Merkblätter Informationssicherheit

Das Wichtigste in Kürze

Kanton Zug

Security Board

Kanton Zug

Merkblätter Informationssicherheit
Ausgabe 2024_2

Liebe Mitarbeiterin, lieber Mitarbeiter

Bearbeiten Sie Personendaten und vertrauliche Informationen, sind Sie in Ihrem Bereich für die Einhaltung von Datenschutz und Informationssicherheit verantwortlich.

Das Security Board des Kantons Zug hat unter anderem den gesetzlichen Auftrag, Merkblätter zur Informationssicherheit für die Instruktion der Mitarbeitenden der kantonalen Verwaltung, der Einwohnergemeinden, der Gerichte und der kantonalen Schulen zur Verfügung zu stellen. Vorliegend handelt es sich um einen Auszug aus den Merkblättern.

Die ausführlichen Merkblätter finden Sie unter https://zg.ch/de/finanzdirektion/amt-fuer-informatik-und-organisation/it-sicherheit#Informationssicherheit und das E-Learning «Schulung Informationssicherheit» unter https://elearning.zg.ch.

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

Security Board des Kantons Zug

1. Sicherer Umgang mit Daten

Geschäftliche 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 sind erhöhte Sicherheitsmassnahmen erforderlich.

- ✓ Verhindern Sie, dass Unberechtigte Zugang zu geschäftlichen Informationen erhalten. Erlauben oder ermöglichen Sie Dritten nicht, Ihr persönliches Arbeitsgerät zu nutzen.

- ✓ Arbeiten Sie mit einem persönlichen Benutzerkonto und geben Sie unter keinen Umständen Benutzername, Passwort oder sonstige Authentisierungshilfsmittel an Drittpersonen weiter.

- ✓ Verwenden Sie ausschliesslich Arbeitsgeräte und Programme, die durch das Amt für Informatik und Organisation (AIO) oder Ihren IT-Dienstleister zur Verfügung gestellt oder autorisiert wurden. Der Einsatz von privaten Geräten für geschäftliche Zwecke muss durch das AIO bzw. Ihren IT-Dienstleister explizit erlaubt werden.

- ✓ Aktivieren Sie beim Verlassen Ihres Arbeitsplatzes bzw. -geräts konsequent die Bildschirmsperre, indem Sie beispielsweise gleichzeitig «Windows-Taste» und «L» drücken.

- ✓ Bewahren Sie vertrauliche Informationen und besonders schützenswerte Personendaten auch bei kurzen Abwesenheiten während der Arbeitszeit unter Verschluss auf.

- ✓ Speichern Sie geschäftliche Informationen an dem vom AIO oder Ihrem IT-Dienstleister zur Verfügung gestellten Netzwerk-Speicherort.

2. 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.

- ✓ Wählen Sie ein Passwort mit mindestens zwölf Zeichen, das drei der folgenden Kriterien enthält: Grossbuchstaben (A … Z), Kleinbuchstaben (a … z), Zahlen (0 … 9) und Sonderzeichen (! ? + -_ % &).

- ✓ Vermeiden Sie einfach zu erratende Bestandteile (Name, Vorname, Telefonnummer, Geburtsdatum), einfache (3333) oder aufeinanderfolgende (1234, 4567) Zahlenreihen oder alphabetisch angeordnete Gross- bzw. Kleinbuchstaben (ABCD, bcde).

- ✓ Tipp: Bilden Sie das Passwort aus den Anfangsbuchstaben eines Satzes, den Sie sich einfach merken können: z. B. «**W**ir **f**ahren **2 M**al **i**m **J**ahr **n**ach **Z**ermatt **i**n **d**ie **F**erien**!**» – ergibt das starke Passwort «Wf2MiJnZidF!».

- ✓ Ändern Sie Ihre Passwörter regelmässig (spätestens nach 120 Tagen) bzw. sofort bei Verdacht auf Missbrauch oder Kenntnisnahme durch Drittpersonen (bspw., weil Sie bei der Eingabe beobachtet wurden).

- ✓ Benutzen Sie im privaten Bereich andere Passwörter als am Arbeitsplatz.

- ✓ Verwenden Sie möglichst verschiedene Passwörter für unterschiedliche Anwendungen.

- ✓ Verwalten Sie Ihre Passwörter mit einem sicheren Passwort-Manager, zum Beispiel «KeePass» oder «SecureSafe».

3. E-Mail

E-Mail-Kommunikation über das Internet ohne Verschlüsselung ist nicht sicher. Auch können durch E-Mails und E-Mail-Anhänge elektronische Schädlinge wie Viren oder Schadsoftware eingeschleppt werden, welche die Sicherheit der IT-Infrastruktur und der Daten bedrohen.

- ✓ Versenden Sie E-Mails innerhalb des Netzwerks des Kantons (umfasst auch die Gemeinden, nicht aber die kantonalen oder gemeindlichen Schulen), ist dies grundsätzlich sicher.

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

- ✓ Geben Sie per E-Mail über das Internet keine Personendaten und vertraulichen Informationen unverschlüsselt weiter.

- ✓ Für eine sichere E-Mail-Kommunikation resp. für den sicheren Datenaustausch mit Stellen ausserhalb des Netzwerks des Kantons und mit Externen stehen Ihnen die folgenden Möglichkeiten zur Verfügung:
  – SecureMail https://securemail.zg.ch
  – Webtransfer https://webtransfer.zg.ch
  – iZug-Arbeitsraum https://extranet.zg.ch
  – oder Schutz des Dokuments mit Passwort

- ✓ Speichern Sie geschäftsrelevante E-Mails bzw. deren Anhänge in der elektronischen Geschäftsverwaltung oder der entsprechenden Projektablage.

- ✓ Leiten Sie eingehende E-Mails nicht automatisiert oder per Regel gesteuert an eine externe oder interne E-Mail-Adresse weiter.

- ✓ Bei mehrtägigen Abwesenheiten nutzen Sie die Funktion des Abwesenheitsassistenten, um über Ihre Abwesenheit und Ihre Stellvertretung zu informieren.

- ✓ Seien Sie vorsichtig bei E-Mails mit unbekanntem Absender, mit zweifelhaftem Absender/Betreff oder mit fragwürdiger Anrede/Signatur. Löschen Sie solche E-Mails resp. melden Sie diese über die Funktion «Verdächtige E-Mail» in Ihrem Outlook.

4. Internet

Im Gegensatz zum Intranet ist das Internet ein offenes, weltweit zugängliches Netzwerk. Deshalb ist darauf zu achten, dass Informationen nicht einsehbar sind. Wer im Internet surft, hinterlässt Datenspuren auf dem Arbeitsgerät und auf den Servern.

- ✓ Achten Sie bei jeder Verbindung darauf, dass der Browser das Symbol für eine verschlüsselte/gesicherte Verbindung anzeigt (Schloss grün  oder Sperrschloss grau/schwarz ).

- ✓ Löschen Sie Cookies, Cache, Verlauf und Auto-Vervollständigen des Browsers regelmässig.

- ✓ Beachten Sie die Nutzungsbeschränkungen; laden Sie u. a. keine ausführbaren Dateien aus dem Internet herunter. Diese können elektronische Schädlinge wie Viren etc. enthalten, welche die Sicherheit der IT-Infrastruktur und der Daten gefährden.

- ✓ Besuchen Sie nur vertrauenswürdige Webseiten und seien Sie beim Anklicken von Links zurückhaltend und vorsichtig.

- ✓ Verwenden Sie die geschäftliche E-Mail-Adresse niemals für private Registrierungen wie z. B. LinkedIn, Post, Zalando usw.

5. Mobile Geräte und Datenträger

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.

- ✓ Lassen Sie Ihr mobiles Gerät in öffentlich zugänglichen Räumen nie unbeaufsichtigt.
- ✓ Schützen Sie Ihr mobiles Gerät mit einem starken Passwort oder einer PIN. Stellen Sie den Passwortschutz so ein, dass er spätestens nach 5 Minuten mit der Bildschirmsperre automatisch einsetzt.
- ✓ Verhindern Sie, dass Unberechtigte Einsicht auf den Bildschirm Ihres Geräts nehmen können oder Kenntnis Ihres Passworts erhalten.
- ✓ Verbinden Sie mobile Geräte nicht gleichzeitig mit dem internen Netzwerk des Kantons und mit einem externen Netz (z. B. WLAN Kantonsschule Zug).
- ✓ Speichern Sie auf mobilen Geräten keine Personendaten und keine vertraulichen Informationen unverschlüsselt ab.
- ✓ Arbeiten Sie, wenn immer möglich, über das kantonale Netzwerk. Falls dies nicht möglich ist, verwenden Sie den persönlichen Hotspot Ihres Mobiltelefons anstatt unbekannte offene WLANs.
- ✓ Schalten Sie vorhandene Funktechnologien (WLAN, Bluetooth etc.) aus, wenn Sie nicht mit dem mobilen Gerät arbeiten.
- ✓ Prüfen Sie mobile Datenträger wie USB-Sticks, CD-ROM, DVD vor Gebrauch stets mit dem Virenscanner.

Informationen/Kontakte

Für Fragen zum Datenschutz und zur Informationssicherheit von Personendaten
Wenden Sie sich an die Datenschutzstelle des Kantons Zug:
www.datenschutz-zug.ch, datenschutz.zug@zg.ch

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

Meldungen von Sicherheitsvorfällen
Stellen Sie mutmasslich sicherheitsrelevante Vorkommnisse fest, informieren Sie per Telefon umgehend den AIO-Service-Desk (+41 41 594 51 11) bzw. Ihren IT-Dienstleister.

Bei Verlust oder Diebstahl Ihres mobilen Geräts informieren Sie umgehend den AIO-Service-Desk (+41 41 594 51 11) bzw. Ihren IT-Dienstleister. Haben Sie Ihren Badge verloren, so lassen Sie diesen umgehend bei der zuständigen Stelle (für die kantonale Verwaltung: Hochbauamt, Abt. Betrieb, Verwaltungsgebäude an der Aa 5, helpdesk.hba@zg.ch oder Tel. 041 594 54 00) sperren. Ausserhalb der Bürozeiten (vor 8.00 Uhr / nach 17.00 Uhr) hilft Ihnen unser Servicepartner unter +41 58 800 41 41 weiter.

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