PUBLICS

Gemeinde Pfäffikon

NUTZUNGSRICHTLINIE (AUP)

über den Gebrauch von Informatik-Mitteln

Erlass des Gemeindeschreibers
1. Februar 2013

STATIONSSTRASSE 57 CH-8606 NÄNIKON ✆ 044 440 30 20
PARTNER@PUBLICSPARTNER.CH WWW.PUBLICSPARTNER.CH

PUBLICS

Inhalt

©PUBLICS

1. Zweck

Diese Nutzungsrichtlinie (Acceptable Use Policy AUP) in Form einer Weisung hat das Ziel, die ordnungsgemässe Nutzung der Informatikmittel der Gemeindeverwaltung Pfäffikon sicherzustellen und einen störungsfreien Betrieb zu gewährleisten.

2. Geltungsbereich

Dieser Weisung sind als BenutzerInnen unterstellt: Personal, Behördenmitglieder, externe Mitarbeiter fremder Firmen und alle weiteren Personen, die Zugang zu den Informatikmitteln der Verwaltung haben.

3. Zulässige Nutzung

Die Nutzung der Informatikmittel ist für diejenigen Zwecke erlaubt, für welche die Informatikmittel zur Verfügung gestellt werden (bestimmungsgemässe Nutzung).

Eine Nutzung für private nicht-kommerzielle Zwecke ist erlaubt, soweit sie nicht übermässig ist und die Erfüllung der Arbeitspflichten nicht beeinträchtigt. Alle Daten, die auf Informatikmitteln der Gemeinde gespeichert sind, können bei Abwesenheit, bei Verdacht auf missbräuchliche Nutzung oder bei Austritt durch eine funktionale Stellvertretung eingesehen werden.
Eine kommerzielle Nutzung der Informatikmittel ist nicht zulässig.

E-Mails können bei Abwesenheit der BenutzerInnen durch den Administrator an eine funktionale Stellvertretung oder die vorgesetzte Stelle weitergeleitet werden. Bei Abwesenheit der BenutzerInnen kann der Zugriff auf gespeicherte Daten einer funktionalen Stellvertretung oder der vorgesetzten Stelle ermöglicht werden.

Bei Austritt eines Mitarbeiters kann sein Mailarchiv an die Nachfolge übergeben werden.

4. Sicherheitsvorschriften

Es ist ausschliesslich mit den Benutzerkennungen zu arbeiten, deren Nutzung gestattet wurde. Die Weitergabe von Benutzernamen und Passwörtern ist untersagt. Unsichere Passwörter sind zu vermeiden, jede Sitzung muss ordnungsgemäss mit dem Abmelden oder Sperren beendet werden.

Die BenutzerInnen tragen die Verantwortung für alle Aktionen, die sie mit ihrer Benutzerkennung vornehmen oder die durch Dritte vorgenommen werden, wenn sie diesen den Zugang zumindest fahrlässig ermöglicht haben.

©PUBLICS

5. Missbräuchliche Nutzung

Das Herunterladen, die Verwahrung und die Verbreitung oder Verwertung von rechtswidrigen oder rechtswidrig erlangten Daten, Programmen oder Anleitungen sind untersagt.

Die Informatikmittel dürfen nicht verwendet werden für Angriffe auf eigene oder andere Systeme, zur Verteilung von unerwünschten Massenmails (Spam) sowie für jede weitere nicht zweckgemässe Tätigkeit wie z.B. Missbrauch von Mailverteiler-Listen.

Untersagt sind insbesondere:

- Unbefugtes Verändern, Löschen, Unbrauchbarmachen oder Unterdrücken von Daten;
- Unbefugtes Verändern von System- und Netzwerkkonfiguration;
- Unbefugte Installation von Software.

6. Ausserordentliche Nutzung

Werden Einsätze von Informatikmitteln geplant, die den allgemein üblichen Umfang übersteigen oder den Betrieb gefährden könnten (z.B. Netzwerkbelastung, Sicherheit), so ist dafür die Zustimmung des IT-Sicherheitsbeauftragten einzuholen.

BenutzerInnen, die durch ihre ordnungsgemässe Tätigkeit die Möglichkeit zur Einsicht in personelle und andere vertrauliche Geschäftsdaten haben, unterstehen besonderen Verpflichtungen wie den allgemeinen Datenschutzbestimmungen sowie den personalrechtlichen Erlassen. Sie haben zum Schutz dieser Daten die nötigen Vorkehrungen zu treffen.

7. Datenschutz

Jeglicher Einsatz von Informatikmitteln, der die Privatsphäre oder die Persönlichkeit von Personen verletzen könnte, ist untersagt.

Personendaten und Finanzdaten dürfen nur soweit erfasst, verarbeitet und weitergegeben werden, als dies zur Ausführung der anvertrauten Aufgabe notwendig ist. Die einschlägigen Gesetze und Verordnungen zum Datenschutz und zur Archivierung sind einzuhalten.

Die BenutzerInnen von Informatikmitteln sind dafür verantwortlich, keinerlei Fahrlässigkeit zu begehen, die ermöglichen, dass Daten durch unbefugte Dritte missbräuchlich verwendet werden können.

©PUBLICS

8. Verpflichtungen der BenutzerInnen

Informatikmittel müssen sorgfältig, verantwortungsvoll, sicher und ökonomisch eingesetzt werden.

BenutzerInnen sind für den fachlich und rechtlich korrekten Einsatz und Umgang mit den ihnen zur Verfügung stehenden Informatikmittel verantwortlich. Sie haben alles zu vermeiden, was den Betrieb beeinträchtigen, Schäden am System oder bei anderen BenutzerInnen verursachen könnte.

Die BenutzerInnen sind verpflichtet, das ihnen Zumutbare zu unternehmen, um zu verhindern, dass Malware (Viren etc.) auf die Informatikmittel übertragen wird. Sie haben dazu den Empfehlungen des IT-Sicherheitsbeauftragten zu folgen.

Zum rechtlich korrekten Einsatz gehören insbesondere die Beachtung von Urheber- und Lizenzrechten, Bestimmungen zum Schutz der Persönlichkeit sowie der strafrechtlichen Bestimmungen über Pornographie und Rassendiskriminierung.

BenutzerInnen sind ausserdem verpflichtet, die zur Verfügung gestellten Anleitungen zur Benutzung zu beachten.

©PUBLICS

9. Massnahmen bei Verstössen

E-Mail- und Internet-Verkehr werden protokolliert.

Aufgezeichnet werden:
- Internetzugriffe (Datum, Zeit, URL, Adresse) Aufbewahrungszeit: 2 Monate.
- E-Mail Versand oder Empfang an externe Empfänger (kein Inhalt). Aufbewahrungszeit:2 Monate
- Zugriffe auf Netzwerkkomponenten wie Switches oder Router. Aufbewahrungszeit: 2 Monate.

Diese Aufzeichnungen sind vertraulich und dienen ausschliesslich zur Kontrolle der Einhaltung dieser Richtlinien.

Bei Verdacht auf missbräuchliche Nutzung können die Aufzeichnungen nach Mitteilung an den Betroffenen ausgewertet werden.
Bei Verstössen entscheidet Gemeindeschreiber von sich aus oder auf Antrag des IT-Sicherheitsbeauftragten über die weitere Nutzung dieser Aufzeichnungen wie z.B.:

- Beweislieferung an Behörden (Polizei) im Falle einer Strafuntersuchung
- Anonymisierte statistische Auswertungen
- Fehlerdiagnose bei Problemen (Mail ist nicht angekommen, etc.)

Liegt ein Verstoss, der die Sicherheit der gesamten Infrastruktur oder die Integrität der Daten gefährdet vor, können weitere Aufzeichnungen (Aufbewahrungszeit 2 Monate):angeordnet werden wie:
- Zugriffe auf Dateien
- Zugriffe auf Datenbanken
- Zugriffe auf Server oder andere Geräte
- Den Netzwerkverkehr zwischen bestimmten Geräten

Bei Zuwiderhandlungen gegen diese Weisung kann der Gemeindeschreiber von sich aus oder auf Antrag des IT-Sicherheitsbeauftragten ungeachtet einer allfälligen strafrechtlichen Ahndung oder Schadenersatzforderungen einer fehlbaren Person:

- den Zugang zu den Informatikmitteln einschränken
- oder ihr den Zugang vollständig untersagen;
- sowie disziplinarische Massnahmen anordnen.

Die infolge grobfahrlässigen oder vorsätzlichen Missbrauchs verursachten Kosten (Aufklärung, Sanktionierung, Untersuchungs-, Gerichts- und Anwaltskosten) kann die Verwaltung auf den fehlbaren Nutzer abwälzen.
Vorbehalten bleiben weitere arbeitsrechtliche, disziplinarische und strafrechtliche Massnahmen durch entsprechende Stellen.

Der IT-Sicherheitsbeauftragte kann die folgenden Massnahmen anordnen:

- Blockierung missbräuchlicher oder rechtswidriger Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken,
- Löschung missbräuchlicher oder rechtswidriger Daten, soweit dies aus Sicherheitsgründen erforderlich ist.

©PUBLICS

10. Inkrafttreten

Diese Weisung tritt per 1.2.2013 in Kraft und gilt bis zum Widerruf durch die herausgebende oder deren vorgesetzte Stelle.

©PUBLICS