Pfungen
Leben an der Töss

# Weisung zur Informationssicherheit

vom 25. November 2019

## Änderungsverlauf

| Version | Datum | Text | Instanz |
|---|---|---|---|
| 2019 | 25.11.2019 | Weisung zur Informationssicherheit in der Gemeinde Pfungen | Gemeinderat GRB Nr. 206 |

## Inhaltsverzeichnis

## 1. Allgemeine Bestimmungen

**Art. 1**

*Gegenstand*

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).

**Art. 2**

*Zweck*

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

**Art. 3**

*Geltungsbereich*

Die Weisung gilt für alle fest oder temporär angestellten Mitarbeitenden sowie für die Behördenmitglieder der der Gemeinde Pfungen

**Art. 4**

*Grundlagen*

1. Die rechtlichen Grundlagen der Gemeinde Pfungen sind:
   - Gesetz über die Information und den Datenschutz
   - Verordnung über die Information und den Datenschutz
   - Informatiksicherheitsverordnung
2. Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.
3. Grundlage dieser Weisung bildet zudem die Leitlinie zur Informationssicherheit

## 2. Verantwortung

**Art. 5**

*Informationssicherheitsverantwortliche/r*

Die Gemeindeschreiberin / der Gemeindeschreiber hat die Rolle als Informationssicherheitsverantwortliche / Informationssicherheitsverantwortlichen (nachfolgend ISV) benannt. 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.

**Art. 6**

*Mitarbeitende*

1. Die Mitarbeitenden sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten. Sie haben die Kenntnisnahme dieser Weisung unterschriftlich zu bestätigen.
2. Die Mitarbeitenden 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 der / dem ISV.

## 3. Datenschutz und Informationssicherheit

### Art. 7

*Zugangs- und Zugriffsschutz*

1. Die Mitarbeitenden 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 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.

3. 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 verboten.

4. 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.

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

### Art. 8

*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 (zum Beispiel Vorgesetzten, IT-Verantwortlichen, ISV usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben.

2. 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 regelmässig 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.

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. 9**

*Datensicherung, -löschung und Entsorgung von Informationsträgern*

[1] Geschäftsbezogene Daten müssen auf Serverlaufwerken gespeichert werden. Die / der ISV sorgt für eine regelmässige Sicherung aller Geschäftsdaten und die sichere Lagerung der dazu benötigten Archivmedien.

[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. 10**

*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.

**Art. 11**

*Hard- und Software*

[1] 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 internen Netzwerks verbinden.

[2] 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.

[3] 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

**Art. 12**

*Allgemeine Bestimmungen*

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

**Art. 13**

*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 mehrtägigen Abwesenheiten 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. 14**

*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. Der oder die ISV kann das Herunterladen oder die Installation solcher Dateien erlauben.

[2] Geschäftsrelevante Daten dürfen nur mit dem formellen Einverständnis der verantwortlichen Person 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 (Facebook, Xing usw.) soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

## 5. Private Nutzung von IT-Mitteln

**Art. 15**

*Private Nutzung von IT-Mitteln*

[1] 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. 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 gespeichert werden.

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

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

**Art. 16**

*Einsatz mobiler Geräte*

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Auf mobilen Geräten (zum Beispiel Notebooks, USB-Datenträger, Smartphones) müssen Dokumente mit vertraulichem beziehungsweise 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 respektive dem ISV zu melden.
- Es dürfen keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung der respektive des IT-Verantwortlichen einzuholen.
- Eine Verbindung zu drahtlosen Netzwerken (zum Beispiel WLAN) ist nur zulässig, wenn eine Verschlüsselung eingesetzt wird.
- Drahtlose Komponenten (zum Beispiel Bluetooth, WLAN, NFC) sind bei Nichtgebrauch zu deaktivieren.
- Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

**Art. 17**

*Ausnahmen*

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

## 6. Schlussbestimmungen

**Art. 18**

*Akten der Ressortleiter*

[1.] 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 der Benutzerin respektive des Benutzers möglich.

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

**Art. 19**

*Inkrafttreten*

Der Gemeinderat setzt die vorliegende Weisung zur Informationssicherheit per 1. Dezember 2019 in Kraft.

Pfungen, 25. November 2019

Gemeinderat Pfungen

Max Rütimann
Gemeindepräsident

Stephan Brügel
Gemeindeschreiber