Duggingen

Nr. 0.02.04

Informatik-Richtlinien

vom 18.03.2014

Inhaltsverzeichnis

Einleitung

Das vorliegende Dokument enthält die Informatik-Richtlinien (kurz: IT-Richtlinien) der Gemeinde Duggingen.

Gültigkeit und Verbindlichkeit

Die IT-Richtlinien treten mit dem Gemeinderatsentscheid vom dd.mm.2014 in Kraft und sind bis zum Widerruf oder deren Erneuerung gültig.

Die IT-Sicherheit der Gemeinde und der Schule[1)] ist nur gewährleistet, wenn die Verantwortung von jedem einzelnen Mitarbeitenden wahrgenommen wird. Dazu unterstützend dienen IT-technische Massnahmen. Zudem schützen die IT-Richtlinien die Mitarbeitenden bei ihrer täglichen Arbeit.

Deshalb sind die IT-Richtlinien für sämtliche Mitarbeitenden sowie Externe und Besucher jederzeit verbindlich. Die Mitarbeitenden sind für die Einhaltung der IT-Richtlinien persönlich verantwortlich.

Zweck der IT-Richtlinien

Die IT-Richtlinien haben den Zweck die Sicherheit der innerhalb der Gemeinde vorhandenen elektronischen Informationen und Daten sowie die Mitarbeitenden zu schützen.

Die verantwortungsvolle Anwendung der IT-Richtlinien dient dem Kundennutzen sowie dem Image der Gemeindeangestellten. Dadurch nimmt die Gemeinde sowie ihre Mitarbeitenden die Pflichten gegenüber sämtlichen Kunden sowie der Allgemeinheit wahr.

Grundsätzlich ist bei Unsicherheiten mit den IT-Richtlinien oder deren Anwendung der IT-Verantwortliche der Gemeinde zu kontaktieren.

Dokument

Für die Aktualität und regelmässige Überprüfung des vorliegenden Dokuments „IT-Richtlinien“ ist der IT-Verantwortliche der Gemeinde zuständig.

[1)] Hinweis: Der Umgang mit den ICT-Unterrichtsmitteln der Primarschule und des Kindergartens ist gesondert geregelt.

Begriffsdefinitionen

Rollen und Bezeichnungen

Die unterschiedlichen Rollen im Zusammenhang mit den IT-Richtlinien und deren Bezeichnung sind nachfolgend beschrieben.

Mitarbeitende
Unter Mitarbeitende werden die arbeitsvertraglichen Angestellten der Gemeindeverwaltung sowie der Schulleitung und des Schulsekretariats verstanden. Ist eine spezifische Mitarbeitende-Gruppe gemeint, wird dies explizit erwähnt.

Behörden- und Kommissionsmitglieder
Unter Behörden- und Kommissionsmitglieder werden sämtliche im Miliz-Verhältnis beauftragte Personen verstanden, welche für die Gemeinde tätig sind. Ist eine spezifische Gruppe gemeint, wird dies explizit erwähnt.

Benutzer
Unter Benutzer werden sämtliche Personen verstanden, welche berechtigterweise die IT-Infrastruktur der Gemeinde zur Ausführung von Gemeinde-Tätigkeiten verwenden.

IT-Verantwortlicher
Der Gemeindeverwalter hat die Verantwortung bezüglich sämtlicher Informatik-Mittel und -Belangen.

Zudem vergibt der IT-Verantwortliche oder dessen Stellvertreter als einziger Aufgaben an den externen Dienstleister. Der IT-Verantwortliche entscheidet im Rahmen der festgelegten Finanzkompetenzen und des bewilligten Budgets über die jeweilige Freigabe oder Ablehnung bei kostenpflichtigen Aufgaben des externen IT-Dienstleisters.

Externer IT-Dienstleister
Der externe IT-Dienstleister verantwortet die Administration, den Unterhalt und den Support sowie die Aktualität der gesamten IT-Infrastruktur. Das Ausführen von beauftragten Support- oder anderweitigen IT-Aufträgen gehört ebenfalls zu dessen Aufgaben. Sind Drittfirmen involviert, übernimmt ebenso der externe IT-Dienstleister deren Koordination. Bei allen Aufgaben gilt die Sorgfalts- und Sicherheitspflicht des externen IT-Dienstleisters.

Der externe IT-Dienstleister ist zudem verpflichtet, vor einer kostenpflichtigen Aufgabe den IT-Verantwortlichen der Gemeinde, um dessen Freigabe nachzufragen.

Private vs. dienstliche Daten
Die Gemeinde definiert die Begriffe wie nachfolgend beschrieben.

Private Daten:

- Private Daten haben nichts mit der Gemeinde oder deren dienstlichen Aktivitäten gemeinsam.
- Dabei handelt es sich um private Daten von Mitarbeitenden, bei welchen die Gemeinde in keiner Art und Weise die Verantwortung oder Haftung übernimmt.

Dienstliche Daten:

- Dienstliche Daten haben immer einen Zusammenhang mit den dienstlichen Aktivitäten der Gemeinde bzw. eines Mitarbeitenden.

Dabei kann es sich um Daten handeln, welche die Mitarbeitenden bei der Ausführung ihrer Aufgaben erstellen, jedoch zu einem gewissen Zeitpunkt nicht allgemein zugänglich sein sollen oder dürfen. Meistens entstehen diese bei vorbereitenden oder vertraulichen Aufgaben.

Informatik-Richtlinien

Die Sicherheit der Informatik-Infrastruktur und deren Anwendung richtet sich nach der Datenschutzgesetzgebung (siehe Beilagen und den vorgegebenen Bestimmungen zur Behörden- und Verwaltungstätigkeit auf eidgenössischer, kantonaler und kommunaler Ebene.

Bei der Anwendung der IT-Geräte und Applikationen gilt für den Mitarbeitenden sowie für die Behörden- und Kommissionsmitglieder die Sorgfaltspflicht. Er/Sie verantwortet ebenso den sicheren und gesetzeskonformen Umgang mit den dienstlichen Daten und Informationen.

IT-Geräte

Die Gemeinde Duggingen stellt ihren Mitarbeitenden (mit Ausnahme der Lehrpersonen, Behörden- und Kommissionsmitglieder) sämtliche für die Arbeit erforderlichen IT-Geräte zur Verfügung. Diese sind entsprechend zu nutzen.

Die Behörden- und Kommissionsmitglieder dürfen die IT-Geräte nach Absprache mit dem IT-Verantwortlichen für Gemeinde-Aufgaben nutzen. Der IT-Verantwortliche kann im Bereich seiner Kompetenzen die Nutzung freigeben oder verweigern.

Bei der Anwendung der IT-Geräte gilt die Sorgfaltspflicht für alle Benutzer. Bei Unsicherheit in der Anwendung oder allfällige Auffälligkeiten ist der IT-Verantwortliche zu kontaktieren.

Die Wartung, der Unterhalt, allfällige Erweiterungen oder die Erneuerung sämtlicher(!) IT-Geräte obliegt der Gemeindeverwaltung bzw. dem externen Dienstleister. Mitarbeitende oder Dritte sind ohne expliziten Auftrag nicht befugt, Änderungen an den IT-Geräten vorzunehmen. Ebenso dürfen an den IT-Geräten keine Konfigurations- oder Software-Veränderungen vorgenommen werden, ausdrücklich keine sicherheitsrelevanten Änderungen beim Virenschutz, der Firewall, dem Benutzerkonto, etc.

IT-Plattform Windows

Die Gemeinde hat sich für die Windows-Plattform entschieden, deshalb sind sämtliche IT-Dienste und Anwendungen für diese Plattform optimiert und ausgerichtet. Anderweitige Systeme werden nicht unterstützt, dürfen jedoch z. B. für den Fernzugriff auf eigenes Risiko benutzt werden.

Sperrung der Arbeitsplatzrechner

Die Sperrung der Arbeitsplatzrechner bei Nichtgebrauch erfolgt jeweils nach 10 Minuten automatisch.

Grundsätzlich wird jedoch beim Verlassen des Arbeitsplatzes jedem Mitarbeitenden empfohlen, den Arbeitsplatzrechner manuell zu sperren.

Beim Arbeitsabschluss sind die Arbeitsplatzrechner mittels der Funktion „Herunterfahren“ auszuschalten.

Mobile IT-Geräte (Laptop)

Auch bei den Laptops gelten die oben erwähnten Bestimmungen. Bei deren Anwendung ist jedoch besondere Achtsamkeit geboten. Insbesondere ist bei unbeaufsichtigtem Nichtgebrauch die passwortgeschützte Sperre der Geräte zwingend zu aktivieren.

Die Verwendung der Geräte ausserhalb des Gemeindebereiches ist erlaubt. Allerdings ist jeweils vorgängig der IT-Verantwortliche zu informieren, dieser hat das Recht die Herausgabe zu bewilligen oder abzulehnen.

Externe Speichergeräte

In dienstlich begründeten Fällen darf ein externes Speichergerät (UBS-Sticks, etc.) zur Bearbeitung von Daten ausserhalb der Gemeinderäumlichkeiten verwendet werden. Jedoch muss der Nutzer sicherstellen, dass nach der Bearbeitung auf dem verwendeten Drittgerät keine Gemeinde-Daten oder -Informationen verbleiben.

Private oder fremde IT-Geräte

Der Einsatz von fremden oder privaten IT-Geräten zu dienstlichen Zwecken ist erlaubt. Jedoch muss der Nutzer sicherstellen, dass nach der Bearbeitung oder bei der Auflösung des Arbeitsverhältnisses auf dem verwendeten Drittgerät keine Gemeinde-Daten oder -Informationen verbleiben.

Der Zugriff auf das Gemeinde-Netzwerk mit fremden Geräten ist nicht erlaubt, mit Ausnahme der Drucker.

Eine Unterstützung durch den IT-Verantwortlichen oder den externen IT-Dienstleister wird für Fremd-Geräte nicht angeboten (Ausnahme siehe Kapitel „Anwendungs-Support“).

Diebstahl oder Verlust
Wurde ein Gerät gestohlen oder wird es vermisst, ist unverzüglich der IT-Verantwortliche zu informieren. Dies gilt auch für fremde oder private IT-Geräte, wenn sich darauf Gemeinde-Daten oder Informationen befinden.

Privater Gebrauch Gemeinde-Infrastruktur
Der Gebrauch der IT-Geräte während der Arbeitszeit für private Zwecke ist erlaubt, jedoch auf ein absolutes Minimum zu reduzieren. Ausserhalb der Arbeitszeit ist der Gebrauch für private Zwecke erlaubt. In beiden Fällen ist jedoch die Einhaltung der vorliegenden IT-Richtlinien zwingend.

Die Nutzung erfolgt auf eigenes Risiko, es besteht kein Rechtsanspruch für private Informationen oder Daten gegenüber der Gemeinde.

Durch die private Nutzung dürfen der Gemeinde weder erhöhte Risiken noch Mehrkosten entstehen, die dienstliche Nutzung darf in keiner Art und Weise beeinträchtigt werden.

Benutzerkonten und Passwörter
Das personifizierte Benutzerkonto und dessen Passwort sind persönlich und vertraulich für den jeweiligen Mitarbeitenden. Ebenso gilt dies für die Behörden- und Kommissionsmitglieder, welche über ein persönliches Benutzer- und/oder E-Mail-Konto verfügen. Eine Weitergabe innerhalb oder ausserhalb der Gemeinde ist nicht erlaubt. Dies gilt für die Windows-Anmeldung sowie für sämtliche Applikationen.

Passwörter und/oder Benutzernamen dürfen nicht elektronisch gespeichert werden, weder auf den Arbeitsplatzrechnern noch auf mobilen Geräten wie Tablets, Smartphones, etc.! Auch dürfen keine solchen Notizen an irgendwelchen IT-Geräten selbst angebracht werden.

Der Passwortspeicher eines Browsers (Internetexplorer, Firefox, Chrome, Safari, etc.) darf nicht für dienstliche Anwendungen genutzt werden. Dies gilt auch für mobile Geräte.

Administratoren-Konten
Die Administratoren-Konten der Benutzerverwaltung oder von Applikationen dürfen nicht für die tägliche Arbeit genutzt werden. Diese sind nur in technisch zwingenden Fällen oder im Notfall zu verwenden zur IT-Administration zu benutzen.

Der externe IT-Dienstleister verfügt über ein personifiziertes Administratoren-Konto, darüber erbringt er nachvollziehbar seine Dienstleistungen.

Die Administratoren-Passwörter sind vom IT-Verantwortlichen an einem sicheren Ort aufzubewahren. Bei einer Änderung der Passwörter informiert der externe IT-Dienstleister den IT-Verantwortlichen der Gemeinde unverzüglich. Die Administratoren-Passwörter dürfen nicht elektronisch übermittelt werden.

Austrittsregelung
Beim Austritt eines Mitarbeitenden werden die einzelnen Benutzerkonten am Ende des letzten Arbeitstags deaktiviert, an welchen der Mitarbeitende noch Tätigkeiten für die Gemeinde ausführt (Ferien etc. gelten nicht als Arbeitstage). Die Löschung erfolgt 30 Tage nach dem offiziellen Austritt bzw. der letzten Lohn- oder Aufwandentschädigungszahlung.

Stellvertretung
Die Stellvertretungs-Funktionen innerhalb der Applikationen sind zu nutzen. Verfügt die Applikation über keine explizite Funktionalität, ist die Stellvertretung durch die entsprechenden Zugriffs-Berechtigungen zu beantragen.

Passwortwechsel
Es wird aus Sicherheitsgründen empfohlen die Passwörter, wo möglich und nicht automatisiert, mindestens einmal halbjährlich zu ändern. Das Passwort sollte, wenn möglich, mindestens zwei nummerische Zeichen enthalten.

Folgende Passwörter dürfen nicht verwendet werden:

- Eigener Name oder Vorname
- Eigener Benutzernamen
- Gemeindename „Duggingen“ in irgendeiner Form

Allgemeine öffentlich bekannte Passwörter oder Kombinationen mit den Ausdrücken wie „Internet“, „Password“, „Passwort“ etc. Windows- und Fernzugriffs-Konto
In beiden Fällen ist der automatische Passwortwechsel aktiviert. Alle 90 Tage muss das Passwort geändert werden, das Letzte darf nicht wieder verwendet werden. Zudem muss das Passwort über mindestens 8 Zeichen verfügen.

Wurde zehn Mal eine falsche Eingabe gemacht, wird das Konto gesperrt. Für die Entsperrung muss aus Sicherheitsgründen der IT-Verantwortliche kontaktiert werden. Nur dieser darf den Entsperrungs-Auftrag dem externen IT-Dienstleister übergeben.

Fernzugriff
Die Gemeinderatsmitglieder sowie die Sozialhilfebehörde und die Schule (nur Schulleitung und Sekretariat) erhalten beim Amtsantritt den Fernzugriff automatisch. Ebenso wird der Fernzugriff zur Serviceerbringung im IT-Bereich für den externen IT-Dienstleister freigeschaltet.

Für die anderen Mitarbeitenden kann bei Bedarf und auf Antrag der Fernzugriff zur Verfügung gestellt werden. Jedoch ist ein entsprechender Antrag mit der Begründung an den IT-Verantwortlichen zu richten.

Die vorliegenden IT-Richtlinien, insbesondere der sorgfältige Umgang mit den Daten und Informationen sind vom Nutzer zwingend einzuhalten.

Beim Mitarbeitenden-Austritt oder Auflösung der dienstlichen Zusammenarbeit sind sämtliche Gemeinde-Daten und -Informationen vom Nutzer auf den Drittgeräten nicht wiederherstellbar zu löschen.

Der Anwendungssupport für den Fernzugriff ist im Kapitel „Anwendungs-Support“ geregelt.

Internet und E-Mail
Alle Mitarbeitenden sowie die Gemeinderatsmitglieder und Sozialhilfebehörden haben Zugriff auf das Internet (Web und E-Mail). Die zur Verfügung gestellten Internetdienste sind prinzipiell für dienstliche Zwecke zu nutzen. Die Notwendigkeit für deren Verwendung ergibt sich aus der jeweiligen Aufgabenstellung.

Internet
Der Zugriff auf Websites mit rassistischem, pornografischem und ähnlichem oder anderweitigen verletzlichen Inhalten ist verboten. Ebenso das Versenden solcher Inhalte mittels E-Mail. Der zufällige und sehr kurze Zugriff (aus Versehen / nicht erkennbarer Link) wird nicht als solcher bewertet. Die Verwendung von sozialen Netzwerken wie Facebook, Twitter etc. sind während der Arbeitszeit nicht erlaubt.

Der Gebrauch des Internets während der Arbeitszeit für private Zwecke ist auf ein absolutes Minimum zu reduzieren. Ausserhalb der Arbeitszeit ist der Gebrauch für private Zwecke erlaubt. Jedoch müssen immer die urheberrechtlichen, ethischen und gesetzlichen Regelungen eingehalten werden. Die private Nutzung darf der Gemeinde in keiner Art und Weise Schaden zu fügen. Ebenso ist das Herunterladen von grossen Datenmengen zu privaten Zwecken nicht erlaubt.

Die im Internet publizierten und für den dienstlichen Alltag relevanten Informationen, bei welchen z. B. der Autor oder Absender nicht bekannt ist, sind vor einer Verwendung bezüglich deren Echtheit, Gültigkeit und Glaubwürdigkeit zu überprüfen.

E-Mail
Das Weiterleiten von dienstlichen E-Mails und Daten, welche schützenswerte Personendaten enthalten, auf private E-Mail Konten, ist nicht erlaubt. Ebenso das Versenden von E-Mails mit schädlichem Code (z. B. Viren, Würmer, trojanischen Pferden, Spam etc.).

Der private E-Mailverkehr ist während der Arbeitszeit auf ein Minimum einzuschränken (nur für wirklich dringende private Angelegenheiten).

E-Mail Kalender (Outlook)
Der persönliche E-Mail Kalender ist innerhalb der jeweiligen Mitarbeitenden-Gruppe gegenseitig freizuschalten. Dies dient der Vereinfachung zu erledigenden Aufgaben und zum Beispiel auch bei unvorhergesehenen Abwesenheiten. Allfällige private Termine sind als „Privat“ zu kennzeichnen.

E-Mail Posteingang (Outlook)
Der persönliche E-Mail Posteingang ist innerhalb der jeweiligen Mitarbeitenden-Gruppe gegenseitig freizuschalten. Dies dient der Vereinfachung zu erledigenden Aufgaben bei (unvorhergesehenen) Abwesenheiten. Jedoch werden die E-Mails während einer Abwesenheit vom Stellvertreter nicht bearbeitet, dies dient lediglich für Notfallmassnahmen.

Der Stellvertreter darf nur die dienstlich relevanten E-Mails lesen, das Lesen von privat erkennbaren E-Mails ist aus Datenschutzgründen nicht erlaubt.

Allfällige private E-Mails sind von jedem Mitarbeitenden in einen Ordner namens „Privat“ zu verschieben.

E-Mail Abwesenheitsmeldung
Die nachfolgende Abwesenheitsmeldung ist im persönlichen E-Mail Konto zu hinterlegen und bei einer Abwesenheit zwingend zu aktivieren:

> Sehr geehrte Damen und Herren
>
> Ich bin vom „Wochentag“, xx. Monat 20xx bis „Wochentag“, xx. Monat 20xx abwesend. Ihre E-Mail wird weder gelesen, noch bearbeitet.
>
> In dringenden Fällen bitte ich Sie, sich an die Gemeindeverwaltung zu wenden (Tel. 061 756 99 00) oder Ihr Anliegen an gemeinde@duggingen.bl.ch zu senden.
>
> Mit freundlichen Grüssen
>
> Vorname Nachname

Verhaltensregeln ZID
Die Dienste des Internets und E-Mail werden vom Kanton erbracht. Deshalb gelten auch die Verhaltensregeln und Schutzmassnahmen der Zentralen Informatikdienste Basel-Landschaft (ZID) innerhalb der Gemeinde. Die Regeln befinden sich im Anhang A.

Protokollierung
Sämtlicher Internet- und E-Mail Verkehr wird protokolliert und kann im Bedarfsfall ausgewertet werden.

Nutzung WLAN-Zugriff Gemeinderatszimmer
Die Nutzung des nicht öffentlich sichtbaren und verschlüsselten WLAN Zugriffs im Gemeinderatszimmer ist für die Mitarbeitenden sowie für die Gemeinderatsmitglieder erlaubt. Die Zugriffsinformationen sind vertraulich und dürfen nicht an Dritte weitergegeben werden. Zudem wird das Passwort mindestens einmal jährlich geändert. Das jeweilige Passwort muss den Vorgaben der vorliegenden IT-Richtlinien entsprechen.

Der IT-Verantwortliche stellt sicher, dass der WLAN-Anschluss nur während den effektiv benötigten Zeiten zur Verfügung steht, danach ist dieser jeweils zu deaktivieren. Der Grund dafür ist u.a. der Jugendschutz, da sich die WLAN-Infrastruktur im Schulhaus befindet.

Applikationen

Sämtliche Applikationen, welche für die Ausführung der dienstlichen Tätigkeiten durch die Mitarbeitenden notwendig sind, werden von der Gemeinde im Rahmen der festgelegten Finanzkompetenzen und des bewilligten Budgets zur Verfügung gestellt. Die Installation, die Wartung, der Support sowie die Erneuerung obliegt ausschliesslich dem durch den IT-Verantwortlichen beauftragten externen IT-Dienstleister.

Benötigen die Mitarbeitenden eine zusätzliche Applikation, ist dies mittels Antrag beim IT-Verantwortlichen einzureichen.

Aus Sicherheitsgründen und urheberrechtlichen Gründen ist das Installieren oder Herunterladen von Applikationen aus dem Internet oder anderer Quellen nicht erlaubt.

Applikationsanwendung

Die dienstliche korrekte Anwendung der Applikationen und der sorgfältige Umgang mit den Daten liegen in der Verantwortung jedes Mitarbeitenden sowie dem Organisationseinheitsverantwortlichen.

(Raub-)Kopien der Applikationen durch Mitarbeitende dürfen wegen der Einhaltung der Lizenzbestimmungen nicht gemacht werden.

E-Mail Konten

Die Gemeinde stellt sämtlichen Mitarbeitenden sowie den Gemeinderatsmitgliedern ein E-Mail-Konto mit der Domäne „@duggingen.bl.ch“ zur Verfügung. Dieses ist für sämtliche dienstliche Zwecke zu verwenden.

Für das Bearbeiten der E-Mails wird deshalb für alle nicht Festangestellten der Fernzugriff durch die Gemeinde zur Verfügung gestellt. Ebenso ist es erlaubt die E-Mails auf einem privaten Smartphone oder Tablet, unter Einhaltung der IT-Richtlinien, zu synchronisieren.

Der direkte Fernzugriff auf die Plattform der zentralen Informatikdienste Basel-Landschaft (ZID) ist aus Kosten- und Datenaustausch-Gründen nicht verfügbar. Die einzige diesbezügliche Ausnahme bildet die Funktion des Feuerschauers, welche aus arbeitstechnischen Gründen den direkten Zugriff hat.

Daten

Dateneigentum

Die Eigentümerin sämtlicher Daten und Informationen, welche sich auf den IT-Systemen der Gemeinde befinden, ist die Gemeinde.

Datenweitergabe

Die arbeitsprozessbedingte Weitergabe von Daten an Dritte oder an den Kunden darf nur unter Einhaltung der IT-Richtlinien sowie dem Datenschutzgesetz erfolgen. Dasselbe gilt auch für die Datenanfrage von kommunalen-, kantonalen- oder Bundesstellen.

Bei Unsicherheiten ist vor(!) der allfälligen Weitergabe der IT-Verantwortliche zu kontaktieren, welcher über die Datenweitergabe und deren Bedingungen entscheidet.

Datenverantwortung

Die Datenverantwortung und der sorgfältige sowie gesetzeskonforme Umgang mit den Daten obliegen dem Anwender.

Massenkopieren von Daten

Das Massenkopieren von Gemeinde-Daten auf externe Speichergeräte oder mobile Geräte sowie Drittgeräte ist nicht erlaubt.

Daten-Vertraulichkeit

Die elektronischen Daten der Gemeinde und Schule werden in die nachfolgend beschriebenen drei Klassen unterteilt. Die Einstufung liegt in der Verantwortung des datenerstellenden- oder bearbeitenden Mitarbeitenden und der Anweisung des Vorgesetzten. Bei Unsicherheiten ist der IT-Verantwortliche zu kontaktieren.

Vertraulich

- Die Daten sind nur einem bestimmten Mitarbeitenden oder einer eingeschränkten Mitarbeitenden-Gruppe der Gemeinde zugänglich.
- Die Daten müssen innerhalb der Gemeinde-Infrastruktur verbleiben.
- Eine Bearbeitung ausserhalb der Gemeinde-Infrastruktur benötigt die Zustimmung des Eigners und erfordert die Einhaltung von zusätzlichen IT-Sicherheitsmassnahmen.

Interner Gebrauch

- Die Daten sind für alle Mitarbeitenden zugänglich, welche über die entsprechende Zugriffsberechtigung verfügen.
- Die Daten müssen innerhalb der Gemeinde-Infrastruktur verbleiben.
- Eine Bearbeitung ausserhalb der Gemeinde-Infrastruktur benötigt die Zustimmung des Eigners oder IT-Verantwortlichen.
- Dabei handelt es sich um die Standard-Zuweisung von Daten, sofern keine andere Zuweisung deklariert wurde.

Öffentlich (nicht klassifiziert)

- Die Daten sind allgemein für Mitarbeitende zugänglich.
- Die Daten enthalten keine bedeutsamen Gemeinde-Informationen.

Datenablagen

Nachfolgend werden der Zweck und die Verwendung der einzelnen Datenablagen beschrieben.

Lokale Laufwerke C und D Arbeitsplatzrechner / mobile IT-Geräte

- Die lokalen Laufwerke sind nicht als Datenablage zu benutzen, weder für dienstliche noch für private Daten.
- Die Ausnahme bilden die mobilen IT-Geräte, bei welchen die Laufwerke als Datenablage genutzt werden dürfen. Das Kopieren der Daten auf die Gemeinde-Laufwerke für die Datensicherung obliegt dem Nutzer. Ebenso die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der lokalen Daten.

Laufwerk G (Gemeinderat)

- Ablage aller dienstlichen Daten für die Gemeinderäte.
- Detail-Information zur Nutzung des Laufwerk G, siehe entsprechende Anleitung!

Laufwerk K (Anwendungen)

- Keine Datenablage! Dient lediglich den Anwendungen selbst.

Laufwerk I (Gruppen Verwaltung, SHB, Schule)

- Ablage aller dienstlichen Daten für die entsprechenden Gruppen.
- Die einzelnen Gruppen haben gegenseitig keine Zugriffsberechtigungen.

Laufwerk P (Datenaustausch für alle Mitarbeitende)

- Ablage dienstlichen Daten für den Austausch zwischen allen Mitarbeitenden.
- Alle Mitarbeitenden haben die Zugriffsberechtigung für diese Datenablage.
- Vertrauliche Daten sollten hier nicht(!) gespeichert oder nach dem Austausch gleich gelöscht werden!

Laufwerk H (Mitarbeitende)

- Grundsatz-Hinweis: Sämtliche Mitarbeitende sind verantwortlich, dass alle dienstrelevanten und gültigen Informationen in der entsprechenden zentralen Datenablage zur Verfügung stehen. Die Nutzung des H-Laufwerks ist deshalb auf die nachfolgenden Anwendungen zu beschränken.
- Ablage aller dienstlichen Daten zur persönlichen Bearbeitung, welche nicht unmittelbar auf einem anderen Laufwerk gespeichert werden können (siehe Begriffsdefinitionen).
- Zudem dürfen private Daten gespeichert werden, diese sollen jedoch in der Menge und Grösse gering ausfallen und sind regelmässig zu bereinigen. Die privaten Daten werden vom jeweiligen Mitarbeitenden verantwortet.
- Wird eine zu grosse Anzahl an Daten gespeichert, ist der IT-Verantwortliche berechtigt, eine Grössenbeschränkung zu erlassen und den Mitarbeitenden auf die zwingende Reduktion der Daten hinzuweisen.

Anderweitige Datenablagen (z. B. Cloud-Dienste)
Die Nutzung von anderweitigen Daten-Ablagen (z. B. Cloud-Dienste wie Dropbox etc.) ist aus Sicherheitsgründen nicht erlaubt. Durch die Nutzung kann sehr oft weder der Datenschutz noch der Eigentumsvorbehalt durch die Gemeinde gewährt werden. Eine Anwenderkontrolle über die Daten und deren Verbreitung im Internet bzw. an den weltweiten Standorten des Anbieters ist ebenso in den wenigsten Fällen gegeben.

Kann beim dienstlichen Bedarf einer solchen Datenablage von der Gemeinde keine alternative und zumutbare Lösung zur Verfügung gestellt werden, ist eine Ausnahme möglich. Jedoch muss diese vorgängig unter Angabe des eindeutigen Zwecks sowie den möglichen Dateninhalten und Abgrenzungen mittels Antrag an den IT-Verantwortlichen eingereicht werden. Nach einer allfälligen Freigabe obliegt der verantwortungsvolle Daten-Umgang beim entsprechenden Mitarbeitenden.

Datensicherung
Die Datensicherung kann aus technischen und praktikablen Gründen keine Unterscheidung zwischen dienstlichen oder privaten Daten (Datenablage, E-Mail etc.) machen, es werden deshalb sämtliche Daten gesichert.

Von den lokalen Speichern (Laufwerk C, D etc.) der Arbeitsplatzrechner wird keine Datensicherung erstellt, dies gilt ebenso für mobile IT-Geräte und externe Speichergeräte. Die lokalen Daten der mobilen IT-Geräte müssen vom Nutzer selbst auf das entsprechende Gemeinde-Laufwerk kopiert werden, damit die Daten gesichert werden.

Ausdruck von Daten (Drucker)
Ausdrucke sind zeitnah durch den verursachenden Mitarbeitenden von den Druckern abzuholen. Das Liegenlassen von Ausdrucken, auch auf den lokalen Arbeitsplatz-Druckern ist nicht erwünscht und stellt ein Sicherheitsrisiko da.

Ausdrucke der vertraulichen Art sind kein(!) Altpapier und dürfen nur in den entsprechenden gekennzeichneten Containern entsorgt werden.

Anwendungs-Support
Aus Kosten-Nutzen Gründen wurde kein permanenter Anwendungs-Supportvertrag mit dem externen IT-Dienstleister abgeschlossen. Sämtliche Supportanfragen sind kostenpflichtig (Ausnahme siehe unten). Der externe IT-Dienstleister darf von einem Mitarbeitenden nicht direkt kontaktiert werden!

Für den Anwendungs-Support ist innerhalb der Gemeinde der IT-Verantwortliche zuständig, dies während den regulären Arbeitszeiten. Ausserhalb dieser Arbeitszeiten besteht kein Support-Anspruch.

Sämtliche Mitarbeitende richten ihren Anfragen bezüglich eines jeglichen IT-Belangens an den IT-Verantwortlichen. Dieser entscheidet über die Weitergabe an den externen Dienstleister und die entsprechende Kostenfreigabe. Erst nach der Freigabe darf der Mitarbeitende für diesen expliziten Fall direkt mit dem IT-Dienstleister in Kontakt treten.

Spezialfall Verwaltungsapplikationen Gemeinde
Die Gemeinde-Verwaltungsapplikationen verfügen über einen Support-Vertrag, welcher aber nur die Anwendungsunterstützung beinhaltet. Die Mitarbeitenden der Gemeindeverwaltung dürfen anhand ihres Anwendungsgebiets den IT-Dienstleister bzw. dessen Fachgruppen direkt kontaktieren. Für alle anderweitigen IT-Belangen gelten jedoch die obigen Richtlinien.

Support für private oder fremde Geräte (Dritt-Geräte)
Der Support für Dritt-Geräte ist grundsätzlich nicht Sache der Gemeinde. Die Gemeinde lehnt jegliche Haftung oder rechtliche Ansprüche für private und Dritt-Geräte ab.

Die Kosten für den Support der Ersteinrichtung des Fernzugriffs werden jedoch für die Mitarbeitenden durch die Gemeinde einmalig übernommen. Ergeben sich daraus unvorhergesehene Mehrkosten oder wird weiterer Support benötigt, gehen die Kosten zulasten des Mitarbeitenden. Insbesondere, wenn es sich um zusätzlich notwendige Software für andere Betriebssysteme als Windows handelt. Ebenso wird für diesen Fall keine Funktionsgarantie durch die Gemeinde oder den externen IT-Dienstleister übernommen.

Sind Anpassungen auf Dritt-Geräten notwendig, weil Veränderungen der Gemeinde-Infrastruktur vorgenommen wurden, werden diese Kosten erstmalig von der Gemeinde übernommen. Bei weiterführendem Support gehen die Kosten jedoch zulasten des Mitarbeitenden.

Kontrollen

Die Gemeinde behält sich vor, gelegentliche Stichproben in allen Bereichen zur Überprüfung der Einhaltung der Richtlinien durchzuführen. Es wird dabei keine Unterscheidung zwischen privater oder dienstlicher Nutzung der Gemeinde-Infrastruktur gemacht.

Die Kontrollen dienen dem Schutz der Gemeinde und deren Mitarbeitenden. Wird ein grober Sicherheitsverstoss festgestellt, darf auf Verlangen des Gemeinderats eine personenbezogene Auswertung der elektronischen Protokolle gemacht werden. Eine solche Auswertung ist absolut vertraulich zu behandeln und darf Unbefugten nicht zur Einsicht gebracht werden. Sie wird immer nur mittels 4-Augenprinzip durchgeführt.

Die regelmässige Kontrolle der elektronischen Protokolle von Systemen und Applikationen, im üblichen Rahmen der IT-Auftragserfüllung, wird auf anonymer Basis durchgeführt. Ist dies aus technischen Gründen nicht möglich, ist der externe IT-Dienstleister der Vertraulichkeit verpflichtet.

Rechtliche Bestimmungen

Haftungsauschluss

Die Gemeinde lehnt gegenüber den Mitarbeitenden sämtliche Haftung für private Informationen oder Daten im rechtlich zulässigen Rahmen ab. Aus der privaten Nutzung der Gemeinde IT-Infrastruktur kann kein Rechtsanspruch bezüglich Verfügbarkeit, Vertraulichkeit oder Integrität der privaten Daten und Informationen gegenüber der Gemeinde erhoben werden.

Massnahmen bei Missbrauch

Sämtliche Mitarbeitende nehmen zur Kenntnis, dass bei Missbrauch der Gemeinde IT-Infrastruktur oder Verstössen gegen die IT-Richtlinien Sanktionen in Form von Nutzungseinschränkung, Schadenersatz, rechtlichen Schritten oder einer Ermahnung erhoben werden können. Die Sanktion hängt von der Schwere des Verstosses ab. Erfolgt der Verstoss erneut, kann die fristlose Kündigung ausgesprochen werden.

Duggingen, 18.03.2014

Im Namen des Gemeinderates

Der Präsident Der Gemeindeverwalter

Beat Fankhauser Christian Friedli

Beilagen und Link

Informationen zum Datenschutz des Kantons Basel-Landschaft

- http://www.baselland.ch/idg-htm.317381.0.html

Dokumente zum Datenschutz

- IDG Gesetz: 162.0.pdf
- IDV-Verordnung: 162.11.pdf
  - IDV-Anhang 1: anhang-1_pruefungsschema.pdf
  - IDV-Anhang 2: anhang-2_wichtige-begriffe
  - IDV-Anhang 3: anhang-3_einwohnerregister

Anhang A

Internet und E-Mail Verhaltensregeln und Schutzmassnahmen (gemäss Vorlage des ZID)

Internet

- Die Teilnahme an Rechner-Rechner-Netzwerken und Tauschbörsen ist aus urheberrechtlichen Gründen untersagt.
- Chat, Instant Messaging, Benützen von Kontaktbörsen u.ä. gehören nicht zur täglichen Arbeit der Gemeinde.
- Keine Programme (Spiele, Bildschirmschoner usw.) vom Internet herunterladen. Auf «Abbrechen» oder «Nein» klicken, wenn ungewollt ein Download-Fenster erscheint.
- Niemandem den persönlichen Benutzernamen oder das Passwort bekannt geben. Kein seriöser Anbieter wird (auch nicht telefonisch) nach dem Passwort fragen.
- Keine persönlichen Daten preisgeben. Dies trifft speziell beim Ausfüllen von Webformularen zu.
- Nicht vergessen: Beiträge in Newsgruppen, Foren und Gästebüchern sind noch nach Jahren öffentlich zugänglich.
- Heruntergeladene Dokumente auf Viren prüfen, dies wird bei der Gemeinde automatisch durchgeführt.

E- Mail Gefahren

- Ein unverschlüsseltes E-Mail ist wie eine Ansichtskarte!
- Ein E-Mail kann
  - verloren gehen oder an eine/n falsche/n Empfänger/in gelangen;
  - unterwegs eingesehen, kopiert und/oder verändert werden;
  - fiktiv sein, d.h. gar nicht vom bzw. von der angegebenen Absender/in stammen.

Spam:

- sind unerwünschte Werbemails mit oft unseriösen Angeboten.

Kettenmails:

- fordern ultimativ zur Weiterleitung an eine Vielzahl von Personen auf;
- sind oft verbunden mit einem Anreiz (z.B. Geldversprechen) oder einem Appell an das Mitleid.

Schutzmassnahmen (auch innerhalb der Gemeinde einzuhalten)

- Bei kritischen E-Mails Empfangsbestätigung anfordern.
- Bei Unsicherheit E-Mail-Inhalt bestätigen lassen (z.B. telefonisch).
- Hoch und sehr hoch klassifizierte Informationen nicht unverschlüsselt übermitteln.
- E-Mails mit unbekannter Absenderadresse misstrauen: Keine(!) angefügten Dokumente oder Programme öffnen und keine(!) darin angegebenen Links anwählen
- Keine E-Mail-Anhänge öffnen, die zwei Endungen aufweisen (z.B. picture.bmp.vbs).
- Auf keinen Fall Kettenmails weiterleiten und nicht auf Spam-Mails antworten, dies E-Mails sind sofort zu löschen. Bei häufigem Vorkommen ist der IT-Verantwortliche zu informieren.
- Dateien oder Programme nur aus vertrauenswürdigen Quellen öffnen und dies nur nach vorgängiger Prüfung mit einem aktuellen Virenscanner, dies wird bei der Gemeinde automatisch durchgeführt.