Buttisholz

IT-Richtlinien

vom 31. August 2017

Inhaltsverzeichnis

I. Allgemeine Bestimmungen

Art. 1. Zweck

1 Diese Richtlinien regeln die Beschaffung und die Benutzung von Informatikmitteln der Gemeindeverwaltung Buttisholz.

2 Sie hat zum Zweck, die sensitiven Datenbestände zu schützen, den sicheren und wirtschaftlichen Einsatz der Informatikmittel zu gewährleisten sowie die Persönlichkeitsrechte der Anwenderinnen und Anwender zu wahren.

Art. 2. Geltungsbereich

1 Diese Richtlinien gelten für die gesamte Gemeindeverwaltung Buttisholz und den Gemeinderat Buttisholz, nicht jedoch für die Schule und allfällige gemeindeeigene Betriebe. Diese ausgenommenen Institutionen regeln ihre Informatikbelange soweit nötig in eigenen Vorgaben. Der Schutz der sensitiven Datenbestände muss gewährleistet bleiben.

2 Sie gilt auch für weitere Stellen, soweit sie Informatikmittel der Gemeindeverwaltung Buttisholz benutzen. Die Geschäftsleitung kann auf Anfrage einzelne Personen und Personengruppen vom Geltungsbereich dieses Reglements teilweise ausnehmen, wenn sichergestellt ist, dass der Schutz der sensitiven Datenbestände gewährleistet bleibt.

Art. 3. Begriffe

1 Informationen im Sinne dieser Richtlinien sind Sach- und Personendaten.

2 Der Begriff der Personendaten richtet sich nach dem Gesetz über den Schutz von Personendaten (Datenschutzgesetz) sowie dem Datenschutz-Reglement der Gemeinde Buttisholz.

3 Informatikmittel sind Geräte, Einrichtungen und Dienste, wie insbesondere Computersysteme, Software, Internet- und E-Mail-Dienste, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung oder Vernichtung von Informationen dienen.

4 Unter dem Begriff ICT (information and communication technology) wird Informations- und Kommunikationstechnik, sprich IT, verstanden.

5 Unter dem Begriff ICT-Service Provider wird der Anbieter, welcher die ICT bereitstellt, verstanden.

6 Unter dem Begriff des PCs werden auch Thinclients, Zeroclients und Notebooks verstanden.

7 Mobile devices sind mobile Geräte wie Smartphones (iPhone, Android, etc.), Tablets u.Ä.

8 USB-Sticks sind kompakte Speichersticks, welche über den USB Port mit dem PC verbunden werden können.

9 Unter den Begriffen LAN & WLAN werden das kabelgebundene lokale Netzwerk (Local Area Network) und das Wireless Netzwerk (Wireless Local Area Network) verstanden.

II. Beschaffung

Art. 4. Neu-, Erweiterungs- und Ersatzinvestitionen

1 Die Beschaffung von Informatikmitteln erfolgt nach Rücksprache mit der Geschäftsleitung sowie dem ICT-Service Provider durch die IT-Verantwortliche oder den IT-Verantwortlichen. Eine Beschaffung kann nur erfolgen, wenn die entsprechenden Geldmittel im Budget vorgesehen sind oder durch den Gemeinderat bewilligt wurden.

2 Defekte lnformatikmittel, welche für die Arbeit benötigt werden, dürfen auch ersetzt werden, wenn die entsprechenden Geldmittel im Budget fehlen und die Bewilligung des Gemeinderates ausstehend ist. Der Gemeinderat ist innert nützlicher Frist darüber zu orientieren.

III. Benutzung

Art. 5. Persönliche Verantwortung

1 Alle Anwenderinnen und Anwender sind für die Verwendung der Informatikmittel im Rahmen dieser Richtlinien persönlich verantwortlich. Durch die Unterzeichnung dieser Richtlinien unter Art. 22 bestätigen die Anwenderinnen und Anwender, von diesen Richtlinien Kenntnis zu haben und sie zu befolgen.

2 Insbesondere sind sie dafür verantwortlich, dass an ihrem Arbeitsplatz und in ihrem Zuständigkeitsbereich die entsprechenden Vorgaben zur Gewährleistung von Datenschutz und Datensicherheit befolgt und die notwendigen Massnahmen getroffen werden. Feststellungen über technische Mängel und sicherheitsrelevante Vorkommnisse sind dem ICT-Service Provider unverzüglich zu melden.

Art. 6. Nutzung von Informatikmittel generell

1 Die Nutzung von Informatikmitteln dient ausschliesslich geschäftlichen Zwecken (inkl. Notariatstätigkeit). Eine private Nutzung ist nur ausnahmsweise zulässig und hat immer nach den Grundsätzen der Verhältnismässigkeit zu erfolgen. Die Erfüllung zugewiesener Aufgaben und beanspruchter Ressourcen (Arbeitszeit, Netzkapazität, Speicherplatz, etc.) darf nicht beeinträchtigt werden. Die private Nutzung der Informatikmittel zu kommerziellen Zwecken ist untersagt.

2 Die Anwendungs- und Hardwarelandschaft wird von der Geschäftsleitung nach Rücksprache mit dem ICT-Service Provider definiert. Erst nach dessen Prüfung und Freigabe dürfen zusätzliche Programme und Hardwarekomponenten installiert werden (über die Art der Inbetriebsetzung entscheidet der ICT-Service Provider).

3 Geräte, welche nicht im Eigentum der Gemeinde Buttisholz sind (bspw. USB-Sticks, Smartphones, Digitalkameras usw.), dürfen nur ausnahmsweise und mit äusserster Zurückhaltung an externer Schnittstelle oder direkt am Netzwerk angeschlossen werden (siehe auch Bestimmungen unter Art. 6 Ziff. 12 dieser Richtlinien). Der oder die lCT-Verantwortliche kann auf Gesuch hin Ausnahmen von dieser Bestimmung erteilen.

Standard Arbeitsplatz

4 Mitarbeitenden wird ein Standard-Arbeitsplatz zur Verfügung gestellt. Dieser beinhaltet in der Regel einen PC, zwei Monitore, eine Maus und eine Tastatur. Ausnahmen sind durch die Geschäftsleitung nach Rücksprache mit dem ICT-Service Provider zu bewilligen.

5 Am Ende des Arbeitstages sind der PC und weitere Informatikmittel auszuschalten.

6 Es steht ein Multifunktionsdrucker zur Verfügung, welcher allen Mitarbeitenden zugänglich ist. In den Büros stehen nur Schwarzweiss-Drucker zur Verfügung. Es ist darauf zu achten, dass Ausdrucke sofort vom Drucker genommen werden, damit unberechtigte Personen keinen Einblick in diese Dokumente haben.

Verhalten bei sicherheitsrelevanten ICT-Vorfällen

7 Dateien werden automatisch auf Viren geprüft. Sicherheitsrelevante Ereignisse (z.B. Viren, unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, etc.), sowie erkannte Sicherheitsverletzungen oder Schwachstellen sind umgehend dem oder der lCT-Verantwortlichen zu melden. Die Ereignisse werden geprüft und die Weiterleitung an den ICT- Service Provider koordiniert. Eigenaktionen sind zu unterlassen, weil dabei allenfalls wertvolle Hinweise und Spuren verwischt werden oder verloren gehen.

Mobile Devices

8 Der Datenabgleich via Push-Mail ist gestattet und muss beim ICT-Ausschuss beantragt werden. Die Gemeinde Buttisholz beteiligt sich nicht an den daraus entstehenden Kosten (Smartphone, Abokosten, Datenvolumen, etc.), ausser es handelt sich um ein von der Gemeinde Buttisholz betrieblich zur Verfügung gestelltes Gerät und die Push-Mail-Funktion ist im Interesse der Gemeinde Buttisholz. Um die Push-Mail Funktion nützen zu können, wird ein mind. 4-stelliger PIN Code (Sicherheitssperre) vorausgesetzt. Nach Abschluss der Konfiguration des Push-Mail Services, muss das Gerät vom ICT-Service Provider freigegeben werden.

9 Bei Verlust des mobilen Gerätes oder der SIM-Karte, welche über den Push-Mail Service verfügen, muss sofort eine Kartensperre veranlasst und der ICT-Service Provider zwecks Sperrung des Accounts informiert werden. Geräte, die abhandenkommen und wiedergefunden werden, dürfen erst nach Formatierung und Neuinstallation wiederverwendet werden.

10 Administrationstools für Handys und Smartphones wie beispielsweise iTunes dürfen nicht installiert werden. Die Installation des Administrationstools ist Sache des Benutzers und hat auf privaten Geräten (nicht zu verwechseln mit dem Horne Laufwerk) zu erfolgen.

11 Die Geschäftsleitung kann die Regelungen bezüglich Mobile Devices in einer eigenen Weisung präzisieren.

USB-Sticks

12 Datenimporte aus Fremdsystemen mittels mobilen Datenträgern (USB-Sticks, Digitalkameras, etc.) sind aus Sicherheitsgründen (Virenschutz) nur mit äusserster Zurückhaltung und nur bei vertrauenswürdigen Zulieferern erlaubt. Private mobile Datenträger sind nur erlaubt, wenn diese vor dem Gebrauch und vor dem Anschluss ans Netzwerk mit einem aktuellen Virenschutzprogramm auf Viren geprüft und als virenfrei eingestuft worden sind. Der Benutzer muss sicherstellen, dass keine verseuchten USB-Sticks angeschlossen werden.

Login und Passworte

13 Grundsätzlich arbeitet jeder Benutzer mit einem persönlichen Account. Das persönliche Passwort ist geheim zu halten und darf nicht weitergegeben werden. Falls das Passwort aufgeschrieben werden muss, ist dieses sicher aufzubewahren. Das Passwort soll so gewählt werden, dass es nicht leicht zu erraten ist. Genauere Informationen dazu finden Sie unter "Weisungen zur Passworteingabe am Arbeitsplatz". Das Passwort ist regelmässig zu ändern.

14 Bei Änderung des Passwortes für den persönlichen Account ist gleichzeitig auch das Passwort für das Axioma zu ändern, sofern für das Axioma keine andere Passwortregelung vorhanden ist. Für den persönlichen Account und das Axioma darf nicht das gleiche Passwort verwendet werden.

15 Zur Benutzeridentifizierung wird die Handynummer jedes Mitarbeiters beim ICT-Service Provider zentral gespeichert. Diese kann bei sicherheitsrelevanten Tätigkeiten (z.B. Passwort zurücksetzen) beim Anrufer abgefragt werden. Allfällige neue Passwörter werden per SMS auf die hinterlegte Handynummer zugestellt.

Internet und E-Mails

16 Die Nutzung des Internets und E-Mails steht während der Arbeitszeit allen Mitarbeitenden offen und ist geschäftlichen Zwecken vorbehalten. Die private Nutzung während der Arbeitszeit ist nur ausnahmsweise erlaubt. Die Nutzung ausserhalb der Arbeitszeit ist erlaubt, unterliegt jedoch ebenfalls den vorliegenden Richtlinien.

17 Die maximale Mailboxgrösse beträgt 1GB (1 Gigabyte). Die Mitarbeitenden sind für die Pflege der persönlichen Mailbox verantwortlich. Wird das Kontingent erschöpft, können keine weiteren Nachrichten empfangen werden, bevor die Mailbox (Posteingang, Ausgang, Papierkorb, etc.) bereinigt wird. Elemente im Papierkorb werden nach 30 Tagen automatisch gelöscht.

18 Das Herunterladen (Downloads) von Daten, Bilder, Textdateien etc. aus dem Internet oder aus Anhängen von E-Mails ist nur bei vertrauenswürdigen Datenquellen erlaubt. Das Abrufen von kostenpflichtigen Inhalten oder Dienstleistungen zu privaten Zwecken ist verboten.

19 Das automatische Weiterleiten von E-Mails an Adressen ausserhalb der Gemeinde Buttisholz birgt hohe Risiken bezüglich der Vertraulichkeit, weil auf diesem Weg vertrauliche oder geheime Informationen unverschlüsselt über das Internet übertragen werden können. Das automatische Weiterleiten von E-Mails an Adressen ausserhalb der Gemeinde Buttisholz ist deshalb verboten. Ausnahmen sind im Einzelfall von der IT-verantwortlichen Person in Absprache mit dem ICT-Service Provider explizit zu bewilligen.

20 Die automatische Abwesenheitsmeldung ist bei Ferienabwesenheiten (mehr als ein Arbeitstag) oder anderen dauernden Abwesenheiten einzurichten. Diese ist so zu formulieren, dass Kunden über allfällige Stellvertretungen informiert sind.

21 Das Webmail Portal (https://mail.gict.ch) steht allen Benutzerinnen und Benutzern zur Verfügung.

22 Der Internet Zugriff auf Sozial Media wie Facebook, Twitter, YouTube, etc. ist nur mit grösster Zurückhaltung erlaubt. Gleiches gilt für private WebMail Adressen wie bspw. xy@bluewin.ch, xy@hotmail.com, xy@gmx.ch.

Onlinedienste / Datenspeicherung

23 Das Abonnieren von News Groups (Diskussionsforen/BLOGS/RSS-Feeds etc.) und die Teilnahme an Online-Spielen sowie das Abspielen von TV-Sendungen, Web-Radio, Filmen und Musik ist nur mit grösster Zurückhaltung und vor allem für geschäftliche Zwecke erlaubt. Die Performance der ICT-Anwendungen darf nicht beeinträchtigt werden.

24 Die Verwendung von externen Cloud-Diensten wie z.B. iCloud, Dropbox, Microsoft Skydrive, Mydrive, etc. sind aus Sicherheitsgründen verboten.

25 Das Abspeichern von privaten Daten wie Fotos, Filme, Musik, usw. ist nur mit grösster Zurückhaltung auf dem eigenen Laufwerk erlaubt.

Art. 7. Fernzugriff (Remote Access)

1 Mit der eingesetzten Lösung ist es möglich, von einem Heimarbeitsplatz-PC auf den persönlichen virtuellen IT-Arbeitsplatz zuzugreifen. Da sich die Geräte ausserhalb des LANs des ICT-Service Providers befinden, sind diese nicht in deren Kontrolle.

Berechtigungen und Verfügbarkeiten

2 Der ICT-Service Provider ermöglicht den Mitgliedern des Gemeinderates sowie den Mitarbeitenden der Gemeindeverwaltung auf schriftlichen Antrag hin den Fernzugriff auf die ICT Infrastruktur, wenn in Ausführung geschäftlicher Tätigkeit von extern auf das System zugegriffen werden muss. Der Antrag ist von der Geschäftsleitung zu genehmigen.

3 Die Verfügbarkeit der Systeme ist ausserhalb der Bürozeiten i.d.R. zwar gegeben, jedoch wird diese nicht garantiert. Bezüglich Performance können vom ICT-Service Provider keine Garantien abgegeben werden, da diese zu grossen Teilen von externen Komponenten (lokales LAN, Internet) abhängig sind.

4 Für Zusatzfunktionen wie Print@Home und USB-Redirect kann vom ICT-Service Provider keine Gewährleistung übernommen werden.

Betrieb und Installation

5 Für die Funktionstüchtigkeit des LANs, respektive Wireless (WLAN) beim Benutzer ist dieser selber verantwortlich. Der ICT-Service Provider stellt weder für diese Infrastruktur noch für die verwendeten Geräte Support zur Verfügung. Dies gilt sowohl für die Installation als auch für den laufenden Betrieb.

6 Die Installation auf der lokalen Umgebung (privater PC) erfolgt gemäss einer von der ICT- Service Provider bereitgestellten Dokumentation durch die Benutzerin oder den Benutzer. Der Betrieb und Support für Mac (Apple) Geräte erfolgt nach "best effort".

7 Die Lösung wird unter Windows bereitgestellt. Falls Benutzer andere Betriebssysteme (z.B. Mac OS X) verwenden, ist dies solange möglich wie die entsprechende Client Software verfügbar ist. Die Funktionstüchtigkeit wird jedoch nicht garantiert.

Verantwortung des Benutzers

8 Der externe Zugriff darf nur über Geräte mit aktuellem Virenschutz und aktuellen Betriebssystemupdates erfolgen.

Wlan (Wireless Zugang inhouse)

1 Die Benutzerinnen und Benutzer des durch den ICT-Service Provider bereitgestellten WLANs nehmen zur Kenntnis, dass die Nutzung mit Risiken und Gefahren verbunden sein kann.

2 Der Zugang zum WLAN ist ausschliesslich berechtigten Personen (Mitglieder Gemeinderat, Mitarbeitende Gemeindeverwaltung) vorbehalten. Weitere Personen (bspw. Kommissionsmitglieder) können beim ICT-Ausschuss ein zeitlich begrenztes Gäste-WLAN (Art. 8 Ziff. 4) beantragen. Der oder die ICT-Verantwortliche gibt den berechtigten Personen das Passwort bekannt.

Verfügbarkeit und Support

3 Das WLAN wird durch den ICT-Service Provider nach bestem Wissen und anerkannten Grundsätzen betrieben. Dadurch und bedingt durch den Grad der Abdeckung besteht keine garantierte Verfügbarkeit. Ebenso kann bei individuellen technischen Problemen keine Unterstützung gewährt werden. Für die korrekte Konfiguration und Funktionsfähigkeit der verwendeten Geräte ist der Nutzer oder die Nutzerin selber verantwortlich. Jegliche Haftung wegen Nichtverfügbarkeit wird wegbedungen.

4 Für die Benutzung des Gäste-WLAN muss frühzeitig ein zeitlich begrenztes WLAN Ticket beim ICT-Service Provider bestellt werden.

5 Nutzer und Nutzerinnen dürfen das Passwort keinesfalls anderen Personen oder Gruppen zur Nutzung des Dienstes weitergeben.

Art. 8. Datenschutz und -sicherheit

1 Die Anwenderin oder der Anwender hat zusammen mit dem ICT-Service Provider, entsprechend dem Sicherheitsrisiko von Informationsart und -gehalt, Schutz- und Sicherheitsmassnahmen vorzukehren. Die einmal festgelegten Massnahmen sind strikte einzuhalten. Sie müssen jedoch periodisch in Zusammenarbeit mit dem ICT-Service Provider auf ihre Zweckmässigkeit und dauernde Wirksamkeit überprüft und wenn nötig den neuen Anforderungen angepasst werden.

2 Speicherung von besonders schützenswerten Personen- und Geschäftsdaten dürfen nicht ungeschützt innerhalb allgemein zugänglicher Verzeichnisse erfolgen.

3 Sämtliche geschäftlichen Daten müssen auf den dafür vorgesehenen Servern abgespeichert werden. Die alleinige Speicherung auf dem lokalen Gerät, externer Festplatte oder anderen Medien, ist verboten.

4 Standard Software von Drittfirmen dürfen weder kopiert noch weitergegeben werden. Die übrigen Programme dürfen nur vom Ersteller mit Zustimmung der vorgesetzten Person kopiert und/oder weitergegeben werden.

Art. 9. Schulungs- und Informationspflicht

1 Besteht individueller Schulungsbedarf, hat der betroffene Mitarbeitende bei der vorgesetzten Person ein Gesuch um Weiterbildung zu stellen. Die vorgesetzte Person organisiert die Weiterbildung in Zusammenarbeit mit dem ICT-Verantwortlichen und der Geschäftsleitung.

2 Der ICT-Service Provider informiert alle Nutzerinnen und Nutzer über relevante Ereignisse oder Änderungen im Zusammenhang mit der ICT-Umgebung.

IV. Missbrauch von Informatikmitteln

Art. 10. Missbrauch der Informatikmittel

1 Missbräuchlich ist jede Verwendung der lnformatikmittel, die
   a. gegen diese Weisung verstösst,
   b. gegen andere Bestimmungen der geltenden Rechtsordnung verstösst,
   c. Rechte Dritter verletzt.

2 Missbräuchlich sind insbesondere folgende Handlungen:
   a. Einrichten, Anschliessen oder Installation nicht bewilligter lnformatikmittel,
   b. Manipulation oder Änderung von lnformatikmitteln,
   c. Vorkehrungen zur Störung des Betriebs von Computern oder Netzwerken,
   d. Erstellen, Speichern, Ausführen und Verbreiten von Fernsteuerungs-, Spionage- und Virenprogrammen (z.B. Viren, Trojanische Pferde, Würmer oder Scripte),
   e. Versendung von E-Mails in Täuschungs- oder Belästigungsabsicht und private Massenversände,
   f. Zugriff auf Daten mit rassistischem, sexistischem oder pornografischem Inhalt sowie deren Erfassung, Verarbeitung, Speicherung und Übermittlung,
   g. widerrechtliches Kopieren von Daten oder Software jeglicher Art,
   h. Die Inaktivierung oder Umgehung von angeordneten Vorkehrungen und Massnahmen bezüglich Sicherheit.

V. ICT-Service Provider

Art. 11. Grundsatz

Der ICT-Service Provider ist hauptverantwortlich für die Bereitstellung einer funktionstüchtigen Systemlandschaft.

Art. 12. Aufgaben

1 Der ICT-Service Provider stellt die benötigte Systemlandschaft bereit und organisiert den Zugriff auf die Daten.

2 Der ICT-Service Provider ergreift alle notwendigen organisatorischen und technischen Massnahmen, um unberechtigte Zugriffe auf die Server-Systeme, Programme und Daten zu verhindern.

3 Der ICT-Service Provider ist verantwortlich für die Evaluation und Entwicklung von Programmen für Problemlösungen, die nicht mit den Standard-Programmen zu bewältigen sind. Er kann dabei betroffene Fachabteilungen beiziehen.

4 Der ICT-Service Provider führt ein Teilinventar über ausgewählte, wirtschaftlich relevante Hard- und Software (Systeme, Programme etc.).

VI. Kontrollen

Art. 13. Kontroll- und Überwachungsmassnahmen

1 Kontroll- und Überwachungsmassnahmen bezwecken in erster Linie die Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel. Sie werden nur unter Berücksichtigung des Gebots der Verhältnismässigkeit und unter strikter Einhaltung aller rechtlichen Rahmenbedingungen durchgeführt.

2 Zur Verhinderung des Missbrauchs wird der Zugang zu bestimmten Internet-Adressen mittels Filtersperren beschränkt und es können Netzwerküberwachungs- oder Netzwerkanalysewerkzeuge wie z. B. Portscanner oder Sniffer eingesetzt werden. Nicht gestattet ist der Einsatz so genannter Spionageprogramme.

3 Aufgerufene Internetadressen können aufgezeichnet werden. Es können Benutzername, aufgerufene Internet-Adressen, Zugriffszeit, Datentransfervolumen, etc. protokolliert werden.

4 Der gesamte E-Mail-Verkehr der Anwender kann aufgezeichnet werden (protokolliert).
Der Inhalt der E-Mails darf nur mit Zustimmung des betroffenen Anwenders oder der betroffenen Anwenderin gelesen werden.

Art. 14. Sicherheit, Funktionsfähigkeit und Verfügbarkeit der Informatikmittel

1 Für die Anordnung von Kontroll- und Überwachungsmassnahmen zur Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel sowie die Durchführung von entsprechenden Auswertungen ist der ICT- Service Provider zuständig. Dieser hat dafür zu sorgen, dass solche Auswertungen nur von Mitarbeitenden des ICT-Service Providers durchgeführt und streng vertraulich behandelt werden.

2 Die Protokolldaten sind in anonymisierter Form auszuwerten. Rückschlüsse auf bestimmte Anwender dürfen nicht möglich sein.

3 Werden Störungen festgestellt, welche die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel ernsthaft gefährden, dürfen die Protokolldaten ausnahmsweise personenbezogen ausgewertet werden, sofern dies zur Störungsbehebung unumgänglich ist. Die betroffenen Anwender werden über Tatsache und Umfang der personenbezogenen Auswertung unverzüglich informiert.

4 Bei personenbezogenen Auswertungen hat der ICT-Service Provider die vorgängige Einwilligung der Geschäftsleitung einzuholen und erstattet dieser nachträglich Bericht über die durchgeführte Untersuchung und die allenfalls getroffenen Massnahmen. Kann eine Einwilligung vorgängig nicht eingeholt werden, darf die Auswertung durchgeführt werden, sofern die Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel keinen Aufschub erlaubt.

5 Ansprechperson für den GICT bei Notfällen ist die IT-verantwortliche Person. Sie entscheidet gemeinsam mit der Geschäftsleitung über zu treffende Massnahmen. Dabei sind wirtschaftliche Interessen sowie die Verfügbarkeit der Daten angemessen zu berücksichtigen. Wenn aufgrund der

Umstände unverzüglich entschieden werden muss (Virus, Wurm, Trojaner usw.), ist die IT-verantwortliche Person befugt, einen Datenverlust von maximal 24 Stunden bzw. letzte Datensicherung zu riskieren.

Art. 15. Vollzug

1 Für die Überprüfung des Vollzugs dieser Weisung mittels Auswertung der Protokolldaten ist die Geschäftsleitung zuständig.

2 Besteht begründeter Verdacht auf Missbrauch von Informatikmitteln, kann die Geschäftsleitung gegenüber einem begrenzten Personenkreis eine den Betroffenen im Voraus schriftlich angekündigte, zeitlich befristete Kontrolle durchführen lassen.

3 Die Durchführung der Kontrollen hat unter Aufsicht des ICT-Service Providers zu geschehen.

4 Die Auswertungsresultate werden ausschliesslich der Geschäftsleitung bekannt gegeben und sind streng vertraulich zu behandeln.

VII. Schlussbestimmungen

Art. 16. Sanktionen

Bei Verstoss gegen die Rechtsordnung im Zusammenhang mit dem Gebrauch von Informatikmitteln insbesondere deren Missbrauch und bei Verstoss gegen diese Weisung können personalrechtliche Sanktionen (Verweis bis Entlassung) ergriffen werden.

Art. 17. Inkrafttreten

Die Richtlinien treten auf den 1. September 2017 in Kraft.

Buttisholz, 31. August 2017

Gemeinderat Buttisholz

Franz Zemp	Reto Helfenstein
Gemeindepräsident	Gemeindeschreiber