REGENSDORF

Weisung Informationssicherheit

In Kraft seit 1. Oktober 2021

ICT
Watterstrasse 116
8105 Regensdorf
T: 044 842 36 11
kanzlei@regensdorf.ch
www.regensdorf.ch

Inhalt

Anmerkung

Entsprechend dem Grundsatz der Gleichberechtigung von Mann und Frau gelten alle Bezeichnungen, ungeachtet der männlichen Sprachform, für beide Geschlechter.

Weisung Informationssicherheit

1. Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (IT-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 fest oder temporär angestellten Mitarbeitenden sowie für die Behördenmitglieder der Gemeinde Regensdorf mit Ausnahme der von der Primarschule angestellten Mitarbeitenden.

1.3 Grundlagen

Die rechtlichen Grundlagen der Gemeinde Regensdorf sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Informatiksicherheitsverordnung (ISV, LS 170.8)
- Personalverordnung Gemeinde Regensdorf
- Vollzugsverordnung zur Personalverordnung Regensdorf (insbesondere Kapitel VI. Home Office)

2. Verantwortung

2.1 Informationssicherheitsverantwortliche / -sicherheitsverantwortlicher

Informationssicherheitsverantwortliche / Informationssicherheitsverantwortlicher der Gemeinde Regensdorf (nachfolgend ISV) ist die/der Leiter/in ICT. Der / die ISV ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse. Sie / er ist befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen.

Die weiteren Funktionen im Zusammenhang mit der ICT sind (die Personen werden mit separatem Beschluss bestimmt)

- Leiter/in ICT
- ICT-Administrator/in
- ICT-Administrator/in-Stv.
- ICT-Administrator-Stv. 2 (ohne spez. Funktion, wird vom ICT Administrator bestimmt)
- Verantwortliche/r Homepage

2.2 Mitarbeitende sowie weitere Funktionäre und Behördenmitglieder

Die Mitarbeitenden sowie alle weiteren Funktionäre und Behördenmitglieder sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten.

Sie sind verpflichtet, die ihnen zur Verfügung gestellten IT-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 umgehend der / dem ISV.

3. Datenschutz und Informationssicherheit

3.1 Zugangs- und Zugriffsschutz

Halten sich externe Personen (z.B. Servicetechniker usw.) in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Ab-schliessen von Türen und Verschliessen von Fenstern des Büros, Abschliessen weiterer Räume gemäss Anweisung des ISV, Sperren oder Herunterfahren des PC). Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen. Wo Bildschirmsperren von den Mitarbeitenden selbst eingerichtet werden können, sind sie zu benützen. Vom ISV angeordnete Bildschirmsperren dürfen nicht ausgeschaltet werden.

Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich. Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist nicht erlaubt.

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 Personen stellen sicher, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Gemeinde Regensdorf bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht, der Datenträger muss formatiert werden, i.d.R. rechte Maustaste) oder zurückgegeben wurden.

3.2 Passwörter

Passwörter sind vertraulich zu behandeln. Sie sind verschlüsselt zu speichern und vor Unbefugten zu schützen. Dies gilt insbesondere, wenn Passwörter für den persönlichen Gebrauch notiert werden (beispielsweise mit einem Passwortmanager). Anderen Personen (zum Beispiel Vorgesetzten, IT-Verantwortlichen, ISV usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben.

Passwörter müssen mindestens acht Stellen lang sein und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten. Leicht zu erratende 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 sollten alle sechs Monate geändert 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 den gemeinsam nutzbaren Serverlaufwerken, insbesondere in der Geschäftverwaltungssoftware CMI, gespeichert werden. Die / der ISV sorgt für eine regelmässige Sicherung aller Geschäftsdaten und die sichere Lagerung der dazu benötigten Archivmedien.

Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht, der Datenträger muss formatiert werden, i.d.R. rechte Maustaste). Nicht mehr benötigte Informationsträger (z.B. USB-Datenträger, CD-ROM usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. Schreddern).

3.4 Virenschutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder ihre Konfiguration verändern. E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Links auf Websites sollen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort der / dem ISV gemeldet werden.

3.5 Hard- und Software

Bei der Installation oder beim Anschluss von Software- und Hardware-Erweiterungen (insbesondere Kommunikationseinrichtungen und externe Massen-speicher) ist besondere Vorsicht walten zu lassen.

Nur die beziehungsweise der IT-Verantwortliche darf Geräte in die Reparatur oder zur Entsorgung geben. Sie beziehungsweise er stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Amtsstelle verlassen.

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur durch die zuständige Stelle (zum Beispiel Administrator/-in) 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. Neue Mitarbeitende werden durch die Personalstelle auf die vorliegende Weisung aufmerksam gemacht.

4.2 E-Mail

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

Das E-Mail-System darf in zurückhaltendem Mass auch für private Zwecke verwendet werden. Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt oder 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 / Internetdienste

Der Zugriff auf Websites mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist verboten.

Das Herunterladen und Installieren von Software aus dem Internet ist nicht gestattet. Der oder die ISV kann das Herunterladen oder die Installation solcher Dateien erlauben.

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

4.4 Outlook Kalender

Alle geschäftlichen Termine sind im persönlichen Kalender des Programmes Outlook einzutragen. Private Termine können als "Privat" gekennzeichnet werden, sodass anderen Personen keine Details angezeigt werden. Outlook ist so konfiguriert, dass die geschäftlichen Termine für alle Mitarbeitenden einsehbar sind. Pendenzen und Aufgaben sind nicht als Termin einzutragen, sondern als "Aufgabe".

Für die Mitarbeitenden der Gemeindepolizei gilt diese Bestimmung nicht.

5. Private Nutzung von IT-Mitteln

Die zurückhaltende Benützung von IT-Mitteln 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 und kann von der vorgesetzten Stelle verboten werden. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken. Geschäftsdaten dürfen nicht privat genutzt oder in privaten Datenablagen gespeichert werden. Private Daten müssen lokal in einem persönlichen Verzeichnis mit der Bezeichnung «privat» oder auf dem persönlichen Netzwerklaufwerk «H» gespeichert werden.

Systemkomponenten und Peripheriegeräte dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden. Über Ausnahmen entscheidet der / die ISV.

6. Einsatz mobiler Geräte

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Mobile Arbeitsgeräte (zum Beispiel Notebooks, USB-Datenträger, Smartphones) müssen mit einem Passwort geschützt werden.
- Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst für die lokale Datensicherung und die datenschutzgerechte Aufbewahrung verantwortlich.

Grundsätzlich werden die Daten jedoch in der Citrix-Umgebung gespeichert (Netzlaufwerke). Diese Daten werden täglich gesichert.

- Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.
- Die Geräte dürfen grundsätzlich nicht Dritten zur Nutzung überlassen werden.

Für Geräte, welche sich im Besitz der Gemeinde befinden gilt zusätzlich:

- Der Verlust eines mobilen Gerätes ist unverzüglich der / dem ISV zu melden.
- Es dürfen keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung der / des ISV einzuholen.
- Eine Verbindung zu drahtlosen Netzwerken (zum Beispiel WLAN) ist nur zulässig, wenn eine Verschlüsselung (Zugang mit Passwort) eingesetzt wird.
- Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

7. Homeoffice

Mitarbeitenden, welchen das Arbeiten im Homeoffice gewährt wurde, haben den Leitfaden des Datenschutzbeauftragten dsb "Regeln für das Homeoffice" und die Vollzugsverordnung zur Personalverordnung Regensdorf (insbesondere Kapitel VI. Home Office) zu studieren und zu befolgen.

8. Videokonferenzen

Kommen Videokonferenzsysteme zum Einsatz, müssen allfällig separat erlassene Vorgaben und Bestimmungen befolgt werden.

9. Ausnahmen

Die oder der ISV entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail einzureichen. In einzelnen Bereichen, wie zum Beispiel der Jugendarbeit, der ausserschulischen Betreuung etc. können zusätzliche Handlungsanweisungen im Zusammenhang mit den Sozialen Medien (Facebook, Instagram, WhatsApp etc.) erlassen werden. Diese Weisungen müssen vom ISV genehmigt werden.

10. 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 6 Monate gespeichert. Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin respektive des Benutzers zulässig.

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

11. Inkraftsetzung

Diese Weisung wurde vom Gemeinderat erlassen und per 1. Oktober 2021 in Kraft gesetzt. Sie ersetzt alle vorangegangenen Weisungen.

Regensdorf, 24. August 2021

Gemeinderat Regensdorf

Max Walter	Stefan Pfyl
Präsident	Schreiber