Gemeinderat

Gemeinde Wila

IT-Richtlinien und Sicherheitskonzept

vom 1. Oktober 2012

Inhaltsverzeichnis

Sprachregelung

In diesem Konzept gelten sämtliche Personen- und Funktionsbezeichnungen für beide Geschlechter, ungeachtet der weiblichen oder männlichen Sprachform.

Verteiler

alle Mitarbeitenden der Gemeindeverwaltung Wila (inkl. Förster, Gemeindearbeiter und Betreibungsamt)

1. IT-Organisation

Die Politische Gemeinde Wila benutzt die Hauptapplikationen NEST IS-E (Einwohnerkontrolle, Steuern, Gebühren usw.) sowie Abacus (Buchhaltungsprogramm). Bezüglich Details und den weiteren Unter- bzw. Nebenprogrammen wird auf eine separate Zusammenstellung verwiesen. Der zentrale Server befindet sich im Gemeindehaus, EDV-Raum.

Mit der Kantonalen Verwaltung erfolgt ein regelmässiger Datenaustausch. Dieser Austausch erfolgt über das Leunet des Kantons Zürich.

Datensicherheit und Datenschutz sind mehrstufig geregelt (Leunet: Firewall, Gemeinde: Antivirenprogramm). Die Zuständigkeiten liegen bei Abraxas (Leunet) und der Gemeinde Wila. Soweit die Gemeinde Wila zuständig ist, werden die Mitarbeiter bei Stellenantritt über den aktuellen Stand instruiert und über alle späteren Veränderungen umgehend informiert und instruiert.

Die Software bedarf der periodischen Betreuung vor Ort. Auch personelle Wechsel bedingen immer wieder Anpassungen an den einzelnen Arbeitsplätzen. Jeder PC ist so konfiguriert, dass jedem Mitarbeiter an jedem Arbeitsplatz das Standard-Softwarepaket sowie die für die Tätigkeit benötigten Spezial-Programme zur Verfügung stehen. Die Komplexität der unterschiedlichen Programme stellt hohe Anforderungen an die Wartung der EDV-Anlage. Mit der auf die Hauptapplikationen spezialisierte OBT AG in Zürich steht der Gemeinde Wila seit Jahren eine ausgewiesene Firma zur Verfügung, die auch im Notfall über entsprechende Kapazitäten und Verbindungen zu den Lieferanten verfügt.

2. IT-Verantwortliche / Notfallnummern

IT-Verantwortlicher ist der Stellvertreter Finanz- und Steuersekretär. Die Stellvertretung obliegt dem Gemeindeschreiber.

Für die einzelnen Wartungsdienstleister stehen im Rahmen eines Wartungsvertrages unterschiedliche Notfallnummern zur Verfügung. Liegt eine Störung vor, muss daher situativ die Dringlichkeit und Wichtigkeit einer Behebung abgeklärt und entsprechend gehandelt werden. Die Mitarbeiter der Gemeindeverwaltung sind soweit geschult, dass in der Regel der für die Schadensursache zuständige Dienstleister rasch eruiert und informiert werden kann. Die wichtigsten Notfallnummern (Anhang A) werden sämtlichen Mitarbeitern abgegeben. Die Problembehebung erfolgt zu den im Wartungsvertrag festgelegten Interventionszeiten. Die Kontaktaufnahme mit dem zuständigen Dienstleister ist mit dem IT-Verantwortlichen abzusprechen.

Ein allfälliger Stromausfall kann verwaltungsintern mit dem installierten USV-System (unterbrechungsfreie Stromversorgung) beim Server für die ersten Stunden abgefangen werden. Dies ermöglicht dem IT-Verantwortlichen den Server ordnungsgemäss herunterzufahren und zu restarten.

3. Anwender Richtlinien

Die relevanten Gesetzesgrundlagen (Informatiksicherheitsverordnung, Gesetz über die Information und den Datenschutz [IDG] und Verordnung über die Information und den Datenschutz [IDV]) sind dem Personal bekannt. Gesetzesänderungen werden intern kommuniziert und instruiert.

Folgende Richtlinien sind von den Benutzern einzuhalten:

Arbeitsplatz

- Bei vorübergehender Abwesenheit vom Arbeitsplatz (Mittagspause, Sitzungen) ist durch gleichzeitiges Drücken der Tasten [Ctrl] + [Alt] + [Delete] der Computer vor einem Fremdzugriff zu sperren.
- Am Ende des Arbeitstages oder tagsüber bei längerer Abwesenheit sind alle Anwendungen zu schliessen und die Mitarbeiter melden sich durch Herunterfahren ihres PC vom Server ab.
- Wegwerfbare vertrauliche Papierdokumente sind mit dem Aktenvernichter zu schreddern bzw. in die "Reisswolf-Box" zu werfen.
- Die private Nutzung von Internet und Outlook (E-Mail) hat sich in zeitlicher Hinsicht auf ein Minimum zu beschränken.
- Diverse Seiten sind im Sinne der Policy zwischen KITT und IG ICT Zürcher Gemeinden nicht verfügbar.
- Die Mitarbeiter haben eine "Erklärung zur Nutzung von Internet und E-Mail" sowie eine "Erklärung der Schweigepflicht" zu unterzeichnen.

E-Mail

- Vor jedem Senden muss überprüft werden, ob die Empfängeradresse korrekt eingefügt wurde.
- E-Mails, die dem Empfänger verdächtig vorkommen, dürfen nicht geöffnet werden.
- Anhänge und angegebene Links dürfen nur aus vertrauenswürdigen Quellen geöffnet werden.
- Anhänge, die zwei Endungen aufweisen (z.B. foto.jpg.exe) dürfen nicht geöffnet werden.
- Anhänge mit den Endungen .exe, .com, .pfi, .scr, .vbs, .bat oder .cmd dürfen nicht geöffnet werden.
- E-Mails von unbekannten und dubiosen Adressen werden nicht beantwortet.
- Empfangen oder Versenden von "lustigen" Mails mit entsprechenden Anhängen ist im Interesse eines reibungslosen Betriebes zu unterbinden bzw. zu unterlassen.
- Jedes Mail ist mit einem Disclaimer zu versehen (Hinweis an einen Falschempfänger).

- E-Mails dürfen nicht automatisch an externe-Mail-Adressen umgeleitet werden.
- Untersagt ist zu privaten Zwecken
  - das Ablegen von dienstlichen E-Mail-Adressen im Internet;
  - der Versand von E-Mails mit starker Netzwerkbelastung, insbesondere der Versand an einen grossen Empfängerkreis oder von grossen Datenmengen.
- Bei Unklarheiten oder Fragen ist umgehend der IT-Verantwortliche zu kontaktieren.

Internet

- Das Besuchen von allenfalls nicht gesperrten Websites mit anstössigem, rechtswidrigem, pornographischem, rassistischem, sexistischem, gewaltverherrlichendem oder strafrechtlich relevantem Inhalt ist verboten.
- Die lokal gespeicherten temporären Dateien sind im entsprechenden Browser in regelmässigen Abständen zu löschen.
- Das Downloaden von unbekannten Dateien ist untersagt.
- Eine E-Banking-Sitzung wird immer mit der dafür vorgesehenen Funktion (z.B. "Abmelden") beendet. Anschliessend sind die temporären Internetdateien des Browsers zu löschen.

Missbrauch der Internet-Dienste

Wird ein Missbrauch der Internet-Dienste festgestellt, so können die Internet-Zugriffe personenbezogen protokolliert und ausgewertet werden. Der E-Mail-Verkehr kann bei einem konkreten Verdacht auf Missbrauch personenbezogen protokolliert und ausgewertet werden. In beiden Fällen ist eine personenbezogene Auswertung erst nach erfolgter Abmahnung zulässig. Anonyme Berichte über die Internet-Zugriffe können jederzeit erstellt werden.

Ein Missbrauch hat personalrechtliche Konsequenzen zur Folge. Bei Verstoss gegen das Strafgesetzbuch und bei Verletzung von Rechten Dritter - insbesondere von Urheberrechten - muss mit straf- bzw. zivilrechtlichen Konsequenzen gerechnet werden.

Hardware

- Sämtliche Hardware wird ausschliesslich und nur im Auftrag des IT-Verantwortlichen oder seines Stellvertreters durch Mitarbeiter der OBT AG gewartet, verändert, ergänzt oder ausgewechselt.

Software

- Jedem Mitarbeiter ist es untersagt, Software jeglicher Art auf den Server oder eine Arbeitsstation zu laden oder diese zusammen mit einem externen Speichermedium zu nutzen. Ebenfalls untersagt ist das Verändern, Abziehen oder Kopieren von Software auf dem Server oder einer Arbeitsstation.
- Zu Arbeitszwecken benötigte, zusätzliche Software wird auf Nachweis und Verlangen hin vom IT-Verantwortlichen oder seinem Stellvertreter installiert bzw. gedownloadet.

Archivierung

- Die Abteilungsleiter der Verwaltung entscheiden je für das ihnen zustehende Fachgebiet gemäss entsprechenden Richtlinien über die Archivierung und zeitgerechte Vernichtung der elektronischen Unterlagen.
- Das Vorarchiv im Büro des Gemeindeschreibers und in der Gemeindekanzlei wird periodisch von einem professionellen Archivservice bearbeitet.

Umgang mit vertraulichen Daten

- Es gelten insbesondere die Bestimmungen von IDG und IDV
- Mitarbeiter der Verwaltung unterstehen einer strengen amtlichen Schweigepflicht. Von dieser sind sie nur entbunden, wenn sie im Einzelfall gemäss IDG und IDV ein Mitteilungsrecht oder eine Mitteilungspflicht haben.
- Die Mitarbeiter haben beim Stellenantritt eine "Erklärung der Schweigepflicht" zu unterzeichnen.
- Alle elektronischen Daten und Dateien sind auf das gesicherte Netzlaufwerk zu speichern. Das Speichern von vertraulichen Daten auf lokale oder externe Laufwerke ist untersagt und kann strafrechtlich verfolgt werden. Hiervon ausgenommen sind die täglichen Datensicherungen.

- Abteilungsspezifische Daten sind auf den entsprechenden Abteilungslaufwerken zu speichern. Im Ordner "Gemeinsam" auf dem Laufwerk "Abteilungsdaten" sind keine vertraulichen Daten zu speichern.

4. Passwort

Passwortverwaltung

- Jeder Mitarbeiter ist für seine Passwortverwaltung selber gemäss Richtlinien verantwortlich.

Passwort

- Die Passwörter sind vom Anwender gemäss Richtlinien und Weisung des jeweiligen Software-Anbieters in regelmässigen Abständen zu wechseln.
- Für jeden passwortgeschützten Bereich werden unterschiedliche Passwörter verwendet.
- Je nach Anbieter verfügt ein Passwort in der Regel über mindestens 6 Zeichen und soll/muss neben Gross- und Kleinbuchstaben auch Ziffern und Sonderzeichen enthalten.

5. Virenschutz

Inhouse sind der Server und sämtliche Arbeitsstationen mit einer Antivirus-Software ausgerüstet. Die laufende Aktualisierung dieser Software ist automatisiert.

Werden dem Benutzer Virenwarnungen angezeigt, ist unverzüglich der IT-Verantwortliche zu kontaktieren.

Externe Datenträger

Der Anschluss externer Datenträger (USB-Sticks, CD's etc.) am Client hat besonders sorgfältig zu erfolgen. Die jeweiligen Datenträger sind vorgängig auf Viren zu überprüfen.

6. Datensicherung

Sämtliche elektronischen Daten werden täglich gesichert. Das Sicherungsband wird im feuerfesten Tresor im Gemeindehaus aufbewahrt. Die Freitags-Datensicherung sowie diejenige Ende Monat werden extern an getrennten Orten gelagert.

Der Server generiert täglich eine Meldung mit detaillierten Informationen über die Datensicherung. Diese Meldung wird automatisch dem EDV-Verantwortlichen zur Kontrolle sowie dem Support der OBT AG zugestellt. Bei einer fehlerhaften Sicherung ist die OBT AG zu kontaktieren.
Mindestens einmal Jährlich wird ein Restore-Test des Backups gemacht um sicherzustellen, dass es auch funktioniert.

7. Maximal tolerierte Wiederherstellungszeit

Die maximal tolerierte Wiederherstellungszeit definiert den Zeitraum zwischen Schadenfall und der wieder vollen Verfügbarkeit der Daten. Die Zugangsmöglichkeiten können nach Ablauf der Frist noch beschränkt sein, die Verfügbarkeit der Daten ist jedoch gegeben.

Anwendungen mit unmittelbarem Kundenkontrakt: 1 Tag
Beispiele: NEST IS-E, NEST Steuern, Abacus, E-Mail

Anwendungen ohne unmittelbaren Kundenkontakt: 3 Tage
Beispiele: Office-Anwendungen, ArcaNT etc.

Die Verantwortlichkeiten und Zuständigkeiten sind in den Verträgen mit den verschiedenen Partnern festgehalten.

8. Räumliche Sicherheitsvorkehrungen

Die Haustüre sowie der Kassenbereich sind vor und nach den Schalteröffnungszeiten abzuschliessen.

Zutritt zu den Räumlichkeiten der Gemeindeverwaltung haben nur das Gemeindepersonal, die Gemeinderäte sowie die Reinigungsangestellte. Zutritt zum Server-/Kopierraum ist nur dem Verwaltungspersonal (ausgenommen EDV-Support) erlaubt. Kunden, welche die Erlaubnis zur Benützung des Kopierers haben, müssen sich am Schalter der Einwohnerkontrolle an- und wieder abmelden.

Der Brandschutz (Ersteinsatz) ist gewährleistet durch das im Server-/Kopierraum und Treppenhaus vorhandene Einsatzmaterial (Löschdecke, Feuerlöscher).

9. Überprüfung, Nachführung und Inkraftsetzung

Diese IT-Richtlinien mit Sicherheitskonzept insbesondere die Aktualität der Zugriffsberechtigungen, Loginangaben und Notfallnummern sind regelmässig - mind. jährlich - zu überprüfen und anzupassen.
Verantwortlich ist der IT-Verantwortliche.

Das Konzept wurde vom Gemeinderat mit Beschluss Nr. 184 am 1. Oktober 2012 verabschiedet und per sofort in Kraft gesetzt.

Namens des Gemeinderates Wila

Die Präsidentin:	**Der Schreiber:**
sig. M. Kradolfer	sig B. Zinniker

Anhang A

Notfallnummern

OBT AG Kundennummer: 137‘362	Abacus, NEST IS-E, MS-Office, Hardware	0844 80 35 35
KMS AG	NEST Steuern	041 329 84 20
Abraxas	Exchange / Mail-Hosting	058 660 00 10
Datenlogistik	Datenaustausch	043 259 30 17
Spider Soft	Grundsteuersoftware	043 843 23 00
Greenshare AG	BauPro, ArcaNT	044 930 40 66
Scan-Center W'thur	ARTS (Anwendersupport, Verfügbarkeit)	052 267 69 58
Bonimpex AG	BEA_NT	032 621 52 55