Kanton Zürich
Finanzdirektion
KITT Geschäftsstelle

Entwurf Verordnung ISV Vs. 4.0
Stand 3. März 2015

Entwurf Erläuterungen Vs. 0.1
Stand: 27. Mai 2015

Verordnung über die Informationssicherheit (ISV)

(vom 28.05.2015)

Der Regierungsrat,

gestützt auf § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (IDG)[1]

beschliesst:

I. Grundlagen

A. Allgemeine Bestimmungen	
Zweck	*Erläuterung*
§ 1. [1] Die Verordnung regelt den Schutz der Informatiksysteme und der mit solchen Systemen bearbeiteten Informationen. [2] Die Informatiksysteme und Informationen der öffentlichen Organe sind durch angemessene organisatorische und technische Massnahmen so zu schützen, dass a. die Verfügbarkeit und Richtigkeit der Informationen gemäss Schutzbedarf der Organisationseinheit sichergestellt ist, b. die vom Gesetz, von den Instanzen und den Geschäftsprozessen geforderte Vertraulichkeit gewahrt ist, c. die Nachvollziehbarkeit gewährleistet ist, d. die Beteiligung an einem Geschäftsvorgang nicht abgestritten werden kann, und e. jegliche Bearbeitung der handelnden Person zugerechnet werden	Der Zweck der Verordnung leitet sich ab vom IDG; der Begriff „Informationssicherheit“ ist eine Ausdehnung des ursprünglichen Regelungsbereichs der alten „Informatiksicherheitsverordnung“. Er wurde gewählt, weil das IDG sich mit Schutz und Sicherheit von Informationen beschäftigt, und die Informationen, nicht bloss die Informatik für das Verwaltungshandeln von ausserordentlicher Bedeutung sind. Die Schutzziele sind umfassend und sehr weitreichend formuliert, die Einschränkungen beschreibt dann § 4.

[1] LS 170.4

kann. [3]Die gesetzlichen, vertraglichen und aufsichtsrechtlichen Verpflichtungen sind zu erfüllen.	
Geltungsbereich	
§ 2. Diese Verordnung gilt für sämtliche öffentlichen Organe des Kantons.	Es sind keine Ausnahmen vorgesehen. Jedes öffentliche Organ im Kanton untersteht dem IDG, deshalb gilt auch die ISV für alle.
Begriffe	Es werden nur Begriffe erläutert, die nicht bereits umgangssprachlich oder in anderen kantonalen Regelungen definiert sind.
§ 3. In dieser Verordnung bedeuten: Leistungsbezüger: Teile von öffentlichen Organen oder die öffentlichen Organe selbst, welche Informatikleistungen beziehen. Leistungserbringer: Einheiten, welche Informatiksysteme betreiben oder andere Informatikleistungen für das öffentliche Organ erbringen. Informationsleistung: Informationsbearbeitung durch technische Einrichtungen und Systeme. Schutzbedarfskatalog: Gewichtete Auflistung der zu berücksichtigenden Schadenereignisse und ihrer Folgen. Wird bei der Schutzbedarfsermittlung eingesetzt. Grundschutzkatalog: Detaillierte Beschreibung der Sicherheitsmassnahmen, die umgesetzt sein müssen.	*Leistungsbezüger* sind die „Informatikkunden“, die Abnehmer der Leistungen, die Benutzenden in ihrer Gesamtheit. Also Organisationseinheiten, nicht Einzelpersonen. *Leistungserbringer* sind alle Produzenten, Betreiber, also externe oder interne Informatikbetreiber, auch die in der eigenen Organisationseinheit.

Katalog "erhöhter Schutz": Detaillierte Beschreibung der Sicherheitsmassnahmen, die zusätzlich zum Grundschutzkatalog umgesetzt sein müssen. Sicherheitsstufe: Es werden zwei Stufen unterschieden: Grundschutz und erhöhter Schutz. Sicherheitsstatus: Der Sicherheitsstatus gibt Auskunft über den Grad an Sicherheit beim Leistungsbezüger und beim Leistungserbringer. Notfall: Ausserordentliche Störung, welche nur in seltenen Fällen eintritt und den Informatikbetrieb ernsthaft beeinträchtigt oder gar lahmlegt. Krise: Wenn der Notfall nicht behoben werden kann und daraus folgend grosse Störungen und möglicherweise existenzbedrohende Ereignisse ausserhalb der Informatik verursacht werden. Selbstsorge: Vorsorgliche Massnahmen, um bei Informatikausfällen den Arbeitsprozess beim Leistungsbezüger trotzdem mindestens in reduziertem Umfang aufrechterhalten zu können. Informationseigenschaften: Eigenschaften einer Informationseinheit, wie Verfügbarkeit, Vertraulichkeit, Unveränderlichkeit, Nachvollziehbarkeit, Aufbewahrungsdauer, Zugehörigkeit, Zurechenbarkeit usw. Mögliche Ausprägungen und die Konsequenzen für den Grundschutz oder erhöhten Schutz der Informationseinheit sind in Anhang 1 aufgeführt. Geschäftsrelevanz: Die Akten über ein Geschäft sind dann geschäftsrelevant und deshalb zu bewirtschaften, wenn sie Informationen enthalten, die für das Verstehen, Durchführen und Nachvollziehen eines Geschäfts bedeutsam sind. Es spielt dabei keine Rolle, ob diese Informationen in Papierform, als Brief, als	Die Selbstsorge wird im Business Continuity Management (BCM) oft vergessen: die ISV fordert in § 10, dass sich auch die Leistungsbezüger Gedanken machen müssen über die Fortsetzung dringender oder sehr wichtiger Arbeiten bei Ausfall der Informatik.

Fax, als eMail oder als Datenbankeintrag vorliegen. Archiv: Stelle, welche Informationen zur definitiven Verwahrung übernimmt. Ruhende Ablage: Ablage in Nähe der Benutzer; pro Abteilung, pro öffentliches Organ geführte, ordentliche Ablage für Informationen, welche für das Verwaltungshandeln nicht mehr benötigt werden. NSP: Network Security Policy des Kantons Zürich; Umschreibung und Regelung von Aufbau und Betrieb der kantonalen Datentransportsysteme.	
B. Risikomanagement	In Abweichung zur üblichen Gliederung wird hier zuerst das „was?“ und erst anschliessend das „wer?“ beschrieben, da diese Reihenfolge nach Auffassung der Autoren hier das Verstehen einfacher macht.
Feststellung der Informationssicherheit	*Voraussetzung für das Verbessern der Informationssicherheit ist die Feststellung, wieviel Sicherheit es bereits gibt.*
§ 4. [1] Die Sicherheit der Informatiksysteme und der Informationen gilt als angemessen, wenn der auf einer Risikoeinschätzung basierende Schutzbedarf durch die Sicherheitsvorkehrungen abgedeckt ist. [2] Den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit wird Rechnung getragen. [3] Vorgehensmässig sind vier Schritte zu unterscheiden: a. die Schutzbedarfsermittlung, b. die Ermittlung des Sicherheitsstatus,	Entspricht dem zeitgemässen „risikobasierten“ Ansatz, welcher auch durch die entsprechenden Normen ISO 27000 und ISO 31000 gestützt wird. Hier folgt die Einschränkung, dass Sicherheit kein absolutes Ziel sein kann, sondern immer auch zweckmässig, wirtschaftlich und benutzerfreundlich sein muss. Schutzbedarf aus Sicht Leistungsbezüger, Sicherheitsstatus aus Sicht Leistungserbringer,

c. der Abgleich der beiden Grössen, und d. der Entscheid über allfällig zu ergreifende Massnahmen.	.. dies ergibt, einander gegenübergestellt, ein ausgeglichenes oder eben ein noch zu verbesserndes Gesamtbild. Mit der Feststellung ist es nicht getan, es braucht auch Entscheide!
Ermittlung des Schutzbedarfs	
§ 5. [1]Der Schutzbedarf wird im Rahmen einer Gesamtbeurteilung von Ereignissen ermittelt, welche die Informationsleistungen und die Funktionsfähigkeit der damit betroffenen Prozesse beeinträchtigen oder verunmöglichen könnten. [2]Die Schadensereignisse und ihre Folgen sind anhand des Schutzbedarfskatalogs zu ermitteln. [3]Zu berücksichtigen sind normale Betriebsereignisse sowie Notfälle und Krisenlagen.	Stand des Methodikwissens: Es ist ein Ereigniskatalog (Szenarien) zur Verfügung zu stellen, anhand dessen der Leistungsbezüger festlegen kann, welche Schadensauswirkungen bei ihm zu verzeichnen wären. Diese Szenariotechnik ist mit einem generell gültigen Massstab zu hinterlegen, dann werden die Schutzbedarfserhebungen vergleichbar und damit übertragbar auf die Leistungserbringer. Auf diese Weise wird der Aufwand für die Schutzbedarfsermittlung auf ein noch vertretbares Minimum reduziert.
Sicherheitsstatus beim Leistungsbezüger	
§ 6. [1] Leistungsbezüger haben betreffend der Benutzung von Informatikleistungen und -einrichtungen über den Grad an Sicherheit, welcher bei ihnen diesbezüglich erbracht wird, zu berichten. [2] Als Referenzbasis gelten Auszüge aus dem Grundschutzkatalog und dem Katalog erhöhter Schutz. [3] Der Abdeckungsgrad der Sicherheitsanforderungen wird, gestützt auf diese Prüfung, festgestellt und in einem Sicherheitsstatus-Bericht festgehalten.	Die „Produktion von Sicherheit“ muss auch beim Leistungsbezüger eingeschätzt werden. Leistungsbezüger mit ihren Informatiknutzerinnen und Nutzern können sicher oder unsicher arbeiten. Deshalb sind sie und ihre Einrichtungen zu prüfen. Zum Verhalten gehört etwa der Umgang mit Passwörtern, die Sorgfalt im Umgang mit Daten auf dem Laptop; zu den Einrichtungen gehört der Brand- und Diebstahlschutz am Arbeitsplatz. Zu beachten ist auch Umgang und eingebaute Sicherheit bei transportablen Medien wie Laptop, Smartphone, USB-Stick usw.

Sicherheitsstatus beim Leistungserbringer	
§ 7. [1] Der Sicherheitsstatus jedes Leistungserbringers gibt Auskunft über den Grad an Sicherheit. Als Referenzbasis gelten der Grundschutzkatalog und der Katalog erhöhter Schutz. [2] Der Abdeckungsgrad der Sicherheitsanforderungen wird, gestützt auf diese Prüfung, festgestellt und in einem Sicherheitsstatus-Bericht festgehalten.	Da Leistungserbringer Drittunternehmen sein können, sind die Pflichten per Vertrag zu überbinden. Es kann deshalb nicht angeordnet werden, wie zu prüfen ist, sondern nur, dass es eine Prüfung geben muss und dass ein Prüfbericht zu erstellen ist.
Abgleich Schutzbedarf gegenüber Sicherheitsstatus	
§ 8. [1] Die zusammengehörenden Schutzbedarfsanforderungen und Sicherheitsstatus-Berichte werden abgeglichen und Differenzen festgehalten. [2] Für die Differenzbereinigung sind Anpassungen beim Sicherheitsstatus des Leistungserbringers, die Risikoüberwälzung zum Beispiel durch Versicherung, oder auch die bewusste Akzeptierung der Differenz möglich. [3] Die Entscheide sind schriftlich festzuhalten.	Ein wichtiger Schritt ist der Abgleich der geforderten Sicherheit (Schutzbedarf) mit der erbrachten Sicherheit (Sicherheitsstatus). Dieser Abgleich bedingt einheitliche Massstäbe sowohl auf Leistungsbezüger- als auch Leistungserbringerseite sowie eine „Umrechnungsmethode“, um den Schutzbedarf mit dem Sicherheitsstatus tatsächlich abgleichen zu können. Es ist Sache des Kompetenzzentrums Informationssicherheit der kantonalen Verwaltung, hier konkrete Vorschläge und Musterverfahren zu entwickeln und den öffentlichen Organen zur Verfügung zu stellen.
Sicherheitsstufen	
§ 9. [1] Es werden zwei Sicherheitsstufen unterschieden: Grundschutz und erhöhter Schutz.	Um sowohl beim Abschluss von Vereinbarungen mit Leistungserbringern als auch bei der Sicherheitsüberprüfung einen generell gültigen Massstab anwenden zu können, schreibt die ISV vor,

	dass jeder Leistungserbringer mindestens Grundschutz „liefern“ muss.
[2] Das öffentliche Organ bestimmt, welche Sicherheitsmassnahmen für die Kataloge Grundschutz und erhöhter Schutz grundsätzlich gelten.	Das öffentliche Organ ist autonom in der Festlegung, was bei ihm als Grundschutz rsp. erhöhter Schutz gilt. Es wird empfohlen, im ganzen Geltungsbereich der ISV den gleichen Massstab anzulegen, aber Vorschrift ist dies nicht. Die Autonomie der öffentlichen Organe wurde höher gewichtet als die Einheitlichkeit.
[3] Pro Datenbestand und Prozess ist eine Sicherheitsstufe der Informationen festzulegen. Dabei ist der Schutzbedarf gemäss Schutzbedarfskatalog zu berücksichtigen.	Dieser Passus betrifft die oft „Klassierung“ genannten Aufgaben. Die Zuweisung zu den vorgegebenen Informationseigenschaften erfolgt pro Informationsbestand.
Sicherheit in Not- und Krisenfällen	
§ 10. [1] Als Massnahme der Notfall- und Krisenvorsorge sind besonders gefährdete Prozesse und die verantwortlichen Leistungsbezüger und -erbringer zu bezeichnen.	Im Bereich Notfall- und Krisenvorsorge soll nur ein „Minimalset“ vorgegeben werden. Es macht wenig Sinn, Prozesse mit kleinerer bis mittlerer Bedeutung in die Notfallplanung einzubeziehen.
[2] Die Leistungsbezüger und Leistungserbringer bearbeiten primär die Reaktionsfähigkeit und weniger die Reparaturfähigkeit im Not- oder Krisenfall. Dazu gehören insbesondere Krisenorganisation, einfache Checklisten sowie die Selbstsorge mit prozessnahen Massnahmen beim Leistungsbezüger. Übungen in einer im Voraus festgelegten Kadenz haben die angeordneten Dispositive zu vertiefen.	Die Reparatur kann erst im jeweiligen Einzelfall vorbereitet und durchgeführt werden. Wichtig ist hingegen, dass man personell für diese Not- und Krisenfälle vorbereitet ist. Des weiteren sollten einfache Checklisten und Formulare schon vor dem Krisenfall vorbereitet werden. Ein Anliegen ist auch, dass auf Leistungsbezügerseite minimale Vorkehrungen getroffen werden, um einen Not- rsp. Krisenfall zu überleben. Dazu dient die vorbereitete Selbstsorge.
[3] Die Vorsorgemassnahmen und Krisenpläne müssen so einfach wie möglich und wirtschaftlich vertretbar sein. Sie sind schriftlich festzuhalten.	

C. Organisation der Informationssicherheit	
Grundsatz	
§ 11. Die Verantwortung für Informations- und Informatiksicherheit obliegt der Stelle, welcher die Verantwortung für die Informationsbearbeitung zugeordnet ist.	Der wichtigste Grundsatz: Die Verantwortung liegt nicht bei einer Stabstelle, bei einem kantonalen Gremium, sondern immer dort, wo die Verantwortung für das laufende Geschäft liegt.
Öffentliches Organ	
§ 12. [1] Die öffentlichen Organe sind in ihrem Zuständigkeitsbereich für die Einhaltung und Umsetzung der Grundsätze im Umgang mit Informationen und Informatiksystemen verantwortlich. Jedes öffentliche Organ bezeichnet eine Beauftragte oder einen Beauftragten für Informationssicherheit.	Jedes Organ hat einen Beauftragten oder eine Beauftragte für Informationssicherheit zu bestimmen. Die Aufgaben werden so einer Person zugewiesen. Die Aufgaben sind überblickbar und müssten sowieso irgendwo in der Organisation erledigt werden.
[2] Öffentliche Organe können ihre Organisationen zusammenlegen und gemeinsam ein öffentliches Organ mit der Wahrnehmung der Aufgaben im Bereich Informationssicherheit beauftragen. Die Verantwortung für die Informationssicherheit bleibt beim einzelnen öffentlichen Organ.	Um kleineren öffentlichen Organen die Arbeit zu erleichtern, können diese ihre Organisationen gemeinsam aufbauen und betreiben.
[3] Das öffentliche Organ beurteilt aufgrund der Schutzbedarfsanalysen sowie der Sicherheitsstatus-Berichte die zu erwartende Sicherheit und entscheidet, wie die Differenzen zu bereinigen sind.	Die ISV gibt nicht vor, wer innerhalb der Organisation die Abgleiche macht und über die Differenzbereinigung entscheidet. Dies kann in jeder Organisation individuell gestaltet werden.
[4] Das öffentliche Organ veranlasst die Leistungsbezüger und verpflichtet die Leistungserbringer, dem Schutzbedarf entsprechende, angemessene Vorsorgemassnahmen für Notfälle	

und Krisenlagen zu planen und umzusetzen. [5] Das öffentliche Organ stellt sicher, dass Vorfälle im Bereich Informationssicherheit an eine definierte, allen Mitarbeitenden bekannte Stelle gemeldet und dort systematisch ausgewertet werden.	Das Meldewesen muss organisiert werden und die Mitarbeitenden sind zu instruieren.
Aufgaben der Leistungsbezüger	
§ 13. [1] Der Leistungsbezüger ermittelt den Schutzbedarf. [2] Der Leistungsbezüger ermittelt den Sicherheitsstatus auf Anwenderseite. [3] Der Leistungsbezüger plant und ergreift dem Schutzbedarf entsprechend angemessene Vorsorgemassnahmen (Selbstsorge) für Notfälle und Krisenlagen.	Der Leistungsbezüger: das kann eine Abteilung sein, ein Amt, oder auch eine leitende Person in einem Prozess.
Aufgaben der Leistungserbringer	
§ 14. [1] Die Leistungserbringer haben den Sicherheitsstatus ihrer Systeme, Einrichtungen und Prozesse zu ermitteln und in einer im Voraus festgelegten Kadenz durch fachlich ausgewiesene, unabhängige Auditoren überprüfen zu lassen. [2] Die Sicherheitsstatus -Berichte sind der oder dem Beauftragten für Informationssicherheit des beauftragenden öffentlichen Organs unentgeltlich zu übergeben. Die oder der Beauftragte informiert den Leistungsbezüger angemessen.	Dem Leistungserbringer wird nicht vorgeschrieben, wer die Sicherheitsüberprüfung machen soll. Vorgeschrieben ist einzig, dass es sich um ausgewiesene, unabhängige Fachleute handeln muss. Der Leistungserbringer kann sich nicht selbst überprüfen. Um die Vertraulichkeit zu gewährleisten und trotzdem angemessen zu informieren, ist ein Statusbericht, nicht die detaillierte Auflistung der Befunde, dem oder der Beauftragten für Informationssicherheit zu übergeben. Diese oder dieser informiert die Entscheidungsinstanzen angemessen.

Dienstleistungen der kantonalen Verwaltung	
§ 15. [1] Die kantonale Verwaltung stellt einen Katalog von Massnahmen für die beiden Sicherheitsstufen Grundschutz und erhöhten Schutz sowie einen Schutzbedarfskatalog zur Verfügung, welcher durch das öffentliche Organ angepasst werden kann. Die kantonalen Vorgaben sind möglichst zu übernehmen. [2] Die kantonale Verwaltung stellt Benutzungsreglemente als Muster zur Verfügung.	Es gibt keine „Informationsssicherheits-Zentralinstanz“ im Kanton. Die kantonale Verwaltung hat aber die Aufgabe, den öffentlichen Organen Musterlösungen und Musterkataloge zur Verfügung zu stellen.
Aufgaben der oder des Beauftragten für Informationssicherheit	
§ 16. [1] Die oder der Beauftragte für Informationssicherheit überprüft die Schutzbedarfsanalysen aufgrund der zu berücksichtigenden Risiken. [2] Sie oder er überprüft die Sicherheitsstatus-Berichte und beurteilt, ob der Sicherheitsstatus gegenüber dem Schutzbedarf ausreichend ist. Sie oder er veranlasst die Differenzbereinigung. [3] Sie oder er prüft die Vorsorgemassnahmen für Notfälle und Krisenlagen seitens Leistungsbezüger auf Zweckmässigkeit und Verhältnismässigkeit. [4] Sie oder er überprüft die Vorkehrungen bei Projekten, insbesondere den Sicherheitsbericht vor Inbetriebnahme neuer Verfahren. [5] Sie oder er erstellt jährlich einen Bericht über die Informationssicherheit zuhanden des öffentlichen Organs.	Die Aufgaben der oder des Beauftragten für Informationssicherheit sind nur pauschal beschrieben. Je nach Grösse der jeweiligen Organisation werden die Aufgaben auf mehrere Personen verteilt. Wichtig ist, dass der oder die Beauftragte gegenüber den Instanzen die Leistungen und Verpflichtungen als Ganzes vertritt. Die oder der Beauftragte ist nicht für die Informationssicherheit verantwortlich, dies ist gemäss § 11 geregelt. Berichterstattung nur intern im öffentlichen Organ. Es gibt keine neue, zusätzliche Berichterstattung an übergeordnete Instanzen.

Einhaltung der Regelungen der ISV	
§ 17. Die Einhaltung der Regelungen der ISV wird überprüft. Die Überprüfung erfolgt soweit zulässig und nicht schon durch andere Gesetze und Verordnungen vorgegeben: a. durch die mit Controllingaufgaben beauftragte Stelle des öffentlichen Organs, oder b. durch eine unabhängige fachlich ausgewiesene Überprüfungsinstanz.	Die Compliance, das Einhalten der Regeln, ist zu überprüfen. Keine Spezialprüfinstanz. Die Prüfung erfolgt durch die Organe, die auch sonst die Überprüfungen machen. Durch das öffentliche Organ kann auch eine Drittinstanz bestimmt werden.

II. Besondere Bestimmungen

A. Regelungen für Benutzende	
Erlass von Benutzungsreglementen	
§ 18. [1] Das öffentliche Organ regelt das Verhalten im Umgang mit Informationen und Informatikmitteln, insbesondere auch der Telekommunikations- und Sicherheitseinrichtungen und -verfahren durch den Erlass von Benutzungsreglementen. [2] Diese haben dem Schutz von Arbeitnehmern und Arbeitgebern zu dienen.	
Geltungsbereich der Benutzungsreglemente	

§ 19. [1] Die Benutzungsreglemente gelten für sämtliche Benutzende von Informatik-, Telekommunikations- und Sicherheitseinrichtungen des öffentlichen Organs. [2] Sie sind mittels Vertrag auch für externe Arbeitnehmer und weitere Dritte, welche die Informatikmittel des öffentlichen Organs verwenden, verbindlich zu erklären. [3] Wenn Informatikeinrichtungen oder -verfahren des Kantons benutzt werden, sind die diesbezüglichen Benutzungsregeln zwingend in das Benutzungsreglement des öffentlichen Organs aufzunehmen.	Zwingend ist, dass alle Mitarbeitenden und weitere Benutzende einem Benutzungsreglement unterstellt sind. Dies gilt auch für die Studierenden einer Ausbildungsstätte. Dies betrifft z.B. Benutzungsregeln bei Verwendung von kantonalen Übermittlungseinrichtungen.
B. Klassierung und Sicherheit von Informationen	
Klassierung	
§ 20. Das öffentliche Organ legt beim Leistungsbezüger Regeln und Prozesse fest, wie mit den Informationseigenschaften umzugehen ist.	Die Klassierungsmerkmale, genannt Informationseigenschaften, werden in der Beilage zur ISV beschrieben. Sie sind verbindlich. Die Auswahl der konkreten Eigenschaften für eine Datenmenge erfolgt durch den Leistungsbezüger.
Sicherheitsstufen	
§ 21. [1] Die Sicherheit der klassierten Informationen wird mit einer der beiden Sicherheitsstufen abgedeckt. [2] Sicherheitsmassnahmen zu Informationseigenschaften, welche	Um den Bestimmungsprozess zu vereinfachen, gibt die Tabelle der Informationseigenschaften zwei Varianten vor: Entweder sind die dem Dokument zugewiesenen Eigenschaften mit der Sicherheitsstufe „Grundschutz“ bereits abgedeckt, fallen also in die grüne Fläche in der

mit keiner der beiden Sicherheitsstufen abgedeckt werden, sind in separaten Abmachungen zwischen Leistungsbezüger und Leistungserbringer festzulegen.	Tabelle, dann muss seitens Leistungsbezüger nichts weiter vorgekehrt werden. Sind die Anforderungen höher, gibt es die rote Fläche mit dem erhöhten Schutz. Nur in Fällen, welche weder mit der grünen noch mit der roten Fläche abgedeckt sind, muss im Vertrag oder SLA dieser Spezialfall separat geregelt werden. In jedem Fall obliegt es aber dem Leistungsbezüger, intern zu regeln, wie mit dem derart geschützten Dokument beim Leistungsbezüger umzugehen ist. Zur Illustration: Ein Grundbuchauszug habe die Eigenschaften „rot“, dann sorgt der Leistungserbringer auf seiner Seite für die notwendigen technischen und organisatorischen Sicherheitsmassnahmen. Aber ob der Auszug in den Büros immer unter Verschluss aufzubewahren ist, ob der Auszug innerhalb der Verwaltung frei zirkulieren darf, ob Kopien gemacht werden dürfen, das muss das öffentliche Organ intern regeln (dieser Teil der Verantwortung ist in den Verwaltungen auch meist einwandfrei geregelt). Die Vereinfachung besteht darin, dass nicht für jede Art von Informationsklassierung eine separate technische Lösung festgelegt werden muss.
C. Geschäftliche und private Informationen	
Geschäftliche und private Informationen	
§ 22. [1]Es ist zwischen geschäftlichen und privaten Informationen zu unterscheiden.	Diese Unterscheidung ist obligatorisch, damit dem Post- und Fernmeldegeheimnis nachgelebt werden kann. Private Daten dürfen vom Arbeitgeber nicht eingesehen werden, andererseits darf der Benutzende geschäftliche Daten nicht nach eigenem Gusto

[2] Bei den öffentlichen Organen gelten alle Informationen als geschäftliche Informationen, sofern sie vom berechtigten Benutzer nicht ausdrücklich als private Informationen bezeichnet werden.	verschieben, ändern oder gar löschen. Diese Pauschalregelung verhindert eine unnötige Bürokratie. Das öffentliche Organ hat festzulegen, wie die privaten Informationen zu kennzeichnen sind. Es kann eine einfache Verschiebung in ein privates Postfach sein, eine als privat gekennzeichnete Informationsmappe. Die kantonale Verwaltung gibt Lösungsvorschläge.
Umgang mit geschäftlichen Informationen	
§ 23. [1] Mitarbeitende sind verpflichtet, Geschäftsdokumente nach Weisung abzulegen. [2] Geschäftsrelevante Informationen dürfen vom Benutzenden nicht gelöscht werden.	Diese selbstverständlichen Aufbewahrungsvorschriften wurden in der Vergangenheit – teilweise aus Mangel an Speicherplatz – oft missachtet. Die aufzubewahrenden Informationen dürfen, ja müssen hingegen zeitrichtig in die ruhende Ablage verschoben werden.
Umgang mit privaten Informationen	
§ 24. [1] Mitarbeitende sind berechtigt, private Informationen im Rahmen der Benutzungsreglemente des öffentlichen Organs zu bearbeiten. [2] Den Mitarbeitenden ist durch das öffentliche Organ die Möglichkeit zu verschaffen, private Informationen zu kennzeichnen und/oder getrennt abzulegen. Dem öffentlichen Organ ist der Zugriff auf diese Informationen nicht gestattet.	Ist eigentlich Sache der Personalreglemente, aber diese sind nicht überall auf Gleichstand. Deshalb hier die explizite Erlaubnis, aber auch der Hinweis, präzisere Regeln im Rahmen der Benutzungsreglemente zu erlassen.

D. Sicherheitsanforderungen ruhende Ablage	Die „ruhende Ablage“ ist eine zwingende Voraussetzung, um Dokumente, ja alle geschäftsrelevanten Informationen unverändert aufzubewahren, um sie jederzeit unverändert zur Verfügung zu haben und sie später unversehrt dem Archiv übergeben zu können, sofern dort der Bedarf besteht.
Sicherheitsanforderungen bei der Informationsverwaltung in der ruhenden Ablage	
§ 25. [1] Im laufenden Betrieb sind Informationen, welche später der ruhenden Ablage oder dem Archiv zu übergeben sind, zu kennzeichnen. Zur Kennzeichnung gehört auch ein Archivschlüssel.	Um die Informationen später wieder auffinden zu können, braucht es einen Archivschlüssel. Dieser muss bereits im laufenden Betrieb angebracht werden, denn nur im laufenden Betreib weiss man, wohin eine Informationseinheit gehört.
[2] Informationen sind, sofern sie für das Verwaltungshandeln nicht mehr benötigt werden, in einen gesonderten, technisch abgetrennten Bereich, die ruhende Ablage, zu verschieben.	Die ruhende Ablage muss separat vom laufenden Betrieb geführt werden. Es gibt keine Spezialvorschrift betreffend die Technik, es kann sich um die gleiche Technik handeln wie im laufenden Betrieb.
[3] Informationen in der ruhenden Ablage müssen kumulativ:	
a. jederzeit wieder aufgefunden werden können,	
b. in einem möglichst weitgehend applikationsunabhängigen Datenformat und mit applikationsunabhängigen Zugriffspfaden gespeichert werden,	Die Forderung nach Applikationsunabhängigkeit ist essentiell, anders kann nicht sichergestellt werden, dass die Informationen längerfristig wieder aufgefunden und gelesen werden können.
c. mit besonderen technischen Massnahmen dauerhaft vor Verlust, unberechtigter Einsichtnahme und vor Veränderung geschützt sein,	
d. mit angepassten Zugriffsrechten versehen werden.	Sobald Informationen in die ruhende Ablage verschoben werden, verlieren sie zwangsläufig den Zugriffsschutz der Herkunftsapplikation. Deshalb müssen in der ruhenden Ablage die zur Informationseinheit passenden Zugriffsrechte neu vergeben werden. Dies kann auf die
[4] Jedes öffentliche Organ hat mindestens eine ruhende Ablage einzurichten.	

	gleiche Art erfolgen wie in §§ 20f. vorgegeben.
Löschung und Vernichtung von Informationen	
§ 26. Schreibt eine gesetzliche Bestimmung vor, dass das öffentliche Organ die Informationen zu löschen oder zu vernichten hat, so ist diese Vorschrift erfüllt, wenn ein Zugriff auf diese Informationen mit hoher Wahrscheinlichkeit unmöglich ist, sofern diese Informationen mit technischen Mitteln nicht gelöscht werden können.	IDG § 5, Abs. 3 und §18 Abs.2 verlangen, dass nicht mehr benötigte Informationen zu „vernichten“ sind. Da dies nicht in jedem Informationssystem technisch möglich ist, wurde diese Vorschrift in §26 IDV geschaffen.
E. Sicherheitsverfahren bei der Projektarbeit	
Informationssicherheitskonzept	
§ 27. [1] Das öffentliche Organ sorgt dafür, dass bei Vorhaben betreffend Einsatz oder Ersatz von Informationsverarbeitungsverfahren bereits ab Projektbeginn eine Risikoabwägung und ein Informationssicherheitskonzept erstellt werden. [2] Dieses Konzept muss durch die zuständige Beauftragte oder den zuständigen Beauftragten für Informationssicherheit geprüft und vom öffentlichen Organ genehmigt werden. Das Konzept ist laufend zu aktualisieren.	Es ist wichtig, bereits in der Projektarbeit ab Projektstart an die Sicherheitsproblematik zu denken und diese in die Gestaltungsarbeiten einzubeziehen.
Prüfung vor Inbetriebnahme	

§ 28. Bevor das neue oder geänderte Informationsverarbeitungsverfahren eingesetzt werden darf, muss durch das öffentliche Organ geprüft werden, ob das Sicherheitsverfahren ordnungsgemäss durchgeführt wurde und die beschlossenen Massnahmen umgesetzt sind.	Es braucht nicht nur ein Sicherheitskonzept, es muss auch umgesetzt werden. Es ist zwingend nötig, das Sicherheitsverfahren vor der Inbetriebnahme zu realisieren.
F. Informationsaustausch und Informationstransport	
Netzwerksicherheit	
§ 29 [1] Jeder elektronische Informationsaustausch innerhalb oder zwischen den öffentlichen Organen oder mit Dritten hat gemäss den vom Regierungsrat erlassenen Vorschriften (Network Security Policy NSP) zu erfolgen. [2] Der Betrieb der Netzwerke des öffentlichen Organs, einschliesslich sämtlicher Übergangspunkte zu Drittnetzen, richtet sich nach den in der Network Security Policy aufgeführten Vorgaben. [3] Der Zugriff von aussen auf das Netzwerk des öffentlichen Organs, muss über gesicherte Netzwerkübergänge erfolgen und richtet sich nach den in der Network Security Policy aufgeführten Vorgaben. [4] Das öffentliche Organ bezeichnet die in der Network Security Policy aufgeführten Instanzen für den Betrieb seiner Netzwerke. [5] Die oder der Beauftragte für Informationssicherheit des öffentlichen Organs kann auf Antrag des öffentlichen Organs Ausnahmen bewilligen.	§ 29 ist der Anker zwischen den Vorgaben des IDG und den Detailregelungen der NSP. Vollzugsvorschrift für die generelle Vorgabe in der NSP. Im öffentlichen Organ kann nur die oder der Beauftragte Ausnahmen von der NSP bewilligen.

Sicherheit beim Informationstransport	
§ 30 [1] Der Informationsaustausch über öffentliche Netze ist nur über gesicherte Zugangspunkte zulässig. [2] Der Informationstransport über öffentliche Netze wird entsprechend dem Schutzbedarf der Information geschützt.	„Private“ Anschlüsse sind nicht gestattet, da diese meist nicht ausreichend geschützt sind. Zwingend: der Schutzbedarf muss festgestellt werden, wie in IDV § 5 rsp. § 21 vorgegeben.
G. Auslagerung der Informationsbearbeitung	
Datenbearbeitung durch Dritte	
§ 31. Lagert der Leistungsbezüger das Bearbeiten von Informationen an Dritte, insbesondere an ein anderes öffentliches Organ oder an ein privates Unternehmen aus, gelten die Voraussetzungen von § 6 IDG. Die ABG Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen oder analoge Bestimmungen finden Anwendung.	An sich ist IDG § 6 klar: *§ 6. [1] Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.* *[2] Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.* Zu prüfen ist im Einzelfall, ob z.B. bei einer Auslagerung innerhalb einer Organisation (z.B. eine Direktion zur andern) auch die AGB Anwendung finden sollen.
H. Schlussbestimmungen	
Vollzugsbestimmungen	

§ 32. [1] Für die Umsetzungen der Vorgaben aus dieser Verordnung wird den öffentlichen Organen eine Frist von zwei Jahren ab Inkraftsetzung dieser Verordnung eingeräumt. [2] Die öffentlichen Organe erlassen die für den Vollzug dieser Verordnung erforderlichen Ausführungsbestimmungen.	Die zwei Jahre Umsetzungsfrist scheinen kurz, sind aber nicht unmöglich. Sicherheit darf nicht auf die lange Bank geschoben werden.
Geltung der Ausführungsbestimmungen	
§ 33. Die Ausführungsbestimmungen der kantonalen Verwaltung gelten für die öffentlichen Organe sinngemäss, sofern sie in ihrem Zuständigkeitsbereich keine eigenen Ausführungsbestimmungen erlassen.	Es steht dem öffentlichen Organ frei, die Ausführungsbestimmungen der kantonalen Verwaltung (dort „Richtlinie Nr. 1 zur ISV“ rsp. ISMS genannt) zu übernehmen, oder eigene Ausführungsbestimmungen zu erlassen.
Inkrafttreten	
§ 34. Diese Verordnung tritt per …….. in Kraft und ersetzt die Informatiksicherheitsverordnung LS 170.8 vom 17. Dezember 1997.	

Der Regierungsrat