Muster Informatikweisung

Das vorliegende Dokument umfasst alle üblichen Sicherheitsaspekte die Benutzende von Informatik- und Kommunikationsmitteln zu beachten und umzusetzen haben. Treffen Massnahmen nicht auf die Gegebenheiten ihrer Organisation zu, sind diese entsprechend anzupassen, zu ergänzen oder zu löschen.

Die grau hinterlegten Texte weisen auf allgemeine oder beispielhafte Bezeichnungen hin. Diese Texte sind zwingend auf die richtigen bzw. vorliegenden Bezeichnungen zu ändern.

Die orange hinterlegten Texte weisen auf speziell zu beachtende Eigenschaften hin. Nach entsprechender Berücksichtigung sind diese Texte zu löschen.

Umgang mit Informatik- und Kommunikationsmitteln –
Weisung für Benutzende

1 Allgemeine Bestimmungen

Zweck

Diese Weisung regelt das Verhalten im Umgang mit Informatik- und Kommunikationsmitteln der Organisation/Firma. Die Vorgaben dienen dem sicheren sowie wirtschaftlichen Einsatz der Mittel, dem Schutz der damit verwalteten Informationsbestände, sowie dem Persönlichkeitsschutz der Benutzenden und Betroffenen.

Geltungsbereich

Die Weisung ist für alle Mitarbeitenden der Organisation/Firma und Dritte, die Informatik- und Kommunikationsmittel der Organisation/Firma einsetzen, verbindlich. Sie gilt folglich auch für alle externen informatikrelevanten Vertragspartner der Organisation/Firma, welche permanente oder temporäre ICT Dienstleistungen für Organisation/Firma durchführen.

Die Weisung sollte von allen Personen zum Zeitpunkt des Eintritts in Organisation/Firma unterzeichnet werden, sowie bei der Veröffentlichung einer neuen Version. Die unterzeichneten Dokumente werden im Personaldossier abgelegt.

Verantwortlichkeiten

Die Organisation/Firma definiert eine Person, welche für die Informationssicherheit verantwortlich ist. Diese ist für das Umsetzen der vorliegenden Weisung verantwortlich und ist die Ansprechstelle für Fragen sowie für sicherheitsrelevante Vorfälle. Sie ist befugt, das Einhalten dieser Weisung zu überprüfen, den Benutzenden Weisungen bezüglich Informationssicherheit zu erteilen und Sanktionen zuhanden der jeweils vorgesetzten Stellen oder dem Personalmanagement vorzuschlagen.

Ausnahmen

Ausnahmen von der vorliegenden Weisung und die allfälligen kompensierenden Massnahmen/Auflagen müssen durch die für Informationssicherheit verantwortliche Person abgenommen und schriftlich dokumentiert werden. Entsprechende Gesuche sind schriftlich und mit Begründung einzureichen. Über bewilligte Ausnahmen und Auflagen wird Buch geführt, eine Kontrolle durch das Management der Organisation/Firma findet jährlich statt.

2 Grundsätze zur Nutzung der Informatikmittel

Eigenverantwortung

Wer Informatik- sowie Kommunikationsmittel verwendet, ist für den recht- und zweckmässigen Einsatz dieser Mittel verantwortlich. Diese Verantwortlichkeit umfasst zudem den Schutz der Personen- und Kundendaten (Datenschutz) sowie der System- und Organisationsdaten.

Es dürfen ausschliesslich die persönlichen und die allenfalls zugewiesenen funktionellen Benutzerkonten (Gruppenkonten) verwendet werden. Die Benutzenden sind selbst verantwortlich für alle unter eigenem Benutzernamen getätigten Zugriffe auf Daten und/oder Informatik- sowie Kommunikationsmittel. Es dürfen keine Zugangsdaten mit anderen Mitarbeitenden der Organisation/Firma oder Dritten geteilt werden.

Social Media

Es ist zu beachten, dass immer mehr Phishingkampagnen via Social Media Netzwerken durchgeführt werden. Somit ist Vorsicht geboten bei allen Nachrichten, insbesondere solche die Links und Dateianhänge beinhalten

Die Weitergabe von geschäftsrelevanten Informationen auf Social Media ist untersagt.

Verbotene Aktivitäten

Das Verwenden der Informatik- und Kommunikationsmittel im Zusammenhang mit anstössigen oder illegalen Inhalten ist verboten (Ehrverletzung, Porno, Rassismus, Gewalt usw.).

Ebenso sind das Beantworten, Verbreiten und Weiterleiten von Bittbriefen, Kettenbriefen aller Art, Werbeschreiben, Warnmitteilungen und diskriminierenden Nachrichten untersagt.

Schutz vor Malware / bösartiger Software

Desktop-PCs/Notebooks sind nach Arbeitsschluss vollständig herunterzufahren.

Falls beim Öffnen einer empfangenen Office-Datei ein Hinweis auf Makros erscheint, darf die Schaltfläche „Inhalt aktivieren“ nicht angewählt werden Ausnahmen stellen interne Dokumente dar, welche Makros benötigen. Stellen Sie in einem solchen Fall sicher, dass die Datei von einem internen Absender stammt.

Falls Sicherheitsmeldungen einer Sicherheitssoftware angezeigt werden (z.B. Antivirus, Firewall) soll die Informatik/Helpdesk/Sicherheitsverantwortliche Person kontaktiert werden.

Installation und Wartung

Für die Installation sowie Wartung der Informatik- und Kommunikationsmittel sind ausschliesslich die Mitarbeitenden der Informatik der Organisation/Firma zuständig. Selbständige Änderungen an den Systemeinstellungen sowie das Installieren/Entfernen von Hardware und Software durch die Benutzer sind untersagt.

Informatiksysteme, die am Netzwerk der Organisation/Firma angeschlossen sind, dürfen nicht gleichzeitig mit fremden Netzwerken oder Systemen verbunden sein (z.B. mittels VPN)

Für Reparatur sowie Entsorgung von Informatik- und Kommunikationsmitteln sind ausschliesslich die Mitarbeitenden der Informatik zuständig. Sie stellen sicher, dass keine schützenswerten Daten die Organisation/Firma verlassen.

Private Nutzung

Die Informatik-Infrastruktur der Organisation/Firma ist für den geschäftlichen Gebrauch bzw. die Erfüllung dienstlicher Aufgaben bestimmt. Die Nutzung für private Zwecke wird toleriert, ist aber auf ein Minimum zu beschränken. Sie darf nur erfolgen, wenn die Erfüllung der geschäftlichen Aufgaben nicht beeinträchtigt wird.

Private Geräte dürfen weder mittels Kabel noch drahtlos an die Informatiksysteme und Kommunikationsnetzwerke der Organisation/Firma angeschlossen werden. Davon ausgenommen sind Smartphones und Tablets, die nach einer initialen Bewilligung durch die sicherheitsverantwortliche Person mit dem dafür vorgesehenen Funknetzwerk (Gäste WLAN) verbunden werden.

Wer private oder organisationsfremde Informatikmittel für dienstliche Zwecke einsetzt, ist für wirksame Schutzmechanismen gegen Malware verantwortlich. Insbesondere ist sicherzustellen, dass die Virenschutzlösung aktuell sowie aktiv ist und das Betriebssystem, wie auch die verwendete Anwendung, über die aktuellsten Sicherheitsupdates verfügen. Die Nutzung von privaten Informatikmitteln muss vorgängig von der Sicherheitsverantwortlichen Person autorisiert werden.

Melden von Vorfällen

Wer sicherheitsrelevante Ereignisse feststellt (z.B. Virenbefall, Verlust von Schlüssel, Badge, Chipkarte, USB-Stick, Smartphone, Tablets, Notebook, Zwei-Faktor Tokens usw.) oder wer einen Verdacht bezüglich eines sicherheitskritischen Vorgangs hat (z.B. Nutzung einer Zugangs- oder Zugriffsberechtigungen durch Dritte), meldet dies umgehend der Informationssicherheit verantwortlichen Person. In deren Abwesenheit sind eigene Vorgesetzte zu informieren.

Social Engineering

Benutzende müssen sich den Gefahren des Social Engineering bewusst sein und dürfen sich – weder aus Hilfsbereitschaft noch aus Gutgläubigkeit oder Angst vor Schwierigkeiten – zur unberechtigten Herausgabe vertraulicher Informationen oder zu (unerlaubten) Aktionen verleiten lassen.

Es ist insbesondere Vorsicht geboten, wenn jemand zur Weitergabe von Informationen, der Bekanntgabe von Usernamen/Emailadressen/Passwörtern/Zwei-Faktor Authentisierungs-Codes oder dem Gewähren für einen Zugang zu Büroräumlichkeiten auffordert. Es gelten die nachfolgenden generellen Verhaltensregeln.

- Nie unbekannten Personen Auskünfte über schützenswerte Daten, Geschäftsabläufe oder -informationen erteilen. Bei Zweifeln an einer anfragenden Person kann diese beispielsweise durch Rückruf überprüft werden.
- Keine Fragen ausserhalb des eigenen Zuständigkeitsbereichs beantworten und an zuständige Stellen verweisen (Auskunft, Kommunikationsdienst, Kanzlei, usw.).
- Besuchende sowie unbekannte Personen müssen sich grundsätzlich am Empfang oder an entsprechenden Schalterdiensten melden und haben keinen freien Zutritt zu Büroräumen.
- Nie einer unbekannten Person den Zutritt zu gesicherten Räumlichkeiten ermöglichen. Dabei ist unter anderem auch an vermeintliche Service-Techniker, Überbringer von Paketen, Reinigungsdienste usw. zu denken.
- Besuchende sowie unbekannte Personen sind trotz erlaubter Anwesenheit nie allein in den Büroräumlichkeiten und anderen nicht öffentlich zugänglichen Bereichen (z.B. technischer Infrastruktur) zu belassen.

3 Zugangs- und Zugriffschutz

Physischer Schutz

Zum Vermeiden von Diebstählen und unberechtigten Netzwerkzugängen sind Fenster und Türen beim Verlassen des Arbeitsplatzes soweit möglich zu verriegeln und vorhandene Schliessvorrichtungen zu nutzen.

Ferner ist der Arbeitsplatz so aufzuräumen, dass keine mobilen Datenträger (CDs/DVDs, USB-Sticks usw.) und vertrauliche Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Werden mobile Datenträger und vertrauliche Unterlagen in einem Fahrzeug aufbewahrt, müssen diese von aussen nicht sichtbar eingeschlossen sein.

Computersperre, Bildschirmschutz

Bei Abwesenheiten (Pause, Besprechungen, Arbeitsschluss) ist das unbefugte Verwenden des Computers mittels Bildschirmsperre (Windowstaste+L), dem Abmelden vom System oder dem Herunterfahren des Systems zu verhindern.

Die Bildschirmposition ist so zu wählen, dass unberechtigten Personen keine Einsicht möglich ist. Gegebenenfalls sind Sichtschutzfolien oder spezifische Bildschirm-Modi einzusetzen, welche eine Einsicht erschweren.

Berechtigungsnachweise

Berechtigungsnachweise wie PINs, Passwörter, Zwei-Faktor Backup Codes sowie private Schlüssel der persönlichen Zertifikate sind geheim zu halten. Diese dürfen anderen Personen nicht bekannt beziehungsweise zugänglich gemacht werden – auch nicht für Systemadministratoren.

Passwörter müssen sicher sein und dürfen weder in einem Wörterbuch vorkommen noch in Verbindung zur eigenen Person stehen (z.B. keine Namen, Geburtsdaten, Hobbies, Telefon- und Autonummern).Es sollten Passwörter mit einer Länge von mindestens 12 Zeichen, , Gross- und Kleinbuchstaben, gemischt mit Zahlen und Sonderzeichen verwendet werden.

Zugeteilte Initialpasswörter und bekannt gewordene Passwörter müssen sofort geändert werden. Aktive Passwörter sind regelmässig (alle 365 Tage) zu wechseln. Das neue Passwort darf nicht von dem alten abgeleitet werden. Ein früher bereits benutztes Passwort darf nicht mehr gewählt werden.

Geschäftliche Passwörter sind verschieden von privaten Passwörtern zu wählen. Für unterschiedliche Dienste sind unterschiedliche Passwörter zu wählen.

Passwörter für funktionelle Benutzerkonten (Gruppenkonten) werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert (z.B. Wechsel oder Austritt von Mitarbeitenden).

Zum Verwalten und sicheren Speichern von Passwörtern, sollte der zur Verfügung gestellte Passwortmanager der Organisation/Firma verwendet werden.

Portalzugang, Fernzugriff

Beim Auftreten einer Zertifikatswarnung ist die Verbindung, beispielsweise zum VPN-Dienst, Outlook Web Access (OWA), Microsoft Office 365oder Citrix Gateway, vor Eingabe der Berechtigungsnachweise abzubrechen.

Bei vorhandener Virenmeldung auf einem System, ist es untersagt, sich mit diesem an einem Portalzugang anzumelden beziehungsweise sich über einen Fernzugriff in das Netzwerk der Organisation/Firma einzubinden.

Desktop Sharing Lösungen sind nur temporär einzusetzen. Die Benutzenden von Desktop Sharing Lösungen sind verpflichtet bei Missbrauchsverdacht die Verbindung sofort abzubrechen und den Vorfall zu melden. Die verantwortliche Person für Informationssicherheit bestimmt, welche Desktop Sharing Lösungen zugelassen sind und welche User diese verwenden dürfen.

Beim Verwenden nicht organisationseigener Informatikmittel dürfen die Anmeldeinformationen nicht gespeichert werden (z.B. in Webbrowsern). Spätestens beim Beenden eines Webbrowsers muss dessen lokaler Zwischenspeicher (Cookies & Cache) gelöscht werden. Andernfalls verbleiben möglicherweise Informationen auf der lokalen Festplatte und sind unter Umständen für andere Nutzende zugänglich.

4 Datensicherheit

Grundsätze

Das Erfassen, Speichern, Verarbeiten, Auswerten und Weitergeben personenbezogener Daten hat unter Berücksichtigung des geltenden Datenschutzgesetzes (DSGVO, eidgenössisch, kantonal, kommunal) zu erfolgen.

Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten. Besteht die Möglichkeit einer datenschutzkonformen technischen Lösung, beispielsweise durch das Eingrenzen der Zugriffsrechte, so ist diese umzusetzen. Die Benutzenden melden festgestellte zu weitgehende Berechtigungen unaufgefordert der Person, welche für Informationssicherheit zuständig ist.

Personendaten dürfen nur bekannt gegeben werden, wenn die Betroffenen damit einverstanden sind oder die gesetzlichen Grundlagen dazu vorhanden sind. Die Datenschutzkonformität gilt auch für die Veröffentlichung von Personendaten im Intranet und Internet.

Vertrauliche sowie organisationsinterne Informationen dürfen nie in der Öffentlichkeit bearbeitet oder besprochen werden. Für Diskussionen, Telefongespräche oder Bildschirmarbeiten ist folglich ein ungestörter bzw. abgetrennter Bereich aufzusuchen.

Datenablage

Sämtliche erstellten bzw. empfangenen Daten müssen auf entsprechenden zentralen Laufwerken der Organisation/Firma abgelegt werden. Das Laufwerk X:\ steht ausschliesslich für persönliche Daten zur Verfügung. Lokale Laufwerke (C:\,D:\ etc.) sind nur für Systemdateien, Software sowie temporäre Daten bestimmt und werden grundsätzlich nicht gesichert.

Auf privaten oder organisationsfremden Informatikmitteln dürfen keine besonders schützenswerten Personendaten oder geheime Daten der Organisation/Firma bearbeitet oder gespeichert werden. Dies auch dann nicht, wenn die Datenübermittlung verschlüsselt erfolgt.

Die Benutzenden sind für die korrekte Ablage und Aufbewahrung der von ihnen erstellten sowie empfangenen Daten im Rahmen ihres Aufgabenbereichs selbst verantwortlich. Private Termine und allfällige Einträge mit besonders schützenswerten Personendaten sind zur Wahrung der Vertraulichkeit in Outlook als "Privat" zu kennzeichnen (aktivieren Schlosssymbol).

Wer persönliche Daten der automatischen Archivierung entziehen will, ist verpflichtet, sich über die erforderlichen Massnahmen zu erkundigen.

Drucken und Scannen

Ausdrucke mit vertraulichen Informationen sind sofort aus dem Drucker zu entfernen. Wenn verfügbar, ist die Funktion des Druckens in Anwesenheit zu nutzen (beispielsweise Drucken mittels Eingabe eines PINs oder dem Vorweisen eines Badges).

Originale sind sofort aus dem Kopierer/Scanner zu entfernen. Liegengelassene Dokumente mit vertraulichen Informationen sind umgehend dem Urheber/Besitzer zurückzubringen oder der für Informationssicherheit verantwortlichen Person zu übergeben.

Stellvertretende Zugriffe

Um Zugriffskonflikten bzw. Stellvertretungsproblemen vorzubeugen, sind die Daten generell zentral abzuspeichern (Laufwerke, Sharepoint etc.). Der stellvertretende Zugriff auf anderweitig abgelegte Daten sowie Informationen in Outlook sind mittels Freigaben und Berechtigungen zu gewährleisten, nicht mittels Weitergabe von persönlichen Logins/Passwörtern.

Bei ungeplanten Abwesenheiten (z.B. Krankheit, Unfall)

Berechtigungsnachweise von Benutzenden werden nur zurückgesetzt, um eine Freigabe oder einen Abwesenheitsassistenten einzuschalten, nicht aber um einer stellvertretenden Person das Arbeiten im Namen der abwesenden Person zu ermöglichen.

Der Zugriff auf persönliche Daten ist nur in Ausnahmefällen erlaubt. Es handelt sich dabei um eine in der Regel unvorhergesehene Abwesenheit von längerer oder unbestimmter Dauer und einem dringenden oder wichtigen Auftrag. Die Verantwortung für den Eingriff liegt letztendlich bei der Leitung der ersuchenden Person/Abteilung. Die Nachvollziehbarkeit muss formal sichergestellt sein.

Die Mitarbeitenden der Informatik der Organisation/Firma dürfen keine Freischaltungen ohne schriftliche und fallweise legitimierte Aufforderung durch die Leitung vornehmen. Dies unabhängig von einer allfälligen Vollmacht der abwesenden Person. Die betroffenen Mitarbeitenden müssen in jedem Fall über den Grund, Tätigkeit und die anfragende Person des Datenzugriffs informiert werden.

Datensynchronisation

Die Synchronisation bzw. der Abgleich von Daten der Organisation/Firma mit privaten Informatik- und Kommunikationsmitteln ist untersagt. Eine Ausnahme ist das Verwenden privater Smartphones und Tablets, die einen Datenaustausch über den von der Organisation/Firma definierten und betriebenen zentralen Zugangspunkt ausführen.

Die Informatik der Organisation/Firma behält sich das Recht vor, technische Massnahmen zu erlassen und Konfigurationsrichtlinien/Profil/Sandbox durchzusetzen, um eine angemessene Informationssicherheit zu gewährleisten. Wird dem Durchsetzen der Konfigurationsrichtlinien/Profil/Sandbox nicht zugestimmt, ist der Besitzer des Smartphones oder Tablets verpflichtet die Datensynchronisation mit der Organisation/Firma zu unterlassen beziehungsweise dauerhaft zu löschen.

Cloud Computing

Das Benutzen von Cloud-Diensten wie beispielsweise Microsoft OneDrive, Dropbox oder Google Drive ist nur durch vorgängige Zustimmung der Organisation/Firma erlaubt. Wichtig dabei zu

beachten ist, welche Daten in welcher Form auf welche Cloud-Dienste gespeichert werden dürfen. Eine entsprechende Klassifizierung der Daten bietet hierbei die Grundlage. Nutzende informieren sich bei der sicherheitsverantwortlichen Person, welche Daten auf den Cloud-Diensten abgelegt oder bearbeitet werden dürfen

Falls Cloud Dienste wie zum Beispiel Microsoft M365 eingesetzt werden, dürfen keine Anmeldungen von persönlichen Geräten (Notebook, Smartphone, Tablet etc.) stattfinden. Es dürfen ausschliesslich von geschäftsbezogenen Geräten, Anmeldungen durchgeführt und Dateien heruntergeladen werden.

Sicheres Löschen von Daten

Daten sicher löschen heisst, sie vernichten, ohne dass eine einfache Wiederherstellung durch Dritte möglich ist. Sowohl ausgediente als auch defekte Datenträger (Desktop-PCs, Notebooks, Smartphones, Tablets, Kopierer, Drucker, USB-Sticks, CDs/DVDs, usw.) sind zwecks fachgerechter und sicherer Entsorgung den Mitarbeitenden der Informatik der Organisation/Firma zu übergeben.

Nicht mehr benötigte physische Dokumente mit vertraulichen Informationen sind eigenhändig mittels Aktenvernichter zu entsorgen.

Austretende Behördenmitglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen, die ihnen zugänglich waren und die ausserhalb der Organisation/Firma bearbeitet oder gespeichert wurden, unwiderruflich gelöscht beziehungsweise vernichtet wurden.

5 Schutz in der Datenübermittlung (E-Mail, Internet)

Umgang mit E-Mails

E-Mails mit fragwürdiger Herkunft, verdächtigem Betreff oder unüblichem Inhalt sind sofort und permanent zu löschen. Deren Anhänge und enthaltenen Links dürfen keinesfalls geöffnet werden, auch wenn die E-Mails über bekannte Absender weitergeleitet wurden. Beispiele solcher E-Mails sind Bittbriefe, Werbemails, falsche Virenwarnungen, gefälschte Mitteilungen von Banken, Gewinnversprechen usw. Diese können zu unerwünschten Handlungen verleiten, Schadsoftware beinhalten oder auf mit Schadsoftware verseuchte Internetseiten verweisen.

Benutzende die immer wieder von unerwünschten E-Mails (Spams) belästigt werden, können diese Mails in die so genannte Junk-Mail-Liste ihres Mail-Clients aufnehmen. Sind mehrere Personen von denselben unerwünschten E-Mails betroffen, ist dies der Informatik zur zentralen Sperrung zu melden.

Das Übermitteln grosser Datenmengen mittels E-Mail, wird im KOMSG wie auch bei Dritten begrenzt. Ein Datenaustausch innerhalb der Organisation/Firma hat immer über eine Ablage auf einem gemeinsam zugänglichen Laufwerk und einem entsprechenden Verweis im E-Mail zu erfolgen.

Vertraulichkeit im E-Mail-Verkehr

E-Mails sind auf ihrem Weg zum Bestimmungsort standardmässig nicht vor unberechtigter Einsicht oder vor Fälschung geschützt. Demzufolge dürfen E-Mails mit vertraulichem Inhalt, wie persönlichen Angaben oder anderen zu schützenden Geschäftsinformationen, ausserhalb der Organisation/Firma nur in verschlüsselter Form und lediglich an bekannte oder

vertrauenswürdige E-Mail-Adressen versandt werden. Adressaten ausserhalb der Organisation/Firma und des KOMSG sind mit EXT gekennzeichnet.

Die Empfängeradresse/n ist/sind in jedem Fall vor dem Versand einer E-Mail zu verifizieren. Weil Verteilerlisten und -gruppen wiederum andere Gruppen beinhalten können, sind nur bekannte Verteiler zu verwenden. Es besteht sonst die Möglichkeit, dass eine E-Mail unkontrolliert verbreitet wird.

Entweder folgender Text beibehalten oder Aufzeigen der vorhandenen Verschlüsselungslösung: Aktuell wird keine Lösung angeboten, um die E-Mails zu verschlüsseln. Hingegen kann der vertrauliche Inhalt einer Mitteilung als verschlüsselte E-Mail-Anlage (z.B. zip-Datei) versendet werden.

Das automatische Weiterleiten von E-Mails auf externe Adressen, auch auf die eigene Privatadresse, ist verboten.

Es ist untersagt, das globale Adressbuch zu exportieren und an Dritte weiterzuleiten.

Sicher im Internet

Der Zugriff auf Internetdienste erfolgt ausschliesslich über den standardmässig installierten Webbrowser, dessen Sicherheitseinstellungen nicht verändert werden dürfen.

Schützenswerte Informationen wie Personendaten, Login-Informationen (insb. Passwörter), Kreditkartennummern, usw. dürfen nur verschlüsselt (https) über das Internet übermittelt und einzig auf vertrauenswürdigen Seiten eingetragen werden.

Das Verwenden der E-Mail Adresse zum Abonnieren von Newslettern, Registrieren in Foren, usw. darf nur auf vertrauenswürdigen Seiten und im Rahmen der dienstlichen Aufgabenerfüllung erfolgen.

Informationen, die über das Internet beschafft werden, sind inhaltlich vor dem Gebrauch für dienstliche Zwecke zu verifizieren. Die Verantwortung für die Klärung der inhaltlichen Integrität liegt bei den Benutzenden. In jedem Fall sind Quellenangaben wie Beschaffungsort, Zeitpunkt und Autor zu nennen.

Die in diesem Kapitel erwähnten Schutzmassnahmen gelten sinngemäss für Chat und Unified Communication Tools wie z.B. Microsoft Teams oder Skype.

6 Mobile Geräte und Datenträger

Verlust und Diebstahl

Mobile Geräte und Datenträger wie beispielsweise Notebooks, Tablets, Smartphones, USB-Sticks und CD/DVDs sind bezüglich Verlusts oder Diebstahl besonders gefährdet. Wer mobile Geräte oder Datenträger einsetzt, hat die nachfolgenden Grundsätze zwingend umzusetzen.

- Auf mobilen Geräten und Datenträgern sind nur notwendige Daten zu bearbeiten und speichern. Für die Datensicherung sind die Benutzenden selbst verantwortlich.
- Müssen schützenswerte Daten abgespeichert werden, hat dies jeweils verschlüsselt zu erfolgen. Die Notebooks der Organisation/Firma verfügen standardmässig über verschlüsselte Festplatten. Verschlüsselte USB-Sticks können bei der Informatik bezogen werden.

- Mobile Geräte und Datenträger dürfen bei Gebrauch nie unbeaufsichtigt sein. Ist dies nicht möglich sind diese mit einem Diebstahlschutz zu versehen (z.B. Notebook mit Kensington-Schloss). Bei Nichtgebrauch sind die mobilen Geräte und Datenträger an einem sicheren Ort einzuschliessen.
- Personifizierte Notebooks sowie Tablets und Smartphones dürfen nicht Dritten zur Nutzung überlassen werden.

Notebooks

Drahtlose Komponenten wie WLAN, Bluetooth, NFC usw. sind bei Nichtgebrauch zu deaktivieren. Bei der initialen Verbindung zu einem neuen drahtlosen Netzwerk (WLAN) ist die entsprechend korrekte Zone auszuwählen (Privat, Arbeit, Öffentlich).

Smartphones und Tablets

Vom zentralen Zugangspunkt der Organisation/Firma werden bestimmte Konfigurationen technisch erzwungen. Es gilt zu beachten, dass nur Geräte eingesetzt werden dürfen, auf welche die Konfiguration vollständig angewendet werden kann.

Es sind nur Apps zu installieren, die in einem offiziellen Shop wie dem App Store von Apple, , Google usw. erhältlich sind. Vor dem Herunterladen einer App sind dessen Bewertungen und Datenschutzstatements zu verifizieren.

Viele Geräte bieten die Möglichkeit, Daten in der Cloud zu speichern. Falls auf einem Smartphone oder Tablet ein Datenaustausch (E-Mail, Kalender, usw.) mit der Organisation/Firma erfolgt, ist ein Gebrauch der Cloud untersagt. Nur Ortungsdienste wie „iPhone suchen“ von Apple oder „Lookout“ bei Android-Geräten sind in jedem Fall erlaubt.

Die Datenträger von Smartphones müssen verschlüsselt sein. Dies gilt auch für Speicherkarten, die den internen Speicherplatz erweitern.

Das Modifizieren von Betriebssystemen zum Umgehen herstellerbedingter Sperrfunktionen ist untersagt (in der Fachsprache Jailbreaking oder Rooting genannt). Andernfalls erlischt die Berechtigung zur Datensynchronisation. Ebenfalls können Geräte, welche nicht über ein aktuelles Betriebssystem verfügen, resp. nicht aktuellen Sicherheitsstandards entsprechen, von der Synchronisation ausgeschlossen werden.

Betriebssystem und Apps sind stets auf dem neusten Stand zu halten. Die Benutzenden sind verpflichtet die verfügbaren Aktualisierungen innert zwei Wochen ab Herausgabe durch den Hersteller zu installieren.

Bevor ein Smartphone oder Tablet zur Reparatur gegeben wird, sind nach einer allfällig noch möglichen Datensicherung alle personenbezogenen Daten (z. B. Kontakte, Fotos, SMS und E-Mails, Kontakte, Kalender, usw.) zu löschen und das Gerät auf Standardwerte zurückzusetzen. Ausserdem ist die SIM-Karte zu entfernen.

Bei Verlust eines Smartphones oder Tablets sind die nachfolgenden Massnahmen sofort und in der genannten Reihenfolge auszuführen.

1. Über den Verlust und die getätigten Massnahmen ist die Informatik zu informieren.
2. Sichere Datenlöschung (Wipen) über das MDM (falls möglich)
3. Sperren der SIM-Karte beim Mobilfunkanbieter veranlassen
4. Verwendete Passwörter ändern

7 Missbrauch, Kontrollen und Sanktionen

Konsequenzen

Verstösse gegen diese Weisung stellen Dienstpflichtverletzungen dar und können personalrechtliche Massnahmen und Schadenersatzansprüche zur Folge haben. Bei strafbaren Handlungen wird gegen fehlbare Personen Anzeige erstattet.

Protokollierung

Die Nutzung der Informatik- und Kommunikationsmittel wird zugunsten der technischen Sicherheit (Fehleranalysen, Lastanalysen usw.), dem Klären von Verdachts- oder Streitfällen, dem Sicherstellen der Weisungskonformität sowie zuhanden der Kostenrechnung protokolliert. Es ist zu beachten, dass allfällige private Tätigkeiten ebenfalls protokolliert werden und aus technischen Gründen nicht von der geschäftlichen Nutzung unterschieden werden können.

Anonyme Auswertung der Protokolldaten

Die Protokollierungen werden laufend und anonym durch die Informatik ausgewertet. Dabei geht es um die statistische Analyse der Systembelastungen und Systemnutzungen sowie der Dienstverfügbarkeiten.

Personenbezogene Auswertung der Protokolldaten

Eine personenbezogene Auswertung der Protokolldaten kann in folgenden Fällen erfolgen:

- Wenn auf Grund von anonymen Auswertungen Verstösse gegen die vorliegende Weisung festgestellt werden. In diesem Fall werden sämtliche Benutzende informiert, dass die Auswertung für einen begrenzten Zeitraum personenbezogen erfolgt. Diese Auswertung erfolgt durch die Informatik unter der Leitung der Person, welche für Informationssicherheit verantwortlich ist.
- Wenn ein Missbrauch feststellt oder vermutet wird. In diesem Fall beauftragt die für Informationssicherheit verantwortliche Person die Informatik zur personenbezogenen Auswertung der Protokolldaten. Die betroffene Person muss schriftlich bestätigen, vom Auftrag Kenntnis genommen zu haben.
- Wenn sich ein sicherheitsrelevanter Vorfall ereignet hat (bzw. wenn konkrete Anhaltspunkte für einen bevorstehenden Vorfall vorhanden sind), der auf einem Missbrauch beruht. In diesem Fall darf die Informatik ohne Vorwarnung Verbindungsdaten mit personenbezogenen Daten aufzeichnen. Eine personenbezogene Auswertung der Daten darf jedoch erst nach einem Auftrag durch die für Informationssicherheit verantwortliche Person und der schriftlichen Bestätigung der betroffenen Personen, vom Auftrag Kenntnis genommen zu haben, erfolgen.
- Auf Verlangen des Benutzers selbst oder in Absprache mit ihm, wenn Fehler analysiert und Massnahmen zur Problemlösung entwickelt werden sollen.

8 Schlussbestimmungen

Schriftliche Erklärung

Die Benutzenden bestätigen einmalig pro Version, dass sie diese Weisung erhalten sowie verstanden haben und sie mit den Überwachungs- und Disziplinarmassnahmen vertraut sind. Die Erklärung wird im Personaldossier abgelegt.

Aufhebung bisheriger Bestimmungen

Die vorliegende Weisung ersetzt XXX.

Inkrafttreten

Diese Weisung tritt am Datum in Kraft.

Ort, Datum

Organisation/Firma

Unterzeichnende