Vorlage Selbstdeklaration

Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit der [Gemeinde/Stadt]

Erläuterung zur Vorlage

Die Vorlage Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit ist Teil einer Dokumentenreihe, die sämtliche relevanten Informationssicherheitsdokumente für einen Datenschutzreview mit Selbstdeklaration umfasst. Die empfohlene Vorgehensweise, die Hilfestellungen und die Erläuterungen zu den Vorlagen sind dem Leitfaden Datenschutzreview mit Selbstdeklaration zu entnehmen.

Die Vorlage ist den jeweiligen Gegebenheiten anzupassen. Die anzupassenden Punkte befinden sich in eckigen Klammern [ ].

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Erklärung zur Informationssicherheit sowie über die Nutzung von Internet und E-Mail der [Gemeinde/Stadt]

Die Mitarbeitenden sind verpflichtet, diese Nutzungsvorschriften sowie die Regelungen gemäss Weisung zur Informationssicherheit und Datenschutz (nachfolgend Weisung) der [Gemeinde/Stadt] vom [Datum] einzuhalten.

Internet und E-Mail werden zur Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Informationssicherheit und des Datenschutzes eingesetzt. Vertrauliche Informationen und besondere Personendaten sind verschlüsselt zu übermitteln.

Die Nutzung von E-Mail und Internet während der Arbeitszeit für private Zwecke ist auf ein Minimum zu beschränken. Ausgehende private E-Mails sind in der Betreffzeile als privat zu bezeichnen, um die Unterscheidung zur dienstlichen Kommunikation sicherzustellen. Eingehende private E-Mails sind in einem als privat gekennzeichneten Ordner abzulegen und möglichst bald zu löschen.

Unzulässig sind

* die Anwahl oder Nutzung von Websites mit rechtswidrigem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt,
* das Verbreiten von rechtswidrigem, rassistischem, sittlich oder religiös anstössigem oder illegalem Inhalt,
* das Versenden von E-Mails mit unnötig grossem Verteiler oder mit der Aufforderung zum Weiterversand im Schneeballsystem,
* der unverschlüsselte Versand von externen E-Mails, die besondere Personendaten oder vertrauliche Informationen enthalten,
* die automatische Umleitung (Forwarding) von E-Mails an externe E-Mail-Adressen,
* das Speichern von vertraulichen Personendaten und Informationen auf privaten Speichermedien (z.B. USB, SD, externe HD zu nicht dienstlichen oder privaten Zwecken),
* das Herunterladen oder die Installation von Spielen sowie Audio- und Videodateien aus dem Internet ohne Bewilligung.

Untersagt zu privaten Zwecken sind

* das Ablegen von dienstlichen E-Mail-Adressen im Internet,
* die Benutzung von sozialen und anderen interaktiven Medien während der Arbeitszeit.

Anonymisierte Aufzeichnungen über die Internetzugriffe können jederzeit erstellt werden. Bei einem konkreten Verdacht auf einen Verstoss gegen die Nutzungsvorschriften respektive die Weisung können die Internetzugriffe oder der E-Mail-Verkehr personenbezogen ausgewertet werden. In beiden Fällen erfolgt vor der Auswertung eine Ankündigung. Ein Verstoss gegen diese Nutzungsvorschriften respektive die Weisung kann personalrechtliche Konsequenzen zur Folge haben. Bei einem Verstoss gegen strafrechtliche Bestimmungen und bei Verletzung von Rechten Dritter muss mit straf- respektive zivilrechtlichen Konsequenzen gerechnet werden.

OPTIONAL: Erklärung zur Nutzung von mobilen IKT-Systemen der [Gemeinde/Stadt]

Bei der Nutzung von mobilen IKT-Systemen für dienstliche Zwecke sind folgende Anforderungen einzuhalten:

* Private und dienstliche Nutzung der Geräte ist zu trennen, entsprechende Software zur Unterstützung einer solchen Trennung und zum Schutz von Verwaltungsdaten ist zu verwenden.
* Beim Arbeiten mit mobilen IKT-Systemen sind diese vor Einsicht von Dritten zu schützen.
* Mobile IKT-Systeme sind vor physischem Zugriff durch Dritte zu schützen.
* Betriebssystem und Software auf mobilen IKT-Systemen sind regelmässig zu aktualisieren.
* Mobile IKT-Systeme sind mit einem Passwort, PIN-Code, Fingerabdruck etc. zu schützen.
* Sicherheitsmassnahmen an mobilen Geräten dürfen nicht deaktiviert werden (Firewall, Virenschutz, Betriebssystem-Manipulationen etc.).
* Mobile IKT-Systeme sind zu verschlüsseln, wenn technisch möglich.
* Der Verlust von mobilen IKT-Systemen ist unverzüglich der bzw. dem Informationssicherheitsverantwortlichen zu melden.
* Die Benutzerin/der Benutzer erklärt sich damit einverstanden, dass ein Gerät im Notfall einer Fernlöschung unterzogen werden kann, wo dies vorgesehen und möglich ist.

Die/der Unterzeichnende erklärt, die Nutzungsvorschriften sowie die Weisung Informationssicherheit zur Kenntnis genommen und verstanden zu haben.

Ort und Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

V 1.2 / Dezember 2023