Überall für alle SPITEX Bern	**IT Benutzerrichtlinie**
Richtlinie	

Daten zum Dokument	Person / Gremium	Datum
Autorin / Autor	J. Liechti	07.10.2020
Mitautor(en)	A. Mosimann	25.07.2023
Mitarbeit	IT Support	25.07.2023
Erstelldatum aktuelle Version	-	07.10.2020
Dokumentenprüfung	Leiterin Services	26.07.2023
Dokumentenfreigabe	erweiterte Geschäftsleitung	09.08.2023
Geplante Überprüfung (5 Jahre ab Gültigkeitsdatum)	09/2028 **Durch** IT Support	
Gültigkeitsbereich / gültig ab	SPITEX BERN	01.09.2023

Inhaltsverzeichnis

1 Grundlagen 3
1.1 Zweck 3
1.2 Geltungsbereich 3
1.3 Benutzererklärung 3
1.4 Begriffe und Abkürzungen 3
2 Grundsätze 4
2.1 Nutzung von Informatikmittel der SPITEX BERN 4
2.2 IT-Schulung der Mitarbeitenden 4
2.3 Verhaltenskodex 4
2.4 Meldepflicht von Vorkommnissen 5
3 Sicherheitsvorschriften beim Einsatz von Informatikmitteln 5
3.1 Benutzername und Passwort 5
3.2 Sperrung des Zugriffs auf Informatikmittel 6
3.2.1 Suspendierung von Geräten bei längeren Abwesenheiten 6
3.3 Erlaubte und Nicht erlaubte Anwendungen 6
3.4 Virenschutz 6
3.5 Netzwerk 7
3.6 Arbeitsplatz / Clear Desk 7
4 Sicherheitsvorschriften im Umgang mit Daten 7
4.1 Klassifikation von Daten 7
4.2 Erlaubte und Nicht erlaubte Datenspeicherung 8
4.3 Weitergabe von Daten 8
4.4 Ausdrucken von vertraulichen Informationen 8
4.5 Berufs- und Amtsgeheimnis 8
4.5.1 Strafrechtliches Berufsgeheimnis 9
5 Informatikmittel Tablets, Laptops, Smartphones 9
5.1 Tablets als Arbeitsgeräte 9
5.2 Laptops als Arbeitsgeräte 9
5.3 Smartphones als Arbeitsgeräte 10
5.3.1 Pool Geräte 10

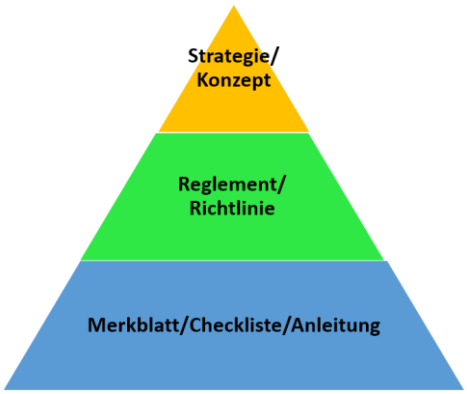
5.3.2 Private Geräte 10
5.3.3 Geschäftsabonnement 10
5.4 Rückgabe von Informatikmittel 10
6 Informatikmittel Outlook (E-Mail und Kalender) 11
6.1 E-Mail Signatur 11
6.2 E-Mail-Postfach und Archivierung 11
6.3 E-Mail Angriffe (Spam, Phishing etc.) 12
6.3.1 Umgang / Verwendung Links 12
6.3.2 PHISHING E-Mails 12
6.3.3 SPAM E-Mails 14
6.5 OUTLOOK Kalender 15
6.5.1 Freigabe des persönlichen Kalenders 15
6.5.2 Kennzeichnung von Kalendereinträgen 15
6.5.3 Aktivierung des Abwesenheitsassistenten 15
7 Handhabung von Internet 16
8 Handhabung von Social Media 17
9 Kontrolle und Sanktionen 17
10 Mitgeltende Dokumente 18
11 Inkrafttreten 18
12 Aktualisierungsverlauf 18

1 Grundlagen

1.1 Zweck

Diese Richtlinie regelt die sichere Benutzung der Informatikmittel, den Schutz der Informationen und deren Bearbeitung sowie die Nutzung von Internet und E-Mails und die Massnahmen bei Missbrauch.

Einbettung in die Dokumentenhierarchie der SPITEX BERN zum Thema Informationssicherheit und Datenschutz (ISDS).



→ ***IT Benutzerrichtlinie***

1.2 Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden der SPITEX BERN. Sie gilt zudem für alle Dienstleistenden und Gäste soweit diese die Informatikmittel der SPITEX BERN benutzen.

1.3 Benutzererklärung

Alle Mitarbeitenden der SPITEX BERN mit einem eigenen IT-Benutzerkonto erhalten eine Kopie dieser Richtlinie und müssen schriftlich bestätigen, dass der Inhalt gelesen und verstanden wurde. Die unterschriebene → ***IT-Benutzererklärung*** wird im jeweiligen Personaldossier aufbewahrt.

1.4 Begriffe und Abkürzungen

Datenschutzberaterin im Betrieb	Judith Liechti, Leitung Services
Informatikmittel	Sind alle Geräte, Einrichtungen und Dienste, die zur elektronischen Bearbeitung von Daten eingesetzt werden (Laptop, Tablet, Smartphone, Computer, Netzwerk, Speicher ……..).
ISDS	Informationssicherheit / Datenschutz
IT	Informationstechnologie
IT-Partner	Ist der externe Hosting Partner der SPITEX BERN
IT-Dienstleistende	Sind alle Unternehmen, welche im Auftrag der SPITEX BERN Informatik Dienstleistungen erbringen (z.B. Installation und Betrieb des IT-Netzwerks , Wartung des Perigon, Installation von Laptops/Tablets, ……)
IT-Support	Sind die Schnittstelle zu den IT-Dienstleistenden, sie unterstützen, befähigen und schulen die IT-Anwender der SPITEX BERN.
IT-Verantwortliche	Sind für die operative Führung der Informatik zuständige Personen
Login	Kombination von Benutzername und Passwort zur Anmeldung und Identifikation bei Informatikgeräten, -systemen und -anwendungen
SUMO	Elektronische Supportmeldung an den IT-Support

2 Grundsätze

2.1 Nutzung von Informatikmittel der SPITEX BERN

Die Informatikmittel dienen der Unterstützung zur Erfüllung der Aufgaben bei der SPITEX BERN. Sie dürfen für private Zwecke ausschliesslich verwendet werden, wenn folgende Grundsätze eingehalten werden:

- Die Informatikmittel dürfen **nicht missbräuchlich** verwendet werden, d.h. eine gesetzwidrige oder gegen interne Richtlinien verstossende Nutzung ist verboten.
- Die Informatikmittel dürfen **nicht zweckwidrig** verwendet werden, d.h. jede übermässige Beanspruchung von Ressourcen (z.B. übermässige Benutzung von Speicherkapazität oder Verbrauchsmaterial, berufliche und private Internetnutzung) ist nicht gestattet.

2.2 IT-Schulung der Mitarbeitenden

Bei der Einführung von IT-Neuerungen und bei Bedarf werden die Mitarbeitenden entsprechend geschult. Die Schulungen werden in Absprache mit der Leitung Services durch den IT-Support geplant und organisiert.

2.3 Verhaltenskodex

Für die Nutzung von Informatikmittel der SPITEX BERN gilt ein einheitlicher Verhaltenskodex.

Verboten sind:

- Verbreiten von beleidigenden oder herabwürdigenden Informationen;
- Verbreiten von unwahren Aussagen über eine Person oder über eine Personengruppe;
- Beleidigungen und Herabwürdigungen von Personen aufgrund ihrer Hautfarbe, Nationalität, Religion, politischen Gesinnung oder sexuellen Ausrichtung;
- Verbreiten von persönlichen oder anderen schützenswerten Informationen über Personen oder Personengruppen;
- Benutzen von Ressourcen über das gestattete Mass hinaus (z.B. Benutzung von Druckern, Netzwerken, Festplatte), das andere Mitarbeitende in ihrer Arbeit behindert;
- Zugriff auf und Kopieren von Daten Dritter, ohne vorher deren ausdrückliche Erlaubnis einzuholen;
- Kopieren und elektronisches Verbreiten von urheberrechtlich geschütztem Material;
- automatisches Weiterleiten von E-Mails an andere interne Benutzer, an externe Benutzer oder an die private E-Mail-Adresse (ausgenommen sind die Verwaltungsratsmitglieder der SPITEX BERN);
- Weitergabe von Zugangsberechtigungen (Benutzername und Passwort) an Dritte;
- Ausspähen von Passwörtern, inkl. der Versuch des Ausspähens mit technischen Hilfsmitteln;
- Manipulation oder Fälschung von elektronischen Informationen, im Speziellen die Vorgabe einer falschen Identität);
- Beschädigen oder zerstören von elektronischen Diensten;
- Ausnützen von erkannten Sicherheits- bzw. administrativen Mängeln.

Falls einem/einer Mitarbeiter/in Sicherheitsmängel auffallen, ist er/sie verpflichtet, sofort den IT-Support zu informieren (→ ***2.4****Fehler! Verweisquelle konnte nicht gefunden werden.* ***Meldepflicht von Vorkommnissen***).

2.4 Meldepflicht von Vorkommnissen

Alle Mitarbeitenden der SPITEX BERN melden dem IT-Support umgehend allfällige Vorkommnisse im Zusammenhang mit der Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel.

Werden Viren oder andere Schadsoftware in einem Informatikmittel vermutet, müssen sofort der IT-Support und der:die Datenschutzberater:in der SPITEX BERN informiert werden.

Meldung von Vorkommnissen

Montag – Freitag 8.00 – 17.00 Uhr: Mit elektronischer Supportmeldung SUMO (→ Intranet)

Notfälle ausserhalb der Betriebszeiten → ***Notfallvorgehen in den Standorten*** *(hängt am Schwarzen Brett in allen Standorten)*

Ebenso müssen Diebstähle oder Verluste von Informatikmitteln unverzüglich gemeldet.

Meldung bei Verlust oder Diebstahl von Informatikmitteln

- **Sofort** den IT-Support (via support@spitex-bern.ch) **und** die vorgesetzte Stelle informieren damit das Gerät (Tablet, Laptop, Smartphone) vom Zugriff auf das Netzwerk und die Systeme der SPITEX Bern gesperrt werden kann
- Das Formular → ***Schadenmeldung Geräte und Material*** ausfüllen und von der vorgesetzten Stelle visieren lassen. Ohne Visum wird das Gerät nicht ersetzt
- Ausgefülltes und visiertes Formular dem IT-Support.
- **Zusätzlich bei Diebstahl:** Der/die Mitarbeitende muss bei der Kantonspolizei Bern eine Anzeige erstatten. Entweder auf einem naheliegenden Polizeiposten oder online unter: https://www.police.be.ch/police/de/index/melden-anzeigen/melden-anzeigen/anzeigen.html

Meldung bei Beschädigung eines Geräts

- Die vorgesetzte Stelle informieren
- Das Formular → ***Schadenmeldung Geräte und Material*** ausfüllen und von der vorgesetzten Stelle visieren lassen. Ohne Visum wird das Gerät nicht ersetzt
- Ausgefülltes und visiertes Formular dem IT-Support

3 Sicherheitsvorschriften beim Einsatz von Informatikmitteln

Die Informatikmittel der SPITEX BERN sind so zu pflegen, dass sie vor Missbrauch durch Dritte, Diebstahl, Defekt oder Verlust bestmöglich geschützt sind.

Insbesondere ist auch dafür Sorge zu tragen, dass kein allfälliger Angriff auf die Geräte im Netzwerk (bspw. Phishing) erfolgreich sein kann oder dass Schadsoftware (bspw. Viren, Trojaner) sich weiter ausbreiten und verteilen können. Derartige Bedrohungen können dazu führen, dass Systeme, Applikationen und Daten nicht mehr zu Verfügung stehen. In schweren Fällen kann es zudem auch noch zu Datenverlust oder Datendiebstahl führen.

3.1 Benutzername und Passwort

Der Benutzername und das Passwort ermöglichen das Einloggen in das IT-System. Es gelten dabei folgende Grundsätze

- Das Passwort ist persönlich und darf nicht weitergegeben werden.
- Passworte dürfen nirgendwo sichtbar notiert und angebracht werden (z. B. an/unter der Tastatur, am Bildschirm/Telefonapparat, Notebook/Tablet).
- Wenn der Verdacht besteht, dass Drittpersonen das Passwort kennen, muss das Passwort sofort geändert werden.
- Wenn das Passwort 3x falsch eingegeben wird, wird das persönliche Login automatisch gesperrt.

Tipps zum Generieren eines starken Passworts

- Die User-Passwörter müssen mindestens 12 Zeichen enthalten (davon mindestens 1 Grossbuchstabe, 1 Zahl und 1 Sonderzeichen). Das persönliche Passwort ist 6 Monate gültig.
- Der eigene Name darf nicht Bestandteil des Passworts sein und auch die letzten 20 verwendeten Passwörter dürfen nicht wiederverwendet werden.
- Ganze Sätze und nicht nur einzelne Wörter verwenden; Eselsbrücken bilden
  z.B. JMbihu08.00UeP für JedenMorgenbenutzeichhierum08.00UhreinPasswort).
  Wem das zu lang ist, kann auch nur eine Kombination aus Buchstaben eines geläufigen Satzes verwenden (z.B. Beg2:1gB für Bern gewinnt 2:1 gegen Basel).
- Einzelnen Buchstaben durch eine Zahl oder ein Sonderzeichen ersetzen:
  den Buchstaben i ersetzen durch ein Ausrufezeichen (!) oder durch die Zahl 1
  den Buchstaben o ersetzen durch die Zahl 0 oder durch Klammern ()
  das Wort und ersetzen durch das Zeichen & oder +.
- Mit dem Link https://www.passwortcheck.ch/passwortcheck/passwortcheck kann die Qualität des Passwortes überprüft werden.**Passworterinnerung**: 14 Tage vor Ablauf des PW wird eine E-Mail an die persönliche Spitex-E-Mailadresse gesendet mit der Aufforderung das PW zu ändern. Diese Meldung wird jeden Tag einmal gesendet bis das Passwort geändert wurde.

→ Die persönlichen Passwörter der Mitarbeitenden werden nicht gesichert aufbewahrt.

3.2 Sperrung des Zugriffs auf Informatikmittel

Aus Gründen des Datenschutzes kann die Leiterin Services anordnen, den Zugriff auf Informatikmittel zu sperren oder einzuschränken.

3.2.1 Suspendierung von Geräten bei längeren Abwesenheiten

Wird ein Gerät ≥ 4 Wochen nicht benutzt (z.B. aufgrund unbezahltem Urlaub, Mutterschaft, Militär-/Zivildienst, Langzeitkrankheit, Unfall), wird der Zugriff auf das Perigon gesperrt und das Abonnement suspendiert (pausiert). So hat der:die Mitarbeiter:in keinen Zugriff auf Daten und die Abokosten fallen weg. Während der längeren Abwesenheit kann das Gerät entweder an den IT-Support zurückgegeben oder auf eigene Verantwortung bis zur Rückkehr am Teamstandort aufbewahrt werden.

3.3 Erlaubte und Nicht erlaubte Anwendungen

Die SPITEX BERN stellt ihren Mitarbeitenden alle für die Ausübung ihrer Tätigkeit erforderlichen Informatikmittel (insb. Anwendungen und Software) zur Verfügung.

Der Einsatz von privater Software, von Freeware (kostenlos erhältliche Programme) oder von Shareware (Software, die allgemein gegen ein geringes Entgelt erhältlich ist) auf den Informatikmitteln der SPITEX BERN ist verboten.

3.4 Virenschutz

Die Informatikmittel der SPITEX BERN verfügen über einen Virenschutz, der durch den IT Dienstleister eingerichtet, überwacht und aktuell gehalten wird → ***Informationssicherheit und Datenschutz (ISDS).***

Bei privaten IT-Geräten, mit denen Zugriff auf die Daten der SPITEX BERN erfolgen können, müssen die Mitarbeitenden zwingend selbst einen Virenschutz installieren, aktivieren und aktuell halten (Bsp. Avast Free Antivirus für Laptop, Tablet und Smartphones, www.avast.com).

3.5 Netzwerk

Das Netzwerk der SPITEX BERN (LAN oder WLAN) steht ausschliesslich den Mitarbeitenden zur Verfügung.

Gäste können sich über das WLAN **spi-guest** anmelden. Das dafür benötigte zeitlich befristete Passwort muss zuvor beim → ***IT-Support*** eingeholt werden.

3.6 Arbeitsplatz / Clear Desk

Der Clear-Desk-Policy-Ansatz besagt, dass Kundendaten bei Abwesenheit der Mitarbeitenden und nach Büroschluss unter Verschluss gehalten werden müssen. Beim Verlassen des Arbeitsplatzes muss darauf geachtet werden, dass keine Kundenunterlagen und Akten der SPITEX BERN offen auf dem Pult herumliegen und der Bildschirm gesperrt ist:

Tipps zum Sperren des Laptop-/Desktop-Bildschirms

Bildschirm mittels Tastenkombination <Ctrl>+<Alt>+<Delete> oder Windowstaste ( )+L sperren.

Danach kann durch Eingabe des persönlichen Passwortes der Bildschirm jederzeit wieder entsperrt werden

Mobile Geräte (Laptop, Tablet, Smartphone, etc.) niemals unbeaufsichtigt liegen lassen!

4 Sicherheitsvorschriften im Umgang mit Daten

Informationen über eine Person und deren gesundheitliche Probleme gehören zu den sensiblen Daten und sind deshalb als **besonders schützenswert** einzustufen. Als Konsequenz muss mit diesen Daten bei der SPITEX BERN besonders sorgfältig umgegangen, eine unbefugte Kenntnisnahme besonders rigoros verhindert werden. Der Umgang mit Informationen im Sinne des Datenschutzes, Berufs- und Amtsgeheimnis ist in der Richtlinie → ***Informationssicherheit und Datenschutz (ISDS)*** festgehalten.

Daten sind für die SPITEX BERN und deren Dienstleistungen von grosser Bedeutung. Die sorgsame Handhabung, Ablage und Sicherung aller Daten und Informationen mit Hilfe der Informatikmittel ist wichtig.

4.1 Klassifikation von Daten

Die SPITEX BERN unterscheidet folgende Stufen der Datenklassifizierung:

- **öffentliche** Daten
- **interne** Daten
- **vertrauliche** Daten

1. **Öffentliche** Daten sind für jedermann, auch ausserhalb der SPITEX BERN, zugänglich.
   Dabei handelt es sich zum Beispiel um Informationen, die auf der öffentlichen Webseite im Internet dargeboten werden, die Anschrift oder die Werbe- und Informationsbroschüre.

2. **Interne** Daten werden lediglich den Mitarbeitenden der SPITEX BERN (und allenfalls ausgewählten Partnerorganisationen) zugänglich gemacht.
   Dies können zum Beispiel Telefonverzeichnisse, Weisungen, Reglemente oder allgemeine Dokumente sein.

3. **Vertrauliche** Daten dürfen lediglich einer begrenzten Anzahl Personen zugänglich sein.
   Zum Beispiel sind Gehaltslisten und Mitarbeiterdossiers ausschliesslich dem HRM und der Geschäftsführung zugänglich.

Daten zu Kunden und deren Gesundheit sind besonders schützenwert und deshalb zwangsläufig als vertraulich zu behandeln.

4.2 Erlaubte und Nicht erlaubte Datenspeicherung

Alle Daten, welche bei den Mitarbeitenden anfallen resp. bei der Ausübung ihrer Tätigkeit erzeugt werden, müssen auf den von der SPITEX BERN zur Verfügung gestellten Informatikmitteln abgelegt und gespeichert werden. Nach Möglichkeit sollen alle Dokumente elektronisch abgespeichert werden.

Grundsätzlich dürfen keine Daten lokal (auf dem Desktop) abgespeichert werden. Diese werden nicht in die zentrale Datensicherung einbezogen.

Die Speicherung von geschäftsrelevanten Daten in externen Cloud-Services (bspw. Dropbox, iCloud, OneDrive) oder auf privaten Datenträger (bspw. USB Sticks, private Geräte) ist verboten.

4.3 Weitergabe von Daten

Die interne Weitergabe von E-Mails, Dokumenten, Verzeichnissen und Briefen – als Ausdruck oder als elektronische Kopie – ist, sofern es sich nicht um vertrauliche Dokumente handelt, grundsätzlich erlaubt.

Dokumente, die zwar öffentlich sind, aber nur von bestimmten Benutzern bearbeitet werden dürfen, müssen mit einem **Schreibschutz** (→ ***IT Anleitung User***) versehen werden.

Vertrauliche oder wichtige Dokumente müssen mit einem **Kennwort** (→ ***IT Anleitung User***) geschützt werden.

An Drittpersonen dürfen elektronische Kopien nur als **pdf-Datei** (→ ***IT Anleitung User***) weitergegeben werden.

E-Mails können jederzeit an interne Empfänger weitergeleitet werden, sofern der Inhalt dafür bestimmt ist. Interne E-Mails dürfen nicht an Drittpersonen weitergeleitet werden.

E-Mails an externe Personen sind ihrem Inhalt entsprechend zu behandeln und nur an involvierte Personen weiterzuleiten.

4.4 Ausdrucken von vertraulichen Informationen

Für den Ausdruck von vertraulichen Informationen oder besonderen Personendaten muss die Funktion **Geschützter Druck** verwendet werden ***(→ IT-Anleitung User)***.

4.5 Berufs- und Amtsgeheimnis[1]

Alle Mitarbeitende der SPITEX BERN müssen über alles, was sie während der Arbeit wahrnehmen, Stillschweigen bewahren (→ ***Anstellungsreglement SPITEX BERN*)*.**

Die Mitarbeitenden der SPITEX BERN sind für den sicheren Umgang mit Daten und Informationen, die ihnen zugänglich sind, verantwortlich. Dies gilt am Arbeitsplatz, an den Betriebsstandorten, bei Kunden sowie im privaten und öffentlichen Umfeld.

Interne Angelegenheiten der SPITEX BERN sollten, wenn immer möglich im geschäftlichem Rahmen besprochen werden. Im öffentlichen Raum (z.B. Arbeitsweg, Freizeit) und in Gesprächen mit Dritten müssen Interna mit der nötigen Verschwiegenheit behandelt werden.

Die Verletzung des Berufs- und Amtsgeheimnisses ist auch nach Beendigung der Berufsausübung, der Studien oder des dienstlichen oder amtlichen Verhältnisses strafbar.

Was gemäss Öffentlichkeitsprinzip öffentlich zugänglich ist, untersteht nicht dem Amtsgeheimnis.

[1] Auszug aus RL Informationssicherheit und Datenschutz ISDS

4.5.1 Strafrechtliches Berufsgeheimnis

Pflegefachpersonen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Ebenso werden Studierende bestraft, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen.

Die Pflegenden unterstehen unmittelbar der Gesetzesbestimmung, die übrigen Mitarbeitenden der SPITEX BERN gelten als Hilfspersonen im Sinne von Art. 321 Ziff. 1 StGB und fallen somit ebenfalls unter das Berufsgeheimnis.

5 Informatikmittel Tablets, Laptops, Smartphones

Anleitungen, Tipps und Hilfen zur Handhabung der Tablets, Laptops oder Smartphones sind in den **→ *IT Anleitung User + IT Anleitung Tablets*** dokumentiert und beschrieben.

Verlust, Diebstahl oder Beschädigung eines Gerätes ist umgehend dem IT-Support zu melden **→ *Meldepflicht von Vorkommnissen.***

5.1 Tablets als Arbeitsgeräte

Alle Mitarbeitende, die Leistungen bei Kunden erbringen, erhalten zur Leistungserfassung und als Arbeitshilfe ein Tablet.

Alle erforderlichen **Applikationen** (Apps) sind darauf installiert. Die Installation von zusätzlichen (privaten) Apps ist nicht erlaubt und wird technisch blockiert.

Die Tablets sind mit einer **SIM-Karte** ausgestattet und können deshalb auch als Kommunikationsmittel (E-Mail, Telefonie, Internet) genutzt werden.

Der Zugang über **Bluetooth** ist deaktiviert.

WLAN darf nur mit verschlüsselten Access Points (Hotspots) benutzt werden. Im öffentlichen Raum darf WLAN nie aktiviert sein. Das Tablet selber darf nicht als WLAN Hotspot genutzt werden. Ausnahmen ab Stufe Kader können von der Geschäftsleitung bewilligt werden.

Das Tablet ist Eigentum der SPITEX BERN und darf deshalb nur bedingt für private Zwecke benutzt werden, die Privatsphäre ist eingeschränkt. Die SPITEX BERN kann als Arbeitgeberin bei Bedarf in die SIM-Kartenabrechnungen (Volumen, Zieladressen) Einsicht nehmen.

5.2 Laptops als Arbeitsgeräte

Alle Mitarbeitende ab Stufe Kader erhalten auf Antrag einen Laptop als Arbeitsinstrument.

Alle erforderlichen **Applikationen** (Software, Apps) sind darauf installiert. Die Installation von zusätzlichen (privaten, Freeware, Shareware) Applikationen ist nicht erlaubt und wird technisch blockiert.

Bluetooth muss deaktiviert sein. SPITEX BERN stellt das nötige Material (bspw. zum Anschluss einer externen Maus oder eines Headsets) zur Verfügung.

WLAN darf nur mit verschlüsselten Access Points (Hotspots) benutzt werden. Im öffentlichen Raum darf WLAN nie aktiviert sein.

An den SPITEX Standorten sind gesicherte und verschlüsselte Accesspoints zum Zugriff auf das Netzwerk der SPITEX BERN installiert. Zugang durch Laptop muss manuell eingerichtet und mit einem Schlüssel aktiviert werden.

Der Laptop ist Eigentum der SPITEX BERN und darf deshalb nur bedingt für private Zwecke benutzt werden, die Privatsphäre ist eingeschränkt. Die SPITEX BERN kann als Arbeitgeberin bei Bedarf die Nutzung und den Verbindungsaufbau eines Laptops durch den **→ *IT-Dienstleister*** überprüfen lassen.

USB Anschluss Nutzung: Für Maus, Tastatur, Präsenter, Bildschirm.

5.3 Smartphones als Arbeitsgeräte

Die SPITEX BERN unterscheidet folgende Kategorien von Smartphones:

- **Pool** Geräte (Gerät und Abonnement im Eigentum der SPITEX BERN)
- **private** Geräte (Gerät und Abonnement im Eigentum der Mitarbeitenden)
- **Geschäftsabonnement** (Gerät im Eigentum der Mitarbeitenden, Abonnement im Eigentum der SPITEX BERN)

5.3.1 Pool Geräte

Für Mitarbeitende, die Leistungen bei Kunden erbringen stehen an den Standorten Ersatztablets und Pikett-telefone (sog. **Poolgeräte**) als Arbeitsinstrumente zur Verfügung.

Alle erforderlichen Applikationen (Apps) sind darauf installiert. Die Installation von zusätzlichen Apps ist nicht erlaubt und wird technisch blockiert.

Der Zugang über **Bluetooth** ist deaktiviert → ***IT Anleitung User***.

WLAN darf nur mit verschlüsselten Access Points (Hotspots) benutzt werden. Im öffentlichen Raum darf WLAN nie aktiviert sein. Das Smartphone darf nicht als WLAN Hotspot genutzt werden.

Die Pool Geräte sind Eigentum der SPITEX BERN und dürfen deshalb nur bedingt für private Zwecke benutzt werden, die Privatsphäre ist eingeschränkt. Die SPITEX BERN kann als Arbeitgeberin bei Bedarf Einsicht in die SIM-Kartenabrechnungen (Volumen, Zieladressen) nehmen.

5.3.2 Private Geräte

Private Geräte von Mitarbeitenden ab Stufe Kader können zum Zugriff auf E-Mail/Kalender der SPITEX BERN genutzt werden.

Bei der Nutzung des privaten Smartphones muss die Installation des SPITEX E-Mail/Kalender und der erforderlichen Sicherheitsmassnahmen gemäss den Vorgaben der SPITEX BERN durchgeführt werden → ***IT Anleitung User***.

Das private Smartphone muss dabei mindestens:

- durch einen PIN-Code zum Starten bzw. Entsperren des Bildschirmes geschützt sein
- über einen aktuellen Antivirus Schutz verfügen (bspw. Avast, Avira o.ä.).

Bei der Nutzung des privaten Laptops muss die Installation des Horizon View Client (Home-Office Zugriff) über den IT-Support der SPITEX BERN durchgeführt werden. Für die Installation auf dem privaten PC erhalten die Mitarbeitenden ab Stufe Kader eine Anleitung vom IT-Support.

5.3.3 Geschäftsabonnement

Leitende Angestellte erhalten ein Geschäftsabonnement, nutzen jedoch ihr persönliches, privates Smartphone.

Auf Wunsch kann die private Telefonnummer auf die SPITEX BERN umgeschrieben werden. Oder sie erhalten eine zweite SIM Card für ihr Smartphone (d.h. eine neue, zusätzliche Nummer).

Das Abonnement ist Eigentum der SPITEX BERN, die Privatsphäre ist deshalb eingeschränkt. Die SPITEX BERN kann als Arbeitgeberin bei Bedarf Einsicht in die SIM-Kartenabrechnungen (Volumen, Zieladressen) nehmen.

5.4 Rückgabe von Informatikmittel

Im Rahmen des Austrittsgesprächs müssen die Geräte inklusive Zubehör der SPITEX BERN zurückgegeben werden. Die SPITEX BERN behält sich vor, fehlendes Material angemessen zu verrechnen.

6 Informatikmittel Outlook (E-Mail und Kalender)

E-Mail und Kalender stellen die zentralen Arbeitsinstrumente in der Kommunikation und Zusammenarbeit aller Mitarbeitenden dar.

E-Mails stellen jedoch auch einen zentralen Angriffspunkt für die Verbreitung von Schadsoftware (Viren, Trojaner etc.) und eine willkommene Plattform für Erpressungs-, Phishing- oder Betrugsversuche dar ***→ 6.3 E-Mail Angriffe (Spam, Phishing etc.).***

Mitarbeitende der SPITEX BERN erhalten bei ihrem Eintritt eine **persönliche E-Mail-Adresse** und damit verbunden ein Outlook **E-Mail-Postfach** und einen Outlook **Kalender**

Die Publikation der SPITEX BERN E-Mailadresse (vorname.nachname@spitex-bern.ch) für private Zwecke (bspw. Vereine, Politik, Private Homepage) ist nicht erlaubt.

6.1 E-Mail Signatur

Die korrekte SPITEX BERN E-Mailsignatur wird für alle Mitarbeitende mit eigenem Postfach automatisch durch den IT-Support nach den folgenden Kriterien hinterlegt.

- Die Bezeichnung der Funktion leitet sich aus dem Arbeitsvertrag/dem Anstellungsprofil ab.

  Beispiel:
  SPITEX BERN, Salvisbergstrasse 6, 3006 Bern
  Telefon +41 (0)31 388 50 50, Fax + 41 (0)31 388 50 40
  E-Mail maria.muster@spitex-bern.ch
  Besuchen Sie auch unsere Website: www.spitex-bern.ch

- Die Ergänzung mit der persönlichen Mobilenummer und/oder der direkten internen Telefonnummer ist fakultativ und kann bei Bedarf beantragt werden

Sind Korrekturen oder Anpassungen notwendig, so kann dies über eine elektronischer Supportmeldung (SUMO) dem ***→ IT Support*** gemeldet werden.

6.2 E-Mail-Postfach und Archivierung

E-Mails mit Anhängen, Grafiken oder Fotos brauchen viel Speicherplatz. Das Postfach jeder Empfängerin muss deshalb laufend aufgeräumt werden, d.h. die gelesenen und bearbeiteten E-Mails müssen regelmässig gelöscht werden.

Gelesene E-Mails, die älter als sechs Monate sind, werden automatisch archiviert und aus dem Postfach entfernt.

Diese archivierten E-Mails können jederzeit durch die Eigentümerin des Postfaches zurückgeholt werden ***→ IT Anleitung User (MailStore)***.

Die automatische Archivierung schliesst auch private E-Mails ein, die von oder an die geschäftliche E-Mail-Adresse geschickt werden. Unter der Angabe der notwendigen Daten (Absender, Datum, Uhrzeit) kann beim IT-Support die Löschung von privaten, archivierten E-Mails verlangt werden.

6.3 E-Mail Angriffe (Spam, Phishing etc.)

Immer wieder versuchen Internet-Betrüger, mit gefälschten Mails an vertrauliche Daten zu kommen. Die Betrüger nutzen die Gutgläubigkeit ihrer Opfer aus, indem sie ihnen E-Mails mit gefälschten Absenderadressen zustellen.

In derartigen E-Mails wird das Opfer beispielsweise darauf hingewiesen, dass seine Kontoinformationen und Zugangsdaten (d.h. Benutzername und Passwort) nicht mehr sicher oder aktuell sind und es diese unter dem im E-Mail aufgeführten Link ändern soll.

- Als **Phishing** werden E-Mails (seltener auch SMS oder Anrufe) bezeichnet, die z.B. versuchen Passwörter zu stehlen oder auf einem Computer einen Virus zu verbreiten.
  Ein Phishing-E-Mail kann beispielsweise eine gefälschte Rechnung oder ein verlockendes Angebot sein. Häufig verlangt es dazu eine sofortige Handlung, um Sie dazu zu bringen ein gefälschtes Formular auszufüllen, den Link zu einer gefälschten Webseite zu klicken oder einen infizierten Anhang zu öffnen.

- Als **Spam** oder **Junk** werden E-Mails bezeichnet, die dem Empfänger unaufgefordert und unerwünscht zugestellt werden, meistens von einem unseriösen Absender.
  Früher konnte man ein Spam-E-Mail an den vielen Grammatikfehlern erkennen. Das ist heute kaum mehr so. Die Absender benutzen Namen bekannter Unternehmen und kopieren auch deren E-Mail-Layouts so, dass sie täuschend echt aussehen

Der → ***IT-Dienstleister*** der SPITEX BERN filtert E-Mails auf **Spam**. Dabei werden alle eingehenden und ausgehenden E-Mails systematisch auf spam-typische Elemente überprüft. Weist ein E-Mail verdächtige Merkmale auf, gelangt es automatisch in den Spam-Ordner.

Der → ***IT-Dienstleister*** der SPITEX BERN unterhält eine **Antivirenprüfung** für E-Mail und E-Mail Anhänge. Dabei werden alle eingehenden und ausgehenden E-Mails systematisch auf verdächtige Anhänge überprüft (Dateitypen). Enthält ein E-Mail verdächtige Anhänge so werden diese automatisch im E-Mail gelöscht.

6.3.1 Umgang / Verwendung Links

Grundsätzlich ist es bei der Spitex Bern nicht erlaubt Links zu öffnen oder zu versenden. Die Gefahr, dass sich eine Phising Mail dahinter verbirgt und grossen Schaden im Betrieb anrichtet, ist sehr gross.

Mittlerweile arbeiten aber viele Dienstleister mit Links und es gibt oftmals keine andere Möglichkeit, als diese zu nutzen (z.B. für Anmeldungen an Aus- und Weiterbildungen, Besuch von Tagungen ect.). Daher gilt für die Mitareitenden der Spitex Bern:

Bevor ein Link geöffnet wird, muss dieser durch den IT Support geprüft und freigegeben werden!

Prüfung auf Links im E-Mail

- Ist der Absendername und die Absender-E-Mail-Adresse bekannt?
- Ist der Betreff sinnvoll?
- Wird ein Anhang von diesem Absender erwartet?

Ergeben diese drei Punkte **ein stimmiges Bild**, so ist das **E-Mail direkt dem IT Support zur Überprüfung weiterzuleiten. Intern wird der Link überprüft und allenfalls freigegeben oder die Mail vernichtet und die Mitarbeitenden darüber informiert.**

Der Absender noreply@contactbot.oxoa.ch sendet immer Links, welche direkt ins Perigon verweisen. Diese Links dürfen von den TL und STV TL gedrückt werden nach dem diese vom ZKS weitergeleitet wurden. Die Mitarbeitenden vom ZKS werden intern durch die IT geschult und aufgezeigt wie die Mail korrekt überprüft wird, bei Unsicherheiten werden auch diese Mails mit Link Inhalte vom IT Support geprüft.

6.3.2 PHISHING E-Mails

Phishing E-Mails stellen ganz gezielte Attacken dar, um an vertrauliche Informationen zu gelangen, um IT Systeme lahmzulegen oder um erpresserische Aktionen durchführen zu können.

Damit man nicht in die Phishing-Falle tappt, sollte jedes E-Mail bevor es geöffnet wird, kurz an Hand der nachfolgenden Kriterien überprüft werden:

Prüfung auf Phishing E-Mail

- Ist der Absendername und die Absender-E-Mail-Adresse bekannt?
- Ist der Betreff sinnvoll?
- Wird ein Anhang von diesem Absender erwartet?

Ergeben diese drei Punkte **kein** stimmiges Bild, so ist das **E-Mail direkt zu löschen** (im Postfach und im Outlook Ordner **Gelöschte Elemente** → ***IT Anleitung User***) und **umgehend** den → ***IT-Support*** zu informieren.

Bei Unsicherheit kann die **E-Mail als Anlage** an den → ***IT-Support*** weitergeleitet werden → ***IT Anleitung User***.

Quelle: https://www.swisscom.ch/de/privatkunden/hilfe/internet/phishing.html

WICHTIG!
Niemals einen Link oder Anhang eines unseriösen E-Mails öffnen.

Es lohnt sich zudem auf weitere Erkennungsmerkmale zu achten und speziell auch die im E-Mail eingefügten Links und Anhängen nach den folgenden Kriterien zu prüfen:

- **Kryptische Mail-Adresse**
  Buchstabensalat und eine Domain (der Teil nach dem @-Zeichen), die nicht zum vorgegaukelten Absender passt, sind ein eindeutiges Zeichen.
  Vorsicht: *Es ist einfach, Absenderadressen zu fälschen. So können auch Phishing-Mails mit einem vordergründig legitimen Absender daherkommen.*
- **Aufforderung, sofort zu handeln**
  Wenn Sie sofort beispielsweise die Kreditkarte aktivieren oder eine Sendebestätigung überprüfen sollen, ist das vielleicht nur ein psychologischer Trick eines Cyberkriminellen
  Wir Menschen neigen unter Stress dazu, mehr Fehler zu machen und bspw. auf einen Phishing-Link zu klicken.
- **Sie sind gar nicht Kunde**
  Wenn Sie Post mit einer Handlungsaufforderung von einem Finanzinstitut erhalten, bei dem Sie gar nicht Kunde sind, handelt es sich mit Sicherheit um ein Phishing-Mail.
- **Link-Text und Link stimmen nicht überein**
  Der Text im Mail zeigt eine vertrauenswürdige Adresse an, der Link dahinter führt aber auf eine ganz andere Seite.
  Das eigentliche Ziel eines Links erkennen Sie, wenn Sie im Mail mit der Maus über den Link fahren – ohne zu klicken!
- **Schreibfehler und einfache Sprache**
  Schlechtes Deutsch oder Englisch und eine einfache Sprache sind Merkmale für ein Phishing-Mail.
  Ziehen Sie nicht den Umkehrschluss, dass ein fehlerfrei formuliertes Mail seriös ist.
- **Unpersönliche Anrede**
  Ansprachen wie «Hello», der vordere Teil meiner Mailadresse oder gar keine Anrede deuten auf ein Phishing-Mail hin.
  Das gilt allerdings nicht für gezielte Angriffe.
- **Verdächtige Anhänge**
  Rechnung oder Lieferbestätigung als Word-Dokument oder eine angehängte Blindbewerbung als PDF: In solchen Fällen ist Vorsicht geboten. Vor allem, wenn der Dateiname sehr generisch gehalten ist («facture.docx»).

- **Anhänge mit ausführbaren Dateien** (bspw. .com, .chm, .cmd, .exe, .jar, .js, .ps1), mit verschlüsselten Archiven (bspw. .7z, .zip, .rar) oder doppelten Dateiendungen (bspw. .pdf, .zip, .doc.exe) weisen auf ein Virus E-Mail hin

  Im Zweifelsfall fragen Sie beim (angeblichen) Absender nach. Aber nicht, indem Sie auf das E-Mail antworten. Sondern, indem Sie die Website des Unternehmens besuchen, dort die Kontaktinformationen suchen und telefonisch nachfragen.
- **Angabe persönlicher Daten**
  Will der Absender, dass Sie aufs Mail antworten mit persönlichen Daten? Das ist eine Garantie für betrügerische Post. Ihre Bank oder sonst ein Online-Dienstleister fragen Sie nie nach Ihrem Passwort. Solche Anfragen sind ein weiteres Indiz.
  Schwieriger ist es, wenn Sie auf eine Login-Seite geführt werden. Im Zweifelsfall klicken Sie nicht auf den Link.

6.3.3 SPAM E-Mails

Damit man nicht in die Spam-Falle tappt, sollte jedes E-Mail bevor es geöffnet wird, kurz an Hand der nachfolgenden Kriterien überprüft werden:

Prüfung auf Spam E-Mail

- Ist der Absendername und die Absender-E-Mail-Adresse bekannt?
- Ist der Betreff sinnvoll?
- Wird ein Anhang von diesem Absender erwartet?

Ergeben diese drei Punkte **kein** stimmiges Bild, so ist die **E-Mail direkt zu löschen** (im Postfach und im Outlook Ordner **Gelöschte Elemente** → ***IT Anleitung User***) und **umgehend** den → ***IT-Support*** zu informieren.

Bei Unsicherheit kann die **E-Mail als Anlage** an den → ***IT-Support*** weitergeleitet werden ***(→ IT-Anleitung User)***.

Quelle: https://www.swisscom.ch/de/privatkunden/hilfe/internet/spam.html

WICHTIG!
Niemals einen Link oder Anhang in einer Spam-verdächtigen E-Mail öffnen.

Spam E-Mails **nicht beantworten**, denn so weiss der Sender, dass die E-Mail-Adresse gültig ist und wird weiter Spam verschicken. Mit Vorsicht ist auch Spam mit «Abbestelloption» zu geniessen. Darin wird versprochen, dass man durch Senden einer E-Mail mit bestimmtem Inhalt von der Verteilerliste gestrichen wird.

6.5 OUTLOOK Kalender

Zur Übersicht und für die Organisation der Zusammenarbeit innerhalb der SPITEX BERN ist der elektronische Kalender ein unverzichtbares Instrument.

6.5.1 Freigabe des persönlichen Kalenders

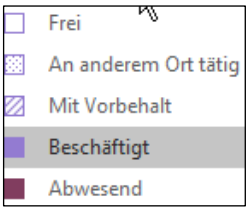
Für jede Mitarbeitende wird bei deren Eintritt ein persönlicher Kalender angelegt.

Damit andere Mitarbeitende innerhalb der SPITEX BERN auf diesen Kalender Einsicht nehmen können, muss dieser einmalig freigegeben werden → ***IT Anleitung User***.

6.5.2 Kennzeichnung von Kalendereinträgen

Die farbliche Kennzeichnung von Kalendereinträgen unterstützt die effiziente Zusammenarbeit und verhindert Missverständnisse bei Terminfindungen oder -absprachen.

Einträge im Outlook Kalender der SPITEX BERN sollten mit der folgenden Farbkennzeichnung versehen werden:



6.5.3 Aktivierung des Abwesenheitsassistenten

Outlook enthält einen Abwesenheitsassistenten, welcher bei Abwesenheiten die E-Mail Absender (intern und extern) mit einer kurzen standardisierten Rückantwort bedient.

Die Abwesenheitsmeldung kann für einen spezifischen Zeitraum oder einzelne Tage aktiviert werden. Die Abwesenheitsmeldung wird nur einmal dem E-Mail Absender zugestellt. Für die Nachricht an die E-Mail Absender wird zwischen einem Absender **innerhalb** der Organisation und einem Absender **ausserhalb** der Organisation unterschieden → ***IT Anleitung User***.

Bei **Abwesenheiten von mehr als einem Tag** ist die untenstehende Abwesenheitsnotiz für Absender ausserhalb der SPITEX Bern Organisation zwingend einzurichten:

Guten Tag

Vielen Dank für Ihre Nachricht. Sie erreichen mich wieder am Wochentag, TT.MM.JJJJ.

Meine Nachrichten werden nicht weitergeleitet. In dringenden Fällen wenden Sie sich bitte direkt an Vorname Name (Telefon 031 388 xx xx oder vorname.name@spitex-bern.ch).

Freundliche Grüsse
Vorname Nachname, Funktion

SPITEX BERN, Salvisbergstrasse 6, 3006 Bern
Telefon +41 (0) 31 388 50 50, Fax + 41 (0) 31 388 50 40
E-Mail maria.muster@spitex-bern.ch
Besuchen Sie auch unsere Website: www.spitex-bern.ch

7 Handhabung von Internet

Das Internet ist ein Arbeitsmittel. Der Internet Zugang der SPITEX BERN dient nur der Beschaffung von Informationen.

Bei Bezug von Informationen ist stets auf die Vertrauenswürdigkeit der Quellen und die Urheberrechte bzw. Schutzrechte (Copyright, Trademarks etc.) der Materialien und Informationen zu achten.

Informationen zu Medikamenten sollten nur auf **Medi Compendium** nachgeschlagen werden.

Wenn der Verdacht besteht, dass von gewissen Internetseiten Schadsoftware verbreitet oder Cyberangriffe ausgelöst werden, kann die IT-Leitung der SPITEX BERN beim → ***IT-Dienstleister*** diese Internetadressen sperren lassen.

Die Nutzung für private Zwecke ist auf ein Minimum zu beschränken und muss ausserhalb der offiziellen Arbeitszeit geschehen. Die Mitarbeitenden dürfen den zur Verfügung gestellten Internet-Zugang weder zur Begehung, noch zur Unterstützung von strafbaren Handlungen, der Aufforderung zu Verbrechen oder Gewalttätigkeit, oder der Rassendiskriminierung nutzen.

Bei Verdacht auf Missbrauch kann die IT-Leitung die Nutzung der Internetseiten pro User überprüfen.

Beim Umgang mit Internet Plattformen, Foren und Informationsquellen gilt folgendes zu beachten:

- Internetseiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt dürfen weder angewählt noch per E-Mail weitergeleitet werden.
- Die Teilnahme an interaktiven Medien, insbesondere an Chatrooms sowie Onlinespielen, ist verboten.
- Das Herunterladen oder die Installation von Spielen aus dem Internet ist grundsätzlich verboten.
- Das Herunterladen von Audio- und Videodateien zu geschäftlichen Zwecken ist nur nach Absprache mit der IT-Leitung zulässig.
- Bei ungewöhnlichen oder zweifelhaften Kontaktaufnahmen keine Information herausgeben und keine Anweisungen befolgen, auch wenn man unter Druck gesetzt wird.
- Müssen Daten über eine Internet-Verbindung übermittelt (hochgeladen) werden, so ist darauf zu achten, dass Verbindung verschlüsselt ist. Dies erkennen Sie daran, dass die Adresszeile des Browsers mit „https://“ beginnt und ein Schloss-Symbol in Ihrer Browserzeile angezeigt wird.

8 Handhabung von Social Media

Die → ***Social Media Guidelines des Spitex Verbandes Schweiz*** gelten vollumfänglich auch für die Mitarbeitenden der SPITEX BERN.

Nachstehend wird auf einzelne Bestimmungen der Guidelines hingewiesen:

- **Verantwortlichkeit**
  Die Verantwortung für den Social Media-Auftritt der SPITEX BERN obliegt der dafür zuständigen Person. Es können weitere Mitarbeitende für den Einsatz autorisiert werden.
  Aktiv sind ausschliesslich die dafür bestimmten Personen. Weiteren Mitarbeitenden kann bei Bedarf die Benutzung bewilligt werden.
- **Internes vertraulich behandeln, Internes bleibt intern!**
  Bemerkungen über interne Projekte (abgeschlossene oder laufende), Probleme oder Fortschritte, Kunden und Dienstleister sind vertraulich ***(→ 4.1 Klassifikation von Daten*)** zu behandeln und gehören nicht in die sozialen Medien.
- **Persönlichkeitsschutz und Bildrecht**
  Der Persönlichkeitsschutz von Mitarbeitenden und von Kunden muss jederzeit gewährleistet sein. Die Bildrechte sind vor dem Veröffentlichen zu klären. Von betroffenen Personen muss das schriftliche Einverständnis eingeholt werden
- **Sprachwahl**
  Die Beiträge sind in einem korrekten, angemessenen und gut verständlichen Stil zu verfassen. Folgende allgemeine Grundsätze sind einzuhalten:
  - Keine Inhalte, die beleidigend, rufschädigend, persönlichkeitsverletzend, rassistisch, vulgär oder sexistisch sind.
  - Keine Aussagen, die der SPITEX BERN schaden
- **Kommentare**
  Nur berechtigte Personen dürfen externe Beiträge kommentieren.
  Die Kommentare sind respektvoll, sachlich und höflich zu beantworten.
  Kommentare dürfen nicht gelöscht werden nur, weil Mitarbeitende anderer Meinung sind oder etwas kritisieren – ausser der Beitrag ist beleidigend, rassistisch, sexistisch oder persönlichkeitsverletzend.
- **Prinzipien für den Privatgebrauch**
  Mitarbeitenden der SPITEX BERN ist es untersagt, sich in ihren privaten Profilen im Namen der SPITEX BERN zu äussern.

9 Kontrolle und Sanktionen

Liegen eindeutige Anhaltspunkte für Verstösse gegen die IT-Benutzerrichtlinien bzw. für Missbräuche, Zweckentfremdung oder nicht erklärbare Vorkommnisse vor, veranlassen die IT-Verantwortlichen persönliche Kontrollen und Abklärungen. Die vorgesetzte Stelle wird informiert.

Um die IT-Sicherheit zu wahren, behält sich die SPITEX BERN vor, unter Berücksichtigung der gesetzlichen Datenschutzvorschriften, in sporadischen Abständen die Soft- und Hardware der Mitarbeitenden zu überprüfen. Es wird dabei nur die Sicherheit der installierten Software und nicht deren Inhalt kontrolliert.

Verstösse gegen diese Richtlinien, sowie die sonstigen Regelungen und Vorschriften bezüglich die Verwendung der Informatikmittel und den Umgang mit personenbezogenen Daten, können dienst- und arbeitsrechtliche, allenfalls auch strafrechtliche Konsequenzen haben. In schwerwiegenden Fällen können sie auch Grund für eine fristlose Auflösung des Anstellungsverhältnisses sein.

10 Mitgeltende Dokumente

Dokumentenart	Dateiname
Anleitung	- IT Anleitung Tablet - IT Anleitung User
Kurzanleitung	- Passwort selber zurücksetzen
Formular	- Schaden-oder Verlustmeldung Geräte_Material
Richtlinie	- Informationssicherheit und Datenschutz ISDS
Checkliste	- Notfallvorgehen in den Standorten

Partner	Dateiname
SPITEX Verband Kanton Bern	- Social Media Guidelines des Spitex Verbandes Schweiz

11 Inkrafttreten

Die überarbeitete Version IT Benutzerrichtlinie wurde durch die erweiterte Geschäftsleitung der SPITEX BERN am 9. August 2023 verabschiedet und tritt per 1. September 2023 in Kraft.

SPITEX BERN
Spitex Genossenschaft Bern

Claudine Bumbacher
Geschäftsführerin

Judith Liechti
Leiterin Services
Mitglied der Geschäftsleitung

12 Aktualisierungsverlauf

Änderung: Inhalt(e) des Dokuments	Datum	Autor/-in
Komplettüberarbeitung	07.10.2020	A. Mosimann
Divierse Aktualisierungen aufgrund neuem DSG ab 01.09.23 Kapitel 4.5 Berufs- und Amtsgeheimnis ergänzt Kapitel 6.3.1 Umgang / Verwendung Links ergänzt	25.07.2023	U.Dolder A. Mosimann