Amt für Informatik des Kantons Graubünden
Uffizi d'informatica dal chantun Grischun
Ufficio d'informatica del cantone dei Grigioni

7001 Chur, Rosenweg 4 Tel. +41 81 257 3170 Fax +41 81 257 2167 www.afi.gr.ch
info@afi.gr.ch

Nutzung von Informations- und Kommunikationstechnologien

Titel	Nutzung von Informations- und Kommunikationstechnologien
Typ	Weisung
Dokument Nr.	AFI-1110
Thema	Informatik-Sicherheit
Version	2.0.1 (Anpassung Verweise auf geltende Weisungen, keine inhaltlichen Anpassungen)
Status	Beschlossen
Beschlossen am	17.08.2020
Gestützt auf	IKT-Verordnung, IKTV (BR 170.500), Art. 4, Abs. 2
Beschlossen durch	AFI
In Kraft ab	17.08.2020
Ersetzt	Version 1.0 vom 24.03.2014
Inhaltliche Verantwortung	Informatik-Steuerung
Verteiler	Via ISV der Dienststellen an alle Mitarbeitenden
Publikationsort	Verwaltungsverordnungen Verwaltung und AFI-Intranet
Klassifizierung	-

Inhalt

Abkürzungsverzeichnis

Begriff/Abkürzung	Bedeutung
AFI	Amt für Informatik (afi.intranet.gr.ch)
InfV	Informatik-Verordnung (Verfügbar unter www.gr-lex.gr.ch)
ISB	Informatik-Sicherheitsbeauftragter
ISV	Informatik-Sicherheitsverantwortlicher
IV	Informatik-Verantwortlicher
MDM	Mobile-Device-Management (Zentrale Verwaltung mobiler Geräte)
PV	Personalverordnung (Verfügbar unter www.gr-lex.gr.ch)

1. Zweck

Ein entscheidender Faktor zur Gewährleistung der Informationssicherheit ist - neben den technischen Sicherheitsmassnahmen - der gewissenhafte Umgang mit Informations- und Kommunikationstechnologien in der täglichen Arbeit durch alle Mitarbeitenden. Die Mitarbeitenden sind im Rahmen ihres Einsatzbereiches für die Sicherheit der von ihnen bearbeiteten Daten verantwortlich. Diese Weisung enthält Regelungen für den Umgang mit Informations- und Kommunikationstechnologien. Zusätzliche Hinweise und Hintergrundinformationen sind in der Seite https://informatiksicherheit.gr.ch auf dem Intranet des Amtes für Informatik (AFI), Bereich Sicherheit, zu finden.

2. Geltungsbereich

Gemäss Art. 2 IKT-Verordnung (IKTV).

3. Begriffe

Schützenswerte Daten sind Daten, deren Kenntnisnahme oder Veränderung durch Unberechtigte den Interessen der Dienststelle oder des Kantons einen Schaden zufügen kann. Der Dateneigner in der Dienststelle bestimmt den Schutzbedarf der Daten, siehe auch Weisung "Organisation der Informatik", AFI-1186.

4. Interne Ansprechpersonen

In jeder Dienststelle gibt es einen Informatik-Verantwortlichen (IV) und einen Informatik-Sicherheitsverantwortlichen (ISV). Der ISV ist die Ansprechperson für alle Sicherheitsbelange, der IV für alle allgemeinen Fragen zur Informatik sowie zur Beschaffung von Informatik-Mitteln.

5. Nutzung des Arbeitsplatzes

Es darf nur die vom Arbeitgeber bewilligte Infrastruktur eingesetzt werden. Sicherheitseinstellungen am Arbeitsplatz, besonders am Internet-Browser, dürfen nicht verändert werden.

Die Weitergabe von persönlichen Benutzerkennungen (insbesondere dem Passwort) ist nicht zulässig. Falls Passwörter notiert oder gespeichert werden müssen, sind sie vor unberechtigtem Zugriff zu schützen. Das AFI empfiehlt die Speicherung von Passwörtern im Passwortsafe, welcher auf allen Arbeitsplätzen installiert ist.

Der Zugang zu Geräten und Dokumenten ist durch die Mitarbeitenden zu schützen. Dies beinhaltet insbesondere das Schliessen von Fenstern, Abschliessen von Türen und Einschliessen von mobilen Geräten. An unbeaufsichtigten Arbeitsplätzen dürfen keine *schützenswerten* Informationen frei zugreifbar sein. *Schützenswerte* Dokumente dürfen nicht unbeaufsichtigt liegen gelassen werden, zu beachten auch bei gemeinsam genutzten Drucker. Nicht mehr benötigte *schützenswerte* Dokumente müssen vernichtet werden.

Der Arbeitsplatz muss beim Verlassen gesperrt werden (z.B. Windows-Taste+L). Um die Installation von Sicherheits-Updates zu gewährleisten, ist der PC jeden Abend herunterzufahren.

6. Private Nutzung

Die Arbeitszeit ist für die Erfüllung der dienstlichen Aufgaben zu verwenden (Personalverordnung Art. 58). Dienstliche Einrichtungen dürfen für private Angelegenheiten nur in notwendigen Fällen benützt werden (PV Art. 59). Die private Nutzung des Internets über die Infrastruktur des Kantons

ausserhalb der Arbeitszeit ist im Rahmen der Weisungen und Einschränkungen des Amtes für Informatik sowie unter Berücksichtigung der personalrechtlichen Vorgaben möglich.

7. Umgang mit Daten

Es dürfen grundsätzlich keine *schützenswerten* Daten ausserhalb der offiziellen Datei-Ablagen und Fachanwendungen der Dienststelle gespeichert werden. Der Datenaustausch von *schützenswerten* Daten mit Externen darf nur mit vom AFI zur Verfügung gestellten, oder von der Dienststelle bewilligten Verfahren erfolgen. Standard E-Mail, unverschlüsselte mobile Datenträger (z.B. USB-Stick) oder externe Cloud-Lösungen bieten in der Regel keinen angemessenen Schutz für den Austausch von *schützenswerten* Daten.

Nicht mehr benötigte Daten müssen gelöscht werden, sofern sie nicht archiviert werden müssen. Nicht mehr gebrauchte Geräte oder Datenträger müssen via ISV dem AFI zur sicheren Entsorgung übergeben werden.

8. Nutzung mobiler Geräte (Notebooks, Convertibles, Smartphones und Tablets)

Es dürfen nur von der Dienststelle zur Verfügung gestellte mobile Geräte verwendet werden, ausgenommen davon sind vom AFI zentral verwaltete private Smartphones. Die Geräte sind persönlich und dürfen nicht an Dritte zur Benutzung oder Aufbewahrung weitergegeben werden. Sie dürfen nicht unbeaufsichtigt liegen gelassen werden.

8.1 Notebooks und Convertibles

Jedes Notebook und Convertible muss gemäss der Weisung "Sicherheit von Windows-Systemen" konfiguriert sein, insbesondere bezüglich der Festplattenverschlüsselung (siehe auch Anleitung "Bitlocker für mobile Windows-Clients"). Alle Notebooks müssen für die Aktualisierung des Virenschutzes und der Software regelmässig (mindestens einmal monatlich) ans kantonale Netz angeschlossen werden.

Notebooks und Convertibles ohne VPN-Client ("Client-to-Site VPN mit Zertifikat") dürfen nur mit vertrauenswürdigen Netzwerken verbunden werden. Unbekannte Internet-Zugänge ausserhalb des kantonalen Netzwerkes, wie z.B. unbekannte öffentliche Drahtlos-Netzwerke (WLAN) gelten als nicht vertrauenswürdig.

8.2 Smartphones und Tablets

Smartphones oder Tablets, mit denen Daten der kantonalen Verwaltung synchronisiert werden, sind in die zentrale Geräte-Verwaltung des AFI oder der KAPO (Mobile-Device-Management) integriert. Die unterstützten Geräte und Betriebssysteme, sowie die erzwungenen Sicherheits-Einstellungen sind in der "Weisung Sicherheit von Smartphones und Tablets" dokumentiert.

8.2.1 Nutzungs-Richtlinien für alle Geräte

- Zentral definierte Profile und Einstellungen dürfen nicht verändert werden.
- Die Geräte müssen, wenn immer möglich, zeitnah vom Benutzer auf das jeweils aktuellste unterstütze Betriebssystem aktualisiert werden.
- Die Synchronisation erfolgt ausschliesslich drahtlos. Die lokale Synchronisation via Kabel mit dem Arbeitsplatz ist untersagt.
- Das Umgehen von Sicherheitsmassnahmen (z.B. "Rooting" oder "Jailbreak") ist nicht erlaubt.

- Bei Verlust des Gerätes wird dieses vom AFI zurückgesetzt, geschäftlich synchronisierte Daten werden gelöscht. Auf Wunsch der Mitarbeitenden können auch private Daten gelöscht werden.
- Es dürfen nur vertrauenswürdige Apps von offiziellen App-Stores installiert werden, welche die Sicherheit der Daten auf dem Gerät nicht beeinträchtigen.
- Es muss von den Mitarbeitenden sichergestellt werden, dass *schützenswerte* Daten nicht auf Online-Dienste (z.B. private E-Mail-Accounts oder Cloud-Storage-Anbieter wie Dropbox), anderen Computern oder Datenträgern übertragen werden.

8.2.2 Nutzungs-Richtlinien für Geräte, die vom Arbeitgeber zur Verfügung gestellt werden

- Das Smartphone darf bei entsprechender Kostenbeteiligung im Rahmen der Einsatzstrategie für Smartphones privat genutzt werden. Die private Nutzung darf auf keinen Fall die geschäftliche Nutzung tangieren und muss verantwortungsvoll erfolgen. Im Zweifel ist die private Nutzung zu unterlassen.
- Die unterstützten Geräte werden im Servicekatalog AFI Kanton Graubünden (AFI-1193) publiziert.

9. Nutzung des Internets

Das Herunterladen und Ausführen von Programmen aus dem Internet ist, ohne vorherige Prüfung und Freigabe durch den IV, untersagt.

Die Nutzung von Internetseiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist untersagt. Ausgenommen sind Mitarbeitende, welche diese Seiten im Rahmen ihres Auftrages aufrufen müssen.

Aus Gründen der Sicherheit ist der Zugriff auf bestimmte Webseiten gesperrt.

10. Nutzung von E-Mail und Kalender

Für die Übertragung von schützenswerten Daten an externe Empfänger mittels E-Mail steht der Dienst "IncaMail" zur Verfügung. Über den grundsätzlichen Einsatz entscheidet die Dienststelle, über den Einsatz im konkreten Fall entscheidet der Sender.

Es dürfen keine *schützenswerten* Informationen in Kalendereinträgen (inkl. angehängten Dokumenten) gespeichert werden.

Das Amt für Informatik prüft eingehende E-Mails auf Spam und Viren. Virenverseuchte E-Mails werden direkt gelöscht, der Umgang mit Spam ist im Dokument "Anleitung zur Filterung von Spam-Mails" beschrieben. Diese technischen Massnahmen schützen jedoch nicht vor weitergehenden Angriffen, wie z.B. "Phishing-Attacken" (weitere Informationen dazu in der Awareness-Broschüre).

Die automatische Weiterleitung von E-Mails oder Kalender-Einträgen an einen privaten E-Mail-Account oder Kalender ist nicht gestattet. Bei Abwesenheit muss eine automatische Antwort eingerichtet werden. Für Mitarbeitende, die E-Mails auf ein mobiles Gerät synchronisieren wird empfohlen, bei längeren Abwesenheiten das Passwort *vorgängig* neu zu setzen um sicherzustellen, dass das Passwort während der Abwesenheit nicht abläuft.

11. Nutzung von externen Online-Meeting-Systemen

Es dürfen grundsätzlich keine *schützenswerten* Daten oder vertrauliche Gespräche über externe Online-Meeting-Systeme (z.B. Zoom) ausgetauscht werden. Auf Anfrage prüft das AFI externe Online-Meeting-Systeme bezüglich Datenschutz und Datensicherheit und publiziert eine Liste der zugelassenen Systeme.

12. Homeoffice und mobiles Arbeiten

Im Homeoffice und beim mobilen Arbeiten gelten dieselben Sicherheitsbestimmungen wie am Büro-Arbeitsplatz. Insbesondere sind die Bestimmungen aus Kapitel 5 zum Schutz des Zuganges zu Dokumenten und Geräten zu beachten. Das Mithören von vertraulichen Telefongesprächen muss durch die Mitarbeitenden verhindert werden.

Geschäftliche Geräte dürfen nicht von Dritten, einschliesslich Familienmitgliedern, genutzt werden.

Bei der Nutzung von Citrix SSL VPN (https://asp.gr.ch) können private Geräte eingesetzt werden. Die Massnahmen zum Schutz von privaten Geräten gemäss Awareness-Broschüre sind zu beachten. *Schützenswerte* Daten dürfen nicht auf privaten Geräten gespeichert werden.

13. Aufzeichnungen und Auswertungen

Zur Aufrechterhaltung des Betriebes, Gewährleistung der Dienstleistungsqualität und Informationssicherheit, sowie zur Ermittlung und Behebung von Betriebsstörungen werden Logfiles aufgezeichnet. Insbesondere werden sämtliche aufgerufene Internet-Seiten protokolliert.

Nicht personenbezogene Auswertungen der Aufzeichnungen können zur Sicherstellung der Qualität der Dienstleistungen, zum Erstellen von Statistiken oder zur stichprobeweisen Überprüfung der Einhaltung von Weisungen erstellt werden.

Personenbezogene Auswertungen der Aufzeichnungen können in folgenden Fällen durchgeführt werden:

a. Sofern dies erforderlich ist, damit die Ursache einer Störung ermittelt werden kann;
b. Aufgrund der Anordnung einer dazu befugten Behörde oder Instanz;
c. Falls die Analyse einer durchgeführten nicht personenbezogenen Auswertung eine offensichtlich nicht dienstlich begründbare Kostensteigerung aufzeigt, kann eine personenbezogene Auswertung erfolgen. Damit kann die Kosten verursachende Person oder Fehlersituation ermittelt werden.

14. Melden von sicherheitsrelevanten Ereignissen, Risiken oder Verlusten

Alle sicherheitsrelevanten Ereignisse (z.B. Vorkommen von Viren, erkannte Risiken oder Fehlkonfigurationen, Verdacht auf Missbrauch) sowie Verlust oder Diebstahl von Geräten (z.B. Smartphones) oder Datenträgern sind sofort dem ISV der Dienststelle zu melden. Der ISV wendet sich nach eigener Einschätzung an den Informatik-Sicherheitsbeauftragen (ISB) der kantonalen Verwaltung.

15. Verzeichnis der Informatik-Weisungen

Auf dem Intranet des Amtes für Informatik (https://afi.intranet.gr.ch) sind alle Informatik-Weisungen verfügbar.