Merkblätter Informationssicherheit

Version 2021-11-17

Security Board des Kantons Zug

www.zg.ch/datenschutz

Kanton Zug

Inhalt

Einleitung

Die Medien berichten fast täglich über Hackerangriffe, Softwarefehler oder Datendiebstahl und machen deutlich, dass mit der Nutzung der Informations- und Kommunikationstechnologien Risiken und Gefahren verbunden sind. Viele dieser Risiken und Gefahren lassen sich vermeiden oder zumindest minimieren. In fünf Merkblättern werden die einzelnen Themen ausführlich beschrieben.

Warum diese Merkblätter?

Der Informationssicherheit kommt in der Verwaltung ein hoher Stellenwert zu. Dies liegt auch daran, dass Sie als Mitarbeiterin und Mitarbeiter der kantonalen Verwaltung in der Regel viele und teilweise auch sehr sensible Daten der Zuger Bevölkerung bearbeiten. Sie sind zudem zur Einhaltung des Amtsgeheimnisses verpflichtet und haben bei der Bearbeitung von Personendaten die Bestimmungen des Datenschutzes zu beachten.

Damit sind Sie auch zur Einhaltung von Nutzungsvorgaben verpflichtet, welche dazu dienen, die Informationssicherheit zu gewährleisten. Die folgenden Ausführungen zeigen Ihnen auf,

a) welche technischen und organisatorischen Massnahmen Sie einzuhalten oder zu treffen haben, um Personendaten und vertrauliche Informationen sicher zu bearbeiten, und
b) welche Vorgaben und Beschränkungen Sie im Rahmen der Nutzung der IT-Infrastruktur der Verwaltung zu beachten haben.

Die Ausführungen in den vorliegenden Merkblättern gelten grundsätzlich bei der Bearbeitung von Personendaten und vertraulichen Informationen unabhängig davon, ob Sie an einem Arbeitsplatz, in einem Verwaltungsgebäude, zu Hause oder unterwegs bzw. mobil arbeiten.

Rechtsgrundlagen

Gestützt auf das Datenschutzgesetz des Kantons Zug (DSG)[1] hat der Regierungsrat die Verordnung über die Informationssicherheit von Personendaten (VIP)[2] erlassen. Diese sieht vor, dass das Security Board Merkblätter für die Instruktion aller Mitarbeitenden zur Verfügung stellt.

Gleichzeitig sei darauf hingewiesen, dass für Sie als Mitarbeiterin oder Mitarbeiter und als Nutzerin oder Nutzer der kantonalen oder gemeindlichen IT-Infrastruktur allenfalls auch weitere gesetzliche Bestimmungen und Vorgaben gelten können.[3] Für weitere Ausführungsbestimmungen für kantonale und gemeindliche Mitarbeiterinnen und Mitarbeiter rund um Mobiletelefonie, PC-Arbeitsplatz, Notebook, elektronischen Datenaustausch und Informationssicherheit siehe iZug https://izug.zg.ch/web/behoerden/finanzdirektion/amt-fuer-informatik-und-organisation/it-nutzungsregeln.

Geltungsbereich

Diese Merkblätter gelten umfassend und verpflichtend für alle Mitarbeitenden der kantonalen Verwaltung, der Einwohnergemeinden, der Gerichte und der kantonalen Schulen sowie für temporär Angestellte und Personen, die für den Kanton tätig sind.

Die Merkblätter gelten sinngemäss auch für die Mitarbeitenden von Bürger-, Kirch- und Korporationsgemeinden sowie von Institutionen, soweit ihnen in Leistungsvereinbarungen öffentliche Aufgaben übertragen werden.

Ihre Verantwortung

Daten und Informationen sind wichtige Werte. Sie erfordern Schutz und sorgsamen Umgang. Angesichts wachsender Regulierung und Sensibilisierung der Öffentlichkeit, der laufenden technischen Fortschritte sowie der allgegenwärtigen Bedrohungen durch Cyberkriminalität ist die öffentliche Verwaltung gefordert, Daten ihrem Schutzbedarf gerecht zu bewirtschaften. Bürgerinnen und Bürger, Firmen, Geschäftspartner und andere Personen, deren Daten im Kanton bearbeitet werden, erwarten einen rechtskonformen, verantwortungsvollen Umgang. Der Kanton Zug setzt dafür auf

[1] § 7 DSG, BGS 157.1

[2] BGS 157.12

[3] Z.B. Kantonale Vorgaben: «Verordnung über die Benutzung von
elektronischen Geräten und Kommunikationsmitteln im Arbeitsverhältnis», BGS 154.28, und «Verordnung über die Nutzung von Mobil- und Festnetzgeräten», BGS 154.29.

verschiedene organisatorische und technische Massnahmen. In vielen Bereichen können Sie, liebe Mitarbeiterin und lieber Mitarbeiter, mit korrektem Verhalten wesentlich dazu beitragen, dass Schäden verhindert und Persönlichkeitsrechte gewahrt werden.

Entsteht ein Schaden, weil Sie Sicherheits- und Nutzungsvorgaben nicht eingehalten haben, können Sie dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden. Gleichzeitig sind Sie mitverantwortlich, dass die vorliegenden Sicherheits- und Nutzungsvorgaben in Ihrem Arbeitsumfeld umgesetzt werden. Stellen Sie fest, dass die Vorgaben in Ihrem Arbeitsumfeld in der Praxis nicht oder nur teilweise umgesetzt werden (können), melden Sie dies Ihrem Vorgesetzten, der Datenschutzstelle, dem IT-Sicherheitsbeauftragten des AIO bzw. Ihres IT-Dienstleisters oder dem AIO-Service-Desk.

E-Learning

Die vorliegenden Merkblätter werden durch eine Schulung in Form eines E-Learning ergänzt, das Ihnen auf der Webseite https://elearning.zg.ch zur Verfügung steht.

Für das E-Learning benötigen Sie etwa eine Stunde, und es endet mit einem kurzen Abschlusstest. Danach erhalten Sie eine Online-Bestätigung. Gemäss Anordnung des Regierungsrats sind die Schulung und der Abschlusstest alle zwei Jahre zu wiederholen.

Informationen/Kontakte

Für Fragen zum Datenschutz und zur Informationssicherheit von Personendaten:

Wenden Sie sich bitte an die Datenschutzstelle des Kantons Zug, www.datenschutz-zug.ch, datenschutz.zug@zg.ch.

Für Fragen zur Informationssicherheit:

Wenden Sie sich bitte an das Amt für Informatik und Organisation (AIO) des Kantons Zug, service-desk@zg.ch, bzw. an Ihren IT-Dienstleister.

1. Merkblatt «Sicherer Umgang mit Daten»

Geschäftliche Daten und Informationen dürfen nur berechtigten Personen zugänglich sein. Die zu treffenden Schutzmassnahmen hängen von der Klassifikation der bearbeiteten Daten ab. Bei besonders schützenswerten Personendaten und vertraulichen Informationen sowie bei einem Profiling sind erhöhte Sicherheitsmassnahmen erforderlich.

1.1 Geschäftliche Arbeitsgeräte

– Ein vom Arbeitgeber zur Verfügung gestellter Geschäfts-PC/Notebook/Tablet darf nur durch kantonale Mitarbeitende oder Personen, welche für die Verwaltung tätig sind, benutzt werden.

– Sie dürfen Dritten Ihr entsperrtes Arbeitsgerät nicht zur Nutzung überlassen. Dritte sind u.a. auch Vorgesetzte, Stellvertreter, andere Mitarbeitende, aber auch Familienangehörige.

– Schliessen Sie keine privaten oder fremden PCs bzw. Notebooks/Tablets an das Verwaltungsnetzwerk an. Jeder Mitarbeitende ist mitverantwortlich, dass in seiner Gegenwart keine fremden PCs bzw. Notebooks/Tablets von Externen ans Verwaltungsnetzwerk angeschlossen werden.

1.2 Sperren von Arbeitsgeräten

– Aktivieren Sie beim Verlassen Ihres Arbeitsplatzes bzw. -geräts konsequent die Bildschirmsperre, indem Sie gleichzeitig «Windows-Taste» und «L» oder «CTRL-ALT-DEL» und Enter-Taste drücken.

– Bei Mac-Geräten drücken Sie die Tastenkombination «CTRL-CMD» und «Q-Taste» um den Bildschirm sofort zu sperren. Alternativ ist der Ruhezustand des Mac zu aktivieren («Apfel» und «Ruhezustand»).

– Stellen Sie sicher, dass die Bildschirmsperre mit Passwortschutz automatisch einsetzt (nach 20 Minuten bei PC-Arbeitsplätzen, nach 10 Minuten bei Laptops und nach 5 Minuten bei mobilen Geräten).

– Falls Sie eine Smartcard im Einsatz haben, ist diese beim Verlassen des Arbeitsplatzes jeweils zu entfernen und mitzunehmen.

1.3 Unterlagen/Datenträger

– Bei der Bearbeitung von Daten ist immer zu verhindern, dass unberechtigte Dritte Zugang zu oder Einsicht in Personendaten und vertrauliche Informationen erhalten. Dies gilt insbesondere auch, wenn Sie in einem Grossraumbüro, unterwegs oder zu Hause arbeiten.

– Bewahren Sie Unterlagen (Papiere, Dossiers) und elektronische Datenträger, die vertrauliche Informationen und/oder besonders schützenswerte Personendaten oder Daten eines Profiling enthalten, auch bei kurzen Abwesenheiten während der Arbeitszeit (z.B. Pause) unter Verschluss auf.

1.4 Bei Arbeitsschluss

– Melden Sie Ihren PC/Laptop immer durch den Befehl «Herunterfahren» vom Netzwerk ab. Schalten Sie den PC nie via Schalter an einer Steckerleiste aus

– Bewahren Sie sämtliche Unterlagen oder Datenträger, die Personendaten und vertrauliche Informationen enthalten, verschlossen auf.

1.5 Software-Installation

– Auf geschäftlichen Arbeitsgeräten ist es verboten, Programme (z.B. exe, dll, msi, cab, etc.) selber zu installieren.

– Sie dürfen ausschliesslich vom AIO bzw. von Ihrem IT-Dienstleister zur Verfügung gestellte, rechtmässig lizenzierte Software verwenden.

1.6 Messenger-Dienste

– Nutzen Sie keine Messenger-Dienste wie WhatsApp, iMessage, Telegramm, Signal und dergleichen für geschäftliche Zwecke. Solche Dienste können in der Regel die notwendige Informationssicherheit nicht gewährleisten, da beispielsweise übermittelte Nachrichten auf Servern im Ausland gespeichert werden oder weil sie unter Umständen auf Kontaktdaten auf Ihrem Gerät zugreifen und diese weitergeben.

– Datenschutzkonformer Ersatz für Bildungseinrichtungen ist Threema.

1.7 Cloud-Dienste

– Die Nutzung von Public-Cloud-Diensten ist für Personendaten und vertrauliche Informationen verboten. Sollen Cloud-Lösungen eingesetzt werden, so sind diese im Rahmen der internen Projekt-/Beschaffungsprozesse durch das AIO bzw. den zuständigen IT-Dienstleister freizugeben.

– Das automatisierte Synchronisieren von Daten in Ordnerverzeichnissen, von geschäftlichen E-Mails, des Kalenders, der Kontakte und der Aufgaben mit externen Cloud-Diensten ist nicht zulässig.

1.8 Speichern von Daten

– Speichern Sie geschäftliche Daten an dem vom AIO bzw. Ihrem IT-Dienstleister zur Verfügung gestellten Netzwerk-Speicherort ab.

– Als Datenablage für geschäftsrelevante Daten stehen Ihnen Fachanwendungen oder alternativ ein dafür vorgesehenes Netzlaufwerk, bspw. das O-Laufwerk, zur Verfügung. Dadurch ist sichergestellt, dass die Daten durch das AIO bzw. Ihren IT-Dienstleister regelmässig gesichert werden.

– Eine temporäre Speicherung auf dem geschäftlichen Arbeitsgerät (Desktop) ist zulässig. Diese Dateien werden jedoch nicht gesichert und sind nur auf dem jeweiligen Arbeitsgerät nutzbar.

– Für die Datenablage von persönlichen (nicht geschäftsrelevanten) Daten steht Ihnen unter Windows der Ordner «Dokumente» zur Verfügung. Diese Dateien werden durch das AIO bzw. Ihren IT-Dienstleister gesichert. Auf diese persönliche Ablage haben nur Sie Zugriff.

– Aus Informationssicherheitsgründen nicht zur Datenspeicherung von Personendaten oder vertraulichen Informationen zugelassen sind

a) Public-Cloud-Dienste (wie etwa Dropbox, iCloud von Apple, oneDrive von Microsoft, Google Drive von Google);
b) jegliche privaten Geräte;
c) die Festplatte des Geschäfts-PC/-Laptops bzw. das C-Laufwerk[4].

1.9 Sichere Bekannt-/Weitergabe

– Stellen Sie im Falle einer Datenweitergabe sicher, dass diese rechtlich zulässig ist und dass der Transfer sicher erfolgt.

– Beachten Sie bei der elektronischen Weitergabe von Dokumenten, dass diese keine ungewollten Informationen enthalten (siehe Ziff. 1.10).

– Überprüfen Sie vor dem Versand die Notwendigkeit einer Verschlüsselung (siehe Ziff. 1.11).

– Wählen Sie bei der physischen Weitergabe von mobilen Datenträgern (siehe Merkblatt «Mobile Geräte und Datenträger») oder Papierakten eine angemessene Zustellungsart wie beispielsweise persönliche Übergabe, Übergabe per Bote, eingeschriebener Brief etc.

– Schützen Sie mobile Datenträger bzw. Ordner/Dateien zudem mit einem starken Passwort (siehe Merkblatt «Passwort»).

– Geben Sie Daten mittels eines mobilen Datenträgers weiter, müssen Sie sicherstellen, dass «alte» Daten auf dem Datenträger unwiderruflich gelöscht worden sind, bevor Sie die zu übermittelnden Daten auf den Datenträger speichern. Beachten Sie, dass Sie mit Befehlen wie «delete», «erase», «löschen» oder «(Quick)Format» die Daten nicht definitiv löschen und diese rekonstruierbar bleiben;

– Daher gilt für CD-ROMs/DVDs: Es dürfen nur neue Datenträger, die noch nie beschrieben worden sind, verwendet werden.

– USB-Sticks und externe Festplatten: Verwenden Sie nur solche Datenträger, die vom AIO bzw. Ihrem IT-Dienstleister autorisiert wurden oder mittels Verschlüsselung eine sichere Datenweitergabe ermöglichen.

1.10 Datenspuren in Dokumenten

– Dokumente, die Sie mit Office-Programmen (Word, Excel, PowerPoint etc.) erstellen, generieren automatisch eine ganze Reihe versteckter Informationen (z.B. Name des Erstellers, Erstellungsdatum, Änderungen, weitere Bearbeitende etc.).

– Stellen Sie deshalb vor der Weitergabe eines Dokuments sicher, dass solche Informationen entfernt wurden. Dies erreichen Sie, indem Sie

a) das fragliche Dokument als PDF abspeichern. So speichern Sie ein Office-Dokument (Word, Excel, PowerPoint) als PDF ab: Reiter «Datei» → «Speichern unter» → «Dateityp» PDF auswählen.
   Dadurch verhindern Sie auch, dass vom Adressaten oder von Dritten Änderungen am Dokument vorgenommen werden können.
b) die Informationen wie folgt entfernen: Im Reiter «Datei» → «Informationen» → «Auf Probleme überprüfen» → «Dokument prüfen». Die versteckten Informationen müssen Sie anschliessend entsprechend entfernen.

[4] Das C-Laufwerk ist für Programme und Systemdateien reserviert. Diese Daten werden durch das AIO nicht gesichert und sind deshalb nicht vor Verlust geschützt. Daten auf dem C-Laufwerk können ohne Ankündigung überschrieben oder durch Dritte eingesehen werden.

1.11 Dokumente verschlüsseln

– Dokumente können verschlüsselt werden. Dazu stehen Ihnen verschiedene Möglichkeiten zur Verfügung:

a) Mit dem Programm 7-Zip oder dem von Ihrem IT-Dienstleister bereitgestellten ZIP-Programm, das Sie im Startmenü finden. Bedenken Sie hier, dass der Name des Zip-Ordners und die Namen der enthaltenen Dokumente unverschlüsselt und damit für Dritte sichtbar bleiben. Verzichten Sie deshalb auf sprechende Bezeichnungen, die einen Hinweis auf den Inhalt des Dokuments geben (keinesfalls «fristlose_Entlassung_Müller.doc», sondern etwa «HR_27NOV2013»).
b) Mit Passwort direkt im Dokument: Bei Office-Dokumenten (Word, Excel, PowerPoint) können Sie das über den Reiter «Datei» → «Informationen» → «Dokument schützen» → «Mit Kennwort verschlüsseln» machen. Um ein passwortgeschütztes PDF zu erstellen, speichern Sie ein Office-Dokument (Word, Excel, PowerPoint) via Reiter «Datei» → «Speichern unter» → «Dateityp» als PDF auswählen → «Optionen» → «Dokument mit einem Kennwort verschlüsseln».

– Bitte beachten Sie: Verschlüsselte Dokumente können aus Virenschutzgründen nicht als Mailbeilage von extern empfangen werden. Wie in diesem Fall vorzugehen ist siehe Ziff. 3.4.

– Verwenden Sie aus Sicherheitsgründen bei allen Varianten, falls möglich, ein längeres und komplexeres Passwort, als die Minimalanforderungen gemäss Ziff. 2.3 es vorschreiben. Teilen Sie dem Adressaten das Passwort nicht auf dem gleichen Kanal mit, wie Sie die Datei übermittelt haben.

1.12 Datenlöschung/Entsorgung

– Stellen Sie Arbeitsgeräte und mobile Datenträger dem AIO bzw. Ihrem IT-Dienstleister zur sicheren Löschung bzw. fachgerechten Entsorgung zu.

– Entsorgen Sie Unterlagen mit Personendaten und vertraulichen Informationen in Papierform nicht im Abfall, sondern entsorgen Sie diese in den dafür vorgesehen Behältern oder schreddern Sie diese. Vorbehalten bleibt eine allfällige Aufbewahrungs- und Archivierungspflicht.

1.13 Protokollierung

– Zur Überwachung der Sicherheit, der Integrität und der Verfügbarkeit der Informatikmittel sowie der Zugangsberechtigung werden Systeme eingesetzt, die Protokolle erzeugen. Die Protokollierungen werden automatisch und grundsätzlich ohne Einsicht durch Personen durchgeführt. Personenbezogene Auswertungen sind im Rahmen der «Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis» zulässig (BGS 154.28).

– Die Protokolldaten werden höchstens sechs Monate bzw. so lange, wie für einen sicheren Betrieb erforderlich, aufbewahrt. Im Falle eines Verfahrens, z.B. wegen Verdachts auf Missbrauch, werden die Protokolldaten erst nach Abschluss des Verfahrens gelöscht.

1.14 Virenprävention

– Malware, Viren, Würmer oder Trojaner sind kleine Programme, die Computersysteme befallen und dabei Daten oder Programme zerstören, verändern oder andere gravierende Schäden anrichten können. Sie werden über E-Mail als Anhänge, über Dateien, die vom Internet heruntergeladen werden (z.B. Bildschirmschoner, Spiele, Freeware) oder über mobile Datenträger (siehe Merkblatt «Mobile Geräte und Datenträger») eingeschleust. Auch der Besuch von entsprechend präparierten Webseiten kann Schadprogramme auf Ihr Gerät laden.

– Öffnen Sie nur E-Mails, die vertrauenswürdig erscheinen. Öffnen Sie Anhänge zu E-Mails nur, wenn Sie diese erwartet haben (siehe Merkblatt «E-Mail»).

– Besuchen Sie nur vertrauenswürdige Webseiten (siehe dazu die Hinweise im Merkblatt «Internet»).

– Überprüfen Sie mobile Datenträger vor Gebrauch stets mit dem Virenscanner (z.B. mit der rechten Maustaste).

– Nehmen Sie keine eigenen Reparaturversuche vor, falls Sie Viren vermuten bzw. sicherheitsrelevante Vorkommnisse feststellen (verdächtige Meldungen, Einschränkungen der nutzbaren Dienste etc.). Informieren Sie per Telefon umgehend den AIO-Service-Desk (041 728 51 11) bzw. Ihren IT-Dienstleister. Fahren Sie – bei Nichterreichbarkeit – das Gerät herunter und nehmen Sie so bald wie möglich mit dem AIO-Service-Desk bzw. mit Ihrem IT-Dienstleister Kontakt auf.

2. Merkblatt «Passwort»

Passwörter sind der Schlüssel zu persönlichen Daten und erlauben Zugriff auf Systeme, Anwendungen und Informationen. Passwörter und PINs sind immer persönlich zu wählen und dürfen Drittpersonen nicht bekannt gegeben werden.

2.1 Persönliche Passwörter

– Arbeiten Sie immer mit Ihrem persönlichen Benutzernamen. Wählen Sie Passwörter und PINs immer persönlich und halten Sie sie geheim.

– Lassen Sie sich bei der Eingabe nicht beobachten bzw. ändern Sie im Zweifelsfall Ihr Passwort / Ihre PIN (Ziff. 2.6).

– Geben Sie ein persönliches Passwort oder eine PIN niemandem bekannt, auch nicht Vorgesetzten, Stellvertretern, Arbeitskollegen, Support-Mitarbeitern, Familienangehörigen etc.

– Notieren Sie keine Passwörter und PINs. Wenn Sie viele Passwörter nutzen, können Sie diese mittels eines Passwort-Managers verwalten (siehe Ziff. 2.8).

2.2 Nicht mehrfach verwenden

– Benutzen Sie im privaten Bereich andere Passwörter als am Arbeitsplatz.

– Verwenden Sie möglichst verschiedene Passwörter für verschiedene Anwendungen. Das PC-/Laptop-Passwort können Sie auch für geschäftliche Fachanwendungen an Ihrem Arbeitsplatz nutzen.

– Das PC-/Laptop-Passwort dürfen Sie nicht für Internet-Anwendungen einsetzen.

2.3 Ein gutes Passwort

– Wählen Sie ein Passwort mit mindestens acht Zeichen, das drei der folgenden vier Kriterien enthält:

a) Grossbuchstaben A…Z
b) Kleinbuchstaben a…z
c) Zahlen 0…9
d) Sonderzeichen wie z.B. !?+-_%&

– Vermeiden Sie …

a) einfach zu erratende Bestandteile wie Name, Vorname, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Auto-Kennzeichen etc.
b) aufeinanderfolgende Zahlen (1234 oder 4567) oder alphabetisch angeordnete Gross-/Kleinbuchstaben (ABCD oder bcde).

– Es gibt verschiedene Programme, mit denen Sie überprüfen können, wie gut bzw. «stark» Ihr Passwort ist (z.B. https://www.passwortcheck.ch). Führen Sie solche Tests allerdings nicht mit dem Original-Passwort durch, sondern nur mit einem ähnlichen.

2.4 Fachanwendungen

– Einige Fachanwendungen kennen Einschränkungen bei der Passwortwahl, die Sie berücksichtigen sollten:

a) Mehr als acht Zeichen werden möglicherweise nicht zugelassen.
b) Umlaute wie ääüéàè werden teilweise nicht akzeptiert oder können bei internationaler Tastatur nicht eingegeben werden.
c) Leerzeichen können zu Fehlern beim Login führen.
d) Sonderzeichen können nicht richtig verarbeitet werden.

– Bei Fragen dazu wenden Sie sich bitte an den entsprechenden Anwendungsverantwortlichen.

2.5 Einfach zu merken

– Wählen Sie ein Passwort, das Sie sich gut merken können, aber von anderen dennoch nicht einfach zu erraten ist. Tipps dazu:

a) Nehmen Sie ein Wort und erweitern Sie es mit Sonderzeichen/Zahlen oder ersetzen Sie einzelne Buchstaben durch Sonderzeichen/Buchstaben, z.B.: «Sonn**EN00schein», «fRan?ziska57».
b) Bilden Sie einen Satz und benutzen dann von jedem Wort den ersten Buchstaben für ein Passwort, so z.B.: «Wir fahren 2 Mal im Jahr nach Zermatt in die Ferien!». Das ergibt das starke Passwort «Wf2MiJnZidF!». Oder: «Morgens stehe ich auf und putze mir drei Minuten die Zähne», wobei Sie zusätzlich «i» durch «1» und «und» durch «&» ersetzen: «Ms1a&pm3MdZ».

2.6 Passwort regelmässig ändern

– Ändern Sie Passwörter regelmässig. Sie werden vom System in der Regel nach 120 Tage aufgefordert, Ihr Passwort zu ändern.

– Ändern Sie das Passwort sofort, wenn Sie vermuten, dass es Dritten bekannt sein könnte, bspw. weil Sie bei der Eingabe beobachtet wurden.

– Bei Verdacht auf Missbrauch ist ein Passwort ebenfalls sofort zu ändern. Melden Sie solche Vorfälle dem AIO-Service-Desk bzw. Ihrem IT-Dienstleister sowie Ihrer vorgesetzten Stelle.

2.7 Administratoren-Passwörter

– Administratoren-Passwörter zu Systemen erfordern eine erhöhte Risikobehandlung und sind daher mit besonderer Sorgfalt zu behandeln. Sie erfüllen die gleichen Anforderungen wie Standard-Passwörter (siehe Ziff. 2.3), weisen aber eine minimale Länge von 12 Zeichen auf.

– Verwenden Sie verschiedene Passwörter für unterschiedliche Systemzugänge (wie PC, Server, Datenbanken etc.). Die Gültigkeit wird zeitlich nicht beschränkt. Wechseln Sie jedoch nach jedem System-Upgrade oder Datenbank-Releasewechsel innerhalb 120 Tagen die Passwörter.

– Legen Sie System-, Datenbank- und sonstige Administratoren-Passwörter an einem sicheren Ort (siehe Ziff. 2.8) ab. Speichern Sie sie keinesfalls in der Konsole und notieren Sie sie ebenso nicht in Systembeschreibungen oder Ähnlichem. Übermitteln Sie Administratoren-Passwörter nur verschlüsselt. In einem Notfallszenario muss der Zugriff auf die sicher gespeicherten Administratoren-Passwörter gewährleistet sein.

2.8 Passwort-Verwaltungsprogramme

– Wenn Sie viele Passwörter nutzen, können Sie diese mittels eines Passwort-Managers[5] verwalten. Allerdings bestehen auch beim Einsatz solcher Programme Risiken. Sie müssen deshalb verschiedene Sicherheitsanforderungen beachten: U.a. ist ein gutes Master-Passwort oder eine zusätzliche Authentisierungsmethode zu wählen. Setzen Sie möglichst nur vom AIO bzw. von Ihrem IT-Dienstleister zur Verfügung gestellte oder empfohlene Programme ein.

[5] Empfehlung siehe iZug https://izug.zg.ch/web/behoerden/finanzdirektion/amt-fuer-informatik-und-organisation/it-nutzungsregeln

3. Merkblatt «E-Mail»

Die unverschlüsselte E-Mail-Kommunikation über das Internet ist nicht sicher. Durch E-Mails und E-Mail-Anhänge können elektronische Schädlinge wie Viren etc. eingeschleppt werden, welche die Sicherheit der IT-Infrastruktur und der Daten bedrohen.

3.1 Vorsicht beim Versand

– Ein Klick und Ihre Nachricht ist – i.d.R. unwiderruflich – weg bzw. beim Empfänger! Vor dem Versand ist daher jeweils Sorgfalt geboten.

– Verhindern Sie eine Amtsgeheimnisverletzung: Eine häufige Fehlerquelle liegt darin, dass das E-Mail-Programm (bspw. Outlook) Ihnen beim Eintippen der Adresse gleich Empfänger vorschlägt. Überprüfen Sie deshalb, insbesondere auch und gerade in hektischen Situationen, ob Sie den richtigen Empfänger eingegeben haben.

– Falls es mehrere Empfänger sind, prüfen Sie, ob tatsächlich alle Informationen (auch alle allfälligen Anhänge) an alle diese Personen zu senden sind.

– Wenn Sie Personendaten oder vertrauliche Informationen per E-Mail übermitteln, müssen Sie stets bedenken, dass allenfalls das Sekretariat oder die Stellvertretung des Adressaten über eine Zugriffsberechtigung verfügt.

– Falls Drittpersonen keine Kenntnis der Informationen erhalten dürfen, müssen Sie

a) mit dem Adressaten vorgängig Rücksprache nehmen;
b) die Nachricht mit einem Passwort geschützt versenden oder
c) einen anderen Kommunikationsweg wählen – etwa Briefpost mit dem Vermerk «Persönlich/Vertraulich».

3.2 Interner Versand

– Das Versenden von E-Mails innerhalb des Netzwerks des Kantons (umfasst auch die Gemeinden, nicht aber die kantonalen oder gemeindlichen Schulen), gilt grundsätzlich als sicher. Ist der Empfänger ebenfalls am verwaltungseigenen Netz angeschlossen, dürfen Sie grundsätzlich auch besonders schützenswerte Personendaten unverschlüsselt übermitteln. In diesen Fällen erfolgt die Zustellung intern, d.h. ohne dass das eigene Netz verlassen wird. Dies gilt namentlich für folgende E-Mail-Adressen:

a) E-Mail-Adressen, die auf «@zg.ch» enden.
b) E-Mail-Adressen, die auf «@gemeindename.ch» enden (bspw. @baar.ch, @oberaegeri.ch).
c) E-Mail-Adressen der Stadt Zug: «@stadt-zug.ch».
d) E-Mail-Adressen der Gemeinde Risch: «@rischrotkreuz.ch».

– Beispiele: In folgenden Fällen dürfen Sie Daten somit unverschlüsselt übermitteln: peter.muster@zg.ch an max.beispiel@zg.ch oder max.beispiel@zg.ch an peter.muster@huenenberg.ch.

– Nicht sicher ist der Versand hingegen etwa hier: peter.muster@zg.ch an max.beispiel@schulen-huenenberg.ch oder an peter.muster@zug.ch (Grund: Diese Adresse endet nicht auf «@gemeindename.ch» und ist daher nur per Internet erreichbar).

3.3 Externer Versand

– Kommunizieren Sie im Rahmen Ihrer geschäftlichen Tätigkeit zurückhaltend über E-Mail. Der E-Mail-Versand ausserhalb des verwaltungseigenen Netzes ist nicht sicher und gilt als weniger vertraulich als der Versand einer Postkarte.

– Unproblematisch ist ein Versand per E-Mail dort, wo es um öffentlich bekannte Informationen geht, etwa die Bekanntgabe von Öffnungszeiten oder der Hinweis auf Gesetzesbestimmungen.

– Ansonsten dürfen Sie als Mitarbeitende/r der Verwaltung keine Personendaten und vertrauliche oder einer besonderen Geheimhaltungspflicht, z.B. dem Amtsgeheimnis, unterstehende Informationen unverschlüsselt per E-Mail über das Internet verschicken. Solche E-Mail-Kommunikation via Internet ist nur verschlüsselt zulässig (die verfügbaren Möglichkeiten sind in Ziff. 3.4 beschrieben).

– Fordern Sie demzufolge Bürgerinnen und Bürger nicht auf, Ihnen persönliche Informationen oder Unterlagen per E-Mail über das Internet zuzustellen.

3.4 Verschlüsselung

– Um die Informationssicherheit zu gewährleisten, können E-Mails verschlüsselt werden.

a) *SecureMail*: Sämtliche Mitarbeitende der kantonalen Verwaltung, der Gerichte und der Gemeinden haben die Möglichkeit, via SecureMail mit externen Dritten Daten bis 15 MB verschlüsselt per E-Mail auszutauschen. SecureMail ist direkt in Ihrem Mailprogramm (Outlook) integriert. Damit der Empfänger die verschlüsselte Nachricht lesen kann, wird ihm per SMS ein von SecureMail generiertes Passwort übermittelt. Falls die Empfängerin bzw. der Empfänger auch

über SecureMail verfügt, ist kein Passwort nötig. Die Übermittlung der Nachricht erfolgt in diesem Fall automatisch verschlüsselt. Eine Schulung in Form eines E-Learning steht Ihnen auf der Webseite https://elearning.zg.ch zur Verfügung. Eine Kurzanleitung zum sicheren E-Mail-Service des Kantons Zug finden Sie unter https://securemail.zg.ch.

b) *Webtransfer*: Grosse Dateien bis 10 GB können nicht via E-Mail versendet werden. Verwenden Sie hierzu die kantonseigene Plattform «Webtransfer für den sicheren Datenaustausch». Eine Hilfestellung dazu finden Sie unter https://webtransfer.zg.ch.

c) *iZug Arbeitsraum*: Dateien bis 500 MB können via kantonseigener Plattform iZug Arbeitsraum intern wie auch extern sicher ausgetauscht werden. Eine Hilfestellung dazu finden Sie unter https://extranet.zg.ch/.

d) E-Mail-Anhänge *mit Passwort* schützen: Sie haben auch die Möglichkeit, Office-Dokumente, PDF oder Verzeichnisse mittels Passwort zu verschlüsseln und diese als E-Mail-Anhang mitzuschicken (siehe Ziff 1.11). Bitte beachten Sie: Verschlüsselte Dokumente können aus Virenschutzgründen nicht als Mailbeilage von extern empfangen werden.

– Verwenden Sie aus Sicherheitsgründen bei allen Varianten, falls möglich, ein längeres und komplexeres Passwort, als die Minimalanforderungen gemäss Ziff. 2.3 es verlangen. Teilen Sie dem Adressaten das Passwort nicht auf dem gleichen Kanal mit, wie Sie die Datei übermittelt haben.

– Wenn es sich um ein Dokument mit vertraulichem Inhalt handelt und Sie sicher sein wollen, dass nur der berechtigte Adressat Kenntnis vom Inhalt erhält, ist der verschlüsselte Versand über SecureMail oder Webtransfer (geschützt mit sicherem Passwort), der Versand per Briefpost oder die persönliche Übergabe zu wählen.

3.5 Ablage

– Geschäftsrelevante E-Mails bzw. deren Anhänge müssen in der elektronischen Geschäftsverwaltung oder in Absprache mit dem Staatsarchiv gespeichert werden.

– Löschen Sie nicht mehr benötigte E-Mails und leeren Sie den Outlook-Ordner «Gelöschte Objekte».

– Synchronisieren Sie Outlook nicht mit externen Kalendern (z.B. Google oder Office 365).

3.6 Abwesenheiten und Weiterleitung

– Bei längeren Abwesenheiten ist die automatische Abwesenheitsmeldung im E-Mail-System zu aktivieren und Ihre Stellvertretung anzugeben.

– Sollen Ihr Outlook-Kalender, Posteingang oder Teile Ihres Posteingangs bei Abwesenheit durch Ihre Stellvertretung geführt werden, darf dies nur nach vorgängiger Absprache zwischen Ihnen und Ihrer Stellvertretung und über die Outlook-Freigabefunktionen auf genau bezeichnete Ordner (Kalender, Posteingang) geschehen.

– Bei unerwarteten Abwesenheiten oder falls jemand trotz länger dauernder Abwesenheit (z.B. wegen Krankheit, Entlassung etc.) keine Abwesenheitsmeldung eingerichtet hat, kann die vorgesetzte Stelle veranlassen, dass der AIO-Service-Desk bzw. der IT-Dienstleister auf dem entsprechenden E-Mail-Konto eine solche einrichtet.

– Eingehende E-Mails dürfen nicht automatisch an eine externe oder interne E-Mail-Adresse weitergeleitet werden. Davon ausgenommen ist die Weiterleitung einer gemeindlichen oder kantonalen Schuladresse (@ksz.ch, @ksmenzingen.ch, @gibz.ch, @kbz-zug.ch, @fms-zg.ch, @aba-zug.ch etc.) an die eigene gemeindliche oder kantonale E-Mailadresse.

3.7 Virenprävention

– Misstrauen Sie suspekten E-Mails, die Sie u.a. daran erkennen können, dass

a) der Absender unbekannt oder zweifelhaft ist;
b) der Betreff Ungereimtheiten aufweist wie «I love you» oder «Herzlichen Glückwunsch – Sie haben gewonnen» etc.;
c) die Anrede und/oder Signatur fragwürdig erscheint, oder
d) Sie zu einer kritischen Tätigkeit aufgefordert werden, wie z.B. sich mit dem Passwort an einem System anzumelden.

– Öffnen Sie entsprechend keine Anhänge und klicken Sie keine angegebenen Links an. Im Zweifelsfall ist beim angegebenen Absender telefonisch nachzufragen. Löschen Sie solche E-Mails ungeöffnet und entfernen Sie sie sogleich aus dem elektronischen Papierkorb.

3.8 Private Nutzung

– Eine zeitlich geringfügige private Nutzung des kantonalen oder gemeindlichen E-Mailkontos ist erlaubt. Sie darf weder die Arbeitsleistung noch die technische IT-Infrastruktur beeinträchtigen.

– Private E-Mails sind nach Empfang zu löschen oder in einem mit «Privat» bezeichneten Ordner getrennt von den geschäftlichen E-Mails abzulegen.

– Die Vertraulichkeit und der Schutz (allenfalls vorhandener) privater Daten sind nicht gewährleistet. Siehe dazu «Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis» (BGS 154.28).

3.9 WEB-Mail

– WEB-Mail erlaubt ab einem externen Gerät Zugriff auf das eigene E-Mail-Konto via Internet. Die Anwendung verschlüsselt den Datenverkehr.

– Für die sichere Nutzung von WEB-Mail dürfen Sie keine Dateien/Mail-Anhänge mit Personendaten und vertraulichen Informationen lokal auf dem externen Gerät abspeichern. Zudem müssen Sie wissen, dass, wenn Sie E-Mail-Anhänge öffnen, immer eine lokale Kopie des Dokuments gespeichert wird. Deshalb sind die folgenden Schritte bei Beendung von WEB-Mail zwingend einzuhalten:

a) Löschen von Browser-Datenspuren: Nachdem Sie sich beim WEB-Mail abgemeldet haben, müssen Sie die durch die Anwendung automatisch temporär gespeicherten Dokumente und Informationen löschen. Je nach Browser, den Sie im Einsatz haben, unterscheidet sich das Leeren des Cache.[6]
b) Browser schliessen: Schliessen Sie unbedingt den Browser nach dem Abmelden und dem Löschen der temporären Daten. Ansonsten besteht die Gefahr des Identitätsdiebstahls.
c) Löschen temporärer Dateien: Schliessen Sie alle Programme. Drücken Sie Windows+R oder klicken Sie auf «Start» und auf «Ausführen». Geben Sie im Feld «%TMP%» ein und klicken Sie dann auf «OK». Den im Anschluss daran angezeigten Ordnerinhalt können Sie ohne Bedenken löschen. Die gelöschten Daten werden dann, wie üblich, in den Papierkorb verschoben. Vergessen Sie nicht, diesen auch zu leeren.

[6] Für eine Übersicht siehe: https://www.cyon.ch/support/a/browser-cache-leeren.

4. Merkblatt «Internet»

Im Gegensatz zum Intranet ist das Internet ein offenes, weltweit zugängliches Netzwerk. Deshalb ist darauf zu achten, dass Daten nicht einsehbar sind. Wer im Internet surft, hinterlässt Datenspuren auf dem Arbeitsgerät und auf den Servern. Beim Surfen im Internet lauern zudem Gefahren wie Viren etc., die Einfluss auf die Sicherheit Ihrer Daten und Ihres PCs/Notebooks/Tablets haben können.

4.1 Allgemeines

– Geben Sie keine Personendaten und vertrauliche Informationen unverschlüsselt per E-Mail über das Internet weiter. Die Übertragung innerhalb des kantonalen Netzwerks gilt grundsätzlich als sicher (siehe dazu «Merkblatt «E-Mail»»).

– Aus Sicherheitsgründen dürfen Sie mobile Geräte nicht gleichzeitig an das interne Netzwerk des Kantons anschliessen und mit einem externen Netz (z.B. WLAN Kantonsschule Zug) verbinden. So stellen Sie sicher, dass unkontrollierbare und ungesicherte Zugriffe auf die kantonale IT-Infrastruktur ausgeschlossen sind.

– Das Herunterladen, Installieren und/oder Starten von ausführbaren Dateien (z.B. exe, com, msi, cab, bat, pif, vbs, scr etc.) aus dem Internet ist untersagt. Diese können elektronische Schädlinge wie Viren etc. enthalten, welche die Sicherheit der IT-Infrastruktur und der Daten gefährden.

4.2 Datenspuren beim Surfen

– Wenn Sie surfen, hinterlassen Sie Datenspuren auf dem Arbeitsgerät und auf den Servern.

a) Cookies: Das sind kleine Textdateien, die Ihnen Dritte ohne Ihr Zutun auf Ihrem Gerät abspeichern. Sie enthalten meist Angaben zu Ihrer Internetnutzung und können vom Zusteller genutzt werden.
b) Im Zwischenspeicher, dem sog. Cache, werden auf Ihrem Gerät alle Webseiten, die Sie besucht haben, und weitere Daten abgespeichert.
c) Der Verlauf, die sogenannte History, speichert in einer Liste alle Webseite, die Sie besucht haben. Der Verlauf Ihres Surf-Verhaltens kann somit nachvollzogen werden.
d) Die Funktion Auto-Vervollständigen speichert frühere Eingaben zu besuchten Webseiten und schlägt diese vor, wenn die gleichen Angaben neu eingegeben werden.

– Löschen Sie Cookies, Cache, Verlauf und Auto-Vervollständigen des Browsers regelmässig (siehe Ziff. 3.9).

– Speichern Sie keine Passwörter im Browser, ausser Sie schützen sie mit einem Masterpasswort.

– Protokollierungen enthalten Informationen über alle Aktivitäten, die Sie auf Ihrem Gerät ausgeführt haben. Diese sind auf den beteiligten Servern gespeichert und enthalten unter anderem etwa die (IP-)Adresse Ihres Geräts, den Zeitpunkt, die besuchten Webseiten etc. Die Protokollierungen können Sie nicht löschen.

4.3 Private Nutzung

– Eine zeitlich geringfügige private Nutzung des Internets ist erlaubt. Sie darf weder die Arbeitsleistung noch die technische Infrastruktur beeinträchtigten.

– Verboten ist insbesondere

a) der Abruf von kostenpflichtigen Webseiten sowie von Webseiten mit erotischem, rassistischem oder gewalttätigem Inhalt sowie allgemein solchen, die gegen geltende Gesetze verstossen;
b) das Tätigen von privaten Geschäften;
c) das Durchführen von Spielen und Finanztransaktionen (Telebanking);
d) das Herunterladen von ausführbaren Dateien sowie von Audio- oder Videodateien aus dem Internet;
e) die Nutzung von interaktiven Medien, Chatrooms und dergleichen.[7]

– Betreffend die Datenspuren, die Sie aus privaten Internetaktivitäten hinterlassen, gelten die allgemeinen Bestimmungen betreffend Auswertung von Protokollierungen gemäss Ziff. 1.13.

4.4 Virenprävention

– Zunehmend ergeben sich Gefahren durch Schadprogramme, die in Webseiten versteckt eingebaut sind. Besuchen Sie daher nur vertrauenswürdige Webseiten und seien Sie zurückhaltend und vorsichtig, bevor Sie etwas anklicken.

– Mit Administratoren-Rechten (erweiterte Standardrechte) dürfen Sie aus Sicherheitsgründen nicht auf das Internet zugreifen.

[7] § 9 Verordnung über die Benutzung von elektronischen Geräten und Kommunikationsmitteln im Arbeitsverhältnis; BGS 154.28.

– Eine Webseite ist möglicherweise nicht vertrauenswürdig, wenn

a) Sie von einer unbekannten Person einen Link per E-Mail erhalten haben;
b) Sie einen gekürzten Link erhalten haben (z.B. http://bit.ly/kY6fN0); solche sollten Sie nicht anklicken, da Sie nicht sehen, wohin der Link führt (unter https://checkshorturl.com können Sie jedoch den gekürzten Link wieder in seiner vollständigen Länge sehen);
c) die Seite fragwürdige oder illegale Inhalte enthält;
d) die Seite Angebote enthält, die zu gut sind, um wahr zu sein;
e) Sie durch Lockvogeltaktik auf die Webseite geleitet werden und die tatsächlich angebotene Information nicht dem entspricht, was Sie eigentlich erwartet haben;
f) Sie zwecks Identifizierung Ihre Kreditkartennummer oder andere persönliche Daten angeben müssen.

4.5 Sichere Verbindung

– Überprüfen Sie bei jeder Verbindung im Voraus, ob der Browser das Symbol für eine gesicherte Verbindung (Schloss grün  oder Sperrschloss grau/schwarz ) anzeigt.

– Achten Sie ebenfalls darauf, dass die Abkürzung «https» am Anfang der Webseitenadresse steht. Das «s» steht für eine Datenverschlüsselung, d.h. dass die Daten nach einem anerkannten Verfahren verschlüsselt übertragen werden und somit vor dem Zugriff Unbefugter geschützt sind. Ist dies nicht der Fall, dürfen Sie keine Personendaten und vertrauliche Informationen auf diesem Wege übermitteln. Beachten Sie zudem, dass lediglich die Datenübermittlung verschlüsselt ist. Der Datenempfänger bzw. der Webseitenbetreiber hat auch in diesem Fall Einsicht in die unverschlüsselten Daten.

5. Merkblatt «Mobile Geräte und Datenträger»

Mobile Geräte sind Notebooks/Netbooks, Tablets, Mobile-/Smartphones und mobile Speichermedien und -träger (USB-Sticks, externe Festplatten, CD-ROM, DVD, etc.), auf denen Daten verarbeitet oder abgespeichert werden können.

Bei mobilen Geräten und Datenträgern sind zusätzliche Sicherheitsbestimmungen und Verhaltensregeln zu beachten, da eine erhöhte Gefahr von Verlust oder Diebstahl besteht und mobile Geräte es ermöglichen, überall und jederzeit zu arbeiten.

5.1 Verhalten in der Öffentlichkeit

– Wenn Sie in der Öffentlichkeit mit mobilen Geräten arbeiten, verhindern Sie, dass Unberechtigte/Dritte

a) auf den Bildschirm Ihres Geräts sehen;
b) Zugang zu Ihrem Gerät erhalten;
c) Kenntnis Ihres Passwortes erlangen;
d) Ihre Unterhaltungen oder Telefongespräche mithören können.

– Es sind geeignete Massnahmen zu treffen:

a) Verwendung eines Privacy-Filters für das Notebook;
b) Aktivieren der Bildschirmsperre;
c) Ihr Verhalten ist anzupassen (Rückruf bei Telefonanruf).

– Halten Sie die Vorgaben auch ein, wenn Sie zu Hause geschäftliche Daten bearbeiten.

5.2 Verschlüsselung von Datenträgern

– Auf den vom AIO bereitgestellten Notebooks werden die Daten verschlüsselt. Bei allen anderen mobilen Geräten und Datenträgern ist die Vertraulichkeit ebenfalls durch angemessene Massnahmen umzusetzen, etwa durch das Aktivieren der Verschlüsselung, das Setzen eines starken Passworts, die Einschränkung des Zugangs etc. Speichern Sie keine Personendaten und keine vertraulichen Informationen unverschlüsselt auf mobilen Geräten und Datenträgern.

– Speichern oder bearbeiten Sie Personendaten und vertrauliche Informationen nur auf USB-Sticks mit eingebauter Verschlüsselungssoftware. Erkundigen Sie sich hierzu beim AIO Service Desk bzw. Ihrem IT-Dienstleister.

– Von mobilen Geräten und Datenträgern dürfen Sie Personendaten und vertrauliche Informationen nicht auf externe private Geräte abspeichern.

5.3 Passwortschutz

– Schützen Sie mobile Geräte mit einem starken Passwort. Bei Smartphones ist eine mindestens 4-stellige PIN zu aktivieren (siehe dazu Merkblatt «Passwort»).

– Stellen Sie den Passwortschutz so ein, dass er spätestens nach 5 Minuten mit der Bildschirmsperre automatisch einsetzt.[8]

– Aktivieren Sie bei Nichtgebrauch konsequent die (Bildschirm-)Sperre.

5.4 Netzwerknutzung

– Arbeiten Sie, wenn immer möglich, über das kantonale Netzwerk. Falls dies nicht möglich ist, verwenden Sie den persönlichen Hotspot Ihres Mobiltelefons anstatt unbekannte offene WLAN‘s.

– Verbinden Sie mobile Geräte nicht gleichzeitig mit dem internen Netzwerk des Kantons und mit einem externen Netz (z.B. WLAN Kantonsschule Zug).

– Schalten Sie vorhandene Funktechnologien (WLAN, Bluetooth, Infrarot, GSM etc.) aus, wenn Sie nicht mit dem mobilen Gerät arbeiten.

– Vermeiden Sie die Nutzung von öffentlichen «Hotspots» bzw. WLAN’s.

5.5 Backup der Daten

– Stellen Sie regelmässig die Synchronisation der Daten mit dem Verwaltungsnetzwerk sicher und speichern Sie Ihre Daten auf den vorgesehenen Laufwerken.

– Wenn dies nicht möglich ist bzw. Sie lange offline gearbeitet haben, sollten Sie die generierten Daten auf ein verschlüsseltes Speichermedium sichern.

– Muss die Harddisk Ihres Geräts ersetzt oder formatiert werden, so sind lokal gespeicherte Daten verloren. Für die Datensicherung von lokal abgelegten Daten sind die Nutzer selbst verantwortlich.

[8] Bei Notebooks oder Tablets nach 10 Minuten.

5.6 Virenprävention

– Schalten Sie den Virenschutz und die automatische Aktualisierung des Virenschutzes auf keinen Fall aus.

– Verbinden Sie mobile Geräte mindestens einmal pro Woche mit dem Internet, damit der Virenschutz aktualisiert wird.

– Melden Sie sich mit Ihrem Notebook/Netbook mindestens einmal monatlich im Verwaltungsnetzwerk an, damit die Programme (Updates) automatisch aktualisiert werden können.

– Überprüfen Sie mobile Datenträger vor Gebrauch stets mit dem Virenscanner.

– Starten Sie keine ausführbaren Dateien (z.B. exe, com, msi, cab, bat, pif, vbs, scr etc.) ab mobilen Datenträgern.

5.7 Verlust/Diebstahl

– Tragen Sie mobile Geräte und Datenträger bei Reisen im Handgepäck mit.

– Beaufsichtigen Sie diese stets bzw. bewahren Sie sie sicher auf.

– Machen Sie nicht unnötig auf die Geräte aufmerksam (z.B. durch Liegenlassen auf dem Rücksitz des Autos).

– Bei Verlust oder Diebstahl Ihres mobilen Geräts oder Datenträgers informieren Sie umgehend den AIO-Service-Desk (041 728 51 11) bzw. Ihren IT-Dienstleister.

– Haben Sie Ihren Badge verloren, so lassen Sie diesen umgehend bei der zuständigen Stelle sperren.[9]

– Falls Ihr Mobiltelefon gestohlen wurde oder verloren gegangen ist, sperren Sie unverzüglich die Rufnummer über die Hotline des jeweiligen Telekom-Providers.

5.8 Fernzugriff

– Der Zugriff ab Ihrem geschäftlichen Laptop via Internet auf das Verwaltungsnetzwerk erfolgt automatisch verschlüsselt. Sie dürfen nur die Ihnen vom AIO bzw. von Ihrem IT-Dienstleister zur Verfügung gestellte Hard- bzw. Software, z.B. Zwei-Faktor-Authentisierung, einsetzen. Dadurch entspricht der Zugang auf geschäftliche Fachanwendungen demjenigen an Ihrem Arbeitsplatz im Büro.

– WEB-Mail und andere Zugangsmöglichkeiten über den Internet-Browser erlauben Ihnen den Zugang auf Anwendungen via Dritt- bzw. private Geräte (siehe dazu Ziff. 3.9). Auch hier dürfen Sie nur die Ihnen vom AIO bzw. von Ihrem IT-Dienstleister zur Verfügung gestellten Lösungen einsetzen.

– Installieren Sie bei der Nutzung von Drittgeräten ein Virenschutzprogramm und halten Sie es aktuell.

[9] Beim Kanton ist die zuständige Stelle das Hochbauamt (Tel. 041 728 54 00) bzw. ausserhalb der Geschäftszeiten Bouygues (041 724 65 50)