Gemeinde
Birmensdorf

Reglement Informationssicherheit

vom 14. Dezember 2020

Behördenerlass des Gemeinderates

Inhaltsverzeichnis

I. Allgemeine Bestimmungen

Art. 1 **Grundlagen**

[1]Auf kommunaler Ebene bildet Art. 20 Ziff. 6 der Gemeindeordnung der Politischen Gemeinde Birmensdorf (GO) die rechtliche Grundlage für dieses Reglement Informationssicherheit.

[2]Auf kantonaler Ebene bilden die folgenden Erlasse die Grundlage für dieses Reglement Informationssicherheit:

a) Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007;

b) Verordnung über die Information und den Datenschutz (IDV) vom 28. Mai 2008;

c) Informatiksicherheitsverordnung (ISV) vom 17. Dezember 1997.

[3]Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.

[4]Grundlage für dieses Reglement Informationssicherheit sind überdies die jeweiligen Informatiksicherheitsrichtlinien der Regionales Informatikzentrum RIZ AG, Wetzikon (RIZ AG).

Art. 2 **Zweck**

[1]Dieses Reglement Informationssicherheit bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

[2]Dieses Reglement Informationssicherheit und die jeweiligen Informatiksicherheitsrichtlinien der RIZ AG bedingen und ergänzen sich wechselseitig.

Art. 3 **Geltung**

[1]Dieses Reglement Informationssicherheit gilt für alle Angestellten gemäss Art. 4 der Personalverordnung sowie für die Behördenmitglieder der Politischen Gemeinde Birmensdorf.

[2]Der Geltungsbereich der Informatiksicherheitsrichtlinien der RIZ AG bestimmt sich nach den jeweiligen Bestimmungen der Informatiksicherheitsrichtlinien der RIZ AG.

Art. 4 **Ziel**

[1]Dieses Reglement Informationssicherheit regelt die Nutzung der Informations- und Kommunikationstechnologie (ICT-Mittel), im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte.

[2]Ziel dieses Reglements Informationssicherheit ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten).

II. Verantwortung

Art. 5 **Informationssicherheitsverantwortliche/r**

[1]Die Gemeindeschreiberin oder der Gemeindeschreiber hat die Funktion der oder des Informationssicherheitsverantwortlichen der Politischen Gemeinde Birmensdorf.

[2]Die oder der Informationssicherheitsverantwortliche ist für die Umsetzung dieses Reglements Informationssicherheit verantwortlich und ist Ansprechperson für Fragen und für sicherheitsrelevante Vorkommnisse.

[3]Die oder der Informationssicherheitsverantwortliche ist befugt, den Angestellten sowie den Behördenmitgliedern Weisungen bezüglich Informationssicherheit zu erteilen.

Art. 6 **Zentrale Dienste**

Die Zentralen Dienste sind zuständig für die Bereitstellung der ICT-Mittel und sind zugleich Verbindungsstelle zur RIZ AG.

Art. 7 **Angestellte und Behördenmitglieder**

[1]Die Angestellten und Behördenmitglieder sind verpflichtet, die gesetzlichen Vorgaben, dieses Reglement Informationssicherheit und andere interne Regelungen zu beachten. Sie haben die Kenntnisnahme dieses Reglements Informationssicherheit sowie der Informatiksicherheitsrichtlinien der RIZ AG unterschriftlich zu bestätigen.

[2]Die Angestellten und Behördenmitglieder sind verpflichtet, die ihnen zur Verfügung gestellten ICT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen.

[3]Die Angestellten und Behördenmitglieder melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Hardware und Software der oder dem Informationssicherheitsverantwortlichen.

III. Datenschutz und Informationssicherheit

Art. 8 **Zugangs- und Zugriffsschutz**

[1]Die Angestellten und Behördenmitglieder sorgen dafür, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

[2]Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen von Türen und Verschliessen von Fenstern des Büros, Abschliessen weiterer Räume gemäss Anweisung der oder des Informationssicherheitsverantwortlichen, 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. Von der oder vom Informationssicherheitsverantwortlichen angeordnete Bildschirmsperren dürfen nicht ausgeschaltet werden.

[3]Die Angestellten und Behördenmitglieder 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 verboten.

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

[5]Austretende Angestellte und Behördenmittglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Arbeitsräumlichkeiten bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden.

Art. 9 **Passwörter**

[1]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 oder

Stellen (z.B. Vorgesetzten, Zentralen Diensten, Informationssicherheitsverantwortlichen usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben.

[2]Die Bildung der Passwörter muss den Informatiksicherheitsrichtlinien der RIZ AG (Punkt 7) entsprechen. 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. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind.

[3]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.

Art. 10 **Datensicherung, -löschung und Entsorgung von Informationsträgern**

[1]Geschäftsbezogene Daten müssen in der GEschäftsVERwaltung BrainCONNECT und/oder auf Serverlaufwerken gespeichert werden.

[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. USB-Datenträger, CD-ROM usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. Schreddern).

Art. 11 **Virenschutz**

Die Angestellten und Behördenmitglieder 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 oder dem Informationssicherheitsverantwortlichen gemeldet werden.

Art. 12 **Hard- und Software**

[1]Die Angestellten und Behördenmitglieder 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 internen Netzwerks verbinden.

[2]Nur die Zentralen Dienste dürfen Geräte in die Reparatur oder zur Entsorgung geben. Die Zentralen Dienste stellen sicher, dass keine schützenswerten Daten auf diesem Weg die Gemeindeverwaltung verlassen.

[3]Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur durch die RIZ AG vorgenommen werden.

IV. Nutzung von E-Mail und Internet

Art. 13 **Grundsätzliches**

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

[2]Die Angestellten und Behördenmitglieder haben sich unterschriftlich zur Einhaltung der Nutzungsvorschriften zu verpflichten.

Art. 14 **E-Mail**

[1]Externe Internetdienste (zum Beispiel Online-Dateiablagen, Online-Kalender) oder E-Mail-Systeme dürfen nicht für geschäftliche Zwecke verwendet werden.

[2]E-Mails mit vertraulichem Inhalt (zum Beispiel besondere Personendaten) müssen verschlüsselt versandt werden. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden.

[3]Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt. Bei Abwesenheiten von mehr als 1 Arbeitstag ist die Funktion des Abwesenheitsassistenten zu nutzen.

[4]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, 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.

Art. 15 **Internet / Internetdienste**

[1]Der Zugriff auf Websites mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt und der zu privaten Zwecken erfolgende Zugriff auf Chatprogramme, Tauschbörsen und Online-Ticker sind verboten. Das Herunterladen und Installieren von Software aus dem Internet ist nicht gestattet. Die oder der Informationssicherheitsverantwortliche kann das Herunterladen oder die Installation solcher Dateien erlauben.

[2]Geschäftsrelevante Daten dürfen nur mit dem formellen Einverständnis der oder des Informationssicherheitsverantwortlichen im Internet publiziert oder zum Beispiel in Formularen bekannt gegeben werden.

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

[4]Die private Nutzung sozialer Netzwerke (z.B. Facebook, Xing usw.) soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

V. Private Nutzung von ICT-Mitteln

Art. 16 **Grundsätzliches**

[1]Die zurückhaltende Benützung von ICT-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. 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.

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

[3]Private Geräte dürfen nur mit Bewilligung der oder des Informationssicherheitsverantwortlichen für dienstliche Aufgaben eingesetzt oder mit dem produktiven Netzwerk verbunden werden.

VI. Einsatz mobiler Geräte

Art. 17 **Voraussetzungen**

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

a) Auf mobilen Geräten (zum Beispiel Notebooks, USB-Datenträger, Smartphones) müssen Dokumente mit vertraulichem beziehungsweise schützenswertem Inhalt verschlüsselt gespeichert werden.

b) Mobile Arbeitsgeräte müssen mit einem Boot-Passwort geschützt werden.

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

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

e) Die Geräte dürfen nicht Dritten zur Nutzung überlassen werden.

f) Der Verlust eines mobilen Gerätes ist unverzüglich der oder dem Informationssicherheitsverantwortlichen zu melden.

g) Es dürfen keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung der Zentralen Dienste einzuholen.

h) Eine Verbindung zu drahtlosen Netzwerken (zum Beispiel WLAN) ist nur zulässig, wenn eine Verschlüsselung eingesetzt wird.

i) Drahtlose Komponenten (zum Beispiel Bluetooth, WLAN, NFC) sind bei Nichtgebrauch zu deaktivieren.

j) Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

VII. Ausnahmen

Art. 18 **Zuständigkeit**

Die oder der Informationssicherheitsverantwortliche entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail an gemeinde@birmensdorf.ch einzureichen.

VIII. Protokollierung und Kontrolle

Art. 19 **Grundsätzliches**

[1]Zur Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit der ICT-Mittel werden Systeme eingesetzt, die Protokolle und Warnmeldungen erzeugen. Die Kontrollen und Protokollierung werden ausschliesslich von der RIZ AG vorgenommen.

[2]Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin respektive des Benutzers möglich. Zuständig für die Anordnung ist die Anstellungsinstanz gemäss Art. 5 Abs. 1 der Personalverordnung; gegebenenfalls unter Information des Gemeinderates.

Art. 20 **Konsequenzen**

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

IX. Schlussbestimmungen

Art. 21 **Bisheriges Recht**

Bisheriges Recht, das im Widerspruch zu den Bestimmungen dieses Reglements Informationssicherheit oder der Informatiksicherheitsrichtlinien der RIZ AG steht, wird auf den Zeitpunkt des Inkrafttretens dieses Reglements Informationssicherheit für nicht anwendbar erklärt.

Art. 22 **Inkrafttreten**

Dieses Reglement Informationssicherheit tritt rückwirkend per 7. Dezember 2020 in Kraft.

Genehmigt vom Gemeinderat
am 14. Dezember 2020 (GRB 594)

Gemeinderat Birmensdorf

Bruno Knecht	Andreas Strahm
Präsident	Schreiber