biberist
EINWOHNERGEMEINDE
121.7

Verordnung für die Nutzung der elektronischen Infrastruktur in der Gemeindeverwaltung

Version vom 14.12.2015

Personen- und Funktionsbezeichnungen werden abwechselnd entweder in der männlichen oder in der weiblichen Form genannt. Sie gelten selbstverständlich für beide Geschlechter gleichermassen.

1. Einführung 3
1.1 Zweck und Umfang 3
1.3 Geltungsbereich 3
2. Nutzungsregeln 3
2.1 Allgemeine Regeln 3
2.2 E-Mail / Internet / andere Datenübermittlung 4
2.3 Geschäfts-Mobiltelefone / Smartphones 5
2.4 Geschäfts-Notebooks 6
2.5 Umgang/Richtlinien mit Passwörtern 6
2.6 Ferien und andere längere Abwesenheiten 7
2.7 Nutzung digitale Identität / Zertifikate (z.B. Suisse ID) 7
3 Umgang mit Social Medias 8
4 Missbrauch und Massnahmen bei Missbrauch 8

1. Einführung

1.1 Zweck und Umfang

Dieses Dokument regelt die Nutzung elektronischer Geräte durch die Mitarbeiterinnen der Einwohnergemeinde Biberist. Diese Richtlinien regeln die Benutzung der lT-Ressourcen in der Gemeindeverwaltung Biberist durch die berechtigten Benutzer.

1.2 Begriffe

lT-Mittel sind alle Geräte, Einrichtungen und Programme materieller und immaterieller Art, die der elektronischen Verarbeitung, Speicherung, Übermittlung oder Vernichtung von Informationen dienen, namentlich:

lT-Mittel

a) Computersystem und Smart Devices;
b) Peripherie-Geräte und Speichermedien;
c) Netzwerke (wired und unwired) und Netzwerk-Geräte (wie z.B. Router, Repeater, Security-Devices, Wireless Access Points);
d) Software.

Informationen sind Sach- und Personendaten.

lT-Dienste beinhalten zentrale Dienste, welche den berechtigten Benutzerinnen zur Verfügung stehen (E-Mail, DNS, Web-Services, Digital Libraries etc.).

lT-Ressourcen beinhalten lT-Mittel, lnformationen und lT-Dienste.

Zentrale lT-Ressourcen beinhalten lT-Mittel, lnformationen und lT-Dienste, welche von der Gemeindeverwaltung angeboten werden.

1.3 Geltungsbereich

Das Dokument gilt für alle Mitarbeiter der Einwohnergemeinde Biberist, welche IT-Mittel der Einwohnergemeinde Biberist benutzen.

2. Nutzungsregeln

2.1 Allgemeine Regeln

1. Die Mitarbeiterin ist für den sachgemässen Gebrauch des PCs besorgt, so auch für die periodische Reinigung des Bildschirmes und der Tastatur.

   Dem Datenschutz und dem Persönlichkeitsrecht jedes einzelnen ist eine besondere Beachtung beizumessen. Die Einsicht auf den Bildschirm ist vor Drittpersonen (nicht Verwaltungsangestellte) zu schützen. Durch die Übertragung von Aufgaben und Verantwortung in der Erfüllung der persönlichen Tätigkeit, wird auch der Schutz der Verwaltungsdaten übertragen. Der Umgang mit dem PC bedingt Eigenverantwortung. Die PC-Benutzung hat unter Berücksichtigung des Datenschutzes zu erfolgen.

2. Die elektronische Infrastruktur darf im Rahmen der übertragenen Aufgaben uneingeschränkt genutzt werden. Die rein private Nutzung ist auf ein Minimum zu beschränken.

3. Veränderungen an der Hardware-Konfiguration des PCs und an der zur Verfügung gestellten Software dürfen nur durch den zuständigen IT-Verantwortlichen vorgenommen werden, oder werden durch ihn zurückdelegiert. Die Verhältnismässigkeit ist dafür Ausschlag gebend.

4. Privat angeschaffte Hard- und Software dürfen grundsätzlich nicht an firmeneigenen PCs installiert und betrieben werden. Ausnahmen sind nach Rücksprache mit dem IT-Verantwortlichen möglich.

5. Sämtliche Daten auf CDs, USB-Sticks und andere Datenträger, welche vom oder zum firmeneigenen PC transferiert werden, sowie via Internet beschaffte Daten sind vor Gebrauch auf Virenbefall zu untersuchen.

6. Die Mitarbeiterin trägt für alle von ihr übermittelten Inhalte die persönliche Verantwortung. Hierbei wird auf die Treu- und Sorgfaltspflicht gem. OR Art. 321a verwiesen. Sie verpflichtet sich insbesondere, nicht Daten folgenden Inhalts zu verarbeiten, aus dem oder in das Internet zu übertragen:

   - Gewaltdarstellung
   - Pornografische Schriften, Bilderaufnahmen und Darstellungen
   - Rassendiskriminierung
   - Aufrufe zur Gewalt
   - Anleitung oder Anstiftung zu strafbarem Verhalten oder dessen Förderung
   - unerlaubte Glücksspiele
   - Verletzungen immaterielle Rechte Drittpersonen

7. Die Mitarbeiterin bemüht sich nach Kräften, durch die strikte Einhaltung der vorliegenden Bestimmungen den Betrieb vor jeglichem Schaden zu schützen. Dies umfasst insbesondere auch die Meldepflicht bei besonderen Vorkommnissen oder möglichen Problemen im vorliegenden Zusammenhang.

2.2 E-Mail / Internet / andere Datenübermittlung

8. Das Internet dient in erster Linie dem Auffinden von Informationen, die für die geschäftlichen Aufgaben benötigt werden. Allgemeines Surfen ist auf ein Minimum zu beschränken. E-Mails dienen ebenfalls in erster Linie dem geschäftlichen Informationenaustausch. Private E-Mails sind auf ein Minimum zu beschränken.

9. Daten dürfen ausschliesslich von vertrauenswürdigen Quellen auf dem Internet heruntergeladen, respektive ausschliesslich vertrauenswürdige E-Mails geöffnet werden.

10. Der IT-Verantwortliche ist unverzüglich zu benachrichtigen, sobald Missbrauch, Viren oder Hackeraktivitäten vermutet werden.

11. Geschäftsinformationen sollen ausschliesslich über die geschäftliche E-Mail-Adresse versendet werden und dürfen nicht über öffentlich zugängliche Online-Dienste laufen.

12. Besonders schützenswerte Personendaten (Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe sowie über administrative oder strafrechtliche Verfolgungen und Sanktionen) dürfen nicht über E-Mail ausgetauscht werden.

13. Der Zugriff auf die gespeicherten Daten der Mitarbeiter ist nur dann erlaubt, wenn der Datenzugriff angekündigt und vom Gemeindepräsidenten oder dem Verwaltungsleiter verlangt wird, die Person persönlich anwesend ist und sich selber einloggt, oder eine schriftliche Einverständniserklärung abgibt. Die Persönlichkeitsrechte und der persönliche Datenschutz können nicht umgangen werden.

14. Die Arbeitgeberin kann Zugriffsstatistiken über ausgewählte Internetseiten führen. Die Auswertung erfolgt anonymisiert. Nicht relevante Seiten, oder sicherheitskritische Seiten können gesperrt werden. In gewissen Fällen kann unter Angabe des Grundes auch die Freigabe einer solchen Seite beim Verwaltungsleiter beantragt werden.

    Bei Verdacht auf Missbrauch oder Zuwiderhandlung im Umgang mit dem Netz können durch den Gemeindepräsidenten oder den Verwaltungsleiter personifizierte Auswertungen anberaumt werden. Vor dieser Auswertung muss die betroffene Person schriftlich informiert werden.

2.3 Geschäfts-Mobiltelefone / Smartphones

15. Die Einwohnergemeinde Biberist stellt bestimmten Funktionsträgerinnen (insbesondere Mitgliedern der Geschäftsleitung) ein Mobiltelefon/Smartphone zur Verfügung. Dieses kann auch für private Zwecke genutzt werden.

16. Das Gerät ist nach dem Kauf im Eigentum des betreffenden Mitarbeiters. Das dazugehörende Abonnement lautet ebenfalls auf ihn. Als Zustelladresse für die Begleichung der Rechnungen, wird die Einwohnergemeinde Biberist hinterlegt.
    Bei einem Austritt des Mitarbeiters aus den Diensten der Einwohnergemeinde sind Geräte, welche jünger als 2 Jahre sind, der Einwohnergemeinde zurückzugeben.

17. Das Mobiltelefon/Smartphone soll ausschliesslich in der Schweiz benutzt werden. Grundsätzlich sollten im Ausland die Mobilen Daten deaktiviert werden. Damit man im Ausland trotzdem erreichbar ist und kostenbewusst surfen bzw. telefonieren kann, sollen sich die Besitzer zwei Wochen vor dem Auslandaufenthalt mit dem IT-Verantwortlichen in Verbindung setzen. Geeignete Datenpakete können vor einer Auslandreise evaluiert und gebucht werden.

18. Die Besitzerin hat das Mobiltelefon/Smartphone sorgfältig zu benutzen, und bei Verlust sind unverzüglich der IT-Verantwortliche und der Verwaltungsleiter zu benachrichtigen.

19. Der Zugriff auf das Mobiltelefon ist aus Sicherheitsgründen mittels persönlichem Passwortschutz (PIN-Code) sicherzustellen. Dieser muss nach spätestens 5 Minuten automatisch erfolgen. Die Verantwortung dafür trägt die einzelne Besitzerin.

20. Die Besitzerin ist für den Schutz der auf Ihrem Mobiltelefon befindlichen geschäftlichen Daten verantwortlich. Sie hat insbesondere durch angemessene Massnahmen zu ver-

hindern, dass Drittpersonen (insbesondere Familienmitglieder, Mitbewohner, Geschäftspartner und andere Personen) auf die geschäftlichen Daten zugreifen oder diese einsehen können. Vergleiche Punkt 19.

2.4 Geschäfts-Notebooks

21. Mitarbeiterinnen, welche für Ihre Arbeit von der Einwohnergemeinde ein Notebook zur Verfügung gestellt erhalten, haben dieses für geschäftliche Zwecke zu nutzen. Im Auslieferzustand werden die Geräte inskünftig lediglich für den Webzugriff konfiguriert sein, um auf die firmeneigene Umgebung zugreifen zu können. Die private Nutzung ist aufgrund der Sicherheit des Netzzugriffs auf die Firma Talus ein Risiko und nicht erwünscht. Das Gerät ist mit Administratorenrechte des IT-Support belegt, damit die Basiskonfiguration nicht geändert werden kann. Konkret bedeutet dies, dass keine Fremd- oder private Software mehr installiert werden kann.

22. Die Besitzerin ist für den Schutz der auf Ihrem Notebook befindlichen geschäftlichen Daten verantwortlich. Sie hat insbesondere durch angemessene Massnahmen zu verhindern, dass Drittpersonen (insbesondere Familienmitglieder, Mitbewohner, Geschäftspartner und andere Personen) auf die geschäftlichen Daten zugreifen oder diese einsehen können.

    Das Notebook darf nicht sichtbar im Auto deponiert werden. Ebenfalls darf das Notebook in den öffentlichen Verkehrsmitteln für Drittpersonen nicht erreichbar sein. Sollte trotz den Vorkehrungen das Notebook entwendet werden oder verloren gehen, ist unverzüglich der IT-Verantwortliche zu informieren.

23. Falls die Besitzerin geschäftliche Daten – auch nur kurzfristig – auf andere Datenträger transferiert (z.B. andere Festplatten, CDs, USB-Sticks, etc.) so hat sie durch angemessene Massnahmen zu verhindern, dass Drittpersonen (insbesondere Familienmitglieder, Mitbewohner, Geschäftspartner und andere Personen) auf die geschäftlichen Daten zugreifen oder diese einsehen können.

24. Bei Beendigung des Arbeitsverhältnisses ist das von der Einwohnergemeinde zu Verfügung gestellte Notebook zurückzugeben. Die Besitzerin hat dafür zu sorgen, dass sämtliche Daten in strukturierter und geordneter Form der Einwohnergemeinde übergeben werden und keine geschäftlichen Daten im Besitz der Mitarbeiterin verbleiben (z.B. auf anderen Festplatten, CDs, USB-Sticks oder anderen privaten Datenträgern der Mitarbeiterin).

25. Die Bestimmungen über den PC-Gebrauch und den Umgang mit elektronischen Medien gelten sinngemäss auch für Notebooks.

2.5 Umgang/Richtlinien mit Passwörtern

26. Jeder Mitarbeiter hat jeweils 2 Passwörter um auf die lokale bzw. das Webinterface von Talus Informatik AG zuzugreifen. Das Passwort vom Webinterface muss mindestens acht Zeichen aus drei der folgenden Kategorien enthalten: Grossbuchstaben, Kleinbuchstaben, Zahlen, nichtalphabetische Zeichen (z.B. $, ?, *, %).

27. Die Mitarbeiterin darf ihr Passwort in keinem Fall und in keiner Form jemandem anderem bekannt geben.

28. Das Passwort darf weder aufgeschrieben, gedruckt noch in einem Dokument gespeichert werden. Im Weiteren sollen die Passwörter nicht aus dem Vor- bzw. Nachnamen der Besitzerin bestehen.

29. Falls die Mitarbeiterin das Passwort vergessen hat, soll sie sich mit dem IT-Verantwortlichen in Verbindung setzen.

30. Die automatische Bildschirmsperre ist mit einer Verzögerung von höchsten 5 Minuten eingestellt. Im Weiteren ist beim Verlassen des Arbeitsplatzes der PC durch den Mitarbeiter zu sperren.

31. Kapitel 2.5 gilt sowohl für PCs als auch für gemeindeeigene Notebooks.

2.6 Ferien und andere längere Abwesenheiten

32. Bei Ferienabwesenheit oder anderen längeren Abwesenheiten ist folgendes zu beachten:

- Das Passwort (vgl. oben 2.5) darf niemandem bekannt gegeben werden, auch nicht der Stellvertreterin oder der Arbeitskollegin.
- Es dürfen aus Datenschutzgründen keine automatischen E-Mail-Weiterleitungen eingerichtet werden.
- Bei voraussehbaren Abwesenheiten von mehr als einem Arbeitstag ist eine automatische Abwesenheitsnotiz im Outlook einzurichten, welche die Absenderin des E-Mails informiert, a) dass die E-Mail aus Datenschutzgründen nicht weitergeleitet oder von anderen Personen kontrolliert wird, b) wer die zuständige Stellvertretung ist (mit Angabe von E-Mail-Adresse und Telefonnummer), c) wann die abwesende Person wieder anwesend sein wird. Ausnahme davon ist, sofern ein externer Zugriff möglich ist, oder im „Home-Office“ gearbeitet wird.

33. Bei unvorhersehbaren längeren Abwesenheiten (Krankheit, Unfall, Todesfall) kann der Verwaltungsleiter prüfen, ob im Sinne einer personalrechtlichen Ersatzvornahme auf das E-Mail-Konto des betreffenden Mitarbeiters zugegriffen werden kann.
Eine Ersatzvornahme ist ausschliesslich möglich, wenn dringlich anstehende Geschäfte erledigt werden müssen. Falls ein entsprechender Zugriff erfolgen soll, ist der Mitarbeiter vorgängig darauf hinzuweisen und es ist ihm eine angemessene Frist zur selbständigen Erledigung einzuräumen. Auf diese Androhung kann verzichtet werden, wenn Gefahr im Verzug ist oder wenn feststeht, dass der Mitarbeiter die Verpflichtung nicht in angemessener Frist erfüllen wird.

34. Kapitel 2.6 gilt sowohl für PCs als auch für gemeindeeigene Notebooks.

2.7 Nutzung digitale Identität / Zertifikate (z.B. Suisse ID)

35. Die Mitarbeiterin hat sich an die Nutzungsbestimmungen für die digitale Identität zu halten. Diese wurden beim Erhalt des Zertifikats mitgeliefert. Die Mitarbeiterin bestätigt mit der Unterschrift des Antragsformulars mit der Veröffentlichung des Zertifikats einverstanden zu sein. Ebenso wird mit der Unterschrift die Richtigkeit aller Angaben für das Zertifikat bestätigt.

36. Es sind keine persönlichen Daten zur Kreierung des PIN-Codes oder des Passwortes zu benutzen. Der Signaturschlüssel ist geschützt und getrennt vom dazugehörenden PIN-Code aufzubewahren.

37. Die Weitergabe des Signaturschlüssels an eine unbefugte Person ist verboten.

38. Sollten die Angaben des Zertifikats nicht mehr stimmen, der Signaturschlüssel oder der Token abhandengekommen sein muss das Zertifikat als ungültig erklärt werden. Jeder dieser eingetretenen Fälle ist unverzüglich dem IT-Verantwortlichen zu melden, welche die Revozierung (Ungültigkeitserklärung) vornimmt.

3 Umgang mit Social Medias

39. Im Umgang mit Social Medias gelten die folgenden Regeln:
    a) Die private Nutzung von Facebook, Twitter, Google+, Instagram, etc. ist während der Arbeitszeit verboten,
    b) das Hochladen von Bildern vom Arbeitsplatz ist zu unterlassen,
    c) Kommentare, Statusmeldungen etc. dürfen keinen Rückschluss auf irgendwelche geschäftlichen Informationen liefern.

4 Missbrauch und Massnahmen bei Missbrauch

4.1 Missbrauch

Missbräuchlich ist jede Veruntreuung der lT-Ressourcen, die:
- im Widerspruch zu den gesetzlichen Bestimmungen, den Anstellungsbedingungen oder zur Erfüllung der übertragenen Aufgaben, steht;
- gegen diese Weisungen verstösst;
- gegen andere Bestimmungen der Rechtsordnung verstösst;
- Rechte Dritter verletzt.

Missbräuchlich sind insbesondere die folgenden Handlungen:
a) Verarbeitung, Speicherung oder Übermittlung von Daten mit rassistischem, sexistischem oder pornographischem lnhalt;
b) widerrechtliches Kopieren, Verändern und Löschen von Daten jeglicher Art *Bemerkung: Alle Daten sind zu archivieren (Öffentlichkeitsprinzip). Nur falsche, fehlerhafte Daten oder Dateien (Irrtum) dürfen selbstätig gelöscht werden;*
c) Erstellen oder Verbreiten von schädlichen Programmcodes (wie z.B. Viren, Trojaner, Würmer);
d) Hacking, namentlich
    - unbefugtes Eindringen bzw. versuchtes Eindringen in fremde Computersysteme;
    - Treffen von Vorkehrungen zur Störung des Betriebs von Computern oder Netzwerken (Denial of Service Attacks);
    - unauthentifiziertes Absuchen auf Schwachstellen (Port-Scanning);
    - Ausspionieren von Passwörtern;
e) Verwenden von vorgetäuschten lP- oder MAC-Adressen (Spooling);
f) Versenden von E-Mails mit vorgetäuschten E-Mail-Absender-Adressen;
g) Veränderungen oder Erweiterungen von Netzwerk-Komponenten im Netzwerk ohne ausdrückliche Erlaubnis des IT-Verantwortlichen;

h) Massenversand von E-Mails zu nicht Verwaltungszwecken im Sinne von Mail-Spamming;
i) Belästigung anderer Personen mit lT-Ressourcen;
j) Manipulation von lT-Ressourcen.

4.2 Massnahmen bei Missbrauch

Die Benutzerinnen sind für die Verwendung der lT-Ressourcen unter Einhaltung der geltenden Rechtsordnung und dieser Richtlinien persönlich verantwortlich. lnsbesondere ist die auf den Login-Namen eingetragene Person für die Folgen der Verwendung der lT-Ressourcen, die unter Eingabe ihres Passwortes erfolgt, persönlich verantwortlich, sofern nicht nachgewiesen werden kann, dass ihr Passwort ohne eigenes Verschulden unbefugt verwendet worden ist.

Bei Verstoss gegen die allg. Rechtsordnung (CH) im Zusammenhang mit dem Gebrauch von den lT-Ressourcen oder bei Verstoss gegen diese Richtlinien kann die IT-Abteilung alle zur Aufrechterhaltung bzw. Wiederherstellung des rechtmässigen Zustandes erforderlichen Massnahmen treffen, namentlich :

a) Sperren des Zugangs zu den lT-Ressourcen oder andere Einschränkungen der Benutzung der lT-Ressourcen
b) Löschen des Accounts
c) Rückgängig machen von Löschungen
d) Hausverbot

Überdies können personalrechtliche Sanktionen ergriffen werden.
Die Strafverfolgung und die Geltendmachung zivilrechtlicher Ansprüche bleiben vorbehalten.

Beschlossen vom Gemeinderat am 14. Dezember 2015 mit Beschluss Nr. 2015-180.