Datenschutz- und Informationssicherheitskonzept

Inhaltsverzeichnis

Spitex Zürich Limmat AG
28. Juni 2016

Spitex Zürich Limmat AG
Spitex Zürich
Nordstrasse 20, 8006 Zürich
Briefadresse: Postfach 434, 8042 Zürich
T 058 404 36 36, F 058 404 36 55
limmat@sec.spitex-zuerich.ch
www.spitex-zuerich.ch

A. Zweck und Ziel

Das Datenschutz- und Informationssicherheitskonzept regelt die Umsetzung des Datenschutzes und der ICT-Nutzung in der Spitex Zürich Limmat AG, deren **Einhaltung ist von grosser Wichtigkeit, bei Fehlverhalten bestehen nicht zu unterschätzende Reputationsrisiken**. Es stützt sich auf das Merkblatt für den Datenschutz und die Datensicherheit der Spitex Zürich Limmat AG vom 1.1.2015 und die Empfehlungen des Datenschutzbeauftragten des Kantons Zürich zum Datenschutz für die Spitex-Organisationen mit öffentlichem Leistungsauftrag im Kanton Zürich vom 22.8.2014 ab.

Das Dokument hat zum Ziel, alle Mitarbeitende der Spitex Zürich Limmat AG zu unterstützen, indem es die wichtigsten Punkte bezüglich Datenschutz und Informationssicherheit festhält.

B. Geltungsbereich

Die Wahrung von Datenschutz und Informationssicherheit ist Aufgabe aller Mitarbeitenden der Spitex Zürich Limmat AG. Sie sind im Rahmen ihrer Tätigkeiten verantwortlich für die sichere und datenschutzkonforme Bearbeitung von Daten. Dies gilt sowohl für die internen als auch externen Mitarbeitenden der Spitex Zürich Limmat AG, welche die ICT-Infrastruktur oder ICT-Dienste nutzen oder Daten der Organisation bearbeiten.

C. Umgang mit Informationen

a Die Mitarbeitenden der Spitex Zürich Limmat AG sind verantwortlich für den sicheren Umgang mit Daten und Informationen, welche ihnen zugänglich sind. Dies gilt sowohl am Arbeitsplatz im Zentrum als auch bei Kunden, zu Hause oder in der Öffentlichkeit.

b Für das Bearbeiten von Geschäftsdaten sind grundsätzlich von der Spitex Zürich Limmat AG zugelassene ICT-Mittel einzusetzen. Bei Telearbeit gelten die Richtlinien und Vereinbarung zur Telearbeit in der Spitex Zürich Limmat AG vom 29.1.2016.

c Vertrauliche Informationen und insbesondere Personendaten[1]
- sind verschlüsselt auszutauschen (z.B. HIN-secured)
- sind mit einem Zugriffsschutz zu versehen (z.B. passwortgeschützte ZIP Datei)
- sind auf mobilen ICT-Mitteln (Memory Stick, portable Disk, Smartphone, Tablett etc.) mit von Spitex Zürich Limmat AG zugelassenen Mitteln verschlüsselt abzulegen
- dürfen nicht elektronisch übermittelt oder auf mobilen ICT-Mitteln abgelegt werden, falls keine Verschlüsselungstechnik zu Verfügung steht.

d Geschäftsinformationen sind immer in der Datenablage der Spitex Zürich Limmat AG (Laufwerk G:\) zu speichern. Im geringen Ausmass dürfen persönliche Daten auf der persönlichen Datenablage (Laufwerk H:\) abgelegt werden.

e Im öffentlichen Raum (z.B. Arbeitsweg, Freizeit, etc.) und in Gesprächen mit Dritten ist die nötige Zurückhaltung zu wahren, wenn es um Spitex Zürich Limmat AG interne An-

[1] PerigonMobile erfüllt alle Bedingungen

gelegenheiten geht. Spitex Zürich Limmat AG Angelegenheiten sind möglichst nur im geschäftlichen Rahmen zu besprechen und zu behandeln.

f Daten über Kunden dürfen von Mitarbeitenden nur soweit eingesehen oder bearbeitet werden, als sie diese für die ihnen übertragenen Aufgaben tatsächlich benötigen.

D. Arbeitsplatz

a **Die Nutzung der Spitex Zürich Limmat-Infrastruktur zu privaten Zwecken darf weder den Dienstbetrieb noch die Erfüllung der dienstlichen Aufgaben beeinträchtigen. Zulässig ist lediglich eine gelegentliche, nicht regelmässige private Nutzung der Office Applikationen inkl. E-Mail und Internet**.

b Die Bildschirmsperre mit Passwortschutz ist immer zu aktivieren, wenn der Arbeitsplatz verlassen wird, auch bei kurzer Abwesenheit (Clear Screen Policy). Die Bildschirmsperre wird mit der Tastenkombination „Crl“ + „Alt“ + „Delete“ und der Auswahl „Sperren“ aktiviert.

c Unterlagen und Datenträger mit vertraulichen Informationen sind, wenn nicht beaufsichtigt, unter Verschluss zu halten (Clear Desk Policy).

d Für Ausdrucke mit vertraulichen Informationen oder besonderen Personendaten ist die Funktion „vertraulicher Druck“ zu verwenden. Wenn diese Funktion nicht zur Verfügung steht, sind die Ausdrucke umgehend vom Drucker/Kopierer abzuholen.

e Bei Sitzungsende sind alle Notizen mit vertraulichem Inhalt (z.B. auf Whiteboard, Flipchartblättern, etc.) zu entfernen.

f Vertrauliche Dokumente sind nicht ins Altpapier zu werfen, sondern zu „schreddern“ oder bei den dafür vorgesehenen Sammelbehälter zu entsorgen.

g Bei Arbeitsschluss müssen die Benutzenden alle ICT-Geräte abschalten. Wenn das nicht möglich ist, müssen sich die Benutzenden zumindest auf allen ICT-Geräten abmelden.

h Abwesenheitsmeldungen im E-Mail, Telefonbeantworter o.ä.: Der Inhalt der eigentlichen Abwesenheitsmeldung ist gemäss Memo E-Mail-Abwesenheitsmeldung & E-MailSignatur anzugeben.

i Nutzung von Software:

- Das Kopieren von in der Spitex Zürich Limmat AG eingesetzten Software ist nicht erlaubt.
- Der Einsatz von Software, die nicht von der eigenen Organisation lizenziert ist, ist nicht erlaubt.
- Der Einsatz von Software, die vom ICT-Team nicht geprüft und/oder freigegeben ist, ist nicht erlaubt.

E. Mobile Geräte und Datenträger

a Beim Einsatz mobiler Geräte (z.B. Notebook, Smartphone, etc.) sind diese gegen unbefugten Gebrauch zu schützen:

- Geräte sind immer zu beaufsichtigen, insbesondere dann, wenn der Benutzer/die Benutzerin eingeloggt ist.

- Verlust oder Diebstahl eines mobilen ICT-Gerätes ist umgehend dem ICT-Support und der/dem Vorgesetzten zu melden.

b Nicht mehr benötigte Datenträger (CD/DVD, Memory-Stick, externe Disk, etc.) sind dem ICT-Support zur sicheren Entsorgung abzugeben.

c Mobile Datenträger unbekannter Herkunft dürfen nicht verwendet werden.

d Zudem sind die Weisungen „Benutzung Smartphones“ sowie „Kosten Smartphones“ einzuhalten.

F. Internet

a Informationen dürfen nur von den dazu beauftragten Stellen publiziert oder verbreitet werden.

b Auf Plattformen und Kanälen (Soziale Netzwerke, Foren, Blogs, Kommentare, Clouds, etc.) dürfen niemals vertrauliche oder interne Informationen und/oder Personaldaten anderer preisgegeben werden.

c In Online-Formularen sind generell nur so viele Informationen wie nötig anzugeben.

d Die Geschäfts-E-Mail-Adresse darf auf einer Internetseite nur dann verwendet werden, wenn diese geschäftlichen Zwecken dient.

e **Die Nutzung des Internets zu privaten Zwecken darf weder den Dienstbetrieb noch die Erfüllung der dienstlichen Aufgaben beeinträchtigen. Zulässig ist lediglich eine gelegentliche, nicht regelmässige private Nutzung des Internets**.

G. E-Mail

a Für Geschäftskorrespondenz ist das E-Mail-Konto von Spitex Zürich Limmat AG zu verwenden.

b E-Mails, deren Absender nicht bekannt ist oder deren Inhalt verdächtig scheint, sind ungesehen zu löschen. Im Minimum ist Folgendes zu befolgen:

- Angehängte Dokumente nicht öffnen sondern löschen
- In der E-Mail enthaltene Links nicht anwählen

c Anhänge aus bekannter Quelle sind vor dem Öffnen mit einem aktuellen Virenschutz zu prüfen, falls dies nicht automatisch erfolgt. Auf den Computer der Spitex Zürich Limmat AG erfolgt der Scan automatisch.

d E-Mails, mit Aufforderung zur Angabe von vertraulichen Informationen (z.B. Passwörter, Kundendaten, Personaldaten, etc.) sind zu ignorieren.

e Die automatische Um- oder Weiterleitung von E-Mails an E-Mail-Adressen ausserhalb der Spitex Zürich Limmat AG ist untersagt.

f Jede missbräuchliche Verwendung von E-Mail ist untersagt, insbesondere:

- Verbreiten von Nachrichten/Mitteilungen in Täuschungs- oder Belästigungsabsicht
- Private Massenversendungen und Spam
- Widerrechtliche Handlungen, insbesondere widerrechtliches Kopieren und/oder Versenden/in Umlauf bringen von Daten oder Software jeglicher Art

H. Cloud-Dienste

a Für Geschäftszwecke und für die Verarbeitung von Geschäftsdaten dürfen nur von der Spitex Zürich Limmat AG zugelassene externe Cloud-Dienste und –Dienstleister genutzt werden.

b Geschäftsinformationen sind in externen Cloud-Diensten verschlüsselt abzulegen.

I. Passwörter / PIN

a Die Mitarbeitenden der Spitex Zürich Limmat AG sind für alle Handlungen verantwortliche, die mit ihrem Benutzernamen, ihren Passwörtern und ihrer PIN ausgeführt werden. **Passwörter und PIN sind deshalb persönlich und in allen Situationen geheim zu halten. Sie dürfen nicht weitergegeben werden, auch nicht zum Zwecke der Stellvertretung**.

b Ebenso sind der Benutzername und das Token für die Generierung von Einmalpasswörter persönlich und dürfen nicht weitergegeben werden, auch nicht zum Zwecke der Stellvertretung.

c Passwörter und PIN dürfen nur mit sicheren, von der Spitex Zürich Limmat AG vorgegebenen elektronischen Hilfsmitteln (z.B. Passwortsafe) abgespeichert, oder in einem verschlossenen Umschlag an einem sicheren Ort aufbewahrt werden.

d Komplexitätsregeln für Passwörter:

- Es muss mindestens 8 Zeichen lang sein
- Es müssen darin mindestens ein Grossbuchstabe, ein Kleinbuchstabe, eine Zahl sowie ein Sonderzeichen vorkommen
- Im Passwort darf nicht enthalten sein: der Vorname, der Nachname und der Benutzername (Login, z.B. hmu1)
- Auf diese Art und Weise kann ein sicheres Passwort erstellen werden, welches gut merkbar ist: Einen Satz nehmen, der gut gemerkt werden kann, das Passwort wird mit den jeweiligen Anfangsbuchstaben gebildet mit Ziffern sowie einem Satzzeichen: **M**eine **T**ochter **T**amara **h**at **a**m **9**. **J**anuar **1**995 **G**eburtstag**!** So entsteht ein Passwort aus einer beliebigen Zeichenfolge, das gut merkbar ist: MTTha9J1G!
- Es ist untersagt, durch einfaches Heraufzählen neue Passwörter zu erzeugen.

e Für Spitex Zürich Limmat AG und private Zwecke sind je unterschiedliche Passwörter und PIN zu verwenden.

f Passwörter sind alle 6 Monate zu ändern, die Systeme fordern automatisch zum entsprechenden Wechsel auf und erzwingen diesen auch.

g Initialpasswörter und PIN sind beim ersten Gebrauch zu ändern.

h Bei Anzeichen eines möglichen Missbrauchs sind Passwort und PIN sofort zu ändern.

i Passwort-Speicherung innerhalb einer Anwendung (wie z.B. „Kennwort speichern“ im Internet Explorer) ist nicht erlaubt.

J. Sicherheitsvorfälle

a Feststellungen über sicherheitsrelevante Vorkommnisse, wie zum Beispiel unerklärliches Systemverhalten, verdächtige Meldungen oder Einschränkungen der nutzbaren Dienste sind unverzüglich dem ICT-Support zu melden.

b Die Untersuchung solcher Vorfälle darf nicht selbst erfolgen. Der ICT-Support veranlasst die notwendigen Schritte.

c Um die Diagnose solcher Vorfälle zu erleichtern, sollen alle wichtigen Details (z.B. Fehlfunktion, Meldungen auf dem Bildschirm, seltsames Verhalten von Systemen oder Personen, sonstige aufgefallene Merkmale und Zeitpunkt) notiert bzw. gespeichert werden.

K. Datenschutzverantwortliche Person

Für die Spitex Zürich Limmat AG sind folgende Personen für den Datenschutz und die Informationssicherheit verantwortlich.

Verantwortliche Person:	Daniel Boller, CFO / Mitglied der Geschäftsleitung
Stellvertretung:	Christina Brunnschweiler, CEO

L. Verweise auf weiterführende Informationen

- Merkblatt für den Datenschutz und die Datensicherheit der Spitex Zürich Limmat AG
- Empfehlungen zum Datenschutz für die Spitex-Organisationen mit öffentlichem Leistungsauftrag im Kanton Zürich
- Richtlinien und Vereinbarung zur Telearbeit in der Spitex Zürich Limmat AG
- Leitfaden für die Bearbeitung von Personendaten und Merkblatt zum Personaldossier
- Rahmenvereinbarung zwischen Spitex Zürich Limmat AG/Zentrum und Kunden
- Allgemeine Geschäftsbedingungen Spitex Zürich
- Weisung Benutzung Smartphones
- Weisung Kosten Smartphones
- Memo E-Mail Abwesenheitsmeldung & E-Mail-Signatur

Das Datenschutz- und Informationssicherheitskonzept wurde von der Geschäftsleitung am 28. Juni 2016 verabschiedet und tritt per sofort in Kraft.