INFORMATIONSSICHERHEIT IN DER KANT. VERWALTUNG

[1] In jeder Dienststelle gibt es neben dem Informatik-Verantwortlichen (IV) einen Informatik-Sicherheitsverantwortlichen (ISV). Der ISV ist Ihre Ansprechperson für alle Sicherheitsbelange.

[2] Auf der Intranetseite http://informatiksicherheit.gr.ch finden Sie alle Informationen und Weisungen zur Informatik-Sicherheit.

[3] Melden Sie Mängel, Sicherheitslücken, Viren-Vorkommen oder Sicherheitsvorfälle sofort dem ISV ihrer Dienststelle.

[4] Der Informatik-Sicherheitsbeauftragte (ISB) Tel. 3164, E-Mail isb@afi.gr.ch ist für die Informatik- und Informationssicherheit in der kantonalen Verwaltung zuständig.

SICHERER UMGANG MIT E-MAIL

[1] E-Mails werden standardmässig nicht verschlüsselt und können von Dritten gelesen werden.

[2] E-Mail Absender können einfach gefälscht werden.

[3] Öffnen Sie Anhänge und folgen Sie Links in E-Mails nur, wenn Sie die Absender und den Inhalt als vertrauenswürdig einstufen.

[4] Eingehende E-Mails dürfen nicht automatisch an einen privaten E-Mail Account weitergeleitet werden.

[5] Nutzen Sie die für Ihre Dienststelle verfügbaren technischen Möglichkeiten (z. B. IncaMail) für die sichere Übermittlung von vertraulichen Informationen an Adressaten ausserhalb der kantonalen Verwaltung.

STARKE PASSWÖRTER

[1] Ein starkes Passwort ist folgendermassen aufgebaut:

- Besteht aus mindestens 8 Zeichen.
- Enthält Klein- und Gross-Buchstaben, Zahlen und Sonderzeichen.
- Enthält keine leicht zu erratende Wörter oder Zahlen, wie z.B. Namen, Auto-Kennzeichen oder Begriffe aus einem Wörterbuch.
- Können Sie sich gut merken, andere aber nur schwer erraten, z. B. Son**nENsch00ein, fRan?zis57ka.

[2] Verwenden Sie nie dasselbe Passwort für verschiedene Anwendungen oder Internet-Dienstleistungen.

SICHER SURFEN IM INTERNET

[1] Verändern Sie die Sicherheitseinstellungen Ihres Internet-Browsers am Arbeitsplatz nicht.

[2] Laden Sie keine Dateien und Programme aus dem Internet herunter, deren Ursprung sie nicht kennen oder als nicht vertrauenswürdig einstufen.

[3] Programminstallationen dürfen nur durch die dafür verantwortlichen Mitarbeiter (in der Regel der Informatik-Verantwortliche) freigegeben werden.

[4] Schon der Besuch einer verseuchten Webseite kann Ihren Arbeitsplatz infizieren, besuchen Sie keine Webseiten denen Sie nicht vertrauen.

[5] Beachten Sie Warnungen des Browsers, und besuchen Sie keine Seiten, bei welcher der Browser vor einem ungültigen Zertifikat warnt.

[6] Lesen Sie Meldungen, Nachrichten und Aufforderungen auf Internetseiten genau und vertrauen Sie ihnen nicht blind.

DATENSCHUTZ

[1] Der Datenschutz dient dem Schutz der Persönlichkeitsrechte und der Privatsphäre.

[2] Öffentliche Organe dürfen Personendaten nur aufgrund einer rechtlichen Grundlage, nur für den angegebenen Zweck und nur soweit erforderlich bearbeiten.

[3] Vor der Eröffnung von neuen Datensammlungen ist eine datenschutzrechtliche Beurteilung vorzunehmen.

[4] Informieren Sie sich über den Datenschutz (Abschnitt Datenschutz in der Awareness-Broschüre), falls Sie in Ihrer Dienststelle Personendaten bearbeiten.

[5] Besonders schützenswerte Personendaten (gemäss Datenschutzgesetz) dürfen nur innerhalb der Schweiz gespeichert werden. Dies ist besonders bei Cloud-Dienstleister zu beachten.

INFORMATIONSSICHERHEIT AM ARBEITSPLATZ

[1] Bei Abwesenheit während der Arbeitszeit:

- Computer sperren (z.B. Windows-Taste+L) sowie, abhängig von Abwesenheitsdauer und weiteren Sicherheitsmassnahmen (z. B. Gebäude- / Raum-Zutrittskontrollen) zusätzlich:
  - Keine vertraulichen Daten (Papiere, Dossiers, Datenträger) offen herumliegen lassen.
  - Bürotür abschliessen, Fenster schliessen

[2] Am Feierabend und bei mehrtägigen Abwesenheiten zusätzlich:

- Dokumente und Datenträger mit vertraulichen Inhalten sowie mobile Geräte wegräumen und allenfalls einschliessen.
- Computer ausschalten

Ein Merkblatt des Amtes für Informatik. Hintergrundinformationen im Intranet unter informatiksicherheit.gr.ch

UMGANG MIT **SOCIAL MEDIA**

[1] Aussagen im Namen des Arbeitgebers sind nicht zulässig.

[2] Für die private Nutzung darf in keinem Fall die geschäftliche E-Mail-Adresse oder das Kantonslogo verwendet werden.

[3] Veröffentlichen Sie in sozialen Netzwerken so wenig Informationen über Ihre berufliche Tätigkeit wie möglich.

[4] Bedenken Sie: Social Media sind noch öffentlicher als ein Bus oder ein Stammtisch. Für publizierte Inhalte sind Sie verantwortlich und Sie können dafür auch rechtlich belangt werden.

SOCIAL ENGINEERING

[1] Social Engineering ist eine Methode, um durch Täuschung unberechtigten Zugang zu Informationen zu erlangen.

[2] Zur Ausbreitung von Schadsoftware werden oft Methoden des Social Engineering angewandt, etwa wenn der Name des E-Mail Anhangs mit einem Virus einen besonders interessanten Inhalt verspricht, oder der Absender angeblich aus der kantonalen Verwaltung stammt.

[3] Der Informatik-Dienstleister fordert sie nie auf vertrauliche Informationen wie ein Passwort per E-Mail oder am Telefon bekannt zu geben.

[4] Lassen Sie sich nicht ausfragen, einschüchtern oder bedrohen und geben Sie keine vertraulichen oder sicherheitsrelevanten Informationen an Unbekannte weiter.

MOBIL UNTERWEGS

[1] Jeder Laptop, der ausserhalb der Büroräumlichkeiten eingesetzt wird, muss mit einem Festplatten-Verschlüsselungsprogramm ausgestattet sein, sofern der Schutzbedarf dies erfordert.

[2] Alle Laptops müssen für die Aktualisierung des Virenschutzes und für Sicherheitsupdates regelmässig ans kantonale Netz angeschlossen werden.

[3] Wer unterwegs mit mobilen Geräten arbeitet muss beachten, dass Unbeteiligte auf den Bildschirm des Laptops oder Tablets sehen und die Gespräche auf dem Mobiltelefon mithören können.

[4] Der Verlust mobiler Geräte muss sofort dem ISV Ihrer Dienststelle gemeldet werden.

SPEICHERN UND LÖSCHEN VON **DATEN**

[1] Speichern Sie Daten nur auf offiziellen Laufwerken und Fachapplikationen Ihrer Dienststelle.

[2] Löschen Sie Daten unwiederbringlich, bevor Sie ein Gerät oder einen Datenträger weitergeben. Mit einem einfachen «löschen» vernichten Sie Daten nicht definitiv. Die zuständigen Informatikmitarbeiter (in der Regel der Informatik-Sicherheitsverantwortliche) können Sie unterstützen.

[3] Stellen Sie beim Drucken von klassifizierten Informationen auf gemeinsam genutzten Geräten sicher, dass Dritte keinen Zugang zu den gedruckten Dokumenten haben.

[4] Schützenswerte Informationen auf Papier müssen im Aktenvernichter zerstört werden.

INFORMATIK-SICHERHEIT **PRIVAT**

[1] Daten- und System-Backup einrichten.

[2] Antivirus Software installieren.

[3] Software regelmässig aktualisieren (Besonders Betriebssystem, Browser, Java, PDF Reader).

[4] Personal Firewall aktivieren (Windows Firewall bietet "nur" Grundschutz).

[5] Starke Passwörter wählen und diese nur einmalig verwenden.

[6] Vertrauliche Daten auf externen Datenträgern oder Cloud-Storage-Diensten verschlüsseln.

Ein Merkblatt des Amtes für Informatik. Hintergrundinformationen im Intranet unter informatiksicherheit.gr.ch