gemeinde mönchaltorf

Weisung der Gemeinde Mönchaltorf zur Informationssicherheit und zum Datenschutz

gültig ab 1. Juli 2026

1. Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

Diese Weisung regelt den Gebrauch von E-Mail und Internet und die Verwendung mobiler, geschäftlich genutzter Geräte. Gegenstand der Weisung ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten) zur Gewährleistung des Datenschutzes.

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 Behörden- und Kommissionsmitglieder. Für den Schulbereich gelten separate Bestimmungen.

1.3 Grundlagen

Die Grundlagen der Gemeinde sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Dokumenten wie Leitlinie, allgemein Richtlinie für Informationssicherheit und Datenschutz und technische Richtlinie für den Betrieb von Informationssystemen oder Weisungen sowie die entsprechenden Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.

2. Verantwortung

2.1 Informationssicherheitsverantwortliche/ Informationssicherheitsverantwortlicher (ISV)

Die/der ISV ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle bei Fragen und bei sicherheitsrelevanten Vorkommnissen. Sie/er ist befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen. Die/der ISV kann die operativen Tätigkeiten für die Umsetzung der Minimalanforderungen delegieren.

2.2 Mitarbeitende, Behörden- und Kommissionsmitglieder

2.2.1 Grundsatz

Die Mitarbeitenden sowie Behörden- und Kommissionsmitglieder sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten und Informationen ausschliesslich gemäss diesen Vorgaben zu bearbeiten. Sie haben die Kenntnisnahme dieser Weisung durch Unterzeichnung der Erklärung über die Nutzung von Internet, E-Mail sowie zur Informationssicherheit zu bestätigten.

Die Mitarbeitenden sowie Behörden- und Kommissionsmitglieder sind verpflichtet, die ihnen zur Verfügung gestellten Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen.

2.2.2 Bei Informationssicherheitsvorfällen

Die Kenntnisnahme von Informationssicherheitsvorfällen sowie Schäden und Verlust von Hard- und Software sind durch die Mitarbeitenden sofort an die bzw. den ISV sowie die Vorgesetzte/den Vorgesetzten zu melden. Wer zudem feststellt, dass Informationen gefährdet, abhandengekommen oder missbraucht worden sind, hat dies ebenfalls umgehend zu melden.

Mögliche Informationssicherheitsvorfälle sind (nicht abschliessend):
- Verlust, unbeabsichtigte Löschung oder Vernichtung von Daten, unberechtigte Kopien von Daten oder von Datenträgern
- Veränderung oder Manipulation von Informationen
- Unberechtigter Zugriff oder Bekanntgabe an Unbefugte
- Funktionalität eines oder mehrerer Informationssysteme gestört

3. Klassifikation von Informationen

3.1 Grundsätze
Jede physische und elektronische Information kann in die Kategorien «Öffentlich», «Intern», «Vertraulich» oder «Geheim» zugeteilt werden. Wer Informationen bearbeitet, ist für die Einhaltung der Informationssicherheitsvorschriften entsprechend diesen Kategorien verantwortlich.

Ist nicht ohne weiteres erkennbar, ob eine Information als vertraulich oder geheim einzustufen ist, beispielsweise weil sie nicht im entsprechenden System abgelegt ist, ist explizit bei Weitergabe in geeigneter Form darauf hinzuweisen.

3.2 Kategorien
Informationen werden als «**Öffentlich**» klassifiziert, wenn sie der Öffentlichkeit zugänglich sein dürfen.
Informationen werden als «**Vertraulich**» klassifiziert, wenn sie nur für einen definierten Benutzerkreis zugänglich sein sollen und/oder wenn durch deren Bekanntmachung (auch innerhalb der Verwaltung) ein wesentlicher Schaden verursacht werden könnte.
Informationen werden als «**Geheim**» eingestuft, wenn Unberechtigte durch deren Kenntnisnahme den Interessen der Gemeinde einen schweren Schaden zufügen könnten.
Informationen gelten als «**Intern**», wenn sie keiner anderen Klassifizierung zugewiesen werden.

3.3 Schutzmassnahmen
Bei «**Öffentlichen**» Informationen ist die Integrität der Informationen (Richtigkeit, Vollständigkeit, Unverfälschtheit, usw.) sicherzustellen.
«**Interne**» Informationen müssen zusätzlich zugriffsbeschränkt aufbewahrt bzw. gespeichert werden.
«**Vertrauliche**» Informationen müssen zusätzlich an einem abschliessbaren Ort aufbewahrt werden. Der Zugriff muss auf einen namentlich oder funktionsbezogenen definierten Personenkreis beschränkt sein. Die Weitergabe nach aussen ist nur bei anerkannten Gründen und unter entsprechenden Sicherheitsmassnahmen zulässig. Der Versand in physischer Form darf nur in einem fest verschlossenen Umschlag erfolgen. Der elektronische Versand von vertraulichen Dokumenten muss grundsätzlich verschlüsselt erfolgen.
«**Geheime**» Informationen müssen an einem stark gesicherten Ort aufbewahrt werden und stehen somit unter physischer Zugangskontrolle. Die elektronischen Daten sind lediglich an einem, dafür explizit definierten Speicherort auffindbar. Die zuständige Person führt eine schriftliche Kontrolle über die Ausgabe und den Verbleib der einzelnen nummerierten

physischen Dokumente oder bei elektronischen Dokumenten die nummerierten Informationsträger. Der Versand muss nachvollziehbar sein.
Um dies sicherzustellen, gilt grundsätzlich:
Elektronische Dokumente dürfen nur auf den dafür vorgesehenen Speicherorten abgelegt werden. Für physische Dokumente sind die dafür zugewiesenen Archive und Ablageorte zu verwenden.

4. Zugangs- und Zugriffsschutz

Die Mitarbeitenden sorgen dafür, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

Beim Verlassen des Arbeitsplatzes muss das „Clean-Desk"-Prinzip (aufgeräumter Arbeitsplatz) herrschen. Notebooks, USB-Sticks, Smartphones, Dokumente, Datenträger und anderen Unterlagen dürfen nicht am Arbeitsplatz unbeaufsichtigt herumliegen, eingesehen oder entwendet werden können. Es dürfen keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen von Türen und Verschliessen von Fenstern des Büros, Abschliessen weiterer Räume gemäss Anweisung des bzw. der ISV, Sperren oder Herunterfahren des PC).

Ausdrucke bei durch mehrere Personen genutzte Drucker sind umgehend aus dem Drucker zu entfernen. Bildschirmsperren sind, wo sie von den Mitarbeitenden selber eingerichtet werden können, zu benützen. Eingerichtete Bildschirmsperren dürfen nicht ausgeschaltet werden.

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

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 Verlust von Schlüsseln, Badges, Chipkarten oder Passwörtern 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.

Die Benutzeridentitäten ausgetretener Mitarbeiter müssen sofort deaktiviert und nach spätestens einem Monat gelöscht werden. Austretende Behördenmitglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (speziell besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Gemeinde bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden.

Austretende Personen haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und aus einem bestimmten Grund die ausserhalb der Gemeinde bearbeitet oder gespeichert wurden, unwiderruflich und vollständig gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden. Die Benutzeridentitäten der ausgetretenen Mitarbeitenden werden sofort deaktiviert und nach spätestens einem Monat gelöscht.

5. Passwörter

Passwörter müssen mindestens 12 Zeichen lang sein und eine Kombination aus mindestens drei der folgenden Kategorien enthalten:

- Grossbuchstabe
- Kleinbuchstabe
- Ziffer
- Sonderzeichen

Geschäftlich genutzte Passwörter dürfen nicht auch privat eingesetzt werden. Passwörter 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.

Passwörter und PINs sind vertraulich zu behandeln. Sie dürfen nicht aufgeschrieben werden. Sie sind verschlüsselt zu speichern und vor Unbefugten zu schützen. Dies gilt beispielsweise, wenn Passwörter für den persönlichen Gebrauch gespeichert werden (z.B. mit einem Passwortmanager). Anderen Personen (Vorgesetzten, ISV usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben.

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.

6. Datensicherung, -löschung und Entsorgung

Geschäftliche Daten müssen an den dafür vorgesehenen Ablageorten gespeichert werden. Der damit beauftragte Dienstleister sorgt für eine regelmässige Sicherung aller relevanten Daten und die sichere Lagerung der dazu benötigten Archivmedien.

Nicht mehr benötigte Daten müssen von Datenträgern wie USB-Datenträger oder Speicherkarten unwiederbringlich gelöscht werden. Einfaches Löschen genügt nicht. Nicht mehr benötigte Datenträger (z.B. USB-Datenträger, CD-ROM usw.), die sensitive Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. durch Schreddern).

Jeder Verwaltungsbereich bereinigt einmal jährlich die elektronisch abgespeicherten Daten und informiert dem Informationssicherheitsverantwortlichen nach den abgeschlossenen Bereinigungsarbeiten über deren Umsetzung. Die elektronisch abgelegten Daten werden entsprechend dem aktuellen Organisationshandbuch und Registraturplan der Gemeindeverwaltung Mönchaltorf abgespeichert.

7. Verwendung und Installation von Hard- und Software

Änderungen an den Systemeinstellungen dürfen nur vom externen Dienstleister auf entsprechenden Auftrag der oder des ICT-Verantwortlichen vorgenommen werden.

Die Mitarbeitenden dürfen die Sicherheitssoftware wie Virenschutz oder Firewall nicht ausschalten, blockieren oder ihre Konfiguration verändern.

Die Mitarbeitenden dürfen ohne Bewilligung der bzw. des ICT-Verantwortlichen keine Software und keine Hardware-Erweiterungen installieren oder anschliessen, insbesondere keine Kommunikationseinrichtungen und externen Massenspeicher. Jeder Verdacht auf Virenbefall ist sofort der/dem ICT-Verantwortlichen zu melden.

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

Nur der damit beauftragte IT-Dienstleister im Auftrag der oder des ICT-Verantwortlichen darf Geräte in die Reparatur oder zur Entsorgung geben. Der Dienstleister stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Amtsstelle verlassen.

8. Nutzung von Internet, E-Mail und mobilen Geräten

E-Mail und Internet werden für die Erfüllung geschäftlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Informationssicherheit und des Datenschutzes eingesetzt. Die Mitarbeitenden haben sich unterschriftlich zur Einhaltung der Nutzungsvorschriften zu verpflichten.

Externe, von der Gemeinde nicht genehmigte Dienste, dürfen nicht für geschäftliche Zwecke verwendet werden. Dies betrifft beispielsweise Online-Dateiablagen, Online-Kalender oder Webmail.

8.1 E-Mail

E-Mails mit sensitivem Inhalt wie besonderen Personendaten müssen ohne Einwilligung der betroffenen Person grundsätzlich verschlüsselt versandt werden. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden.
Das automatische Weiterleiten von E-Mails, die Verwendung einer privaten Mailadresse durch Mitarbeitende und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt. Bei mehrtägigen Abwesenheiten ist die Funktion des Abwesenheitsassistenten zu nutzen. Die IT ist befugt, bei Abwesenheiten eigenständig den Abwesenheitsassistenten einzurichten.

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

E-Mails mit unbekanntem Absender, verdächtiger Betreffzeile oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Links auf Websites sind nur in Absprache zu öffnen.

8.2 Internet

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

und Installieren von Software aus dem Internet sind nicht gestattet. Die oder der ICT-Verantwortliche kann das Herunterladen oder die Installation solcher Dateien erlauben.

Schützenswerte Informationen und grosse Mengen nicht anonymisierter Personendaten dürfen nur verschlüsselt über das Internet übermittelt werden, zum Beispiel über eine https-Verbindung.

Die Nutzung sozialer Netzwerke (LinkedIn, Instagram usw.) zu privaten Zwecken ist während der Arbeitszeit nicht erlaubt.

8.3 Weitere Bestimmungen zur privaten Nutzung

Die zurückhaltende Nutzung 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. Geschäftliche Daten 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 abgespeichert werden.

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

8.4 Nutzung mobiler Geräte und mobiles Arbeiten

Die Gemeinde Mönchaltdorf setzt teilweise private mobile Geräte zur geschäftlichen Nutzung ein (beispielsweise für die obligatorische Notfall-App). Beim Einsatz mobiler Geräte sind generell folgende Punkte zu beachten:

- Auf mobilen Geräten ist die langfristige Speicherung von geschäftlichen Daten nicht erlaubt. Zwischenspeicher wie der Downloadordner sind wieder zu löschen.
- Private und geschäftliche Nutzung der Geräte sind zu trennen, entsprechende Software zur Unterstützung einer solchen Trennung ist zu verwenden. Alle geschäftlich genutzten Geräte sind entsprechend zu registrieren.
- Die Daten/Der Display sind vor Einsicht von Dritten und vor physischem Zugriff durch Dritte zu schützen. Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden. Mobile Geräte dürfen Dritten nicht zur Nutzung überlassen werden, ohne dass der Zugang zu den geschäftlichen Daten gesperrt ist.
- Mobile Systeme sind mit einem Passwort, PIN-Code, Fingerabdruck etc. zu schützen. Für den Zugriff von ausserhalb der Räumlichkeiten der Verwaltung ist eine Zwei-Faktor-Authentifizierung zu verwenden.
- Der Verlust eines mobilen Gerätes ist unverzüglich der respektive dem ISV zu melden.
- Betriebssystem und Software sind regelmässig zu aktualisieren. Apps sind vor der Installation auf ihren Inhalt und ihre Quelle zu prüfen. Geschäftliche Daten sind nur in einer sicheren WLAN-Umgebung abzurufen.

Von der IT installierte Sicherheitsmassnahmen dürfen nicht deaktiviert werden. Die Gemeinde sorgt wo nötig für eine Verschlüsselung der Systeme.

Für das mobile Arbeiten gilt zudem das Reglement «Homeoffice». Das mobile Arbeiten oder der Einsatz von mobilen Geräten sind von dem Gemeindeschreiber/der Gemeinschreiberin zu genehmigen.

8.5 Protokollierung und Auswertung

Aktivitäten der Benutzenden auf den Systemen der Gemeinde können aus Gründen der Nachvollziehbarkeitspflicht wie auch der Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit aufgezeichnet und ein halbes Jahr gespeichert werden.

Sollte ein dieser Weisung widersprechendes oder rechtswidriges Verhalten oder ein Verhalten, das weitere Pflichten schwerwiegend verletzt, festgestellt werden, so können Massnahmen zur Identifizierung der Verfehlenden eingeleitet werden. Eine personenbezogene Auswertung darf grundsätzlich nur nach vorgängiger Information der Benutzerin respektive des Benutzers vorgenommen werden, soweit dieser bekannt ist.

8.6 Verwendung von Wechselmedien

Der Einsatz von nicht genehmigten Wechselmedien ist verboten. Wechselmedien, die vertrauliche oder geheime Informationen enthalten, müssen gesichert aufbewahrt werden, um den Datenverlust oder -diebstahl zu vermeiden. Verluste von Wechselmedien müssen der oder dem ICT-Verantwortlichen gemeldet werden. Wechselmedien müssen mit einem Passwortschutz versehen und durch Verschlüsselung geschützt werden.
Sie müssen zuerst gelöscht werden, bevor sie erneut zum Einsatz kommen. Die Wechselmedien werden ausschliesslich von dem oder der ICT-Verantwortlichen oder einer dafür beauftragten Drittperson mit einer dafür anerkannten, sicheren Methode gelöscht oder physisch zerstört. Eine physische Übergabe darf nur an eine autorisierte Person erfolgen und muss bei geheimen oder vertraulichen Informationen protokolliert werden.
Jede Information, die auf einem Wechselmedium abgelegt ist, muss zusätzlich auf dem dafür vorgesehenen Ablageort gesichert sein.

9. Regelung von Ausnahmen

Die oder der ISV entscheidet über Ausnahmen von dieser Weisung. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail einzureichen und zur Nachvollziehbarkeit zu dokumentieren. Für jede Ausnahme ist ein Zeitpunkt, eine Dauer, die antragsstellende sowie verantwortliche Person zu definieren. Die bestehenden Ausnahmen sind periodisch zu überprüfen.

10. Schlussbestimmungen

11.1 Rechtsfolgen

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

11.2 Genehmigung und Inkrafttreten

Die Weisung der Gemeinde Mönchaltorf zur Informationssicherheit und zum Datenschutz ersetzt die bisherige, wurde von der Gemeindeschreiberin am 2. Juni 2026 genehmigt und tritt per 1. Juli 2026 in Kraft. Sie ersetzt die bisherige Version von Februar 2018.