Gemeinderat
Stadt Bern

ICT-Sicherheit in der Stadt Bern
Weisung ICT-Sicherheit für Benutzerinnen und Benutzer

Herausgegeben
vom Gemeinderat der Stadt Bern

Informatik-Lenkungsausschuss (ILA)
Bümplizstrasse 45
3027 Bern
Telefon 031 321 74 89
ila@bern.ch

1. März 2017

Konzept: Informatik-Lenkungsausschuss
Redaktion: Eric Tönz, Martin Hunziker, Martin Müller
Gestaltung/Druck: Logistik Bern
Foto: Martin Müller, Informatikdienste Stadt Bern
Link Intranet: http://intranetbern/stadtverwaltung/direktion-finanzen-personal-und-informatik/informatikdienste/it-sicherheit

Inhaltsverzeichnis

1. Einleitung

Die professionellen und motivierten Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung Bern sorgen täglich für eine bürgerfreundliche, effektive und kostenbewusste Leistungserbringung zum Wohle der Stadt und ihrer Bewohnerinnen und Bewohner.
Dabei werden sie heute in nahezu allen Arbeitsprozessen durch die Informations- und Kommunikationstechnik (ICT) unterstützt. Die ICT ist somit in zunehmendem Masse eine existenzielle Grundlage für viele Geschäfts- und Verwaltungsprozesse. Grosse Informationsmengen werden digital gespeichert, verarbeitet und in stadteigene respektive stadtfremde Informationsnetze übermittelt. Dabei ist eine Reihe von abgestimmten Massnahmen nötig, um zu verhindern, dass Informationen verloren gehen, in falsche Hände geraten oder nicht rechtzeitig bearbeitet werden können.
Unachtsames Verhalten, kriminelle Handlungen oder technisches Versagen können zum Verlust oder zum Diebstahl von elektronischen Daten führen und so gesetzliche Vorgaben verletzen, dem Ruf der Stadt Bern schaden oder finanzielle Nachteile mit sich bringen.
Obwohl es viele technische Sicherheitsmassnahmen zum Schutz von Informationen gibt, reichen diese alleine nicht aus. Neben den permanent durch die Informatikdienste (ID) überwachten technischen Komponenten wie Zugriffskontrollen, Firewalls, Antivirenprogramme, Mobile Device Management- und Backup-Systeme fällt dem Faktor Mensch eine wichtige Rolle zu. Im Umgang mit Daten ist eine gewisse Sensibilität unabdingbar. Jede Mitarbeiterin und jeder Mitarbeiter trägt dabei einen Teil der Verantwortung.

Beispiele von Sicherheitsvorfällen

- Geschlossene Coop-Filialen: Aufgrund technischer Probleme, verursacht durch eine Softwareanpassung am Kassensystem, mussten am 4. April 2012 sämtliche Coop-Filialen in der Deutschschweiz schliessen. Die Störung dauerte bis zu zwei Stunden.
- Passwörter und Kreditkarteninformationen ergaunert: Im ersten Quartal 2016 zielten Phishing E-Mails im Namen von Cembra Money Bank und UBS direkt auf Schweizer Opfer ab. Die E-Mails, deren Absender den Empfangenden bekannt waren, sollten diese dazu verleiten, Login und Passwort des E-Mail-Kontos anzugeben. Die eingegebenen Zugangsdaten wurden direkt an die Betrüger weitergeleitet. Ein weiterer Fall wurde Ende Mai 2016 bekannt. Betrügende brachten E-Mails in Umlauf, welche scheinbar von ricardo.ch stammten und eine Belohnung für die Teilnahme an einer Umfrage versprachen. Am Ende der Umfrage wurden Personalien und Kreditkartendaten sowie Sicherheitscode abgefragt. Angeblich um die Direktüberweisung für die Belohnung vornehmen zu können.
- Die RUAG im Visier der Hacker: Am 21. Januar 2016 wurde bekannt, dass Unberechtigte bereits seit 2014 auf Daten der RUAG zugegriffen haben. Die RUAG wurde mittels professionell und gezielt eingesetzter Schadsoftware sowie Phishing E-Mails erfolgreich angegriffen und erste Hinweise darauf tauchten erst im Dezember 2015 auf.

2. Allgemeines zur Weisung

Gegenstand	Die vorliegende Weisung stützt sich auf die jeweils gültige ICT-Sicherheitsleitlinie und ICT-Strategie der Stadt Bern. Sie legt die Grundsätze für den sicheren Umgang mit IT- und Kommunikationsmitteln, Anwendungen und digitalen Daten fest.
Geltungsbereich	Die Weisung ist für alle Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung Bern verbindlich. Sie gilt auch für alle externen ICT-relevanten Vertragspartnerinnen und -partner der Stadt. Diese müssen vor Aufnahme der Arbeit eine Vertraulichkeits- und Geheimhaltungserklärung[1] unterzeichnen.
Verantwortlichkeiten	Die ID setzen sich für eine möglichst sichere und stabile ICT-Umgebung ein. Die Linienvorgesetzten sorgen für die Bekanntgabe und Einhaltung dieser Weisung in ihrer Organisationseinheit. Alle Mitarbeiterinnen und Mitarbeiter sind für die vollständige und korrekte Umsetzung der vorliegenden Weisung an ihrem Arbeitsplatz verantwortlich. Die Informatikdienste sowie die/der Informatikkoordinierende der jeweiligen Direktion helfen den Mitarbeitenden bei ICT-Sicherheitsfragen.

Beispiele zu IT- und Kommunikationsmittel:
- Desktop-PCs, Notebooks, THIN-Clients
- Smartphones, Tablet-PCs
- Drucker und Multifunktionsgeräte
- USB-Sticks, externe Festplatten
- Telefone

Anwendungen:
- Betriebssysteme und Office-Programme (Kategorie 1)
- Mietsoftware «out of the box» (Kategorie 2)
- Fachapplikationen (Kategorie 3)
- Mobile Apps

Digitale Daten:
- Dokumente und Bilder
- Geodaten
- Datenbanken
- Kommunikation (E-Mail, VoIP, Unified Communication)

[1] Im Intranet unter Informatik / ICT-Sicherheit zu finden.

3. Grundsätze zur Nutzung der ICT

Eigenverantwortung	Jede Benutzerin und jeder Benutzer ist selbst verantwortlich für alle unter eigenem Benutzendennamen getätigten Zugriffe auf IT- und Kommunikationsmittel, Anwendungen und digitale Daten. Alle Aktivitäten unter einem anderen Benutzendennamen sind verboten. Ausnahmen sind im Supportfall (durch dafür vorgesehene Personen) sowie bei den Unpersönlichen- und Gruppen-Accounts (siehe unten) erlaubt.
Verbotene Aktivitäten	Für die Installation und Wartung der Hardware und Software sind die Leistungserbringenden ID und GIS-Kompetenzzentrum Bern (GKB) zuständig. Jegliche Manipulationen ohne Absprache mit den Leistungserbringenden sind untersagt. Private Geräte dürfen nicht mittels Netzwerkkabel an das Kommunikationsnetz der Stadtverwaltung Bern angeschlossen werden. Auch an den USB-Anschluss der städtischen IT- und Kommunikationsmittel dürfen keine privaten Geräte angeschlossen werden. Es sind ausschliesslich durch die ID bewilligte Geräte und Datenträger zu verwenden.[2] Die Verwendung der städtischen ICT-Infrastruktur im Zusammenhang mit rassistischen, gewalttätigen, sexistischen oder illegalen Inhalten ist verboten. Nähere Informationen sind im Intranet-Auftritt des Personalamtes ersichtlich[3]. Das Verbreiten und Weiterleiten von Bittbriefen, Werbemails und diskriminierenden Nachrichten ist verboten.
Unpersönliche- und Gruppen-Accounts	Unpersönliche- und Gruppen-Accounts werden auf das notwendige betriebliche Minimum beschränkt..
Private Nutzung	Die städtische ICT-Infrastruktur ist für den geschäftlichen Gebrauch bzw. die Erfüllung dienstlicher Aufgaben bestimmt. Die Nutzung zu privaten Zwecken darf weder den Dienstbetrieb noch die Erfüllung der dienstlichen Aufgaben beeinträchtigen (vgl. Art. 57 Abs. 1 Personalreglement und in analoger Anwendung Art. 76a Abs. 1 Personalverordnung). Alle elektronisch übermittelten und gespeicherten Daten gelten als geschäftliche Daten. Die erstellten bzw. empfangenen Daten und geschäftliche Informationen müssen auf entsprechenden zentralen Laufwerken der Stadt gespeichert werden. Daten persönlicher Natur und ohne Relevanz für die geschäftlichen Interessen sind im persönlichen Laufwerk abzuspeichern.

[2] Diese befinden sich im Hardwareportfolio der Stadt Bern auf dem Intranet

[3] Intranet / Personelles / Personalverordnung (PVO) / Art. 117a

Empfang von Radio- und Fernsehprogramm	Der Empfang von Radio- und Fernsehprogrammen in Betrieben unterliegt der gesetzlichen Melde- und Gebührenpflicht. Es ist den Mitarbeiterinnen und Mitarbeitern der Stadt Bern deshalb untersagt mit IT- und Kommunikationsmitteln Radio- und Fernsehprogramme zu empfangen. Nimmt eine Mitarbeiterin oder ein Mitarbeiter sein privates Empfangsgerät mit an den Arbeitsplatz und nutzt sie/er dieses Gerät dort für sich allein, so ist dieser Empfang in ihrer/seiner Meldung für den privaten Radio- und/oder Fernsehempfang eingeschlossen.
Social Media	Bei der Nutzung von Social Media ist der Leitfaden der Stadtverwaltung[4] zu beachten.
Melden von Vorfällen	Sicherheitsrelevante Probleme (Virenbefall, Passwortverlust, Datenverlust, ungewöhnliche Vorkommnisse, Diebstahl, usw.) oder ein Verdacht auf sicherheitskritische Vorgänge (z.B. Vermutung, dass unberechtigte Personen versuchen mit dem Benutzendennamen eines Dritten zu arbeiten) müssen sofort dem Kundenservice und Betrieb (KB; Nachfolgend IT-Support genannt) und dem zuständigen Informatikkoordinierenden gemeldet werden. Allfällige Auswertungen von Vorfällen erfolgen unter Berücksichtigung des Datenschutzgesetzes nach den Prinzipien wie in Kapitel 12 der vorliegenden Weisung definiert. Die wichtigsten Anlaufstellen sind im Anhang A aufgelistet.
Kompetenzregelung	Mitarbeitende der Leistungserbringenden verfügen zur Ausübung ihrer zugeordneten Tätigkeiten teilweise über erweiterte Rechte. Sämtliche Mitarbeiterinnen und Mitarbeiter der ID und GKB unterstehen der Geheimhaltungspflicht. Ihre Rechte und Pflichten sind in verschiedenen Weisungen festgehalten, die betroffenen Personen werden instruiert. Die Einhaltung der Rechte und Pflichten wird durch die ICT-Sicherheitsbeauftragten wiederkehrend überprüft.

[4] Social Media Leitfaden für die Stadtverwaltung, verantwortlich ist der Informations-dienst der Stadt Bern.

4. Social Engineering

Bewusstsein

Alle Mitarbeitenden müssen sich den Gefahren des Social Engineering bewusst sein und dürfen weder aus Hilfsbereitschaft noch aus Leichtgläubigkeit oder Angst vor Schwierigkeiten sich zur Missachtung der ICT-Sicherheit verleiten lassen.
Es ist Vorsicht geboten, wenn jemand Mitarbeitende zu unerlaubten Handlungen verführen will, wie:

- das Weitergeben von Informationen
- die Bekanntgabe von Passwörtern
- den Zugang zu den Büroräumlichkeiten zu gewähren.

Verhalten

Nie unberechtigten Personen Auskünfte über schützenswerte Daten, Geschäftsabläufe oder -informationen gewähren. Bei Zweifeln an einer anfragenden Person kann diese durch Rückruf via Hauptnummer bzw. Telefonverzeichnis überprüft werden.
Keine Fragen ausserhalb des eigenen Zuständigkeitsbereichs beantworten und an zuständige Stellen verweisen (Auskunft, Informationsdienst, Stadtkanzlei, usw.).
Besucherinnen und Besucher sowie unbekannte Personen müssen sich grundsätzlich am Empfang oder einer zentralen Stelle melden und haben keinen freien Zutritt zu Büroräumen.
Nie einer unbekannten Person den Zutritt zu gesicherten Räumlichkeiten ermöglichen. Dabei ist unter anderem an vermeintliches Service-Personal, Überbringende von Paketen, usw. zu denken.
Besucherinnen und Besucher sowie unbekannte Personen sind trotz erlaubter Anwesenheit nie alleine in den Büroräumlichkeiten und anderen nicht öffentlich zugänglichen Bereichen (z.B. technischer Infrastruktur) zurückzulassen.
Bei der Abwesenheitsmeldung in Outlook ist zwischen innerhalb und ausserhalb der Stadtverwaltung zu unterscheiden. Externe Abwesenheitsmeldungen sind zur Wahrung der Privatsphäre lediglich mit Informationen über die Abwesenheit und einer Stellvertretung zu versehen. Nie die Dauer der Abwesenheit nennen.
Vorsicht und Zurückhaltung ist auch beim Publizieren von privaten Informationen im Internet (Fotos, Hobbies, Videos usw.) geboten, insbesondere wenn solche Informationen mit der Stadtverwaltung in Verbindung gebracht werden können.
Youtube, Facebook, Twitter, Instagram, LinkedIn und Xing beispielsweise sind beliebte Quellen für Social Engineering.

Gezielte Angriffe auf das menschliche Verhalten

- Social Engineers geben sich gerne als jemand anderen aus, um sich durch geschickte Fragen nach internen Telefonnummern, Namen von Mitarbeitenden, verwendeter ICT-Infrastruktur, Passwörtern oder ähnlichen Informationen Zugang zu Systemen von Verwaltungen oder Unternehmen zu verschaffen.
- Je besser Systeme mit technischen Mitteln geschützt werden, desto wahrscheinlicher werden Angriffe mit Hilfe von nichtsahnenden oder hilfsbereiten Mitarbeitenden mittels Social Engineering.

Mitarbeitende der ID und GKB fragen NIE nach persönlichen Passwörtern.

5. Arbeitsplatz / Umfeld

Physischer Schutz aller Informatikmittel

Zur Vermeidung von Hardware-Schäden sind folgende Gefahren zu beachten:

- Feuer (Kerzen, defekte/überlastete Elektroinstallationen, abgedeckte oder verschmutzte Lüftungsschlitze von Geräten, usw.)
- Wasser (Blumenvasen, Getränke, usw.)
- Windstösse (offene Fenster, Durchzug)
- Ungeeignete Büroeinrichtung (wackelige Abstellflächen, Stolperdrähte, usw.)

Zur Vermeidung von Diebstählen und unberechtigten Netzwerkzugängen sind Fenster und Türen beim Verlassen des Arbeitsplatzes soweit möglich zu verriegeln und vorhandene Schliessvorrichtungen zu nutzen.

Bei Abwesenheiten (Pause, Besprechungen, Arbeitsschluss usw.) ist die unbefugte Verwendung des Desktop-PCs, THIN-Clients oder Notebooks durch Dritte mittels Computersperre, abmelden oder herunterfahren des Systems, zu verhindern. Ferner ist der Arbeitsplatz so aufzuräumen, dass keine mobilen Datenträger (CDs/DVDs, USB-Sticks usw.), mobile Geräte und vertrauliche Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden.

Verhalten ausserhalb des städtisches Netzwerks

Mobile Geräte und Datenträger dürfen nicht unbeaufsichtigt gelassen werden und sind wann immer möglich mit einer Diebstahlsicherung zu schützen. Werden mobile Geräte und Datenträger in einem Fahrzeug aufbewahrt, müssen diese von aussen nicht sichtbar und im Kofferraum eingeschlossen sein.

Es ist darauf zu achten, dass niemand vertrauliche Informationen mitlesen oder mithören kann. Alle Arbeitsunterlagen müssen verschlossen aufbewahrt und der Zugang zum Client durch einen aktivierten Schutz gesichert werden.

Vertrauliche Informationen dürfen nie in der Öffentlichkeit besprochen werden. Zum Telefonieren ist ein ungestörter Bereich aufzusuchen.

Outlook Web App (OWA), Portalzugang

Die Anmeldeinformationen (Benutzendennamen und Berechtigungsnachweise wie Passwort, M.ID Pin und M.ID Passcode) dürfen im Webbrowser nicht gespeichert werden. Auf den städtischen Geräten ist dies technisch unterbunden, für alle anderen Geräte ist der/die Benutzer/in dafür verantwortlich.

Beim Auftreten einer Zertifikatswarnung ist die Verbindung zu OWA und dem Portalzugang vor Eingabe der Berechtigungsnachweise abzubrechen.

Spätestens beim Beenden des Webbrowsers muss dessen lokaler Zwischenspeicher (Cache) gelöscht werden. Andernfalls verbleiben möglicherweise Informationen auf der lokalen Festplatte und sind unter Umständen für andere Nutzende zugänglich. Auf den städtischen Geräten ist dies technisch unterbunden, für alle anderen Geräte ist der/die Benutzer/in dafür verantwortlich.

Nach Beendigung des Fernzugriffs (OWA- und Portalsitzung) muss der Webbrowser immer geschlossen werden.

Einschalten der Computersperre

Die Sperre (auch «Bildschirmschoner mit Passwortschutz» genannt) schaltet sich nach einer gewissen inaktiven Zeit automatisch ein. Um beim Verlassen des Arbeitsplatzes einen sofortigen Schutz zu erreichen, wird die Sperre wie folgt manuell eingeschaltet:

- Ctrl+Alt+Delete drücken und «Computer sperren» anwählen oder
- Windows-Taste + L drücken

Risiken in einer fremden Umgebung

Die Anmeldeinformationen können unbemerkt aufgezeichnet (Tasteneingaben, Video usw.) und für ein späteres missbräuchliches Anmelden durch eine angreifende Person benutzt werden.

Ausgedruckte und gespeicherte Informationen können unbemerkt gelesen, kopiert sowie fotografiert werden. Informationen am Bildschirm können mitgelesen oder unbemerkt aufgezeichnet (Bildschirmspeicher, Video usw.) werden.

Diebstahlsicherung mobiler Geräte

Geräte wie Notebooks, Bildschirme und Beamer mit der Möglichkeit zur Diebstahlsicherung sind mit einer speziellen Öffnung am Gehäuse versehen. In dieses wird ein Schloss, meist mit einem Drahtseil ausgestattet, in geöffnetem Zustand eingeführt. Das Drahtseil kann um Verankerungen geschlungen und das Gerät somit festgemacht werden.

Oft wird für eine Diebstahlsicherung auch der Begriff Kensington Schloss verwendet. Dabei handelt es sich um eine Produktbezeichnung, die ursprünglich von der Firma Kensington hergestellt wurde.

Solche Diebstahlsicherungen bieten zwar keinen abschliessenden physischen Schutz, verhindern aber auf einfache und kostengünstige Weise Gelegenheitsdiebstähle.

Wie verhindere ich im Privatumfeld das Speichern von Anmeldeinformationen?
In den Einstellungen des Webbrowsers ist das automatische Vervollständigen von Eingabefeldern wie Benutzendennamen und Passwörter zu deaktivieren. Im Internet Explorer: Extras > Internetoptionen > Inhalte > AutoVervollständigen > Einstellungen > zumindest Kästchen «Benutzendennamen und Kennwörter für Formulare» deaktivieren. Für anderweitige Webbrowser ist dies sinngemäss umzusetzen.

Wie überprüfe ich ein Zertifikat?
Zertifikate werden genutzt, um Verbindungen zu verschlüsseln und dem Anwendenden Sicherheit zu geben, mit der korrekten Website verbunden zu sein. Jeder Webbrowser kann Zertifikate selber auf Echtheit und Gültigkeit überprüfen. Beim OWA- und Portalzugang dürfen keine Fehlermeldungen auftreten, andernfalls stimmt mit der aufgerufenen Webseite oder der Verbindung etwas nicht. Bei korrekten Zertifikaten erscheint beispielsweise im Internet Explorer eine grüne oder weisse Adresszeile. Beispiele mit anderen Webbrowsern und weitergehende Informationen sind unter www.ebas.ch ersichtlich.

Wie lösche ich den Browser-Cache?
Mit dem Löschen des Browser-Caches werden temporär gespeicherte Daten, der Browserverlauf wie auch automatisch gespeicherte Formulareingaben entfernt. Dies kann entweder über das automatische Löschen beim Beenden des Webbrowsers oder mittels einer manuellen Löschung erfolgen. Einstellung automatisches Löschen im Internet Explorer: Extras > Internetoptionen > Allgemein > Kästchen «Browserverlauf beim Beenden löschen» aktivieren. Manuelles Löschen im Internet Explorer: Extras > Internetoptionen > Allgemein > Browserverlauf > Löschen > Kästchen aktivieren > Löschen. Für anderweitige Webbrowser ist dies sinngemäss umzusetzen. Entsprechende Informationen können den Merkblättern von «E-Banking aber sicher!» auf deren Website[5] entnommen werden.

[5] E-Banking aber sicher!, www.ebas.ch

6. Persönliche Daten der Mitarbeitenden

Grundsätze für den Zugriff auf persönliche Daten von Mitarbeitenden	Vor dem Zugriff muss die Einwilligung des betroffenen Mitarbeitenden eingeholt werden (Ausnahmen siehe weiter unten). Um Zugriffskonflikten vorzubeugen, sind die Daten generell auf den Abteilungslaufwerken abzuspeichern und der stellvertretende Zugriff auf anderweitig abgelegte Daten sowie Informationen in Outlook vor Abwesenheit konkret zu regeln. Bei längeren Abwesenheiten ist eine geordnete Datenübergabe sicherzustellen. Private Termine und allfällige Einträge mit besonders schützenswerten Personendaten sind zur Wahrung der Vertraulichkeit in Outlook als «Privat» zu kennzeichnen (aktivieren Schlosssymbol).
Stellvertretende Zugriffe	Geplante Zugriffe durch stellvertretende Personen sind mittels Freigaben und Berechtigungen zu gewährleisten, nicht mittels Weitergabe von persönlichen Logins/Passwörtern. Die Korrespondenzpartner sind über die Stellvertretungsregelungen und die Grenzen der Vertraulichkeit zu informieren.
Bei ungeplanten Abwesenheiten (z.B. Krankheit, Unfall)	Das Öffnen von Zugriffen auf persönliche Daten ist nur in Ausnahmefällen erlaubt. Es handelt sich dabei um eine in der Regel unvorhergesehene Abwesenheit von längerer oder unbestimmter Dauer. Es muss ein überwiegendes Interesse der Öffentlichkeit (Geschäftskontinuität) oder der korrespondierenden Personen geltend gemacht werden. Würde beispielsweise die Stadt Bern ohne den sofortigen Zugriff auf persönliche Daten einer Mitarbeiterin oder eines Mitarbeiters einen bedeutenden finanziellen oder nicht wieder gut zu machenden immateriellen oder materiellen Schaden nehmen, dann darf auch ohne Einwilligung des Mitarbeitenden darauf zugegriffen werden. Handelt es sich um einen aufschiebbaren, also nicht dringenden Auftrag, dann ist die Rückkehr des betroffenen Mitarbeitenden abzuwarten. Die Verantwortung für den Eingriff liegt letztendlich bei der Leitung der ersuchenden Abteilung. Die ID weisen auf die Ordnungsmässigkeit hin und stellen die Nachvollziehbarkeit sicher. Der schriftliche und unterzeichnete Antrag[6] für den notfallmässigen Zugriff auf elektronische Daten von abwesenden Mitarbeitenden muss in jedem Fall vorliegen. Dies unabhängig von einer allfälligen Vollmacht der abwesenden Person.

[6] Im Intranet unter Informatik / ICT-Sicherheit zu finden.

Berechtigungsnachweise (Passwort, M.ID Pin) von Mitarbeitenden werden nur zurückgesetzt, um eine Freigabe oder einen Abwesenheitsassistenten einzuschalten, nicht aber um einer stellvertretenden Person das Arbeiten im Namen der abwesenden Person zu ermöglichen.
Als persönlich erkennbare E-Mails sind wie persönliche Briefpost zu behandeln und dürfen nicht geöffnet werden. Die restlichen E-Mails sind geschäftliche E-Mails und dürfen gelesen werden. Wird beim Lesen einer E-Mail ein privater Charakter eruiert ist diese unverzüglich zu schliessen.
Die betroffenen Mitarbeitenden müssen in jedem Fall über den Grund, Tätigkeit und die anfragende Person des Datenzugriffs informiert werden.

Privatsphäre der Mitarbeitenden
Die Stadt Bern wahrt die Privatsphäre ihrer Mitarbeitenden am Arbeitsplatz gemäss schweizerischem Recht (insb. verfassungsmässiges Fernmeldegeheimnis, kantonales Datenschutzgesetz, Personalrecht).

- Dazu gehört u.a. der Anspruch auf Vertraulichkeit beim Telefonieren, bei der Benutzung des Internets oder des E-Mails.
- Auf das persönliche Laufwerk hat nur der/die jeweilige Benutzer/in Zugriff.
- Die Systemadministratoren haben nur im Rahmen ihrer Aufgaben Zugriff auf sämtliche unverschlüsselten Daten und Programme (siehe Kompetenzregelung in Kapitel 3).

Mitarbeitende dürfen jederzeit Auskunft darüber verlangen, ob und welche Daten über sie bearbeitet werden (Auskunftsrecht).
Bei Fragen oder Unsicherheiten können sie sich an die zuständigen Direktionspersonaldienste, die ICT-Sicherheitsbeauftragten oder die/den Datenschutzbeauftragte/n der Stadt Bern wenden.

Wie kann ich Termineinträge als Privat kennzeichnen?
Im Termineintrag ist in der Gruppe Kategorien das Schlosssymbol «Privat» zu aktivieren. Dabei ist zu beachten: werden «private» Termineinträge mittels Smartphones und Tablet-PCs erstellt, muss die Kennzeichnung nachträglich im Outlook vorgenommen werden, wenn diese Funktion in den mobilen Geräten nicht vorhanden ist.

Möglichkeiten Stellvertretungsregelung in Outlook

- Freischalten Einsicht in Terminkalender innerhalb der Abteilung. Kalendereinträge, die für andere auch sichtbar sind, dürfen aber keine schützenswerten Personendaten enthalten.
- Freischalten Einsicht in Posteingang für mindestens eine Vertrauensperson innerhalb der Abteilung.
- Automatisches Weiterleiten von E-Mails innerhalb der Abteilung.

Interessensabwägung bei Ausnahmefällen
Bei der Übersteuerung von Zugriffsrechten in Ausnahmefällen geht es vorgängig um eine dreiseitige Interessensabwägung.

Geschäftskontinuität der Stadtverwaltung:
- Interesse von Vorgesetzten und Stellvertretenden
- Interesse von Bevölkerung und Politik

Persönlichkeitsschutz der Mitarbeitenden:
- Vertraulichkeit privater Korrespondenz und Dokumente
- Vertraulichkeit privater Kontakte und Termine

Persönlichkeitsschutz von Drittpersonen:
- Vertrauensverhältnis zu Mitarbeitenden
- Vertraulichkeit von Korrespondenz und Geschäftsfällen

Im Einzelfall sind die Interessen der beteiligten Parteien nicht unbedingt offensichtlich. Beispiel: Möchte ein E-Mail Absender lieber eine persönliche Behandlung mit Verzögerung oder eine rasche Erledigung durch einen Stellvertretung?

7. Berechtigungsnachweise

Geheimhaltung	Berechtigungsnachweise wie Passwörter, M.ID Pin und M.ID Passcode sind geheim zu halten. Diese dürfen anderen Personen nicht bekannt beziehungsweise zugänglich gemacht werden (auch nicht dem IT-Support oder einer systemadministrierenden Person).
Passwörter	Ein Passwort muss gut zu merken, für andere schwer zu erraten und durch automatisierte Angriffe schwer herauszufinden sein. Es darf weder in einem Wörterbuch noch in Assoziation zur eigenen Person stehen (z.B. keine Namen, Geburtsdaten, Hobbies, Telefon- und Autonummern). Es muss sich aus Sicherheitsgründen aus einer Kombination von mindestens 10 Zeichen, bestehend aus Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen zusammensetzen. Passwörter müssen regelmässig gewechselt werden. Das neue Passwort darf nicht durch eine einfache logische Überlegung aus dem alten Passwort abgeleitet werden können. Geschäftliche Passwörter sind verschieden von privaten Passwörtern zu wählen. Für unterschiedliche Dienste sind unterschiedliche Passwörter zu wählen.

Tipp für Passwort-Wahl:
Nehmen Sie einen Satz, den Sie sich gut merken können. Erstellen Sie dann mit den Anfangsbuchstaben der Wörter ein starkes Passwort, z.B.: «Welcher der 2 Bären frisst gerne Rüben im Winter?» Daraus ergibt sich folgendes Passwort: Wd2BfgRiW?

Beispiele für gute Passwörter
- Agai07dAC! (Alinghi gewann auch im 07 den America's Cup!)
- Fss,iws3Wd (Ferien sind schön, insbesondere wenn sie 3 Wochen dauern)

Beispiele für ungenügende Passwörter
- 10.02.1970_Peter (Geburtsdatum und Name)
- 34R?u (zu wenig Zeichen)

Weitere Tipps zum Erstellen von guten und sicheren Passwörtern finden Sie auf der Intranet Seite der ICT-Sicherheit[7]

[7] Im Intranet unter Informatik / ICT-Sicherheit zu finden

8. Datensicherheit

Wahrung der Sicherheitsaspekte	Zum Schutz vor Abfluss, Manipulation und Zerstörung digitaler Daten sind diese vor unberechtigter Einsicht und fremdem Zugriff zu schützen.
Datenschutzgesetz	Die Bearbeitung, Speicherung und Weitergabe personenbezogener Daten hat unter Berücksichtigung des geltenden Datenschutzgesetzes[8] zu erfolgen. Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten. Ausdrucke mit Personendaten sind nach dem Druckvorgang per Follow-2-Print (vertrauliches Drucken) umgehend aus dem Drucker zu entfernen und der/die Benutzende ist am Gerät abzumelden. Bei der Möglichkeit von Direct Printing ist die Funktion des vertraulichen Druckens (Begriff kann je nach Drucker variieren), wenn verfügbar, zu nutzen. Personendaten dürfen nur bekannt gegeben werden, wenn die Betroffenen damit einverstanden sind oder die gesetzlichen Grundlagen dazu vorhanden sind. Dies gilt auch für die Veröffentlichung von Personendaten im Intranet und Internet.
Datenspeicherung / Aufbewahrung	Alle Mitarbeitenden sind für die korrekte Ablage und Aufbewahrung der von ihnen erstellten sowie empfangenen Dokumente, Dateien, E-Mails usw. im Rahmen ihres Aufgabenbereichs selbst verantwortlich. Sämtliche für die Stadt Bern erstellten bzw. empfangenen Daten müssen auf entsprechenden zentralen Laufwerken der Stadt abgelegt werden. Das persönliche Laufwerk steht ausschliesslich für persönliche Daten zur Verfügung. Alle Serverlaufwerke werden täglich gesichert. Lokale Laufwerke (C:\ und D:\) sind nur für Systemdateien, Software und temporäre Daten bestimmt und werden nicht gesichert.
Datensynchronisation	Die Synchronisation von Daten der Stadt Bern mit privaten IT- und Kommunikationsmitteln ist untersagt. Hierzu gehört insbesondere die Verwendung der App Outlook Anywhere. Eine Ausnahme ist das Verwenden privater Smartphones und Tablet-PCs, welche einen Datenaustausch über den von der Stadt Bern definierten und betriebenen zentralen Zugangspunkt ausführen sowie Services, die von den ID bereitgestellt und betrieben werden.

[8] Bestimmungen des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) sowie des kantonalen Datenschutzgesetzes vom 19. Februar 1986 (KDSG; BSG 152.04). Siehe auch www.bern.ch/stadtverwaltung/datenschutz.

	Die ID behalten sich das Recht vor, technische Massnahmen zu erlassen und Konfigurationsrichtlinien durchzusetzen, um eine angemessene Informationssicherheit zu gewährleisten. Wird dem Durchsetzen der Konfigurationsrichtlinien nicht zugestimmt, ist der/die Besitzer/in des Smartphones oder Tablet-PCs verpflichtet die Datensynchronisation mit der Stadt Bern dauerhaft zu unterbinden.
Cloud Computing	Das Benutzen von Cloud Diensten ist grundsätzlich untersagt wenn diese Services nicht von den ID bereitgestellt und betrieben werden (Bsp. Arbeitsräume, BernBox). Die ID entscheiden über Ausnahmen. Entsprechende Gesuche sind mit Begründung per Ticketsystem an die ID zu richten.
Entsorgung / Löschung von Daten	Daten löschen heisst nicht, sie vernichten. Selbst wenn ein Datenträger mit neuen Daten überschrieben wird, bleiben die ursprünglichen Daten rekonstruierbar. Deswegen sind sowohl ausgediente städtische Geräte (Desktop-PCs, Notebooks, PDAs, Handys, Smartphones, Kopierer, Drucker, Fax, usw.) mit eingebauten Datenträgern als auch städtische mobile Datenträger (CDs, DVDs, USB-Sticks, Speicherkarten, usw.) zwecks Recycling bzw. fachgerechter, sicherer Entsorgung den ID zurückzugeben. Fehl- oder Testausdrucke sowie nicht mehr benötigte Dokumente mit vertraulichem Inhalt sind eigenhändig im Aktenvernichter zu entsorgen.

Was ist Cloud Computing?
Mit Cloud Computing werden, meist durch einen externen Dienstleistenden, Informatikressourcen über das Internet bereitgestellt. Die existierenden Dienste reichen von der Nutzung bestimmter Anwendungen, über eigen verwaltete Softwareumgebungen bis hin zur Auslagerung von Infrastrukturkomponenten wie beispielsweise Server- und Speichersysteme. Die verschiedenen Dienste richten sich nach den Anforderungen der Nutzenden aus und weisen ein hohes Mass an Skalierbarkeit aus.
Software und Daten werden nicht mehr lokal bearbeitet und gespeichert, sondern auf einer externen Infrastruktur. Im Grundprinzip ist es das Auslagern von Software- oder sogar Hardwarefunktionen, so dass in vielen Fällen gar nicht mehr genau feststellbar ist, wo sich die Informationen geografisch gesehen befinden.
Immer beliebter werden Cloud Speicherdienste wie beispielsweise Dropbox und iCloud-Lösungen von Apple, auch aufgrund der steigenden Anzahl privat und geschäftlich genutzter Smartphones und Tablet-PCs. Diese Speicherdienste ermöglichen eine zentral und von überall her zugängliche Datenablage sowie eine einfache Datensynchronisation zwischen verschiedenen Endgeräten.

Informationsabfluss durch Verlust der Datenhoheit
Die Cloud-Anbietenden und deren Infrastrukturen sind meist ausserhalb der Schweiz angesiedelt. Die betroffenen Anwendungen und Daten befinden sich somit nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der (metaphorischen) Wolke (engl. «cloud»). Die Nutzung von Cloud-Diensten wirft aber viele Sicherheitsbedenken auf. Denn mit der Nutzung dieser Dienste wird die Datenhoheit de facto aus der Hand gegeben und das ganze Vertrauen betreffend Zugriff auf Daten und Sicherung von Daten liegt in den Händen eines Dritten. Kommt hinzu, dass Cloud-Anbietende wie Amazon, Apple, Google, Microsoft usw. den amerikanischen Strafverfolgungsbehörden Zugriff auf von Kundinnen und Kunden gespeicherte Daten gewähren müssen. Dies betrifft auch in der EU ansässige Firmen und in europäischen Rechenzentren liegende Daten. Dieses Risiko muss nicht sein, denn die ID bieten auf der städtischen Infrastruktur schon seit längerem die sichere Synchronisation von Daten (Teamräume, BernBox), Kontakten, Terminen und E-Mails an.

Risiko des Verstosses gegen übergeordnetes Recht
Die Stadtverwaltung und ihre Mitarbeitenden unterstehen beim Bearbeiten von Daten den gesetzlichen Datenschutzbestimmungen. Auch wenn Daten ins Ausland übermittelt werden, besteht die Verpflichtung, die allgemeinen Grundsätze zu beachten. So hält Art. 6 Abs. 1 DSG fest, dass Personendaten grundsätzlich nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Cloud-Dienste sind daher aus datenschutzrechtlichen Gründen nicht unproblematisch und das Risiko eines Verstosses gegen Bundesrecht nimmt mit steigender Nutzung solcher Dienste zu.

9. Schutz der Datenübermittlung

Umgang mit E-Mails

E-Mails unklarer Herkunft (auch wenn sie über bekannte Adressen weitergeleitet wurden) mit unüblichen Betreff vermerken oder mit undefinierter Empfängeradresse sowie suspekte Anhänge und Links dürfen nicht geöffnet werden. Solche E-Mails sind ungeöffnet zu löschen und definitiv im «Posteingang» sowie in den Ordnern «Gelöschte Objekte» und «Gelöschte Elemente wiederherstellen« zu löschen. Beispiele sind Bittbriefe, Werbemails, falsche Virenwarnungen, gefälschte Mitteilungen von Banken, Gewinnversprechen, Bestellbestätigungen usw. Diese können unerwünscht sein (Spam), Sie zu einer Handlung drängen (Phishing), Schadsoftware beinhalten (Ransomware) oder auf mit Schadsoftware verseuchte Internetseiten verweisen.

Aus Gründen der ICT-Sicherheit und Wirtschaftlichkeit wird die Übermittlung grosser Datenmengen mittels E-Mail bei der Stadt Bern wie auch bei Dritten begrenzt. Ein Datenaustausch innerhalb der Stadtverwaltung sollte über eine Ablage auf einem allgemein zugänglichen Laufwerk und einem entsprechenden Verweis im E-Mail erfolgen. Beim Datenaustausch ausserhalb der Stadtverwaltung sind unter Berücksichtigung der Vertraulichkeit der Service BernBox der ID zu nutzen.

Die Empfängeradresse/n ist/sind in jedem Fall vor dem Versand einer E-Mail zu verifizieren.

Die automatische Weiterleitung von E-Mails an eine externe E-Mail-Adresse (z.B. bluewin.ch oder gmail.com) ist verboten.

Vertraulichkeit im E-Mail Verkehr

Auf E-Mails mit vertraulichem Inhalt wie persönlichen Angaben oder anderen zu schützenden Geschäftsinformationen im externen Verkehr (ausserhalb des Stadtnetzes) ist grundsätzlich zu verzichten oder dürfen nur in verschlüsselter Form und an bekannte oder vertrauenswürdige Web- oder E-Mail-Adressen versandt werden. Im Idealfall wird der Dienst BernBox in Kombination mit 7-Zip verwendet. Aktuell können in der Stadt Bern E-Mails nicht verschlüsselt werden. Hingegen kann der vertrauliche Inhalt einer Mitteilung als verschlüsselte E-Mail-Anlage versendet werden. Hierzu sind die ergänzenden Hinweise zu beachten.

	Bei der Kommunikation mit verwaltungsexternen Dritten dürfen E-Mails nur dann Personendaten enthalten, wenn die betroffene/n Person/en schriftlich (per E-Mail oder Brief) eingewilligt hat/haben, diese Personendaten in einer allgemein zugänglichen amtlichen oder amtlich bewilligten Veröffentlichung enthalten sind oder die Bekanntgabe dieser Personendaten gemäss Datenschutzgesetz erlaubt ist. Auf den unverschlüsselten Versand anderer vertraulicher Informationen per E-Mail ist zu verzichten. Innerhalb des Stadtnetzes (E-Mail-Adressen mit den Endungen …@bern.ch) darf vertraulicher Inhalt auch unverschlüsselt übermittelt oder ausgetauscht werden.
Neue Kommunikationswege	Die Schutzmassnahmen im Zusammenhang mit E-Mail gelten sinngemäss für die neuen Arten der Kommunikation (Chat, Unified Communication usw.).
Sicher im Internet	Der Zugriff auf Internet Dienste erfolgt ausschliesslich über die standardmässig installierten Webbrowser, deren Sicherheitseinstellungen nicht verändert werden dürfen. Schützenswerte Informationen wie Personendaten, Passwörter, Kreditkartennummern usw. dürfen nur verschlüsselt (https) über das Internet übermittelt werden. Der Zugang auf Internetseiten kann durch die ID selektiv erlaubt oder gesperrt werden.

E-Mail ist grundsätzlich unsicher

- Die Vertraulichkeit von unverschlüsselten E-Mails wird oft mit dem Versand einer Postkarte verglichen. Das Sicherheitsniveau von E-Mails ist jedoch noch tiefer, da diese weltweit an mehreren Stellen zwischengespeichert werden (Absender, Empfänger, Provider, Server usw.).
- Eine E-Mail, die an eine stadtexterne Adresse gesendet wird, kann grundsätzlich:
  - eingesehen und kopiert,
  - manipuliert oder gefälscht werden,
  - unterwegs liegen bleiben, verloren gehen oder an eine falsche Adresse gelangen.
- Wenn Zweifel bestehen, dass eine gesendete E-Mail unversehrt am Ziel eingetroffen ist oder dass eine empfangene E-Mail authentisch (echt) ist, sollte von der Gegenseite eine Bestätigung eingeholt werden (z.B. telefonisch).

Verschlüsselte E-Mail-Anlagen

- Verschlüsselte E-Mail-Anlagen sind Dateien oder Dateisammlungen, welche unter Verwendung eines zu bestimmenden Verschlüsselungsverfahrens und einem Kennwort für Dritte «unleserlich» gemacht werden. Das Kennwort muss zur Wahrung der Vertraulichkeit auf einem anderen Kanal, beispielsweise per Telefon oder SMS mitgeteilt werden.
- Die auf den städtischen Computern vorhandene Verschlüsselungsmöglichkeit ist die Software 7-Zip (im Fenster des Dialogs «Hinzufügen» unten rechts unter «Verschlüsselung», «Passwort eingeben»). Es existieren noch diverse andere Möglichkeiten um Dateien zu verschlüsseln. Diese werden jedoch durch die ID nicht aktiv unterstützt.
- Wichtig ist, dass je nach verwendeter Verschlüsselung und/oder Software die Empfangenden für eine erfolgreiche Entschlüsselung diese verwendete Verschlüsselung und/oder Software auch besitzen müssen. Deshalb bei einer ersten Benutzung unbedingt immer Testen, ob der Datenversand auch wirklich den Zweck erfüllt.

Daten an Externe sicher mit BernBox übermitteln

- Wie Daten sicher über BernBox BBx für Externe bereitgestellt werden, kann im Intranet[9] nach gelesen werden

Filterung ein- und ausgehender E-Mail Anhänge (Attachments)

Zur Risikoverminderung eines Virenbefalls bzw. der Virenverbreitung werden sämtliche E-Mail Anhänge an einem zentralen Punkt nach Dateityp gefiltert. Dies heisst, nur Dateitypen, die auf einer von der ID geführten «Blacklist» eingetragen sind, werden blockiert. Es ist aber zu beachten, dass auch Dateien, die durchgelassen werden, ein Risiko darstellen können.

[9] Intranet / Informatik / BernBox (BBx)

10. Mobile Geräte und Datenträger

Grundsätze	Der Umgang mit mobilen Geräten und Datenträgern hat gemäss den Vorgaben in Kapitel 5 zu erfolgen. Auf mobilen Geräten und Datenträgern sind nur notwendige Daten zu bearbeiten und zu speichern. Geschäftliche Daten auf mobilen Geräten sind umgehend zu löschen, sobald sie nicht mehr benötigt werden. Für die Datensicherung ist der/die Benutzer/in selbst verantwortlich. Müssen schützenswerte Daten abgespeichert werden, hat dies jeweils verschlüsselt (z.B. 7-Zip) zu erfolgen. Bei den ID können verschlüsselbare USB-Sticks und Harddisks bezogen werden. Der Verlust von mobilen Geräten und Datenträgern ist zwingend und unverzüglich dem IT-Support zu melden.
Notebooks	Es ist untersagt, Sicherheitsvorkehrungen und funktionseinschränkende Einstellungen auszuschalten, zu umgehen oder dies zu versuchen. Beim Anschluss an drahtlose Netzwerke (WLAN) sind diese bei erscheinender Auswahl richtig einzustufen (Privat, Arbeit, Öffentlich). Drahtlose Komponenten wie WLAN, Bluetooth, Infrarot usw. sind bei Nichtgebrauch zu deaktivieren. Mitarbeiterinnen und Mitarbeiter, die im Besitz eines mobilen Gerätes sind, müssen sich mindestens zwei Mal pro Monat am Netzwerk der Stadt Bern anmelden um sicherheitsrelevante Updates durchzuführen.
Smartphones und Tablet-PCs	Bei der Datensynchronisation mit der Stadt Bern wird zwischen einem Privat- oder einem Firmengerät unterschieden. In jedem Fall ist das Gerät über mobil.bern.ch zu registrieren ansonsten ist keine Synchronisation möglich. Bei der Registrierung als Privatgerät, wird über eine bereitgestellte App auf E-Mails, Kalender, Kontakte und BernBox zugegriffen. Diese App ist über einen vom Benutzenden definierten PIN geschützt und es werden keine Konfigurationen technisch auf dem Gerät erzwungen. Bei der Registrierung als Firmengerät, können die vom Gerätelieferanten bereitgestellten Apps für E-Mail, Kalender, und Kontakte verwendet werden.

Vom zentralen Zugangspunkt der Stadt Bern werden jedoch bestimmte Konfigurationen technisch erzwungen. Es gilt zu beachten, dass nicht alle Geräte die gesteuerten Konfigurationen übernehmen, teilweise sogar ignorieren. Benutzerinnen und Benutzer von Smartphones und Tablet-PCs sind verpflichtet, die genannten Konfigurationen laufend zu prüfen und wenn notwendig die Einstellungen (wo möglich) manuell durchzuführen.

Mindestens geforderte Konfigurationen sind:

- Das Gerätekennwort ist aktiviert, die minimale Kennwortlänge ist 6 Zeichen. Das Kennwort ist geheim und darf nicht an Dritte weitergegeben werden.
- Nach maximal 5 Minuten Inaktivität (ohne Benutzendeneingabe) wird das Gerät automatisch gesperrt.
- Nach maximal 10 fehlerhaften Kennworteingaben werden alle auf dem Smartphone enthaltenen Daten automatisch gelöscht bzw. das Gerät in den Werkszustand versetzt.

Die Verschlüsselungsfunktion für die Speichermedien und das Datenbackup sind aktiviert. Es ist untersagt, die vom zentralen Zugangspunkt durchgesetzten Konfigurationsrichtlinien auszuschalten, zu umgehen oder dies zu versuchen.
Kann ein Gerät nicht alle genannten Konfigurationen umsetzen, ist von einer Datensynchronisation mit der Stadt Bern abzusehen.

Bei der Verwendung von Apps wird Zurückhaltung gefordert. Bevor eine App heruntergeladen und installiert wird ist auf folgendes zu achten:

- Laden Sie nur Apps herunter, welche von den offiziellen Onlineshops wie dem App Store von Apple, Windows Phone Marketplace von Microsoft, Google Play Store, usw. erhältlich sind.
- Überprüfen Sie die Bewertungen von Apps – je mehr Leute eine App gut bewertet haben (4 Sterne und mehr), desto vertrauenswürdiger ist sie.
- Verifizieren Sie die Vertrauenswürdigkeit von Apps durch Recherchen im Internet.

Das Modifizieren von Betriebssystemen zum Umgehen herstellerbedingter Sperrfunktionen (in der Fachsprache Jailbreaking oder Rooten genannt) ist untersagt und wird technisch geprüft. Andernfalls erlischt die Berechtigung zur Datensynchronisation zur Stadt Bern.

Betriebssystem und Apps sind stets auf dem neusten Stand zu halten. Der/die Benutzer/in ist verpflichtet die verfügbaren Aktualisierungen innert zwei Wochen ab Herausgabe durch den Hersteller zu installieren.
Auf Smartphones und Tablet-PCs muss ein Virenschutzprogramm installiert sein[10].
Bevor ein Smartphone oder Tablet-PC zur Reparatur gegeben wird, sind nach einer allfällig noch möglichen Datensicherung alle personenbezogenen Daten (z.B. Anrufspeicher, gespeicherte SMS und E-Mails, Kontakte, Kalender, usw.) zu löschen und das Gerät auf Standardwerte zurückzusetzen. Ausserdem ist die SIM-Karte zu entfernen.
Bei Verlust eines Smartphones bzw. Tablet-PCs sind die nachfolgenden Massnahmen sofort und in der genannten Reihenfolge auszuführen. Bei Unklarheiten ist der IT-Support zu kontaktieren.

1. Sperren der SIM-Karte beim Mobilfunkanbieter veranlassen
2. Verwendete Passwörter ändern
3. IT-Support über den Verlust und die getätigten Massnahmen informieren. Dieser wird bei einem Privatgerät die MDM App löschen oder bei einem Firmengerät dieses komplett Löschen (Wipen)

Viele Geräte bieten die Möglichkeit, Daten in der Cloud zu speichern. Falls auf einem Smartphone oder Tablet-PC ein Datenaustausch (E-Mail, Kalender usw.) mit der Stadt Bern erfolgt, ist ein Gebrauch der Cloud untersagt, wenn dieser Austausch nicht über die bereitgestellte MDM App geschieht. Nur Ortungsdienste (ohne Datensicherung) wie «iPhone suchen» von Apple oder «Lookout» bei Android-Geräten sind in jedem Fall erlaubt.
Die ICT-Sicherheitsbeauftragten der Stadt Bern sind befugt, städtische wie auch private Smartphones und Tablet-PCs im Beisein der Benutzenden auf Einhaltung der Sicherheitsvorgaben zu überprüfen.

Erhöhte Risiken
Der verantwortungsvolle Umgang mit mobilen Geräten und Datenträgern ist für die ICT-Sicherheit von grosser Bedeutung, denn der Markt bietet heute eine Riesenauswahl an Elektronik mit Kommunikations- und Datenverarbeitungsfunktionen (Notebooks, Handys, PDAs, Smartphones, Kameras usw.). Zudem steht auf immer kleineren Datenträgern (z.B. USB-Sticks oder Speicherkarten) immer mehr Speicherplatz zur Verfügung.

[10] Entsprechende Hinweise sind im Intranet unter Informatik / ICT-Sicherheit zu finden.

Über mobile Geräte und Datenträger können sich Fremde relativ einfach Zugang zu heiklen Geschäftsinformationen und Personendaten verschaffen. Mobile Geräte und Datenträger sind zudem für Diebe besonders attraktiv und können unterwegs vergessen werden oder verloren gehen.

Sicherheitsmassnahmen mit Smartphones und Tablet-PCs
Wichtige und heute bei den neuen städtischen Notebooks standardmässig umgesetzte Sicherheitsmassnahmen wie etwa der Zugriffschutz, die Datenverschlüsselung, der Virenschutz und die Aktualisierung der installierten Software sind bei Smartphones und Tablet-PCs nicht standardmässig voreingestellt.

Unbeabsichtigte Offenlegung von Informationen
Der Funktionsumfang von Smartphones und Tablet-PCs wächst durch die Installation von immer neuen Anwendungen (sogenannter Apps) ständig. Allerdings stecken in den neuen Möglichkeiten und Funktionen auch Gefahren. Das Herunterladen und Installieren von schädlichen oder auch nur schlecht programmierten Anwendungen kann eine unbeabsichtigte Offenlegung von Daten zur Folge haben. So können Anwendungen Zugriff auf zahlreiche Informationen haben, wie beispielsweise Angaben über den Ort der Gerätenutzung, Kontaktinformationen inklusive der getätigten Telefonate oder Daten des E-Mail-Kontos und sämtlichen Tastatureingaben einschliesslich Passwörter. Nebst gezielten Angriffen besteht auch die Gefahr, dass viele Nutzende mit den Einstellungen ihrer benutzten Anwendungen überfordert sind und dadurch eigene wie auch geschäftliche Informationen offenlegen, ohne sich dessen bewusst zu sein. Zudem ermöglichen Kamera und Mikrofon unerlaubt und unbemerkt Gespräche aufzuzeichnen oder kritische Informationen zu fotografieren. Die aufgezeichneten Informationen können dann ohne weiteres an Dritte weitergeleitet werden.

Einschleusen von schädlichem Programmcode
Alle Smartphones und Tablett-PCs ermöglichen eine E-Mail Kommunikation und den Zugriff auf das Internet. Dementsprechend sind die Nutzerinnen und Nutzer von mobilen Endgeräten ebenso den Gefahren von Viren, Würmern und Trojanern ausgesetzt wie PC-Anwenderinnen und Anwender. Zu berücksichtigen ist, dass die Attraktivität von speziell auf mobile Geräte zugeschnittener Schädlingssoftware für deren Urheber mit zunehmender Verbreitung der entsprechenden Geräte zunimmt. Es ist bereits erwiesen, dass vermehrt Schadensfälle im Bereich mobile Geräte auftreten.

11. Virenschutz

Präventive Massnahmen	Mobile Datenträger (z.B. CDs, DVDs, USB-Sticks, Speicherkarten, usw.) sind vor deren Verwendung (lesen, schreiben) in der städtischen ICT-Infrastruktur und nach jeder auswärtigen Verwendung auf Viren zu prüfen. Nach dem Beenden der Benutzung – spätestens vor einem Neustart des Computers – sind sie aus dem Laufwerk zu entfernen. Das Herunterladen (Download) von Dateien aus dem Internet ist nur zulässig, wenn die Quelle vertrauenswürdig ist. Falls beim Öffnen einer von extern elektronisch empfangenen Office-Datei ein Hinweis auf Makros erscheint, ist die Option «Makros deaktivieren» zu wählen. Desktop-PCs/Notebooks sind nach Arbeitsschluss in der Regel vollständig herunterzufahren (wichtige Aktualisierungen werden erst bei Neustart vollständig übernommen).
Vorgehen beim Auftreten von Viren	Bei unerwartetem Verhalten oder einem Verdacht auf einen Virus, der nicht wie im Normalfall automatisch vom Virenschutzprogramm beseitigt wird, ist unverzüglich der IT-Support zu benachrichtigen. Benutzerinnen und Benutzer dürfen Viren nicht eigenhändig bekämpfen.

Überprüfung auf Viren bei mobilen Datenträgern
In der Taskleiste unter den ausgeblendeten Symbolen findet sich das blaue Symbol der Antivirensoftware OfficeScan. Mit einem Rechtsklick auf das Symbol wird dieses via Menüpunkt «Open OfficeScan-Agent Console» gestartet und das Scannen des mobilen Datenträgers oder eines Downloads ist möglich. Alternativ wird OfficeScan mit einem Rechtsklick auf das Symbol des mobilen Datenträgers im Explorer und dem Menüpunkt «Scan with OfficeScan» gestartet.

Wie bedrohlich sind Viren?
- Ständig wirkungsvolleren Virenschutzprogrammen stehen täglich neue, immer raffiniertere Viren gegenüber. Durch die weltweite Vernetzung verbreiten sie sich in kürzester Zeit lawinenartig.
- Auch beim Auftreten von harmlos scheinenden Viren können beträchtliche Schäden entstehen. Die Auswirkungen sind nicht unbedingt direkt sichtbar (z.B. wenn ein Desktop-PC für Angriffe auf Dritte missbraucht wird). Zudem fällt jedes Mal Arbeitsaufwand für die koordinierte Diagnose und Beseitigung an.

Wo können Viren auftreten?
- Viren können beispielsweise über Datenträger (z.B. USB-Sticks, Smartphones), E-Mail-Attachments und Internet-Downloads eingeschleppt werden.
- Oft genügt schon der Besuch von präparierten Internet-Seiten (z.B. bei Klick auf Links in Spam-Mails) oder unter Umständen der Besuch absolut seriöser Websites, die manipuliert worden sind (z.B. ist die Website von 20min.ch Opfer von Hackern geworden).

12. Kontrolle / Überwachung und Folgen bei Missbrauch

Konsequenzen für Mitarbeitende

Verstösse gegen diese Weisung stellen Dienstpflichtverletzungen dar und können personalrechtliche Massnahmen zur Folge haben.
Bei strafbaren Handlungen wird gegen die fehlbaren Mitarbeitenden Anzeige erstattet.

Protokollierung
Die Nutzung der Informatik- und Kommunikationsmittel wird zur Sicherstellung der technischen Sicherheit und Einhaltung der vorliegenden Weisung sowie der gesetzlichen Bestimmungen protokolliert.
Es ist zu beachten, dass allfällige private Tätigkeiten ebenfalls protokolliert werden und aus technischen Gründen nicht von der geschäftlichen Nutzung unterschieden werden können.

Periodische anonyme Auswertung der Protokolldaten
Die Protokollierungen werden flächendeckend und anonym durch die ID ausgewertet. Dabei geht es um die statistische Analyse der Protokollierungen z.B. nach folgenden Kriterien:

- Internet: Meist besuchte Internetseiten, Inhalt der Internetseiten, Dauer der Verbindungen
- E-Mails: Anzahl versendeter und empfangener E-Mails, Typ der Anhänge, beteiligte Adressen
- Handys / Festnetz: Anzahl und Dauer der geführten Gespräche, Zeitpunkt der geführten Gespräche, gewählte Telefonnummern.

Personenbezogene Auswertung der Protokolldaten
Eine personenbezogene Auswertung der Protokolldaten kann in folgenden Fällen erfolgen:

- wenn auf Grund von anonymen Auswertungen Verstösse gegen die vorliegende Weisung festgestellt werden. In diesem Fall werden sämtliche Mitarbeitenden informiert, dass die Auswertung für einen begrenzten Zeitraum personenbezogen erfolgt. Diese Auswertung erfolgt durch die ID unter der Leitung der ICT-Sicherheitsbeauftragten.
- wenn die Abteilungsleitung einen Missbrauch feststellt oder vermutet. In diesem Fall kann sie den ICT-Sicherheitsbeauftragten einen schriftlichen Auftrag zur personenbezogenen Auswertung der Protokolldaten erteilen. Die betroffene Person muss schriftlich bestätigen, vom Auftrag Kenntnis genommen zu haben.
- wenn sich ein sicherheitsrelevanter Vorfall ereignet hat (bzw. wenn konkrete Anhaltspunkte für einen bevorstehenden Vorfall vorhanden sind), der auf einem Missbrauch beruht. In diesem Fall dürfen die ID unter der Leitung der ICT-Sicherheitsbeauftragten sämtliche Verbindungsdaten ohne Auftrag und ohne Information personenbezogen aufzeichnen. Über die etwaige Auswertung der gesammelten Daten sind die betroffenen Personen vorgängig zu informieren.

- wenn ein konkreter Verdacht auf eine Straftat vorliegt. Die zuständige Abteilungsleitung, Direktion und das Personalamt entscheiden, ob die Strafverfolgungsbehörden eingeschaltet werden. Falls ja, können die ID nach Absprache mit den Strafverfolgungsbehörden aufgefordert werden entsprechende Beweise zu sichern.

Für das Öffnen persönlicher E-Mails muss vorgängig die Einwilligung des betroffenen Mitarbeitenden oder der Strafbehörden eingeholt werden.
Die ID melden die Namen von fehlbaren Mitarbeitenden ausschliesslich deren Vorgesetzten (Abteilungsleitung). Ausnahmen sind nur im Einzelfall mit der Einwilligung der betroffenen Person oder bei strafrechtlich relevanten Sachverhalten möglich.

13. Schlussbestimmungen

Aufhebung bisheriger Bestimmungen

Die folgenden Bestimmungen werden aufgehoben:

- Weisung IT-Sicherheit für Benutzerinnen und Benutzer vom 1. Oktober 2012

Inkrafttreten

Diese Weisung tritt am 1. März 2017 in Kraft.

Informatiklenkungsausschuss (ILA) im Namen des Gemeinderats der Stadt Bern
Sig. Vorsitzender ILA

Anhang A: Wichtige Anlaufstellen

Betriebliche, technische und ICT-Sicherheitsfragen der alltäglichen Informatik
Informatikkoordinierende der Direktionen

Erste Anlaufstelle bei IT-Problemen (ausser Geografischen Informationssystemen)
IT-Support (Kundenservice und Betrieb – KB) der Informatikdienste
Tel.: 031 321 74 74, Ticket-System (Intranet: PC-Support),
E-Mail: it.servicezentrum@bern.ch

Erste Anlaufstelle bei IT-Problemen mit Geografischen Informationssystemen (GIS)
GIS-Kompetenzzentrum (GKB) des Vermessungsamtes
Tel.: 031 321 67 77, Ticket-System (Intranet: PC-Support),
E-Mail: gis.support@bern.ch

Fragen und Informationen zur ICT-Sicherheit und deren Umsetzung
Eric Tönz, strategischer ICT-Sicherheitsbeauftragter
Tel.: 031 321 74 89, E-Mail: eric.toenz@bern.ch
Martin Müller, ICT-Sicherheitsbeauftragter
Tel.: 031 321 74 47, E-Mail: martin.mueller@bern.ch
Im Intranet unter Informatik / ICT-Sicherheit

Datenschutzfragen
Mirjam Graf, Datenschutzbeauftragte
Tel.: 031 312 09 09, E-Mail: ombudsstelle@bern.ch
www.bern.ch/stadtverwaltung/datenschutz

Anonyme Meldungen
Mirjam Graf, Ombudsstelle
Tel.: 031 312 09 09, E-Mail: ombudsstelle@bern.ch

Anhang B: Glossar

Begriff / Abkürzung	Bedeutung
App	Der Begriff App bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für Smartphones und Tablet-PCs gemeint, die über einen in das Betriebssystem integrierten Onlineshop bezogen und so direkt auf dem Smartphone installiert werden können.
Berechtigungsnachweise	Unter Berechtigungsnachweise wird das Passwort, der M.ID Pin oder der M.ID Passcode verstanden.
BernBox	BernBox ist ein von den ID betriebener Cloud Dienst zum einfachen und sicheren Datenaustausch innerhalb und ausserhalb der Stadtverwaltung Bern und beherbergt die darin befindlichen Daten im Rechenzentrum der Stadt Bern.
Cloud Computing	Siehe ergänzende Hinweise in Kapitel 8
Computervirus	siehe unter Virus
Datenschutz	Beim Datenschutz geht es um den Schutz der Persönlichkeit und der Privatsphäre von Personen, über die Daten bearbeitet werden. Das Recht auf Datenschutz gehört zu den verfassungsmässig geschützten Grundrechten. Darunter fallen im ICT-Bereich beispielsweise Daten wie Personaldaten, persönliche E-Mails und Telefonate der Mitarbeitenden, Daten von Steuerpflichtigen, Sozialhilfeempfangende, Schulkindern usw. Jedes Lesen, Verändern, Aufbewahren, Löschen, Weiterleiten, Bekanntgeben usw. solcher Daten kann das Grundrecht der betroffenen Personen auf Datenschutz verletzen.
Firewall	Eine Firewall sichert Ihren Rechner gegen unerlaubte Zugriffe von aussen ab – zum Beispiel Hackerangriffe. Fast noch wichtiger ist jedoch die Kontrolle des ausgehenden Datenverkehrs. Schädlinge, Software oder das Betriebssystem schicken im Hintergrund Informationen ins Internet. Das kann bei gefährlichen Programmen vom Rapportieren Ihrer Surfgewohnheiten bis hin zu den Zugangsdaten vom Onlinebanking-Konto reichen. Ist eine Firewall installiert, müssen Sie alle Verbindungen ins Internet manuell erlauben. Das heimliche Verschicken von Benutzendeninformationen ist so nicht mehr möglich. Eine Firewall bietet aber keinen Schutz vor Viren, Würmern und anderen Schadprogrammen. Sie kontrolliert nur den Datenverkehr.

GKB	Das GIS-Kompetenzzentrum Bern (GKB) ist verantwortlich für das GIS-Bern. GIS ist die Abkürzung für Geoinformationssysteme. Zum GIS-Bern gehört neben der technischen Infrastruktur auch die zentrale Verwaltung der städtischen Geodaten.
Hacking	Im Bereich der Computersicherheit wird die Herausforderung des Hackens darin gesehen, Sicherheitsmechanismen zu überwinden und somit Schwachstellen erkennen zu können oder genauer, Systeme zum Beispiel per Social Engineering zu unterwandern oder per Reverse Engineering (engl., bedeutet: umgekehrt entwickeln, rekonstruieren) auf Design- und Programmierfehler hin zu untersuchen. Unter Umgehung der Sicherheitsvorkehrungen können die Hacker so Zugriff auf ein Computernetzwerk, einen Computer, eine gesicherte Komponente (z.B. Chipkarte) oder Zugang zu gesperrten Daten oder einer sonst geschützten Funktion eines Computerprogramms erhalten.
ICT	information and communications technology, englisch für Informations- und Kommunikationstechnik (IKT)
ID	Die Informatikdienste (ID) sind der Direktion FPI unterstellt und der führende IT Service Provider der Stadt Bern. Gemäss den Zuständigkeitsabgrenzungen im Schichtenmodell sind die ID verantwortlich für die Bereitstellung, den Betrieb und Unterhalt der Anwendungen sowie für die Planung und Bereitstellung sowie den Betrieb und die Betreuung der technischen Infrastruktur.
ILA	Der Informatiklenkungsausschuss plant, koordiniert und stimmt den Informatikeinsatz auf strategischer Ebene in der Stadtverwaltung ab, verabschiedet die entsprechenden Zielsetzungen, überwacht deren Einhaltung und bereitet die durch den Gemeinderat der Stadt Bern (GR) zu behandelnden Informatikgeschäfte vor. Der ILA ist ein im Rahmen der Informatikstrategie geschaffenes, vom GR bestelltes Gremium. Gemäss Führungs- und Organisationskonzept der Informatikstrategie ist der ILA als ein ständiges Gremium positioniert. Der ILA ist organisatorisch dem GR unterstellt (siehe auch im Intranet: Informatik / ILA).
IT	Informationstechnik ist ein Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software (Informationstechnisches System)
IT-Servicezentrum	Alter Name für den Bereich Kundenservice und Betrieb (KB), siehe KB.

IT-Support	siehe KB
ICT-Sicherheit	Bei der ICT-Sicherheit geht es primär darum, wichtige Arbeitsprozesse, die durch die IT unterstützt werden, angemessen zu schützen. Dabei sind vier Grundwerte von zentraler Bedeutung: • Vertraulichkeit (Schutz vor unberechtigter Kenntnisnahme) • Verfügbarkeit (Schutz vor IT-Ausfällen) • Verlässlichkeit (Integrität; Schutz vor unerwünschten Veränderungen) • Verbindlichkeit (Authentizität; Schutz vor Identitätsfälschung/ Verschleierung)
KB	Der Bereich Kundenservice und Betrieb (KB) betreibt den IT-Support als zentrale Anlaufstelle bei Informatik-Anliegen aller Mitarbeitenden der Stadtverwaltung.
M.ID	M.ID steht für Mobile Identity. Der Identitätsnachweis wird auf Grund des Besitzes des Mobiltelefons erbracht, da der Passcode per SMS auf dieses zugestellt wird.
M.ID Passcode	Als Passcode wird eine zufällig generierte Zeichenkette bezeichnet, welche beispielsweise als SMS auf das Mobiltelefon verschickt wird.
M.ID Pin	Der M.ID Pin wird von den Benutzenden gesetzt und muss geheim bleiben. Er autorisiert das Auslösen eines Passcodes.
Mietsoftware «out of the box»	Lösungen, die sofort einsatzbereit sind – vor allem bei Software unter «Auspacken, Installieren und Benutzen ohne zusätzliche Konfiguration oder Anpassung» bekannt.
OWA	Der Outlook Web App ist eine Technik von Microsoft um von einem beliebigen Computer oder mobilen Gerät mit Internetanschluss und Webbrowser auf den eigenen städtischen Outlook Account zugreifen zu können.
Passcode	Siehe M.ID Passcode.
Passsatz	Ein aus mehreren Wörten, Zahlen und Sonderzeichen zusammengesetzter Satz, der als Passwort eingesetzt wird und nur sehr schwer zu entschlüsseln ist.
Passwort	Ein Passwort ist ein vom Benutzenden vollkommen frei gewähltes geheimes Kennwort, das sich aus Buchstaben, Ziffern und Sonderzeichen zusammensetzt.

Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.
Besonders schützenswerte Personendaten	Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe und administrative oder strafrechtliche Verfolgungen und Sanktionen.
Persönlichkeitsprofil	Eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt.
Persönliche Daten	Geschäftliche Daten, Informationen, usw. persönlicher Natur.
Phishing	Unter dem Begriff Phishing (Neologismus von Phishing, engl. Für «Angeln») versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzenden zu gelangen und damit Identitätsdiebstahl zu begehen.
Pin	Siehe M.ID Pin.
Private Daten	Daten und Informationen ohne geschäftlichen Zusammenhang.
Ransomware	Ransomware gelangt meistens über einen verseuchten Anhang einer E-Mail auf Ihren Computer, verschlüsselt alle Daten und verlangt anschliessend Geld in Form von Bitcoins für die Entschlüsselung. Eine Garantie, dass die Daten nach der Zahlung wieder entschlüsselt werden, gibt es nicht.
Social Engineering	Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking. Social Engineering umgeht alle technischen Sicherheitsvorkehrungen und zielt auf das schwächste Glied in der Sicherheitskette: Den Menschen.

Social Media	Social Media wie Facebook, Twitter und Xing sind soziale Netzwerke und Gemeinschaften, bei denen das Teilen von Informationen und der Austausch, das Kommentieren, Bewerten und Empfehlen im Mittelpunkt stehen. Die sozialen Medien haben sich in den letzten Jahren zu Massenmedien mit grosser Reichweite entwickelt. Für einen wachsenden Personenkreis sind sie bereits die hauptsächliche Informationsquelle.
Spam	Unter Spam versteht man unverlangt zugestellte E-Mails. Spams werden aufgrund der geringen Kosten für den Versender stets in grossen Massen verschickt. Am häufigsten sind kommerzielle Spam-Mails. Aber auch Viren werden auf diesem Weg verbreitet. Bei Handys gibt es das Phänomen der SMS-Spams.
Starkes Passwort	Von einem starken Passwort wird dann gesprochen, wenn ein Passwort mit modernen Entschlüsselungstechniken nur sehr schwer zu entschlüsseln ist. Im Allgemeinen wird davon ausgegangen, dass Passwörter mit mehr als 10 Zeichen, die rein zufällig gewählte Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten, starke Passwörter sind. Siehe auch «Passsatz»
Trojaner (Trojanisches Pferd)	Dies ist Schadsoftware, deren unangenehme Eigenschaften gut als z.B. ein Spiel, ein Tool, ein Add-On etc. getarnt sind. Der Zweck von Trojanern ist z.B. einen Computer fernzusteuern, Benutzendenaktionen auszuspionieren und vieles mehr.
Unified Communications	Unified Communications (UC), englisch für «vereinheitlichte Kommunikation», kurz UC genannt, ist der Begriff für die Integration unterschiedlicher Kommunikationsmedien in einer Anwendungsumgebung. Die Idee hinter Unified Communications ist, durch eine Zusammenführung aller Kommunikationsdienste und die Integration mit Präsenzfunktionen, die Erreichbarkeit von Kommunikationspartnern zu verbessern und so geschäftliche Prozesse zu beschleunigen.
Verschlüsselung	Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text (oder auch Informationen anderer Art, wie Ton- oder Bildaufzeichnungen) mit Hilfe eines Verschlüsselungsverfahrens in eine «unleserliche», das heisst nicht einfach interpretierbare Zeichenfolge umgewandelt wird.

Virus (Computervirus)	Ein Virus ist ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Die Bezeichnung «Virus» wird häufig als Sammelbegriff für schädlichen Programmcode verwendet (Bootsektorviren, Makroviren, Würmer, Trojaner, usw.). Fachleute bevorzugen den Begriff «Malware». Die Schadensfunktionen von Viren reichen von einfachen PC-Störungen bis hin zu Netzwerkausfällen und Datenabfluss.
VoIP	Voice over IP (kurz VoIP), auch IP-Telefonie (kurz für Internet-Protokoll-Telefonie) genannt, ist das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Dabei werden die für Telefonie typischen Informationen, d. h. Sprache und Steuerinformationen über ein auch für Datenübertragung nutzbares Netz übertragen. Bei den Gesprächsteilnehmenden können sowohl Computer, auf IP-Telefonie spezialisierte Telefonendgeräte als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung herstellen.
Zertifikat	Digitale Zertifikate werden genutzt, um Verbindungen zu verschlüsseln sowie die Authentizität von Personen und Objekten zu prüfen. Beispiele von Zertifikaten sind: Suisse-ID, welche zur Prüfung der Authentizität einer Person verwendet werden kann; ein Serverzertifikat (SSL), welches dem Anwendenden die Sicherheit gibt, mit der korrekten Website verbunden zu sein.

Anhang C: Quellenangaben

http://www.bern.ch/stadtverwaltung/datenschutz/
http://www.edoeb.admin.ch/
http://www.melani.admin.ch/
http://de.wikipedia.org/wiki/
http://www.bsi.de/
https://www.ebas.ch/

Beispiele und Empfehlungen des Kantons Bern, des Bundes und der Schweizerischen Informatikkonferenz (SIK)