Weisung zur Informationssicherheit der Stadt Adliswil

vom 14. November 2014

Stadt Adliswil

Inhaltsverzeichnis

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 sowie die Verwendung mobiler Geräte. Weiter wird der verantwortungsvolle Umgang mit Informationen, insbesondere mit Personendaten, thematisiert.

Das Einhalten und Umsetzen der Massnahmen bezweckt den Schutz der Informationen in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität.

1.2. Geltungsbereich

Die Weisung gilt für alle Mitarbeitenden der Stadt Adliswil. Als Mitarbeitende im Sinne dieser Weisung gelten alle fest oder temporär angestellten Mitarbeitenden und Dritte, sofern sie Zugang zu den Informatikmitteln der Verwaltung haben.

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)
- Informatiksicherheitsverordnung (LS 170.8)
- Gemeindegesetz (GG, LS 131.1)

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

In der Stadt Adliswil ist der Leiter/die Leiterin Informatik für die Informationssicherheit verantwortlich. Dieser/diese Informationssicherheitsverantwortliche/r (nachfolgend ISV) 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 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.

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. Bildschirmsperren sind, wo sie von den Mitarbeitenden selber eingerichtet werden können, zu benützen. Vom ISV eingerichtete 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 verboten. Mitarbeitende, die durch ihre ordnungsmässige Tätigkeit die Möglichkeit zur Einsicht in personelle und andere vertrauliche Geschäftsdaten haben, unterstehen besonderen Verpflichtungen wie den allgemeinen Datenschutzbestimmungen sowie den personalrechtlichen Erlassen. Sie haben zum Schutz dieser Daten die nötigen Vorkehrungen zu treffen und die Anweisungen vorgesetzter Stellen zu befolgen. Personen- und Finanzdaten dürfen nur soweit erfasst, verarbeitet und weitergegeben werden, als dies zur Ausführung der anvertrauten Aufgabe notwendig ist. Die einschlägigen Gesetze und Verordnungen zum Informations- und Datenschutz und zur Archivierung sind einzuhalten.

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.

3.2. Passwörter

Passwörter sind vertraulich zu behandeln. Sie dürfen nicht aufgeschrieben, unverschlüsselt auf Systemen gespeichert oder anderen Personen bekannt gegeben werden.

Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind zu vermeiden. 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. 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.) durch die Informatikabteilung gelöscht werden. 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 umkonfigurieren. 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 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 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 Informatikabteilung darf Geräte in die Reparatur oder zur Entsorgung geben. Sie stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Stadtverwaltung verlassen. Änderungen an der Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur von der Informatikabteilung 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. Werden Einsätze von Informatikmitteln geplant, die den allgemein üblichen Umfang übersteigen oder den Betrieb gefährden können (z.B. Netzwerkbelastung, Sicherheit), so ist dafür die Zustimmung des ISV einzuholen.

4.2. E-Mail

Externe Internet-Dienste (i.d.R. Online-Dateiablagen, Online-Kalender usw.) oder E-Mail-Systeme dürfen nur für geschäftliche Zwecke verwendet werden, wenn sie von der Stadtverwaltung zur Verfügung gestellt 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.

4.3. Internet / Internet-Dienste

Der Zugriff auf Internet-Seiten mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist verboten. Das Herunterladen und Installieren von Spielen sowie Audio- und Videodateien aus dem Internet ist nicht gestattet. Die Verwaltungsleitung kann das Herunterladen oder die Installation solcher Dateien erlauben.

Geschäftsrelevante Daten dürfen nur mit dem formellen Einverständnis der Verwaltungsleitung 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 usw.) darf nur ausserhalb der Arbeitszeit oder für geschäftliche Zwecke erfolgen.

5. Private Nutzung von IKT-Mitteln

Die zurückhaltende Benützung von IKT-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.

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 abgespeichert werden.

6. Einsatz mobiler Geräte

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.

7. Ausnahmen

Die Verwaltungsleitung 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. Eine personenbezogene Auswertung kann von der Verwaltungsleitung in Auftrag gegeben werden, wenn der Verdacht auf ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit besteht.

9. Massnahmen bei Verstössen

Bei Zuwiderhandeln gegen diese Weisung kann die Verwaltungsleitung von sich aus oder auf Antrag der ISV einer fehlbaren Person:

- den Zugang zu den Informatikmitteln einschränken
- sowie disziplinarische Massnahmen anordnen.
- Blockierung missbräuchlicher oder rechtswidriger Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken
- Löschung missbräuchlicher oder rechtswidriger Daten, soweit dies aus Sicherheitsgründen erforderlich ist.

Die infolge grobfahrlässigen oder vorsätzlichen Missbrauchs verursachten Kosten (Aufklärung, Sanktionierung, Untersuchungs-, Gerichts- und Anwaltskosten) kann die Verwaltungsleitung auf den fehlbaren Nutzer abwälzen.

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

Adliswil, 14. 11. 14

Geschäftsleiterin

Stadt Adliswil