Gemeinde
Oberengstringen

Oberengstringen, 1. Februar 2015

Weisung zur Informationssicherheit

Inhalt

1 Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (IKT-Mittel). Im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand der Weisung ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten).

Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

1.2 Geltungsbereich

Die Weisung gilt für alle Mitarbeitenden der Gemeinde.

Als Mitarbeitende der Gemeinde im Sinne dieser Weisung gelten alle fest oder temporär angestellten Mitarbeitenden der Gemeindeverwaltung sowie die Behörden- und Kommissionsmitglieder.

1.3 Grundlagen

Die rechtlichen Grundlagen sind:
- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Gemeindegesetz (GG, LS 131.1)
- Informatiksicherheitsverordnung (LS 170.8)

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.
Grundlage dieser Weisung bildet zudem die Leitlinie zur Informationssicherheit.

2 Verantwortung

2.1 Informationssicherheitsverantwortliche/r

Die Gemeinde bezeichnet eine Informationssicherheitsverantwortliche oder einen Informationssicherheitsverantwortlichen (nachfolgend ISV). Diese bzw. dieser ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse. Sie bzw. er ist befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen.

2.2 Mitarbeitende

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

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 an und Verlust von Hardware und Software der bzw. dem ISV.

3 Datenschutz und Informationssicherheit

3.1 Zugangs- und Zugriffsschutz

Die Mitarbeitenden haben zu verhindern, dass Unbefugte Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) in den Büroräumlichkeiten auf, ist dafür zu sorgen, dass diese keinen unbefugten Zugang zu Informationen erhalten.

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen des Büros, Sperren oder Herunterfahren des PCs).

Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkonti oder die ihnen zugeteilten funktionellen Konti verwenden. Sie sind für die auf ihre Konti erfolgten Zugriffe verantwortlich.

Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

Der Verlust von Schlüsseln, Badges, Chipkarten usw. ist umgehend der oder dem ISV zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist die oder der ISV umgehend zu informieren.

Austretende Behördenmitglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die

ihnen zugänglich waren und die ausserhalb der Gemeindeverwaltung bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder der Verwaltung zurückgegeben wurden.

3.2 Passwörter

Passwörter sind vertraulich zu behandeln. Sie dürfen nicht aufgeschrieben, unverschlüsselt auf Systemen gespeichert oder anderen Personen (z.B. Vorgesetzten, Informatikverantwortlichen [nachfolgend IV], ISV usw.) bekannt gegeben werden.

Passwörter müssen mindestens acht Stellen lang sein und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten.

Leicht erratbare Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden.

Passwörter müssen regelmässig (alle 90 Tage) gewechselt werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind.

Ein früher bereits benutztes Passwort darf nicht mehr gewählt werden.

Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert. Gleiches gilt, wenn sie unautorisierten Personen bekannt geworden sind.

Initialpasswörter müssen sofort geändert werden.

3.3 Datensicherung, -löschung und Entsorgung von Informationsträgern

Geschäftsbezogene Daten müssen auf Serverlaufwerken gespeichert werden.

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. Shreddern).

3.4 Virenschutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder um konfigurieren.

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 und Links sollen keinesfalls geöffnet werden.

Jeder Verdacht auf Virenbefall muss sofort der bzw. dem ISV gemeldet werden.

3.5 Hard- und Software

Die Mitarbeitenden dürfen keine Software und keine Hardware-Erweiterungen, insbesondere keine Kommunikationseinrichtungen und externe Massenspeicher installieren bzw. anschliessen.

Die Mitarbeitenden dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des Gemeinde-Netzwerkes verbinden.

Nur die bzw. der IV darf Geräte, welche im Eigentum der Gemeinde sind, in die Reparatur oder zur Entsorgung geben. Sie bzw. er stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Amtsstelle verlassen.

Änderungen an der Systemeinstellung (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur vom Administrator vorgenommen werden.

4 Nutzung von E-Mail und Internet

4.1 Allgemeine Bestimmungen

E-Mail und Internet werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit und des Datenschutzes eingesetzt.

4.2 E-Mail

Externe Internet-Dienste (wie z.B. Online-Dateiablagen, Online-Kalender usw.) oder E-Mail-Systeme dürfen nicht für geschäftliche Zwecke verwendet werden.

E-Mails mit vertraulichem Inhalt (z.B. besondere Personendaten) müssen verschlüsselt versandt werden. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden.

Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt. Bei mehrtägigen Abwesenheiten ist die Funktion des Abwesenheitsassistenten zu nutzen.

Das E-Mail-System darf in zurückhaltendem Masse auch für private Zwecke verwendet werden. Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, mit unnötig grossem Verteiler oder mit der Aufforderung zum Weiterversand im Schneeballsystem ist verboten.

Private E-Mails müssen entweder gelöscht oder in einem persönlichen Ordner mit der Bezeichnung „PRIVAT" abgelegt werden.

4.3 Internet / Internet-Dienste

Der Zugriff auf Internet-Seiten mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt und der zu privaten Zwecken erfolgende Zugriff auf Plauderboxen („chat"), Tauschbörsen und Online-Ticker ist verboten.

Das Herunterladen und Installieren von Spielen sowie Audio- und Videodateien aus dem Internet ist nicht gestattet. Die Gemeindeschreiberin bzw. der Gemeindeschreiber kann das Herunterladen oder die Installation solcher Dateien erlauben.

Geschäftsrelevante Daten dürfen nur mit dem formellen Einverständnis der Gemeindeschreiberin bzw. des Gemeindeschreibers im Internet publiziert oder z.B. in Formularen bekannt gegeben werden.

Schützenswerte Informationen (besondere Personendaten) und grosse Mengen nicht anonymisierter Personendaten dürfen nur verschlüsselt (z.B. mit https) über das Internet übermittelt werden.

Die Nutzung Sozialer Netzwerke (Facebook, XING etc.) ist nicht erlaubt.

5 Private Nutzung von IKT-Mitteln

Die zurückhaltende Benützung von IKT-Mittel für private Zwecke ist grundsätzlich gestattet, soweit dadurch die Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden.

Die private Nutzung soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

Geschäftsdaten dürfen nicht privat genutzt oder in privaten Datenablagen gespeichert werden.

Systemkomponenten und Peripheriegeräte dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden.

Private Geräte dürfen nur mit Bewilligung der bzw. des ISV für dienstliche Aufgaben eingesetzt oder mit dem produktiven Netzwerk verbunden werden.

Private Daten müssen lokal in einem persönlichen Verzeichnis mit der Bezeichnung „PRIVAT“ oder auf dem persönlichen Netzwerklaufwerk „H:\“ abgespeichert werden.

6 Einsatz mobiler Geräte

Auf mobilen Geräten (z.B. Notebooks, USB-Datenträger, Smartphones usw.) müssen Dokumente mit vertraulichem bzw. schützenswertem Inhalt verschlüsselt gespeichert werden.

Mobile Arbeitsgeräte müssen mit einem Boot-Passwort geschützt werden.

Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung verantwortlich.

Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.

Die Geräte dürfen nicht Dritten zur Nutzung überlassen werden.

Der Verlust eines mobilen Gerätes ist unverzüglich der bzw. dem ISV zu melden.

Es dürfen keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung der bzw. des IV einzuholen.
Eine Verbindung zu drahtlosen Netzwerken (z.B. WLAN) ist nur zulässig, wenn eine Verschlüsselung eingesetzt wird.

Drahtlose Komponenten (z.B. Bluetooth, WLAN, Infrarot etc.) sind bei Nichtgebrauch zu deaktivieren.

Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

7 Ausnahmen

Die oder der ISV entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail einzureichen.

8 Protokollierung und Kontrolle

Zur Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit der Informatik werden Systeme eingesetzt, die Protokolle und Warnmeldungen erzeugen.

Internetzugriffe werden aufgezeichnet und ein halbes Jahr gespeichert. Eine personenbezogene Auswertung ist nur nach vorgängiger Information des Benutzenden möglich.

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

Oberengstringen, 1. Dezember 2014

André Bender, Gemeindepräsident Peter Menzi Gemeindeschreiber

....

Der/Die Mitarbeiter/in hat die Weisung zur Informationssicherheit gelesen und bestätigt mit seiner/ihrer Unterschrift, diese einzuhalten.

Name Mitarbeiter/in

.....

Gemeinde Oberengstringen

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
Fax 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch

Diese Weisung ist auf der Grundlage des Datenschutzbeauftragten des Kantons Zürich entstanden.