STADTRAT

sRS 181.6
Nr. 185

Umgang mit Informatik- und Kommunikationsmitteln – Weisung für Benutzerinnen und Benutzer

vom 4. November 2015

Der Stadtrat erlässt folgende Weisung für den Umgang mit Informatik- und Kommunikationsmitteln:

I. Allgemeine Bestimmungen

Zweck

Art. 1
Dieses Reglement regelt das Verhalten im Umgang mit Informatik- und Kommunikationsmitteln (Data + Voice) der Stadt Wil. Die Vorgaben dienen dem sicheren sowie wirtschaftlichen Einsatz der Mittel, dem Schutz der damit verwalteten Informationsbestände sowie dem Persönlichkeitsschutz der Benutzenden.

Geltungsbereich

Art. 2
Dieses Reglement ist für alle Behördenmitglieder und Mitarbeitenden der Stadt Wil sowie für Personen jener Institutionen, welche sich durch Vertrag an die Informatik-Infrastruktur der Stadt Wil angeschlossen haben, verbindlich. Es gilt auch für alle externen informatikrelevanten Vertragspartner der Stadt Wil. Für die Schulen der Stadt Wil erlässt der Stadtrat eine separate Weisung.

Verantwortlichkeiten

Art. 3
Die Leiterin oder der Leiter der Informatik-Dienste ist Informationssicherheitsverantwortliche oder Sicherheitsverantwortlicher bzw. Informatiksicherheitsbeauftragte oder Informatiksicherheitsbeauftragter. Sie oder er ist für das Umsetzen der vorliegenden Weisung verantwortlich und ist Ansprechstelle für Fragen sowie für sicherheitsrelevante Vorkommnisse. Sie oder er ist befugt, das Einhalten dieser Weisung zu überprüfen und den Benutzenden zusätzliche Weisungen bezüglich Informationssicherheit zu erteilen.

Bei den Technischen Betrieben Wil nimmt die kaufmännische Leiterin oder der kaufmännische Leiter die Aufgaben der oder des Informationssicherheitsverantwortlichen wahr.

STADT WIL

Ausnahmen

Art. 4
Die oder der Informationssicherheitsverantwortliche entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihr oder ihm schriftlich und mit Begründung einzureichen. Über bewilligte Ausnahmen wird ein Register geführt. Die bewilligten Ausnahmen sind jährlich auf ihre Notwendigkeit hin zu überprüfen.

Schriftliche Erklärung

Art. 5
Die Benutzenden bestätigen, dass sie diese Weisung erhalten sowie verstanden haben und mit den folgenden Überwachungs- und Disziplinarmassnahmen vertraut sind. Diese Erklärungen werden bei den Informatik-Diensten in elektronischer Form aufbewahrt.

II. Grundsätze zur Nutzung der Informatikmittel

Eigenverantwortung

Art. 6
Wer Informatik- sowie Kommunikationsmittel verwendet, ist für den recht- und zweckmässigen Einsatz dieser Mittel verantwortlich, insbesondere für den Umgang mit Personen- und Kundendaten.

Es dürfen einzig die zugeteilten funktionellen Konten verwendet werden. Die Benutzenden sind selbst verantwortlich für alle unter eigenem Benutzendennamen getätigten Zugriffe auf elektronische Daten und Informatik- sowie Kommunikationsmittel.

Social Media

Art. 7
Soziale Netzwerke wie beispielsweise Facebook, YouTube, Twitter und XING verändern die Art, wie privat und beruflich kommuniziert wird. Alle Benutzenden sind sich dabei der Gefahren des Informationsabflusses und dem Einhalten der kommunikativen Gepflogenheiten bewusst.

Jede Äusserung, ob beruflich oder privat, ist vor ihrer Veröffentlichung sorgfältig abzuwägen. Die Regeln des Anstands und des respektvollen Verhaltens sind auch in sozialen Medien zu befolgen. Gesetzliche Vorgaben wie beispielsweise Datenschutz, Urheber- und Markenrecht sind einzuhalten, ebenso das Bewahren von Betriebs- und Geschäftsgeheimnissen.

Verbotene Aktivitäten

Art. 8
Das Verwenden der Informatik- und Kommunikationsmittel im Zusammenhang mit sexistischen, rassistischen, gewalttätigen oder illegalen Inhalten ist verboten. Ebenso ist das Beantworten, Verbreiten und Wei-

terleiten von Bittbriefen, Werbeschreiben (Spam-Mails) und diskriminierender Nachrichten untersagt.

Schutz vor Malware

Art. 9
Desktop-PCs/Notebooks sind nach Arbeitsschluss in der Regel vollständig herunterzufahren. Teilweise werden Aktualisierungen erst bei Neustart vollständig übernommen.

Falls beim Öffnen einer von extern elektronisch empfangenen Office-Datei ein Hinweis auf Makros erscheint, ist die Option „Makros deaktivieren" zu wählen.

Externe, mobile Datenträger sind nach dem Beenden der Benutzung – spätestens vor einem Neustart des Computers – zu entfernen.

Installation und Wartung

Art. 10
Für die Installation sowie Wartung der Informatik- und Kommunikationsmittel sind ausschliesslich die Mitarbeitenden der Informatik-Dienste der Stadt Wil bzw. der Technischen Betriebe Wil zuständig. Das Herunterladen und das Installieren von Programmen sowie Programm-Updates sind untersagt. Jegliche Änderungen an den Systemeinstellungen, dazu gehören auch das Installieren und Entfernen von Hardware und Software, ohne Absprache mit den Informatik-Diensten sind untersagt.

Informatiksysteme, die am Netzwerk der Stadt Wil bzw. am Netzwerk der Technischen Betriebe Wil angeschlossen sind, dürfen nicht gleichzeitig mit einem weiteren Netzwerk oder System ausserhalb der Stadt Wil resp. der Technischen Betriebe Wil verbunden sein bzw. müssen mit einer separaten Firewall getrennt sein.

Nur die Mitarbeitenden der Informatik-Dienste resp. der IT der Technischen Betriebe Wil dürfen Informatik- und Kommunikationsmittel in die Reparatur oder zur Entsorgung geben. Sie stellen sicher, dass auf diesem Weg keine schützenswerten Daten die Stadt Wil verlassen.

Private Nutzung

Art. 11
Die Informatik-Infrastruktur der Stadt Wil ist für den geschäftlichen Gebrauch bzw. die Erfüllung dienstlicher Aufgaben bestimmt. Die Nutzung für private Zwecke ist gestattet, aber auf ein Minimum zu beschränken. Sie darf nur erfolgen, wenn die Erfüllung der geschäftlichen Aufgaben nicht beeinträchtigt wird und die Ressourcenbeanspruchung vernachlässigbar ist.

Private Geräte dürfen nicht an die Informatiksysteme und Kommunika-

tionsnetzwerke der Stadt Wil angeschlossen werden sowohl physisch wie kabellos. Davon ausgenommen sind Smartphones und Tablets, die nach einer initialen Bewilligung durch die Informationssicherheitsverantwortliche oder den Informationssicherheitsverantwortlichen mit dem dafür vorgesehenen Funknetzwerk verbunden werden.

Wer nicht organisationseigene Informatikmittel für dienstliche Zwecke – z.B. für Fernzugriff – einsetzt, ist für effektive Schutzmechanismen gegen Malware verantwortlich. Insbesondere wird sichergestellt, dass der Virenschutz aktuell sowie aktiv ist und das Betriebssystem wie auch die verwendete Anwendung über die aktuellsten Sicherheitsupdates verfügt.

Radio- und Fernsehempfang

Art. 12
Der Empfang von Radio- und Fernsehprogrammen in Betrieben unterliegt der gesetzlichen Melde- und Gebührenpflicht. Es ist den Benutzenden der Stadt Wil deshalb untersagt, mit Informatik- und Kommunikationsmitteln Radio- und Fernsehprogramme zu empfangen.

Nimmt eine Person ihr privates Empfangsgerät mit an den Arbeitsplatz und nutzt dieses, so ist dieser Empfang in ihrer Meldung für den privaten Radio- und Fernsehempfang eingeschlossen.

Melden von Vorfällen

Art. 13
Wer sicherheitsrelevante Ereignisse feststellt (z.B. Virenbefall, Verlust von Schlüssel, Badge, Chipkarte, USB-Stick, Smartphone, Notebook usw.) oder ein Verdacht bezüglich eines sicherheitskritischen Vorgangs besteht (z.B. Nutzung einer Zugangs- oder Zugriffsberechtigungen durch Dritte), meldet dies umgehend der oder dem Informationssicherheitsverantwortlichen. In deren oder dessen Abwesenheit ist die oder der eigene Vorgesetzte zu informieren.

Social Engineering

Art. 14
Benutzende müssen sich den Gefahren des Social Engineering (= zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Informationen oder technische Infrastrukturen zu gelangen) bewusst sein und dürfen sich – weder aus Hilfsbereitschaft noch aus Leichtgläubigkeit 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 Passwörtern oder dem Gewähren für einen Zugang zu Büroräumlichkeiten auffordert. Die nachfolgenden generellen Verhaltensregeln sind stets anzuwenden.

- Nie unbekannten Personen Auskünfte über schützenswerte Daten, Geschäftsabläufe oder -informationen gewähren. Bei Zweifeln an einer anfragenden Person kann diese beispielsweise durch Rückruf überprüft werden.
- Keine Fragen ausserhalb des eigenen Zuständigkeitsbereichs beantworten, sondern an zuständige Stellen verweisen (Informatik-Diente, Fachstelle Kommunikation, Stadtkanzlei, Geschäftsleitung 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, Überbringende von Paketen usw. zu denken.

Besuchende sowie unbekannte Personen sind trotz erlaubter Anwesenheit nie alleine in den Büroräumlichkeiten und anderen nicht öffentlich zugänglichen Bereichen (z.B. technischer Infrastruktur) zurückzulassen.

III. Zugangs- und Zugriffschutz

Physischer Schutz

Art. 15
Zur Vermeidung von Diebstählen und von 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.

Sind ergänzend zur Zugriffsberechtigung physische Medien wie Smart-Card, SuisseID etc. im Einsatz, sind diese beim Herunterfahren des Systems aus der Leseeinheit zu entfernen und nicht sichtbar aufzubewahren.

Computersperre, Bildschirmschutz

Art. 16
Bei Abwesenheiten (Pause, Besprechungen, Arbeitsschluss etc.) ist das unbefugte Verwenden des Computers mittels des Aktivierens der Bildschirmsperre (Windows+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 einzusetzen.

Berechtigungsnachweise

Art. 17

Berechtigungsnachweise wie PINs, Passwörter sowie private Schlüssel der persönlichen Zertifikate sind geheim zu halten. Diese dürfen anderen Personen nicht bekannt beziehungsweise zugänglich gemacht werden – auch nicht einer Systemadministratorin oder einem Systemadministrator.

Passwörter müssen sicher sein und dürfen weder in einem Wörterbuch vorkommen, noch in Assoziation zur eigenen Person stehen (z.B. keine Namen, Geburtsdaten, Hobbies, Telefon- und Autonummern). Als sicher gelten Passwörter mit einer Länge von mindestens 10 Zeichen, kein Wort, Gross- und Kleinbuchstaben gemischt mit Zahlen und/oder Sonderzeichen.

Zugeteilte Initialpasswörter und bekannt gewordene Passwörter müssen sofort geändert werden. Aktive Passwörter sind regelmässig (alle 90 Tage) zu wechseln. Das neue Passwort darf nicht durch eine einfache logische Überlegung aus dem alten abgeleitet werden können. 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. Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert.

Portalzugang, Fernzugriff

Art. 18

Beim Auftreten einer Zertifikatswarnung ist die Verbindung, beispielsweise zum VPN-Dienst, Outlook Web Access (OWA), Exchange ActiveSync (EAS) oder 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 Stadt Wil einzubinden.

Desktop Sharing Lösungen sind nur temporär und einzig durch die von den Informatik-Diensten bestimmten Benutzenden einzusetzen. Diese kennen Steuerungs- sowie Kontrollmöglichkeiten der eingesetzten Produkte und setzen diese sinngemäss ein. Die Benutzenden von Desktop

Sharing Lösungen sind verpflichtet, bei Missbrauchsverdacht die Verbindung sofort abzubrechen und den Informationssicherheitsverantwortlichen über den Vorfall zu informieren.

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

IV. Datensicherheit

Grundsätze

Art. 19
Die Bearbeitung, Speicherung und Weitergabe personenbezogener Daten hat unter Berücksichtigung des geltenden Datenschutzgesetzes zu erfolgen.

Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten. Besteht die Möglichkeit einer technischen Lösung, beispielsweise durch das Eingrenzen der Zugriffsrechte, melden die Benutzenden dies unaufgefordert der oder dem Informationssicherheitsverantwortlichen.

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

Vertrauliche Informationen dürfen nie in der Öffentlichkeit besprochen werden. Zum Telefonieren ist ein ungestörter Bereich aufzusuchen.

Datenablage

Art. 20
Sämtliche erstellten bzw. empfangenen Daten müssen auf entsprechenden zentralen Laufwerken beziehungsweise in Datenbanken der Stadt Wil abgelegt werden. Das Departement Finanzen, Kultur und Verwaltung (FKV) ist befugt, entsprechende Weisungen zu erlassen. Das Laufwerk H:\ steht ausschliesslich für persönliche Daten zur Verfügung. Alle Serverlaufwerke werden täglich gesichert. Lokale Laufwerke C:\; D:\; E:\) sind nur für Systemdateien, Software sowie temporäre Daten bestimmt und werden nicht gesichert.

Auf nicht organisationseigenen Informatikmitteln, insbesondere auf privaten Geräten, dürfen keine besonders schützenswerten Personen-

daten oder geheime Daten der Stadt Wil bearbeitet oder gespeichert werden. Dies auch, 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. Die Benutzenden sind verpflichtet, ihre Terminplanung lückenlos im Outlookkalender vorzunehmen. Den relevanten Teammitgliedern und dem Telefonvermittlerarbeitsplatz im Rathaus ist mindestens das Leserecht zu erteilen. Private Termine und allfällige Einträge mit besonders schützenswerten Personendaten sind zur Wahrung der Vertraulichkeit im Outlook als "Privat" zu kennzeichnen (aktivieren Schlosssymbol).

Wer persönliche Daten der automatischen Archivierung entziehen will, ist verpflichtet, sich bei der Leiterin oder beim Leiter Informatik-Dienste über die erforderlichen Massnahmen zu erkundigen.

Drucken, Scannen, Faxen

Art. 21
Ausdrucke mit vertraulichen Informationen sind sofort aus dem Drucker zu entfernen. Wenn verfügbar, ist die Funktion des Druckens unter Aufsicht zu nutzen, beispielsweise Drucken mittels Eingabe eines PINs oder dem Vorweisen eines Badges.

Originale sind immer aus dem Kopierer/Scanner zu entfernen. Liegengelassene Dokumente mit vertraulichen Informationen sind umgehend der Urheberin resp. dem Urheber zurückzubringen oder der resp. dem Informationssicherheitsverantwortlichen zu übergeben.

Enthalten abgehende Faxe vertrauliche Angaben, ist die Empfängerperson vorgängig zu informieren.

Stellvertretende Zugriffe

Art. 22
Um Zugriffskonflikten vorzubeugen, sind die Daten generell auf den Abteilungslaufwerken abzuspeichern. Der stellvertretende Zugriff auf anderweitig abgelegte Daten sowie Informationen im Outlook sind mittels Freigaben und Berechtigungen zu gewährleisten, nicht mittels Weitergabe von persönlichen Logins/Passwörtern.

Ungeplante Abwesenheiten

Art. 23
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 (Krankheit, Unfall etc.) 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 Mitarbeitenden der Informatik-Dienste der Stadt Wil weisen auf die Ordnungsmässigkeit hin und stellen die Nachvollziehbarkeit sicher. Der schriftliche und unterzeichnete Antrag für den notfallmässigen Zugriff auf elektronische Daten von abwesenden Benutzenden muss in jedem Fall vorliegen. 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

Art. 24

Die Synchronisation von Daten der Stadt Wil mit privaten Informatik- und Kommunikationsmitteln ist untersagt. Hierzu gehört insbesondere das Verwenden von Outlook Anywhere. Eine Ausnahme ist das Verwenden privater Smartphones und Tablets, die einen Datenaustausch über den von der Stadt Wil definierten und betriebenen zentralen Zugangspunkt ausführen.

Die Informatik-Dienste der Stadt Wil behalten sich das Recht vor, technische Massnahmen zu erlassen und Konfigurationsrichtlinien durchzusetzen, um eine angemessene Informationssicherheit zu gewährleisten. Wird dem Durchsetzen der Konfigurationsrichtlinien nicht zugestimmt, ist die Besitzerin oder der Besitzer des Smartphones oder Tablets verpflichtet, die Datensynchronisation mit der Stadt Wil zu unterlassen beziehungsweise dauerhaft zu löschen.

Cloud Computing

Art. 25

Das Benutzen von Cloud Diensten, wie beispielsweise Dropbox, ist grundsätzlich untersagt. Wo ein geschäftsbezogener Nutzen das Risiko des Informationsabflusses überwiegt, sind Ausnahmen möglich. Entsprechende Gesuche sind mit Begründung an die Informationssicherheitsverantwortliche oder den Informationssicherheitsverantwortlichen zu richten.

Sicheres Löschen von Daten

Art. 26

Daten sicher löschen heisst, sie zu vernichten. Selbst wenn ein Datenträger mit neuen Daten überschrieben wird, bleiben die ursprünglichen Daten rekonstruierbar. Deswegen sind sowohl ausgediente als auch defekte Datenträger (Desktop-PCs, Notebooks, Smartphones, Tablets, Kopierer, Drucker, Fax, USB-Sticks, CDs / DVDs usw.) zwecks fachge-

rechter und sicherer Entsorgung den Mitarbeitenden der Informatik-Dienste der Stadt Wil zu übergeben.

Nicht mehr gebrauchte Dokumente mit vertraulichen Informationen sind eigenhändig im Aktenvernichter zu entsorgen.

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

V. Schutz in der Datenübermittlung (E-Mail, Internet)

Umgang mit E-Mails

Art. 27
E-Mails mit fragwürdiger Herkunft, verdächtigem Betreff oder unüblichem Inhalt sind sofort und permanent zu löschen – d.h. im "Posteingang" und im Ordner "Gelöschte Objekte". Deren Beilagen und enthaltene Links dürfen keinesfalls geöffnet werden, auch wenn die E-Mails über bekannte Absendende weitergeleitet wurden. Beispiele solcher E-Mails sind Bittbriefe, Werbemails, falsche Virenwarnungen, gefälschte Mitteilungen von Banken, Gewinnversprechen usw. Diese können unerwünscht sein (Spam), 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 bei der oder dem Informationssicherheitsverantwortlichen die zentrale Sperrung zu beantragen.

Die Ressourcen der E-Mail Infrastruktur dürfen nicht übermässig beansprucht werden. Daher wird das Übermitteln grosser Datenmengen mittels E-Mail im KOMSG wie auch bei Dritten begrenzt. Ein Datenaustausch innerhalb der Stadt Wil hat über eine Ablage auf einem gemeinsam zugänglichen Laufwerk – z.B. Laufwerk T:\ – und einem entsprechenden Verweis (Link) im E-Mail zu erfolgen. Bei E-Mails an Gruppen – z.B. „gg-wil alle" – ist äusserste Zurückhaltung zu üben.

Vertraulichkeit im E-Mail Verkehr

Art. 28
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

Stadt Wil und des KOMSG nur in verschlüsselter Form und lediglich an bekannte oder vertrauenswürdige E-Mail-Adressen versandt werden. Adressaten ausserhalb der Stadt Wil und des KOMSG sind mit EXT gekennzeichnet.

Die Empfängeradresse ist resp. die Empfängeradressen 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. Wird ein E-Mail falsch adressiert, kann es mit der Outlook-Funktionalität unmittelbar nach dem Versand zurückgerufen werden. Allenfalls ist mit dem fehlerhaft adressierten Empfängerin oder Empfänger telefonisch Kontakt aufzunehmen.

Aktuell werden in der Stadt Wil die E-Mails nicht verschlüsselt. Hingegen kann der vertrauliche Inhalt einer Mitteilung als verschlüsselte E-Mail-Anlage (z.B. zip-Datei) versendet werden. Das zip-Passwort ist der Empfängerin oder dem Empfänger per Telefon oder in einem separaten E-Mail zu übermitteln.

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

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

Sicher im Internet

Art. 29

Der Zugriff auf Internet-Dienste 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 authentifizieren und verifizieren. Beschaffungsort und Autorin oder Autor sind anzugeben.

Sperrung von Internet-Adressen

Art. 30
Die Departemente bzw. die Informationssicherheitsverantwortlichen können häufig verwendete und nicht geschäftlichen Zwecken dienende Internetadressen sperren lassen.

Neue Kommunikationswege

Art. 31
Das in diesem Kapitel erwähnten Schutzmassnahmen gelten sinngemäss für die neuen Arten der Kommunikation (Chat, Unified Communication usw.).

VI. Mobile Geräte und Datenträger

Verlust und Diebstahl

Art. 32
Mobile Geräte und Datenträger wie beispielsweise Notebooks, Tablets, Smartphones, USB-Sticks und CD/DVDs sind besonders gefährdet durch Verlust oder Diebstahl. Wer mobile Geräte oder Datenträger einsetzt, hat die nachfolgenden Grundsätze zwingend umzusetzen:

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

Art. 33
Benutzende, die im Besitz eines Notebooks sind, müssen sich mindestens zwei Mal pro Monat am Netzwerk der Stadt Wil anmelden, damit sicherheitsrelevante Aktualisierungen durchgeführt werden können.

Drahtlose Komponenten wie WLAN, Bluetooth, Infrarot usw. sind bei Nichtgebrauch zu deaktivieren. Beim Anschluss an drahtlose Netzwerke (WLAN) sind diese bei erscheinender Auswahl richtig einzustufen (privat, Arbeit, öffentlich).

STADT WIL

Smartphones und Tablets

Art. 34

Vom zentralen Zugangspunkt der Stadt Wil werden bestimmte Konfigurationen technisch erzwungen. Es gilt zu beachten, dass nicht alle Geräte die gesteuerten Konfigurationen übernehmen, teilweise sogar ignorieren. Benutzende von Smartphones und Tablets sind verpflichtet, die nachfolgend aufgelisteten Konfigurationen laufend zu prüfen und wenn notwendig die Einstellungen manuell durchzuführen. Kann ein Gerät nicht alle zwingenden Konfigurationen umsetzen, ist von einer Datensynchronisation mit der Stadt Wil abzusehen.

Zwingende Konfigurationen:

- Das Gerätekennwort ist aktiviert, die minimale Kennwortlänge sind 4 Zeichen.
- Nach maximal 10 Minuten Inaktivität (ohne Benutzendeneingabe) wird das Gerät automatisch gesperrt.
- Nach maximal 10 fehlerhaften Kennworteingaben werden alle auf dem Gerät enthaltenen Daten automatisch gelöscht beziehungsweise das Gerät in den Werkszustand versetzt.
- Die Verschlüsselungsfunktion für die Speichermedien und das Datenbackup sind aktiviert.

Es sind nur Apps zu installieren, die in einem offiziellen Shop wie dem App Store von Apple, Windows Phone Marketplace von Microsoft, Google Play usw. erhältlich sind. Vor dem Herunterladen einer App sind dessen Bewertungen zu verifizieren – je mehr Leute eine App gut bewertet haben, desto vertrauenswürdiger ist sie.

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 Stadt Wil erfolgt, ist ein Gebrauch der Cloud untersagt. Nur Ortungsdienste (ohne Datensicherung) wie „iPhone suchen" von Apple oder „Lookout" bei Android-Geräten sind in jedem Fall erlaubt.

Das Modifizieren von Betriebssystemen zur Umgehung herstellerbedingter Sperrfunktionen ist untersagt (in der Fachsprache Jailbreaking oder Rooten genannt). Andernfalls erlischt die Berechtigung zur Datensynchronisation.

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. Anrufspeicher, gespeicherte 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 frühzeitig und in der genannten Reihenfolge auszuführen:

1. Sichere Datenlöschung (Wipen) über das OutlookWebAccess - OWA.
2. Sperren der SIM-Karte beim Mobilfunkanbieter veranlassen.
3. Verwendete Passwörter ändern.
4. Information an die Informationssicherheitsverantwortliche oder den Informationssicherheitsverantwortlichen über den Verlust und die getätigten Massnahmen informieren.

VII. Missbrauch, Kontrolle und Sanktion

Konsequenzen

Art. 35
Verstösse gegen dieses Reglement stellen Dienstpflichtverletzungen dar und können personalrechtliche Massnahmen und Schadenersatzansprüche zur Folge haben. Bei strafbaren Handlungen wird gegen fehlbare Personen Anzeige erstattet.

Protokollierung

Art. 36
Die Nutzung der Informatik- und Kommunikationsmittel wird zum Sicherstellen der technischen Sicherheit und Einhalten der vorliegenden Weisung sowie der gesetzlichen Bestimmungen 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

Art. 37
Die Protokollierungen werden laufend und anonym durch die Informatik-Dienste ausgewertet. Dabei geht es um die statistische Analyse der Protokollierungen.

Personenbezogene Auswertung der Protokolldaten

Art. 38
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

STADT WIL

erfolgt durch die Informatik-Dienste unter der Leitung der oder des Informationssicherheitsverantwortlichen.
- Wenn die oder der Informationssicherheitsverantwortliche einen Missbrauch feststellt oder vermutet. In diesem Fall werden die Protokolldaten ausgewertet. Die betroffene Person muss schriftlich bestätigen, davon 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 dürfen die Informatik-Dienste ohne Vorwarnung Verbindungsdaten mit personenbezogenen Daten aufzeichnen. Eine personenbezogene Auswertung der Daten darf jedoch erst nach einem Auftrag durch die Informationssicherheitsverantwortliche oder den Informationssicherheitsverantwortlichen und der schriftlichen Bestätigung der betroffenen Personen, vom Auftrag Kenntnis genommen zu haben, erfolgen. Die der verursachenden Person vorgesetzte Stelle wird über einen solchen Vorfall orientiert.

VIII. Schlussbestimmungen

Aufhebung bisheriger Bestimmungen

Art. 39
Die vorliegende Weisung ersetzt das Reglement über den Einsatz von Informatikmitteln in der Stadt Wil vom 22. Februar 2006.

Inkrafttreten

Art. 40
Diese Weisung tritt am 1. Dezember 2015 in Kraft.

Stadt Wil

Susanne Hartmann
Stadtpräsidentin

Christoph Sigrist
Stadtschreiber