Gemeinde Dänikon
Wohn-, Arbeits- und Lebensraum

Reglement zur Informationssicherheit

vom 18. November 2013

Inhaltsverzeichnis

A. Allgemeine Bestimmungen

B. Verantwortung

C. Informationssicherheit

D. Datenschutz und Datensicherung

E. Nutzung von E-Mail und Internet

F. Protokollierung und Kontrolle

Inhaltsverzeichnis

G. Übergangs- und Schlussbestimmungen

A. Allgemeine Bestimmungen

Art. 1 Gegenstand und Zweck

[1] Dieses Reglement regelt die Nutzung und Massnahmen zur Verhinderung des Missbrauchs von Internet und E-Mail mit gemeindeeigenen Informatikmitteln durch die Mitarbeitenden der Politischen Gemeinde Dänikon. Weiter wird der verantwortungsvolle Umgang mit Informationen, insbesondere mit Personendaten, thematisiert.

[2] Entsprechend dem Grundsatz der Gleichberechtigung von Mann und Frau gelten alle Personen und Funktionsbezeichnungen dieses Reglements, ungeachtet der männlichen oder weiblichen Sprachform, selbstverständlich für beide Geschlechter.

Art. 2 Geltungsbereich

[1] Die Weisung gilt für alle Mitarbeitenden der Politischen Gemeinde Dänikon. Als Mitarbeitende im Sinne dieser Weisung gelten alle fest oder temporär angestellten Mitarbeitenden sowie die Behörden- und Kommissionsmitglieder.

Art. 3 Grundlagen

[1] Grundlage bilden das Gesetz über die Information und den Datenschutz (IDG) 170.4, die Informatiksicherheitsverordnung 170.8, die Verordnung über die Nutzung von Internet und E-Mail 177.115 sowie die Bestimmungen betreffend Amtsgeheimnis.

B. Verantwortung

Art. 4 Informationssicherheitsverantwortliche/r

[1] Der Gemeinderat Dänikon bezeichnet einen Informationssicherheitsverantwortlichen (nachfolgend ISV genannt). Dieser ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse. Er ist befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen.

[2] Der gemäss Stellenbeschreibung für den IT-Betrieb Verantwortliche wird zum Informationssicherheitsverantwortlichen ernannt. Die Stellvertretungsregelung für den IT-Betrieb wird auch für den Informationssicherheitsverantwortlichen angewendet.

Art. 5 Mitarbeitende

[1] Die Mitarbeitenden sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten. Sie haben die Kenntnisnahme dieser Weisung unterschriftlich zu bestätigen.

[2] Die Mitarbeitenden sind verpflichtet, die ihnen zur Verfügung gestellten IKT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen. Die Mitarbeitenden melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Hardware und Software dem ISV.

C. Informationssicherheit

Art. 6 Externe Datenträger

[1] Das Anschliessen von externen Datenträgern (z.B. USB-Sticks, externe Festplatten etc.) ist nur in Ausnahmefällen und in Rücksprache mit dem ISV gestattet. Vor der Nutzung von Daten ab externen Datenträgern ist die Datenquelle auf Viren manuell zu scannen. Primär jedoch sollen, wenn immer möglich, die zu bearbeitenden Daten via online-Kanäle (Internet, Mail) beschafft werden.

Art. 7 Hard- und Software

[1] Nur der ISV oder eine von ihm beauftragte Person ist berechtigt, Hardware und Treiber zu installieren oder zu entfernen. Er verwaltet die Lizenzen, registriert die Konfigurationen und erteilt Genehmigungen für zugelassene Anschlüsse von externen Geräten am Laptop oder Desktop.

Art. 8 Fremde IT-Netze

[1] Der Anschluss von Hardware (z.B. Laptops) der Politischen Gemeinde Dänikon an fremde IT-Netze ist nicht erlaubt.

Art. 9 Fremde Hardware

[1] Der Anschluss von fremder Hardware am IT-Netz der Gemeinde Dänikon ist nicht erlaubt.

Art. 10 Mobile Geräte

[1] Der Gebrauch von mobilen Geräten (u.a. Laptops) der Politischen Gemeinde Dänikon durch Dritte ist nur nach erfolgter Rücksprache mit dem ISV erlaubt.

Art. 11 Virenschutz

[1] Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder umkonfigurieren. E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind im Hinblick darauf, dass sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten, vorsichtig zu behandeln. Deren Beilagen sollen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort dem ISV gemeldet werden.

C. Informationssicherheit

Art. 12 Zugriffsschutz

[1] Wird der Arbeitsplatz während der Arbeit verlassen, ist der Bildschirm des Computers grundsätzlich mittels Bildschirmsperre mit Passwortschutz zu sperren (die automatische Sperre hilft nur beim Vergessen). Alle mobilen Datenträger wie DVD, CD, USB-Stick etc.) mit schützenswerten Informationen wie Personendaten gemäss IDG müssen analog Papierdaten von der Arbeitsfläche entfernt werden.

Art. 13 Passwörter

[1] Passwörter sind persönlich und vertraulich. Sie dürfen nur dem Benutzer selbst bekannt sein und auf keine Weise an Vorgesetzte oder Dritte weiter gegeben werden. Zugeteilte Initialpasswörter und bekannt gewordene Passwörter müssen unverzüglich geändert werden.

Art. 14 Defekte an Hard- und Software

[1] Werden Unregelmässigkeiten an der Hardware (wie Defekte, Beschädigungen, Diebstahl) oder an der Software (wie Fehlberechnungen, Speicherfehler, Virenbefall) festgestellt, so sind diese unverzüglich dem ISV zu melden. Vorkommnisse, welche die Vertraulichkeit betreffen, sind direkt dem Gemeindeschreiber mitzuteilen.

Art. 15 Private Nutzung von IKT-Mitteln

[1] Die Benützung von Informatikmitteln durch Angestellte für private Zwecke ist gestattet, hat sich aber auf ein absolutes Minimum zu beschränken und darf die Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belasten.

Art. 16 Verstösse gegen die Weisung zur Informationssicherheit

[1] Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und / oder personalrechtliche Konsequenzen haben.

D. Datenschutz und Datensicherung

Art. 17 Datenschutz

[1] Das Gesetz und die Verordnung bilden die Gesetzesgrundlagen im Rahmen von Informatikdienstleistungen und müssen von allen Mitarbeitern befolgt werden:

- Gesetz über die Information und den Datenschutz (IDG) 170.4
- Informatiksicherheitsverordnung 170.8

[2] Als sensible und schützenswerte Daten gelten gemäss IDG § 3 zum Beispiel:

- Informationen, welche die Erfüllung einer öffentlichen Aufgabe betreffen
- Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen
- Informationen, bei denen die Gefahr einer Persönlichkeitsverletzung besteht wie beispielsweise religiöse, politische oder gewerkschaftliche Ansichten, Gesundheit, Rassenzugehörigkeit, ethnische Herkunft, administrative oder strafrechtliche Verfolgungen oder Massnahmen der sozialen Hilfe

Art. 18 Datensicherung

[1] Geschäftsbezogene Daten müssen auf Serverlaufwerken gespeichert werden. Der ISV sorgt für eine regelmässige Sicherung aller Geschäftsdaten und die sichere Lagerung der dazu benötigten Archivmedien.

[2] Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht). Nicht mehr benötigte Informationsträger (z.B. CD-ROM, USB-Datenträger usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. schreddern).

E. Nutzung von E-Mail und Internet

Art. 19 Allgemeine Bestimmungen

[1] E-Mail und Internet werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit und des Datenschutzes eingesetzt. Die Mitarbeitenden haben sich unterschriftlich zur Einhaltung der Nutzungsvorschriften zu verpflichten.

Art. 20 Umgang mit E-Mail und Internet

[1] Die folgenden Punkte umschreiben den Umgang mit Internet und E-Mail:

- Internetseiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt dürfen weder angewählt noch per E-Mail weiter geleitet werden.
- Die Teilnahme an interaktiven Medien, insbesondere an Chatrooms sowie Onlinespielen, ist verboten.
- Das Herunterladen oder die Installation von Spielen sowie von Audio- und Videodateien aus dem Internet ist grundsätzlich verboten. Das Herunterladen von Audio- und Videodateien zu geschäftlichen Zwecken ist nur nach Absprache mit dem IT-Verantwortlichen zulässig.
- Die Nutzung von Internetseiten zum Herunterladen von grossen Dateien (beispielsweise YouTube, Radio- oder TV-streaming), welche das LEUnet grossen Belastungen aussetzt, ist verboten.
- E-Mails fragwürdiger Herkunft sind umgehend und ohne Öffnen der E-Mail, respektive des Anhangs, zu löschen. Die „Autovorschaufunktion“ in Outlook muss deaktiviert sein.
- Die Publikation der geschäftlichen E-Mailadresse (vorname.nachname@daenikon.ch) für private Zwecke wie beispielsweise Seiten von Sportclubs, Private Homepage usw. ist nicht erlaubt.
- Die automatische Umleitung von E-Mails (Forwarding) an externe E-Mail-Adressen wie beispielsweise bluewin.ch ist nicht erlaubt.

F. Protokollierung und Kontrolle

Art. 21 Vorgehen bei Missbrauch

[1] Die Protokollierung von Internet und E-Mail dient der Überwachung der auf Stufe Kanton erlassenen Sicherheitsbestimmungen. Die Protokollierung wird laufend vom Provider mit einer Software durchgeführt und anonym ausgewertet. Mit anonym ist gemeint, dass die Auswertungen keine Rückschlüsse auf einzelne Mitarbeitende oder auf einzelne Arbeitsplätze zulassen.

[2] Der Arbeitgeber kann im Rahmen seiner Aufsichtspflicht jederzeit solche anonymisierten Protokolle beim Provider verlangen.

[3] Wenn bei Internet-Zugriffen Missbräuche vorliegen oder wenn beim E-Mail-Verkehr ein konkreter Verdacht auf Missbrauch besteht, erfolgt zuerst eine Abmahnung. Nach erfolgter Abmahnung können die Internet-Zugriffe und / oder der E-Mail-Verkehr personenbezogen für maximal drei Monate protokolliert und ausgewertet werden. Protokolliert werden folgende Daten:

- bei Onlinediensten: wer (Benutzer-Account), wann (Zeit) und welche Dienste (Internetseite) benutzt hat.
- beim E-Mailverkehr: den Empfänger, den Absender, den Zeitpunkt und den Betreff sämtlicher gesendeter und empfangener E-Mails.

[4] Der Personalvorstand und der Gemeindeschreiber entscheiden auf Grund der personenbezogenen Berichte, ob personalrechtliche oder allenfalls strafrechtliche Massnahmen einzuleiten sind.

G. Übergangs- und Schlussbestimmungen

Art. 22 Schlussbestimmungen

[1] Änderungen dieses Reglements zur Informationssicherheit werden durch den Gemeinderat erlassen.

Art. 23 Rekursrecht

[1] Gegen Beschlüsse und Verfügungen aufgrund dieses Reglements kann innert 30 Tagen, von der Zustellung an gerechnet, beim Bezirksrat Dielsdorf, Geissackerstrasse 24, Postfach 273, 8157 Dielsdorf, schriftlich Rekurs erhoben werden.

Art. 24 Inkrafttreten

[1] Dieses Reglement zur Informationssicherheit tritt am 1. Januar 2014 in Kraft.

[2] Alle Beschlüsse, die im Widerspruch zu diesem Reglement stehen, werden auf den 1. Januar 2014 nach Eintritt der Rechtskraft aufgehoben.

Art. 25 Übergangsbestimmungen

[1] Alle Tatbestände vor dem 1. Januar 2014 werden nach den bisherigen Regelungen behandelt.

8114 Dänikon, 18. November 2013

GEMEINDERAT DÄNIKON

Der Präsident: Der Schreiber:

Daniel Zumbach Lukas Kalberer

Publikation im Furttaler:

22. November 2013 Gemeinderatsbeschluss