA	Personalamt
RIVA	Risikoverantwortliche/r
RR	Regierungsrat
SDI	Gremium Steuerung Digitale Verwaltung und IKT
SK	Staatskanzlei
STAZH	Staatsarchiv

Inhalt

1. Geltungsbereich und Zweck

Diese Richtlinie ist die übergeordnete Informationssicherheitsrichtlinie für die kantonale Verwaltung des Kantons Zürich. Sie gilt damit für:

- die **Direktionen** und die **Staatskanzlei**,
- die **Bezirksverwaltung**,
- die **unselbstständigen Anstalten**.

Die Richtlinie gilt nicht für den Kantonsrat und die Gerichte, die dem Kantonsrat und den Gerichten angegliederten Einheiten, die selbstständigen Anstalten, die Gemeinden und die übrigen Aufgabenträger auf Gemeindeebene. Der Informationsaustausch der kantonalen Verwaltung mit diesen Einheiten richtet sich jedoch nach den Grundsätzen dieser Richtlinie über Beziehungen zu externen Personen. Den genannten Einheiten wird daher die Einhaltung der Richtlinie empfohlen, um diesen Informationsaustausch zu erleichtern.

Die Richtlinie dient der Umsetzung der gesetzlichen Regelungen zur Informationssicherheit in der kantonalen Verwaltung. Dies sind namentlich:

- § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (**IDG**; LS 170.4),
- §§ 12 ff. der Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (**IVSV**; LS 170.8).

Gemäss § 7 IDG haben die öffentlichen Organe Informationen durch angemessene organisatorische und technische Massnahmen zu schützen (Abs. 1). Die Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik (Abs. 3). Sie dienen den folgenden Schutzzielen (Abs. 2):

- **Vertraulichkeit**
  («Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen»),
- **Unversehrtheit** («Integrität»)
  («Informationen müssen richtig und vollständig sein»),
- **Verfügbarkeit**
  («Informationen müssen bei Bedarf vorhanden sein»),
- **Zurechenbarkeit**
  («Informationsbearbeitungen müssen einer Person zugerechnet werden können»),
- **Nachvollziehbarkeit**
  («Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein»).

Die Bestimmungen von §§ 12 ff. IVSV führen die Grundsätze von § 7 IDG aus und regeln insbesondere die Risiko- und Schutzbedarfsanalyse, die Sicherheitseinstufung, die Massnahmenplanung, den Überprüfungsmechanismus und die Informationsbearbeitung durch Dritte.

Die vorliegende Richtlinie führt diese Regelungen weiter aus, indem sie Folgendes festlegt:

- die **Grundsätze** zur Wahrung der Informationssicherheit (Ziffer 2 hinten),
- den **Aufbau** des Informationssicherheits-Managementsystems (Ziffer 3 hinten),
- die **Organisation** der Informationssicherheit (Ziffer 4 hinten),
- die inhaltlichen **Grundzüge** der untergeordneten Regelungen (Ziffer 5 hinten).

Die Regelungen dieser Richtlinie lehnen sich an international anerkannte Standards an und sind im Zweifel in deren Sinne auszulegen.

Die Richtlinie ist eine rechtlich verbindliche Weisung des Regierungsrates an die untergeordneten Einheiten der kantonalen Verwaltung. Sie geht früheren Richtlinien und Weisungen des Regierungsrates und der Verwaltungsstellen bei Widersprüchen vor. Abweichende gesetzliche Regelungen gehen ihr vor.

2. Grundsätze zur Informationssicherheit

In der kantonalen Verwaltung gelten die folgenden Grundsätze zur Wahrung der Informationssicherheit:

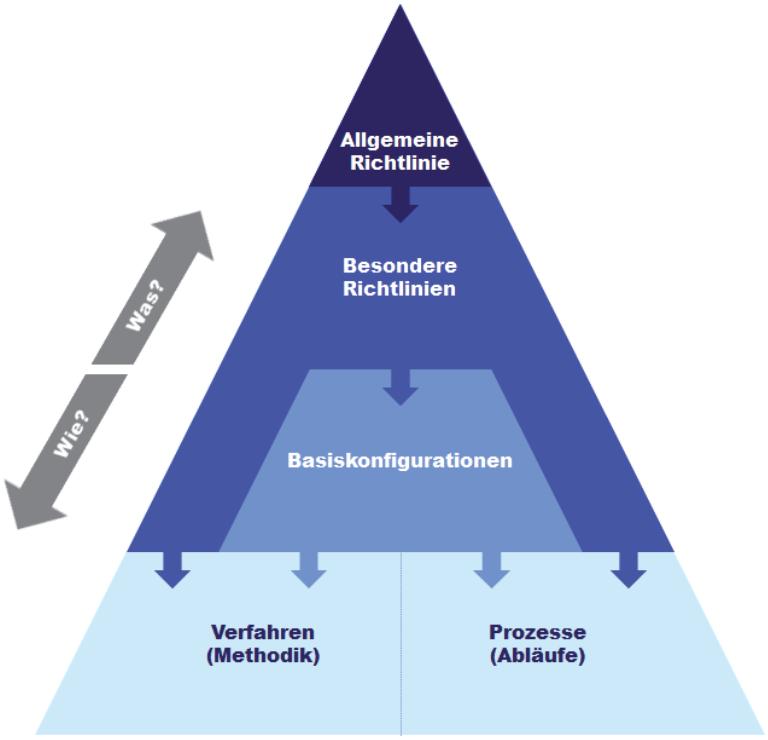
- **Rechtmässigkeit**
  Die gesetzlichen Vorschriften werden eingehalten.
- **Förmlichkeit**
  Die Aufgaben, Kompetenzen und Verantwortlichkeiten werden eindeutig festgelegt. Sicherheitsvorschriften werden in einem formell geregelten Prozess erlassen. Sicherheitsmassnahmen werden formell geplant und plangemäss umgesetzt.
- **Wirtschaftlichkeit**
  Der Aufwand für Sicherheitsmassnahmen steht in einem angemessenen Verhältnis zu den damit bekämpften Risiken, zur Risikobereitschaft des Kantons und zu ihrem Nutzen.
- **Bewusstsein**
  Der Regierungsrat und die Führungskräfte der kantonalen Verwaltung fördern eine positive Haltung zur Informationssicherheit. Die Mitarbeitenden werden für die Informationssicherheit sensibilisiert und dazu geschult.
- **Einbindung**
  Die Informationssicherheit wird in den Geschäftsprozessen und Projekten berücksichtigt.
- **Abstimmung**
  Die Tätigkeiten im Bereich der Informationssicherheit werden an den Legislaturzielen des Regierungsrates ausgerichtet und innerhalb der kantonalen Verwaltung abgestimmt. Die Verantwortlichen pflegen einen angemessenen Erfahrungsaustausch mit dem Bund und anderen Kantonen sowie in Interessen- und Berufsverbänden und spezialisierten Foren.
- **Auswertung**
  Die Wirksamkeit und Wirtschaftlichkeit der Sicherheitsmassnahmen wird regelmässig überprüft und nach Möglichkeit verbessert.

3. Aufbau des ISMS

Das Informationssicherheits-Managementsystem (ISMS) ist eine Sammlung von verbindlichen Regelungen, die alle für die kantonale Verwaltung massgeblichen Informationssicherheitsbereiche abdecken. Diese Regelungen stehen in der folgenden Rangordnung (von oben nach unten):

- Die **Allgemeine Informationssicherheitsrichtlinie** (AISR) ist die ranghöchste Regelung des ISMS. Sie bestimmt die Grundsätze zur Wahrung der Informationssicherheit, den Aufbau des ISMS, die Organisation der Informationssicherheit und die inhaltlichen Grundzüge der untergeordneten Regelungen.
- Die **Besonderen Informationssicherheitsrichtlinien** führen die Ziele und Grundsätze der AISR aus, indem sie Schlüsselanforderungen für die massgeblichen Informationssicherheitsbereiche festlegen.
- Die **Basiskonfigurationen** legen die technischen Einzelheiten fest, die zur Einhaltung der Schlüsselanforderungen gemäss den Besonderen Informationssicherheitsrichtlinien erforderlich sind.
- In **Verfahren** und **Prozessen** kann bei Bedarf näher ausgeführt werden, mit welchen Ansätzen und Abläufen die übergeordneten Regelungen umzusetzen sind.

Die übergeordneten Regelungen gehen den untergeordneten Regelungen bei Widersprüchen vor.



4. Organisation der Informationssicherheit

4.1 Zuständigkeiten

Die AISR ist von allen Mitarbeitenden der kantonalen Verwaltung einzuhalten. Die auftraggebenden Stellen haben sicherzustellen, dass die Richtlinie auch von externen Personen eingehalten wird, die im Dienst der kantonalen Verwaltung stehen.

Die Einhaltung der Richtlinie ist durch regelmässige Schulung und Überprüfung der Kenntnisse sicherzustellen. Bei Fragen und Unklarheiten sollen die Mitarbeitenden und externen Personen die IKT-Sicherheitsbeauftragte oder den IKT-Sicherheitsbeauftragten ihrer Direktion oder der Staatskanzlei (ISID) um Auskunft und Anweisung ersuchen.

Die folgenden Stellen tragen die Hauptverantwortung für die Umsetzung, Aufrechterhaltung und Überprüfung der Informationssicherheit in der kantonalen Verwaltung:

Steuerungsgremien	
Gremium	**Beschreibung**
Regierungsrat (RR)	Der Regierungsrat (RR) trägt als oberste leitende und vollziehende Behörde des Kantons die Gesamtverantwortung für die Informationssicherheit in der kantonalen Verwaltung. Er nimmt die Berichte des Gremiums SDI entgegen, insbesondere zur laufenden Verbesserung und Anpassung der Vorschriften, zu den bewilligten Abweichungen, zu den gemeldeten Informationssicherheitsvorfällen und zum Notfallmanagement. Der RR erlässt auf Antrag der Finanzdirektion und nach Vorberatung durch das Gremium SDI die AISR und passt diese bei Bedarf an.
Gremium «Steuerung Digitale Verwaltung und IKT» (SDI)	Das Gremium SDI befasst sich bei Bedarf im Auftrag des RR, auf Antrag seiner Mitglieder oder auf Antrag der Fachgruppe IKT-Sicherheit (FAGIS) mit Fragen, Entscheidungen und Regelungen zur direktionsübergreifenden Informationssicherheit. Es nimmt die Berichte der zuständigen Stellen zur laufenden Verbesserung und Anpassung der Vorschriften, zu den bewilligten Abweichungen, zu den gemeldeten Informationssicherheitsvorfällen und zum Notfallmanagement entgegen. Es berät den RR bei der Erfüllung seiner Aufgaben und erstattet ihm nötigenfalls Bericht. Das Gremium SDI berät die Anträge an den RR auf Erlass und Anpassung der AISR vor. Es erlässt die Besonderen Informationssicherheitsrichtlinien und passt diese bei Bedarf an. Die oder der Vorsitzende des Gremiums SDI informiert den RR bei Bedarf mit zusammenfassenden Mitteilungen über die wesentlichen Geschäfte des Gremiums SDI im Bereich der Informationssicherheit, insbesondere über die Berichterstattung der zuständigen Stellen zur laufenden Verbesserung und Anpassung der Vorschriften, zu den bewilligten Abweichungen, zu den gemeldeten Informationssicherheitsvorfällen und zum Notfallmanagement.

Fachstellen im Bereich der Informationssicherheit im Allgemeinen	
Stelle	**Beschreibung**
Staatsarchiv (STAZH)	Das Staatsarchiv (STAZH) ist verantwortlich für die Sicherheit der ihm abgelieferten Akten. Es pflegt einen regelmässigen Erfahrungsaustausch mit den öffentlichen Organen und berät diese im Rahmen der aus seiner Tätigkeit gewonnenen Erkenntnisse.
Risikoverantwortliche/r (RIVA)	Jede Verwaltungseinheit bestimmt für jedes wesentliche Informationssicherheitsrisiko in ihrem Zuständigkeitsbereich eine Risikoverantwortliche oder einen Risikoverantwortlichen. Die Risikoverantwortlichen sind zuständig für das Management der betreffenden Risiken, insbesondere für deren Überwachung und Einschätzung, die Bewertung ihrer Tragbarkeit, die daraus folgende Beurteilung des Schutzbedarfs sowie die Beantragung der nötigen Schutzmassnahmen.

Fachstellen im Bereich der IKT-Sicherheit im Besonderen	
Stelle	**Beschreibung**
Amt für Informatik (AFI)	Das Amt für Informatik (AFI) gewährleistet die IKT-Sicherheit im Rahmen der von ihm erbrachten IKT-Grundversorgung im Sinne der kantonalen IKT-Strategie. Es stellt die IKT-Sicherheitsbeauftragte oder den IKT-Sicherheitsbeauftragten des Kantons Zürich (ISIK) an.
Kantonspolizei (KAPO)	Die Kantonspolizei (KAPO), die vom Geltungsbereich der kantonalen IKT-Strategie ausgenommen ist, gewährleistet die IKT-Sicherheit in ihrem gesamten Bereich, einschliesslich der IKT-Grundversorgung, selber. Sie stimmt sich diesbezüglich mit dem AFI ab. Die KAPO bestimmt eine Verbindungsperson, die der Fachgruppe IKT-Sicherheit (FAGIS) angehört.
IKT-Sicherheitsbeauftragte/r des Kantons Zürich (ISIK)	Die oder der IKT-Sicherheitsbeauftragte des Kantons Zürich (ISIK) wird vom AFI angestellt. Sie oder er ist die zentrale Ansprechperson für alle Fragen der IKT-Sicherheit in der kantonalen Verwaltung. Sie oder er koordiniert die Bestrebungen zur nachhaltigen Erreichung eines angemessenen Grads an IKT-Sicherheit innerhalb der kantonalen Verwaltung, insbesondere durch Beratung, Schulung, Bereitstellung von Hilfsmitteln und Mitwirkung in Projekten, und unterstützt die IKT-Sicherheitsbeauftragten der Direktionen und der Staatskanzlei (ISID) bei der Erfüllung ihrer Aufgaben. Im Übrigen hat die oder der ISIK die Aufgaben und Kompetenzen gemäss den anwendbaren Informationssicherheitsvorschriften, insbesondere die Kompetenz zur Bewilligung von Ausnahmen sowie die Pflicht zur Berichterstattung über bewilligte Ausnahmen und gemeldete Informationssicherheitsvorfälle. Die oder der ISIK leitet die Fachgruppe IKT-Sicherheit (FAGIS), stellt dort die erkannten Probleme im Bereich der IKT-Sicherheit zur Diskussion und vertritt die Fachgruppe gegen aussen.
IKT-Sicherheitsbeauftragte/r der Direktion oder Staatskanzlei (ISID)	Jede Direktion und die Staatskanzlei bestimmt eine IKT-Sicherheitsbeauftragte oder einen IKT-Sicherheitsbeauftragten (ISID). Diese oder dieser ist in die Informatikorganisation der Direktion oder Staatskanzlei eingebunden und kennt deren Bedürfnisse. Die oder der ISID ist verantwortlich für die Umsetzung der IKT-Sicherheit in der Direktion oder der Staatskanzlei. Sie oder er legt für die Direktion oder die Staatskanzlei auf der Grundlage der Informationssicherheitsrichtlinien Basiskonfigurationen im Bereich der IKT-Sicherheit fest und passt diese bei Bedarf an. Die oder der ISID ist Mitglied der Fachgruppe IKT-Sicherheit (FAGIS) unter der Leitung der oder des ISIK.

Fachstellen im Bereich der IKT-Sicherheit im Besonderen	
Stelle	**Beschreibung**
Informatikverantwortliche/r der Direktion oder Staatskanzlei (IVAD)	Jede Direktion und die Staatskanzlei bestimmt eine Informatikverantwortliche oder einen Informatikverantwortlichen (IVAD). Die oder der IVAD legt für die Direktion oder die Staatskanzlei auf der Grundlage der Informationssicherheitsrichtlinien und der Basiskonfigurationen Verfahren und Prozesse im Bereich der IKT-Sicherheit fest und passt diese bei Bedarf an. Die Funktion der oder des IVAD ist vollständig von der Funktion der oder des ISID zu trennen.
Fachgruppe IKT-Sicherheit (FAGIS)	Die Fachgruppe IKT-Sicherheit (FAGIS) besteht aus zehn Mitgliedern, nämlich der oder dem ISIK und allen acht ISID sowie einer Verbindungsperson zur KAPO, die von dieser bestimmt wird. Die FAGIS wird von der oder dem ISIK geleitet. Bei Abstimmungen hat jedes Mitglied eine Stimme; bei Stimmengleichheit hat die oder der ISIK den Stichentscheid. Die FAGIS kann bei Bedarf weitere Fachleute wie z. B. die Datenschutzbeauftragte oder den Datenschutzbeauftragten oder eine Vertretung der Finanzkontrolle mit beratender Stimme beiziehen. Die FAGIS berät und koordiniert die Anliegen der Direktionen, der Staatskanzlei, der Bezirksverwaltung und der unselbstständigen Anstalten in allen Fragen der IKT-Sicherheit. Sie sorgt für eine ausreichende Regelungsdichte im Bereich der IKT-Sicherheit auf Stufe Gesamtverwaltung und unterstützt die ISID und die IVAD bei ihren Regelungsaufgaben. Die FAGIS stellt dem Gremium SDI Antrag für den Erlass und die Anpassung der Besonderen Informationssicherheitsrichtlinien im Bereich der IKT-Sicherheit. Sie berät das Gremium SDI bei der Erfüllung seiner Aufgaben und erstattet ihm nötigenfalls Bericht, insbesondere über wesentliche Probleme im Bereich der IKT-Sicherheit.

4.2 Risikomanagement

In einer Besonderen Informationssicherheitsrichtlinie wird geregelt, wie mit Risiken umzugehen ist. Es geht dabei um Risiken verschiedener, insbesondere rechtlicher, wirtschaftlicher, technischer, umweltbezogener, personeller, organisatorischer, gesellschaftlicher und politischer Art.

Die Richtlinie regelt insbesondere, wie Risiken sowie deren Ursachen und Auswirkungen erkannt werden sollen, wie die Wahrscheinlichkeit ihres Eintritts und ihrer Auswirkungen abgeschätzt werden sollen, wie die Risiken hinsichtlich ihrer Tragbarkeit bewertet werden sollen, wie die Risiken bewältigt werden sollen (sei dies durch Hinnahme, Vermeidung, Verminderung oder Überwälzung), welcher Schutzbedarf sich daraus ergibt, wie die nötigen Schutzmassnahmen geplant und umgesetzt werden sollen, wie dieser Prozess sowie die Wirksamkeit und Wirtschaftlichkeit der getroffenen Massnahmen überwacht werden sollen und wie die nötigen Anpassungen vorgenommen werden sollen. Die Richtlinie enthält ferner die notwendigen Zuständigkeits- und Berichterstattungsregelungen, insbesondere mit Bezug auf die Risikoverantwortlichen, und gibt Hinweise zum angemessenen Aufwand sowie zu Prioritäten und Intervallen.

Besondere Informationssicherheitsrichtlinien **Die folgende Richtlinie spezifiziert die Anforderungen an die Verwaltung von Informationsrisiken:**	
Kapitel	**Besondere Informationssicherheitsrichtlinien**
Verwaltung von Informationsrisiken	Richtlinie für die Verwaltung von Informationsrisiken [16]

Tabelle 1: Verwaltung von Informationsrisiken – Besondere Informationssicherheitsrichtlinien

4.3 Vorschriften

Die **AISR** wird auf Antrag der Finanzdirektion vom Regierungsrat erlassen.

Für die Erarbeitung und Beantragung sowie den Erlass der **Besonderen Informationssicherheitsrichtlinien** sind in den jeweiligen Regelungsbereichen die folgenden Stellen zuständig:

	Regelungsbereich	**Zuständigkeit für Richtlinien**		
	Themen nach ISO 27001	Entwurf	Antrag	Erlass
02	Verwaltung von organisationseigenen Werten	AFI	FAGIS	SDI
03	Informationsklassifikation und -handhabung	AFI (mit SK)	FAGIS	SDI
04	Identitäts- und Zugriffskontrolle	AFI	FAGIS	SDI
05	Personalsicherheit	PA (mit KAPO)	PA	SDI
06	Schulungsmassnahmen in Informationssicherheit	PA (mit SK und AFI)	PA	SDI
07	Mobile Endgeräte	AFI (mit PA)	FAGIS	SDI
08	Verwaltung von Wechselmedien	AFI (mit PA)	FAGIS	SDI
09	Telearbeit	AFI (mit PA)	FAGIS	SDI
10	Passwörter	AFI	FAGIS	SDI
11	Verschlüsselungsmassnahmen	AFI	FAGIS	SDI
12	Physische Sicherheit und Schutz vor Umwelteinflüssen	IMA (mit AFI)	IMA	SDI
13	Datensicherung und -wiederherstellung	AFI	FAGIS	SDI
14	Protokollierung und Überwachung	AFI (mit PA)	FAGIS	SDI
15	Verwaltung von Bedrohungen und Schwachstellen	AFI (mit SK)	FAGIS	SDI
16	Verwaltung von Informationsrisiken	AFI (mit SK und CB)	FAGIS	SDI
17	Verwaltung der Netzwerksicherheit	AFI	FAGIS	SDI
18	Sicherheit von Informationsübertragungen	AFI	FAGIS	SDI
19	Sicherheit von Informationssystemen	AFI	FAGIS	SDI
20	Sicherheit in Entwicklungs- und Unterstützungsprozessen	AFI	FAGIS	SDI
21	Sicherheit von Testdaten	AFI	FAGIS	SDI
22	Beziehungen zu externen Personen (insbesondere Liefernden)	PA (mit BD, SK und AFI)	PA	SDI
23	Sicherheit von Datenzentren	AFI (mit IMA)	FAGIS	SDI
24	Umgang mit Informationssicherheitsvorfällen	AFI (mit SK und CB)	FAGIS	SDI
25	Kontinuität von Informationssicherheit	AFI (mit SK und CB)	FAGIS	SDI
26	Konformität und Prüfung von Informationssicherheit	AFI (mit SK und CB)	FAGIS	SDI
27	Regelung von Ausnahmen	AFI (mit SK und CB)	FAGIS	SDI

Basiskonfigurationen werden nur im Bereich der IKT-Sicherheit erlassen. Dafür zuständig sind die IKT-Sicherheitsbeauftragten der Direktionen und der Staatskanzlei.

Verfahren und **Prozesse** werden im Bereich der IKT-Sicherheit von den Informatikverantwortlichen der Direktionen und der Staatskanzlei erlassen, in den übrigen Bereichen von denjenigen Stellen, welche die Besonderen Informationssicherheitsrichtlinien bezeichnen.

Die zuständigen Stellen verbessern diese Vorschriften laufend, indem sie:

- geeignete Regeln entwerfen,
- die geltenden Regeln umsetzen,
- deren Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit überprüfen und
- die Regeln bei Bedarf anpassen.

Eine Überprüfung erfolgt in regelmässigen Abständen, im Falle der Besonderen Informationssicherheitsrichtlinien mindestens einmal jährlich. Unabhängig davon erfolgt eine Überprüfung bei jeder wesentlichen Änderung im regulatorischen, organisatorischen oder technischen Umfeld sowie bei jeder Entdeckung wesentlicher Bedrohungen und Schwachstellen.

Die zuständigen Stellen erstatten dem Gremium «Steuerung Digitale Verwaltung und IKT» (SDI) zeitnah Bericht über wesentliche neue Erkenntnisse und über die erfolgten Anpassungen. Das Gremium SDI informiert den Regierungsrat regelmässig mit einer zusammenfassenden Mitteilung über diese Berichterstattung.

Die AISR und die Besonderen Informationssicherheitsrichtlinien werden allen Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung elektronisch mitgeteilt. Basiskonfigurationen sowie Verfahren und Prozesse werden denjenigen Personen elektronisch mitgeteilt, an die sie sich richten. Die Mitteilung wird jeweils von der Direktion veranlasst, der die Stelle angehört, welche die Richtlinie entworfen hat. Im Bereich der IKT-Sicherheit erfolgt sie durch die IKT-Sicherheitsbeauftragte oder den IKT-Sicherheitsbeauftragten des Kantons Zürich.

Von den Besonderen Informationssicherheitsrichtlinien sollen diejenigen, die von der FAGIS zu beantragen sind, spätestens auf Mitte 2020 und die übrigen spätestens auf Mitte 2021 in Kraft gesetzt werden. Die Richtlinien können Umsetzungsfristen von bis zu zwei Jahren vorsehen. Die Basiskonfigurationen, Verfahren und Prozesse zu den Besonderen Richtlinien sollen innert zweier Jahre seit deren Inkrafttreten in Kraft gesetzt werden, soweit diese nichts anderes vorsehen.

Das gesamte Informationssicherheits-Managementsystem (ISMS) ist alle fünf Jahre, erstmals im Jahr 2027, von einer unabhängigen Stelle auf seine Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit zu überprüfen. Anschliessend ist es soweit erforderlich anzupassen.

4.4 Ausnahmen von den Vorschriften

In einer Besonderen Informationssicherheitsrichtlinie wird geregelt, unter welchen Umständen Ausnahmen von Informationssicherheitsvorschriften bewilligt werden können.

In bestimmten Fällen kann es zur Erfüllung der Verwaltungsaufgaben nicht tunlich oder nicht sinnvoll sein, die Informationssicherheitsvorschriften uneingeschränkt anzuwenden.

Abweichungen von Vorschriften sind deshalb ausnahmsweise zulässig, wenn die Nachteile ihrer Anwendung das Risiko der Nichtanwendung und die Vorteile der Anwendung für die kantonale Verwaltung überwiegen. Abweichungen werden nur für einen bestimmten Zeitraum bewilligt. Dieser richtet sich nach der Höhe des Risikos. Nach Ablauf des Zeitraums kann die Bewilligung erneuert werden, wenn die Voraussetzungen dafür weiterhin erfüllt sind.

Für die Bewilligung von Abweichungen von den Informationssicherheitsrichtlinien und den untergeordneten Dokumenten ist die oder der IKT-Sicherheitsbeauftragte des Kantons Zürich (ISIK) zuständig, soweit die Besonderen Informationssicherheitsrichtlinien dafür im Bereich ausserhalb der IKT-Sicherheit keine anderen Stellen bezeichnen.

Für Anträge auf die Bewilligung von Abweichungen ist eine Vorlage zu verwenden, die von der oder dem IKT-Sicherheitsbeauftragten des Kantons Zürich (ISIK) genehmigt worden ist. Die Anträge und die Entscheide darüber sind zu begründen und geordnet abzulegen.

Die oder der IKT-Sicherheitsbeauftragte des Kantons Zürich (ISIK) und die übrigen zuständigen Stellen berichten dem Gremium «Steuerung Digitale Verwaltung und IKT» (SDI) mindestens einmal jährlich über die bewilligten Abweichungen. Das Gremium SDI informiert den Regierungsrat mit einer zusammenfassenden Mitteilung über diese Berichterstattung.

Besondere Informationssicherheitsrichtlinien

Die folgende Richtlinie spezifiziert die Regelung von Ausnahmen:

Kapitel	Besondere Informationssicherheitsrichtlinien
Regelung von Ausnahmen	Richtlinie zur Regelung von Ausnahmen [27]

Tabelle 2: Regelung von Ausnahmen – Besondere Informationssicherheitsrichtlinien

5. Grundzüge der Regelungen

Im Folgenden werden die inhaltlichen Grundzüge der Regelungen festgelegt, die der AISR untergeordnet sind, insbesondere der Besonderen Informationssicherheitsrichtlinien. Diese haben alle Regelungsbereiche abzudecken. Eine Besondere Informationssicherheitsrichtlinie kann mehrere Bereiche abdecken; umgekehrt kann auch ein Bereich von mehreren Richtlinien abgedeckt werden.

5.1 Mobile Endgeräte und Telearbeit

In einer Besonderen Informationssicherheitsrichtlinie werden die Anforderungen an das Verhalten der Mitarbeitenden und externen Personen ausserhalb der Räumlichkeiten der kantonalen Verwaltung geregelt.

Besprechungen im öffentlichen Raum über Gegenstände, die dem Amtsgeheimnis unterliegen, sind zu vermeiden. Über Routinegeschäfte kann in anonymisierter Form gesprochen werden, sofern dabei weder die Gefahr einer Beeinträchtigung des Ansehens der kantonalen Verwaltung besteht, noch die Möglichkeit von Rückschlüssen auf die beteiligten Personen. Im Übrigen sind Besprechungen im öffentlichen Raum so zu führen, dass ihr Inhalt von Dritten ohne technische Hilfsmittel nicht wahrgenommen werden kann.

Akten, Datenträger und Gerätschaften der kantonalen Verwaltung sind im öffentlichen Raum in geschlossenen Behältnissen (z. B. Aktenmappen) zu transportieren.

Dokumente dürfen im öffentlichen Raum nur so gelesen und bearbeitet werden, dass sie von Dritten ohne technische Hilfsmittel nicht eingesehen werden können.

Besondere Informationssicherheitsrichtlinien **Die folgenden Richtlinien spezifizieren die Anforderungen an mobile Endgeräte und Telearbeit:**	
Kapitel	**Besondere Informationssicherheitsrichtlinien**
Mobile Endgeräte und Telearbeit	Richtlinie für mobile Endgeräte [7]
	Richtlinie für Telearbeit [9]

Tabelle 3: Mobile Endgeräte und Telearbeit – Besondere Informationssicherheitsrichtlinien

5.2 Personalsicherheit

In einer Besonderen Informationssicherheitsrichtlinie wird die Prüfung der persönlichen Integrität der Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung geregelt. Je nach deren Ausgestaltung sind die gesetzlichen Grundlagen anzupassen.

a) Vor der Beschäftigung

Bei Mitarbeitenden und externen Personen ist darauf zu achten, dass diese ihre Stellung in der kantonalen Verwaltung und das in sie gesetzte Vertrauen nicht missbrauchen. Vor Beginn ihrer Tätigkeit für die kantonale Verwaltung und regelmässig auch während deren Dauer ist deshalb zu prüfen, ob persönliche Umstände oder der Gegenstand der Tätigkeit diesbezüglich auf ein besonderes Risiko schliessen lassen. Bestehen Anhaltspunkte für ein solches Risiko, ist die persönliche Integrität der Mitarbeitenden und externen Personen unter Einhaltung der rechtlichen Rahmenbedingungen, insbesondere des Grundsatzes der Verhältnismässigkeit, vertieft zu prüfen. Diese Prüfung muss in einem angemessenen Verhältnis zu den fachlichen Anforderungen an die Tätigkeit, der Klassifizierungsstufe der dabei zugänglichen Informationen und den sonstigen mit der Beschäftigung verbundenen erkennbaren Risiken stehen.

b) Während der Beschäftigung

Alle Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung haben die Informationssicherheit unter Beachtung der für sie geltenden Informationssicherheitsvorschriften zu wahren.

Die Gewährleistung der Informationssicherheit erfordert nicht nur ein integres und sorgfältig ausgewähltes, sondern auch ein angemessen ausgebildetes Personal. Die Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung müssen ihre Verantwortlichkeiten im Hinblick auf die Informationssicherheit kennen. Sie sind bei Beginn ihrer Tätigkeit für die kantonale Verwaltung und regelmässig auch während dieser Tätigkeit über ihre wesentlichen Pflichten und die Folgen der Nichterfüllung dieser Pflichten aufzuklären.

Alle Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung müssen geeignete und angemessene Schulungsmassnahmen in Informationssicherheit erhalten und über die für ihre Funktion massgeblichen Informationssicherheitsvorschriften unterrichtet werden. Die grundlegenden Schulungsmassnahmen sind nach Möglichkeit zentral vom Personalamt zu konzipieren und anzubieten. Das Personalamt sorgt insbesondere für die regelmässige Schulung aller Angehörigen des höheren Kaders hinsichtlich der für sie wesentlichen Aspekte der Gewährleistung der Informationssicherheit. Die Besondere Informationssicherheitsrichtlinie legt eine den Risiken und dem Schulungsbedarf angemessene Verpflichtung zur Teilnahme an Schulungsmassnahmen fest.

c) Nach der Beschäftigung

Bei Beendigung ihrer Tätigkeit sind die Mitarbeitenden und externen Personen über die Pflichten aufzuklären, die auch darüber hinaus bestehen bleiben (z. B. die Verschwiegenheitspflicht der Angestellten).

Besondere Informationssicherheitsrichtlinien Die folgenden Richtlinien spezifizieren die Anforderungen an die Personalsicherheit:	
Kapitel	**Besondere Informationssicherheitsrichtlinien**
Personalsicherheit	Richtlinie für Personalsicherheit [5]
	Richtlinie für Schulungsmassnahmen in Informationssicherheit [6]

Tabelle 4: Personalsicherheit – Besondere Informationssicherheitsrichtlinien

5.3 Verwaltung von organisationseigenen Werten

Organisationseigene Werte sind Infrastruktur und IT-Mittel der kantonalen Verwaltung, die Informationen und das Verarbeiten von Informationen betreffen. Diese umfassen Informationen, Software, physische Werte wie Computer- und Kommunikationsanlagen, Dienstleistungen, sowie immaterielle Werte.

a) Inventar der Informationsbestände und Anwendungen

Die für die Informationssicherheit wesentlichen organisationseigenen Werte der kantonalen Verwaltung im Bereich der Informationsverarbeitung sind unter Bezeichnung der für ihren Schutz verantwortlichen Personen in einem Verzeichnis zu erfassen. Das Verzeichnis ist laufend nachzuführen. Eine Besondere Informationssicherheitsrichtlinie regelt den Aufbau, den Inhalt und die Führung des Verzeichnisses.

Sämtliche organisationseigenen Werte der kantonalen Verwaltung, die sich im Besitz von Mitarbeitenden und externen Personen befinden, werden bei der Beendigung des Beschäftigungsverhältnisses an die kantonale Verwaltung zurückgegeben.

b) Informationsklassifikation

Informationen sind entsprechend den rechtlichen Anforderungen, ihrem Wert, ihrer Vertraulichkeit, ihrer Wichtigkeit für die kantonale Verwaltung und den zu schützenden Interessen zu klassifizieren und demgemäss zu kennzeichnen. Für die Klassifizierung und Kennzeichnung sowie deren Auswirkung auf den Umgang mit Ressourcen der kantonalen Verwaltung sind Verfahren festzulegen. Die grundlegenden Klassifizierungsstufen sind «öffentlich» (blau), «intern» (grün), «vertraulich» (gelb) und «geheim» (rot). Besondere Personendaten im Sinne von § 3 IDG sind in der Regel als vertraulich oder als geheim zu klassifizieren.

c) Verwaltung von Wechselmedien

Um zu verhindern, dass Informationen, die auf mobilen Datenträgern gespeichert sind, unbefugt offengelegt, verändert, entnommen oder zerstört werden, sind Verfahren zur Verwaltung von mobilen Datenträgern festzulegen. Diese sind mit dem Plan zur Klassifizierung der Informationen abzustimmen.

Bei der physischen Weitergabe von mobilen Datenträgern sind die darauf gespeicherten Informationen vor unbefugtem Zugriff und Missbrauch zu schützen.

Nicht mehr benötigte mobile Datenträger sind sicher und in einem dafür festgelegten Verfahren zu entsorgen.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die Verwaltung von organisationseigenen Werten:

Kapitel	Besondere Informationssicherheitsrichtlinien
Verwaltung von organisationseigenen Werten	Richtlinie für die Verwaltung von organisationseigenen Werten [2]
	Richtlinie für Informationsklassifikation und -handhabung [3]
	Richtlinie für die Verwaltung von Wechselmedien [8]

Tabelle 5: Verwaltung von organisationseigenen Werten – Besondere Informationssicherheitsrichtlinien

5.4 Zugriffskontrolle

a) Benutzendenverwaltung und -verantwortung

Als Grundlage für die Regelung des Zugriffs auf Informationen und informationsverarbeitende Einrichtungen besteht eine Benutzendenverwaltung. Diese dient dem Ziel, dass autorisierte Benutzende Zugriff auf Systeme, Netzwerke und Dienste erhalten, nicht autorisierte Benutzende dagegen nicht. Zu diesem Zweck besteht ein Prozess zur An- und Abmeldung von Benutzenden, der die Vergabe von Zugriffsrechten ermöglicht. Ein Verfahren zur Benutzendeneinrichtung regelt für jeden Benutzendentyp die Zuweisung und den Widerruf von Zugriffsrechten für die verschiedenen Systeme, Netzwerke und Dienste.

Die für den Schutz von Informationen und informationsverarbeitenden Einrichtungen zuständigen Personen haben die Zugriffsrechte der Benutzenden zu dokumentieren und regelmässig zu überprüfen. Bei Beendigung des Anstellungs- bzw. Auftragsverhältnisses sind den Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung sämtliche Zugriffsrechte zu entziehen. Bei einer Änderung sind die Zugriffsrechte entsprechend anzupassen.

Bei der Vergabe von Zugriffsrechten ist eine sinnvolle Aufgabentrennung zur Vermeidung von Interessenkonflikten sicherzustellen. Die Vergabe richtet sich nach dem Grundsatz, dass die Mitarbeitenden und externen Personen im Dienst der kantonalen Verwaltung jeweils nur auf diejenigen Informationen und Anwendungen sollen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen (Need-to-know-Prinzip). Dieser Grundsatz ist hinreichend weit zu verstehen, damit die Mitarbeitenden und externen Personen auch Querbezüge zu Geschäften ausserhalb ihres Zuständigkeitsbereichs erkennen können.

b) Zugriffskontrolle

Zur Verhinderung des unbefugten Zugriffs auf Systeme und Anwendungen ist der Zugriff auf Funktionen von Informations- und Anwendungssystemen zu beschränken und über ein sicheres Anmeldeverfahren zu überwachen. Die Verwendung von Hilfsprogrammen, die System- und Anwendungskontrollen ausschalten oder umgehen können, ist zu beschränken und streng zu überwachen. Ebenfalls zu beschränken ist der Zugang zum Quellcode von Anwendungen.

Die Vergabe und Nutzung von privilegierten Zugriffsrechten (z. B. Administrations-Konten) erfolgt unter einschränkenden Voraussetzungen und ist zu überwachen. Die Vergabe von geheimen Authentisierungsinformationen wie Passwörtern ist in einem eigens dafür festgelegten Prozess zu überwachen.

c) Passwörter

Die Benutzenden sind für den Schutz ihrer Authentisierungsinformationen verantwortlich.

Zur Vermeidung von unsicheren Passwörtern stellt ein interaktives Passwortverwaltungssystem sicher, dass die Qualität der Passwörter höchsten Anforderungen entspricht.

Besondere Informationssicherheitsrichtlinien	
Die folgenden Richtlinien spezifizieren die Anforderungen an die Zugriffskontrolle:	
Kapitel	**Besondere Informationssicherheitsrichtlinien**
Zugriffskontrolle	Richtlinie für die Identitäts- und Zugriffskontrolle [4]
	Richtlinie für Passwörter [10]

Tabelle 6: Zugriffskontrolle – Besondere Informationssicherheitsrichtlinien

5.5 Verschlüsselung

Eine Besondere Informationssicherheitsrichtlinie sieht angemessene Verschlüsselungsmassnahmen zum Schutz der Vertraulichkeit, Echtheit und Unveränderheit der Informationen der kantonalen Verwaltung vor. Sie regelt die Gültigkeitsdauer der Verschlüsselungsschlüssel sowie deren Schutz während der gesamten Dauer.

Besondere Informationssicherheitsrichtlinien **Die folgende Richtlinie spezifiziert die Anforderungen an die Verschlüsselung:**	
Kapitel	**Besondere Informationssicherheitsrichtlinien**
Verschlüsselung	Richtlinie für Verschlüsselungsmassnahmen [11]

Tabelle 7: Verschlüsselung – Besondere Informationssicherheitsrichtlinien

5.6 Physische Sicherheit und Schutz vor Umwelteinflüssen

a) Sicherheitsbereiche

Unbefugte physische Zugriffe auf Informationen und informationsverarbeitende Einrichtungen sowie deren Beschädigung oder Störung sind zu verhindern.

Zum Schutz von Bereichen, in denen sich vertrauliche oder wichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitsbereiche festzulegen. Diese sind durch angemessene physische Zugangskontrollen vor unbefugtem Zutritt zu schützen. Insbesondere müssen Zugangspunkte wie Anliefer-, Lade- und andere Bereiche, über die nicht dazu befugte Personen Verwaltungsgelände oder -gebäude betreten könnten, nach Möglichkeit von informationsverarbeitenden Einrichtungen getrennt werden. Für das Arbeiten in Sicherheitsbereichen sind Verfahren festzulegen.

Die Benutzenden müssen dafür sorgen, dass unbeaufsichtigte Endgeräte angemessen geschützt sind. Es gelten zudem die Grundsätze des aufgeräumten Schreibtischs («clean desk») und des leeren Bildschirms («clear screen»), d. h., bei jedem Verlassen des Arbeitsplatzes sind vertrauliche und wichtige Dokumente und Informationsträger wegzuschliessen sowie ein passwortgeschützter Bildschirmschoner zu aktivieren.

Entsprechende Sicherheitsvorkehrungen sind für alle Räumlichkeiten und Anlagen der kantonalen Verwaltung zu treffen

b) Ressourcen (insbesondere Gerätschaften)

In einer Besonderen Informationssicherheitsrichtlinie wird geregelt, wie die Ressourcen der kantonalen Verwaltung im Bereich der Informationsverarbeitung, insbesondere Räume, Geräte und Datenträger, vor einer Beeinträchtigung durch äussere Umstände geschützt werden.

Zum Schutz der Ressourcen im Bereich der Informationsverarbeitung vor Verlust, Diebstahl, Beschädigung, Störung und andersartiger Gefährdung sind Massnahmen zu treffen. Zum Schutz vor Naturkatastrophen, Angriffen und Unfällen sind besondere Sicherheitsvorkehrungen zu treffen, ebenso für das Arbeiten ausserhalb der Räumlichkeiten der kantonalen Verwaltung, wobei Nutzen und Risiken einer solchen Arbeit zu berücksichtigen sind.

Ohne vorherige Erlaubnis der zuständigen Stelle dürfen Ressourcen im Bereich der Informationsverarbeitung nicht aus den Räumlichkeiten der kantonalen Verwaltung entfernt werden.

Ressourcen, die sich im Besitz von Mitarbeitenden und externen Personen befinden, sind bei der Beendigung des Anstellungs- oder Auftragsverhältnisses zurückzuverlangen.

Gerätschaften sind fachgerecht instand zu halten, um ihre Verfügbarkeit und Unversehrtheit sicherzustellen. Sie sind so zu platzieren und zu schützen, dass die Risiken einer Beeinträchtigung durch äussere Umstände sowie die Möglichkeiten eines unbefugten Zugangs gering gehalten werden. Insbesondere sind sie vor Stromausfällen und anderen Unterbrechungen zu schützen, die durch Ausfälle in Versorgungseinrichtungen verursacht werden. Für die Sicherheit der Verkabelung müssen Strom- und Fernmeldekabel, die für die Datenübertragung oder für Informationsdienste verwendet werden, vor Überwachung (d. h. dem Abfangen von Daten), Störung und Beschädigung geschützt werden. Gerätschaften, die Speichermedien enthalten, müssen vor ihrer Entsorgung oder Wiederverwendung überprüft werden, um sicherzustellen, dass vertrauliche Daten und lizenzierte Software entfernt oder sicher überschrieben wurden.

c) Datenzentren

Zum Schutz vor Gefahren, welche die Sicherheit von Datenzentren bedrohen, sind besondere Sicherheitsmassnahmen zu treffen.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die physische Sicherheit und den Schutz vor Umwelteinflüssen:

Kapitel	Besondere Informationssicherheitsrichtlinien
Physische Sicherheit und Schutz vor Umwelteinflüssen	Richtlinie für physische Sicherheit und Schutz vor Umwelteinflüssen [12]
	Richtlinie für die Sicherheit von Datenzentren [23]

Tabelle 8: Physische Sicherheit und Schutz vor Umwelteinflüssen – Besondere Informationssicherheitsrichtlinien

5.7 Betriebssicherheit

a) Betriebsverfahren und Zuständigkeiten

Zur Sicherstellung des ordnungsgemässen und sicheren Betriebs der informationsverarbeitenden Einrichtungen sind Betriebsverfahren festzulegen. Diese sind allen Benutzenden, die sie benötigen, zugänglich zu machen.

Änderungen an der Organisation der kantonalen Verwaltung sowie an Geschäftsprozessen, informationsverarbeitenden Einrichtungen und Systemen, welche die Informationssicherheit berühren, sind im Rahmen eines Änderungsmanagements zu prüfen.

Über ein Kapazitätsmanagement wird sichergestellt, dass die Systeme die erforderliche Leistung aufweisen. Dazu ist die Nutzung von Systemressourcen zu überwachen und abzustimmen, und es sind Prognosen über zukünftige Kapazitätsanforderungen anzustellen.

b) Schutz vor Malware

Zum Schutz von Informationen und informationsverarbeitenden Einrichtungen vor Malware sind Erkennungs-, Vorbeugungs- und Wiederherstellungsmassnahmen zu treffen. Die Benutzenden innerhalb der kantonalen Verwaltung sind durch Schulungsmassnahmen angemessen für Malware zu sensibilisieren.

c) Datensicherung und -wiederherstellung

Zur Verhinderung eines Datenverlusts sind Sicherungskopien von Informationen, Software und System-Imagedateien zu erstellen. Diese sind in regelmässigen Abständen zu prüfen.

d) Protokollierung und Überwachung

Zur Dokumentation und Beweissicherung sind Ereignisprotokolle der Benutzendenaktivitäten, Ausnahmen, Fehler und Informationssicherheitsereignisse aufzuzeichnen, soweit der Aufwand dafür in einem angemessenen Verhältnis zu den Risiken steht. Insbesondere sind die Aktivitäten der Systemadministrierenden zu protokollieren. Die Protokolle sind entsprechend den Vorgaben, insbesondere zur Aufbewahrungsdauer, aufzubewahren und regelmässig zu prüfen.

Protokollierungseinrichtungen und -informationen sind vor Manipulation und unbefugtem Zugriff zu schützen.

Die Uhren aller informationsverarbeitenden Systeme innerhalb der kantonalen Verwaltung sind auf eine Bezugszeitquelle abzustimmen.

e) Kontrolle von Betriebssoftware

Zur Sicherung der Integrität der Systeme im Betrieb sind Verfahren zur Prüfung von Softwareinstallationen auf betriebsrelevanten Systemen festzulegen.

Die Umgebungen für die Entwicklung, das Testen und den Betrieb von Software müssen voneinander getrennt sein, um das Risiko eines unbefugten Zugriffs oder von unbefugten Änderungen an Betriebsumgebungen zu vermindern.

f) Verwaltung technischer Schwachstellen

Um zu verhindern, dass technische Schwachstellen der verwendeten Informationssysteme ausgenutzt werden, sind rechtzeitig Informationen über solche Schwachstellen einzuholen. Die Anfälligkeit der kantonalen Verwaltung für die Ausnutzung technischer Schwachstellen ist zu bewerten; gestützt darauf sind Massnahmen zur Behandlung des damit verbundenen Risikos zu ergreifen. In diesem Zusammenhang sind Regeln zur Installation von Software durch Benutzende festzulegen.

g) Prüfungen von Informationssystemen

Die Prüfung von betriebsrelevanten Systemen sowie die Anforderungen an eine solche Prüfung sind sorgfältig zu planen und innerhalb der kantonalen Verwaltung abzustimmen, um die Unterbrechung der Geschäftsprozesse auf ein Mindestmass zu verringern.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die Betriebssicherheit:

Kapitel	Besondere Informationssicherheitsrichtlinien
Betriebssicherheit	Richtlinie für Datensicherung und -wiederherstellung [13]
	Richtlinie für Protokollierung und Überwachung [14]
	Richtlinie für die Verwaltung von Bedrohungen und Schwachstellen [15]
	Richtlinie für die Verwaltung von Informationsrisiken [16]
	Richtlinie für die Sicherheit von Informationssystemen [19]
	Richtlinie für Schulungsmassnahmen in Informationssicherheit [6]

Tabelle 9: Betriebssicherheit – Besondere Informationssicherheitsrichtlinien

5.8 Kommunikationssicherheit

a) Verwaltung der Netzwerksicherheit

Die Netzwerke der kantonalen Verwaltung sind über Netzwerkkontrollen zu verwalten und zu kontrollieren, um die Informationen in den Systemen, Netzwerken und Anwendungen sowie den unterstützenden informationsverarbeitenden Einrichtungen zu schützen.

Verträge über Netzwerkdienste müssen Bestimmungen zu Sicherheitsmassnahmen, Serviceniveaus und Anforderungen für die Verwaltung von Netzwerkdiensten enthalten, unabhängig davon, ob Netzwerkdienste verwaltungsintern erbracht oder ausgelagert werden.

Gruppen von Informationsdiensten, Benutzenden und Informationssystemen müssen in Netzwerken voneinander getrennt werden.

b) Datenübertragung

Zur Aufrechterhaltung der Sicherheit von Informationen, die innerhalb der kantonalen Verwaltung und im Austausch mit externen Organisationen übertragen werden, sind Verfahren und Kontrollmassnahmen zu erlassen, die dem Schutz der Informationsübertragung über alle Arten von Kommunikationseinrichtungen dienen.

Die sichere Informationsübertragung ist durch Vereinbarungen zwischen der kantonalen Verwaltung und externen Parteien festzulegen.

Informationen, die über elektronische Nachrichten übermittelt werden, müssen angemessen geschützt werden.

Die Anforderungen an die Vertraulichkeit und an Geheimhaltungsvereinbarungen sind gemäss den Bedürfnissen der kantonalen Verwaltung hinsichtlich des Schutzes von Informationen festzulegen und regelmässig zu überprüfen.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die Kommunikationssicherheit:

Kapitel	Besondere Informationssicherheitsrichtlinien
Kommunikationssicherheit	Richtlinie für die Verwaltung der Netzwerksicherheit [17]
	Richtlinie für die Sicherheit von Informationsübertragungen [18]

Tabelle 10: Kommunikationssicherheit – Besondere Informationssicherheitsrichtlinien

5.9 Beschaffung, Entwicklung und Wartung von Systemen

a) Sicherheitsanforderungen an Informationssysteme

Die Informationssicherheit muss während der gesamten Lebensdauer Bestandteil von Informationssystemen sein.

Informationssysteme sind aufgrund einer Risikobeurteilung, welche die Wahrscheinlichkeit des Eintritts und der Auswirkungen umfasst, einer Schutzstufe zuzuweisen. Die massgeblichen Schutzstufen sind «1 – Grundschutz» (grün) und «2 – erhöhter Schutz» (orange). Den Zusammenhang dieser Schutzstufen mit der Informationsklassifikation gemäss Ziffer 5.3 b) regelt eine Besondere Informationsrichtlinie.

Die Anforderungen an neue Informationssysteme und an Weiterentwicklungen bestehender Informationssysteme müssen Anforderungen zur Informationssicherheit enthalten.

Informationen, die im Zusammenhang mit Anwendungsdiensten über öffentliche Netze übertragen werden, müssen vor betrügerischen Handlungen, Vertragsstreitigkeiten und unbefugter Offenlegung und Veränderung geschützt werden.

Informationen, die im Zuge von Transaktionen in Verbindung mit Anwendungsdiensten übertragen werden, müssen geschützt werden, um eine unvollständige Übertragung, eine Fehlleitung sowie eine unbefugte Offenlegung, Veränderung, Vervielfältigung oder Wiedergabe von Nachrichten zu verhindern.

b) Sicherheit in Entwicklungs- und Unterstützungsprozessen

Die Informationssicherheit ist im Rahmen des Entwicklungszyklus von Informationssystemen zu entwickeln und umzusetzen. Eine Besondere Informationssicherheitsrichtlinie regelt die Entwicklung von Software und Systemen, insbesondere für Entwicklungen innerhalb der kantonalen Verwaltung. Für die Konstruktion von sicheren Systemen sind Grundsätze festzulegen, die bei jeder Einrichtung von Informationssystemen anzuwenden sind. Für die Prüfung von Änderungen an Systemen, die sich im Entwicklungszyklus befinden, sind Änderungskontrollverfahren festzulegen.

Bei Änderungen an Betriebsplattformen sind die für die kantonale Verwaltung wichtigen Anwendungen zu prüfen und zu testen, um sicherzustellen, dass sich aus der Änderung keine nachteiligen Folgen für die Verwaltungsarbeit und die Sicherheit ergeben.

Der Veränderung von Softwarepaketen ist entgegenzuwirken. Sie ist auf notwendige Änderungen und auf nützliche Änderungen ohne Nachteile zu beschränken und streng zu überwachen. Verbesserungen von Software ohne sicherheitskritische Folgen sollen nicht unnötig erschwert werden.

Es sind sichere Entwicklungsumgebungen für die Entwicklung und Integration von Systemen einzurichten und zu schützen. Sichere Entwicklungsumgebungen haben den gesamten Entwicklungszyklus von Systemen abzudecken.

Ausgelagerte Systementwicklungstätigkeiten sind von der kantonalen Verwaltung zu beaufsichtigen und zu überwachen.

Das Testen von Sicherheitsfunktionen hat während der Entwicklung von Systemen stattzufinden. Für den Abnahmetest von neuen Informationssystemen, Änderungen auf eine höhere Konfiguration sowie neuen Versionen sind Programme und Kriterien festzulegen.

c) Testdaten

Testdaten sind sorgfältig auszuwählen, zu schützen und zu überwachen. Sie sind, soweit dies mit verhältnismässigem Aufwand möglich ist, zu anonymisieren.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die Beschaffung, Entwicklung und Wartung von Systemen:

Kapitel	Besondere Informationssicherheitsrichtlinien
Beschaffung, Entwicklung und Wartung von Systemen	Richtlinie für die Sicherheit von Informationssystemen [19]
	Richtlinie für die Sicherheit in Entwicklungs- und Unterstützungsprozessen [20]
	Richtlinie für die Sicherheit von Testdaten [21]

Tabelle 11: Beschaffung, Entwicklung und Wartung von Systemen – Besondere Informationssicherheitsrichtlinien

5.10 Beziehungen zu externen Personen (insbesondere Liefernden)

In einer Besonderen Informationssicherheitsrichtlinie wird der Umgang mit externen Personen (z. B. Lieferenden) geregelt.

a) Informationssicherheit in Beziehungen zu externen Personen

Die personellen, materiellen und immateriellen Ressourcen der kantonalen Verwaltung (z. B. Geräte, Software, Knowhow und andere Informationen), auf die externe Personen Zugriff haben, sind vor Missbrauch zu schützen. Dies gilt insbesondere in Beziehungen zu Liefernden, die Zugriff auf Informationen der kantonalen Verwaltung haben, diese verarbeiten, speichern oder weiterverbreiten oder IKT-Infrastruktur-Komponenten bereitstellen.

Zu diesem Zweck ist mit den externen Personen zu vereinbaren, dass sie die nötigen Informationssicherheitsanforderungen erfüllen, insbesondere zur Verminderung der Informationssicherheitsrisiken im Zusammenhang mit der Dienstleistungs- und Produktelieferkette im IKT-Bereich. Die Besondere Informationssicherheitsrichtlinie regelt in Ergänzung von § 25 der Verordnung über die Information und den Datenschutz die Mindestanforderungen, insbesondere die Frage, in welchen Fällen Personenintegritätsprüfungen durchgeführt werden.

b) Verwaltung der Dienstleistungserbringung durch externe Personen

Die Einhaltung der vereinbarten Pflichten durch die externen Personen ist im Rahmen der Verhältnismässigkeit zu überwachen. Die Qualität der erbrachten Leistungen ist regelmässig zu überprüfen.

Die Informationssicherheitsanforderungen an externe Personen, die dazu getroffenen Vereinbarungen und durchgeführten Kontrollen sowie die diesbezüglichen Änderungen sind systematisch zu erfassen. Dabei sind die Wichtigkeit der betroffenen Informationen, Systeme und Prozesse sowie die Risiken und deren aktuelle Bewertung zu berücksichtigen.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an Beziehungen zu externen Personen:

Kapitel	Besondere Informationssicherheitsrichtlinien
Beziehungen zu externen Personen (insbesondere Liefernden)	Richtlinie für Beziehungen zu externen Personen (insbesondere Liefernden) [22]
	Richtlinie für die Sicherheit von Datenzentren [23]

Tabelle 12: Beziehungen zu externen Personen – Besondere Informationssicherheitsrichtlinien

5.11 Umgang mit Informationssicherheitsvorfällen

Auf Informationssicherheitsvorfälle ist ordnungsgemäss, schnell und wirksam zu reagieren. Zu diesem Zweck ist eine möglichst beständige Regelung der Zuständigkeiten und Verfahren zu erlassen.

Beobachtete oder vermutete Informationssicherheitsereignisse und -schwachstellen sind der oder dem IKT-Sicherheitsbeauftragten des Kantons Zürich (ISIK) so rasch wie möglich auf direktem Weg zu melden. Die Meldung kann anonym erfolgen. Informationssicherheitsereignisse sind daraufhin zu beurteilen, ob sie ernsthafte Informationssicherheitsvorfälle darstellen. Die Behandlung von Informationssicherheitsvorfällen richtet sich nach der Regelung in einer Besonderen Informationssicherheitsrichtlinie. Die Erkenntnisse aus der Untersuchung und Behebung von Informationssicherheitsvorfällen sind zur Verringerung der Wahrscheinlichkeit und der Auswirkungen von zukünftigen Vorfällen zu verwenden.

Zur Auffindung, Sammlung, Erfassung und Sicherung von Informationen, die der Beweisführung dienen, sind Verfahren festzulegen.

Die oder der IKT-Sicherheitsbeauftragte des Kantons Zürich (ISIK) berichtet dem Gremium «Steuerung Digitale Verwaltung und IKT» (SDI) mindestens einmal jährlich über die gemeldeten Informationssicherheitsvorfälle sowie deren Beurteilung und Behandlung. Das Gremium SDI informiert den Regierungsrat mit einer zusammenfassenden Mitteilung über diese Berichterstattung.

Besondere Informationssicherheitsrichtlinien

Die folgende Richtlinie spezifiziert die Anforderungen an den Umgang mit Informationssicherheitsvorfällen:

Kapitel	Besondere Informationssicherheitsrichtlinien
Umgang mit Informationssicherheitsvorfällen	Richtlinie für den Umgang mit Informationssicherheitsvorfällen [24]

Tabelle 13: Umgang mit Informationssicherheitsvorfällen – Besondere Informationssicherheitsrichtlinien

5.12 Informationssicherheitsaspekte des Betriebskontinuitätsmanagements

Die Kontinuität der Informationssicherheit ist Bestandteil der Systeme der kantonalen Verwaltung für das Betriebskontinuitätsmanagement. Eine Besondere Informationssicherheitsrichtlinie legt nähere Anforderungen an die Kontinuität und die Handhabung der Informationssicherheit bei Zwischenfällen fest.

Die Direktionen und die Staatskanzlei haben sicherzustellen, dass die nötigen Verfahren und Prozesse sowie Massnahmen festgelegt, festgehalten, umgesetzt und aufrechterhalten werden, um das erforderliche Mass an Kontinuität während eines Zwischenfalls zu gewährleisten. Die Verfahren und Prozesse sowie die Massnahmen sind in regelmässigen Abständen zu überprüfen, um ihre Anwendbarkeit und Wirksamkeit bei Zwischenfällen zu gewährleisten.

Die IKT-Sicherheitsbeauftragten der Direktionen und der Staatskanzlei (ISID) berichten dem Gremium «Steuerung Digitale Verwaltung und IKT» (SDI) mindestens einmal jährlich über diese Verfahren und Prozesse sowie Massnahmen. Das Gremium SDI informiert den Regierungsrat mit einer zusammenfassenden Mitteilung über diese Berichterstattung.

Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sicherzustellen. Diese sind mit ausreichender Redundanz einzurichten, damit die Anforderungen an die Verfügbarkeit erfüllt sind.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die Informationssicherheitsaspekte des Betriebskontinuitätsmanagements:

Kapitel	Besondere Informationssicherheitsrichtlinien
Informationssicherheitsaspekte des Betriebskontinuitätsmanagements	Richtlinie für die Kontinuität von Informationssicherheit [25]
	Richtlinie für die Sicherheit von Informationssystemen [19]

Tabelle 14: Informationssicherheitsaspekte des Betriebskontinuitätsmanagements – Besondere Informationssicherheitsrichtlinien

5.13 Einhaltung der Richtlinien

In einer Besonderen Informationssicherheitsrichtlinie wird geregelt, wie die Einhaltung der Informationssicherheitsvorschriften sichergestellt wird. Dies betrifft nicht nur die Informationssicherheitsrichtlinien und die Dokumente, die diesen untergeordnet sind, sondern auch gesetzliche Vorschriften, Weisungen und vertragliche Regelungen.

a) Einhaltung der gesetzlichen und vertraglichen Anforderungen

Als Grundlage für das Informationssicherheits-Managementsystem sind die Sicherheitsanforderungen für jedes Informationssystem in der kantonalen Verwaltung zu ermitteln, festzuhalten und einzuhalten. Die zuständigen Stellen haben darzulegen, wie sie die ermittelten Anforderungen einhalten.

Entsprechend den Anforderungen sind Aufzeichnungen vor Verlust, Zerstörung, Fälschung, unerlaubtem Zugriff und unerlaubter Freigabe zu schützen und Verschlüsselungsmassnahmen anzuwenden. Weiter sind geeignete Verfahren einzurichten, um den Schutz geistigen Eigentums sicherzustellen, insbesondere bei urheberrechtlich geschützten Softwareprodukten. Die Privatsphäre und der Schutz von Personendaten sind gemäss dem Gesetz über die Information und den Datenschutz (IDG) zu gewährleisten.

Die möglichen rechtlichen Folgen der Nichteinhaltung von Informationssicherheitsvorschriften sind klar und verständlich aufzuzeigen. Dies gilt beispielsweise für personalrechtliche Massnahmen bis hin zur Beendigung des Arbeitsverhältnisses, die Beendigung des Vertragsverhältnisses mit externen Personen und deren Unternehmen, Schadenersatzforderungen sowie Strafanzeigen bei Verdacht auf strafbare Handlungen.

b) Informationssicherheitsprüfung

Es ist in regelmässigen Abständen von einer unabhängigen Stelle überprüfen zu lassen, ob die Umsetzung der Informationssicherheit den massgeblichen Vorschriften entspricht. Besondere Beachtung ist dabei wesentlichen Änderungen von Informationssicherheitsrichtlinien, untergeordneten Dokumenten, Kontrollzielen und Kontrollen zu schenken. Die Informatikverantwortlichen der Direktionen und der Staatskanzlei (IVAD) haben regelmässig zu überprüfen, ob die Informatikverfahren und -prozesse in ihrem Verantwortungsbereich den massgeblichen Informationssicherheitsrichtlinien und weiteren Sicherheitsanforderungen entsprechen. Die technische Konformität ist laufend zu überprüfen.

Besondere Informationssicherheitsrichtlinien

Die folgenden Richtlinien spezifizieren die Anforderungen an die Einhaltung der Richtlinien:

Kapitel	Besondere Informationssicherheitsrichtlinien
Einhaltung der Richtlinien	Richtlinie für die Konformität und Prüfung von Informationssicherheit [26]
	Richtlinie für die Regelung von Ausnahmen [27]

Tabelle 15: Einhaltung der Richtlinien – Besondere Informationssicherheitsrichtlinien