ICT-WEISUNG

Abteilung: Legal & Compliance

Verfasser: Christina Hooker Legal Counsel

Erstellt: Bern, 07.06.2021

Dieses Reglement beschreibt den Umgang mit Informatik-Mitteln und Informationen der Unternehmen der BMS. Ein unsachgemässer Gebrauch von Informatik-Mitteln setzt BMS unterschiedlichen Risiken aus wie Computer-Viren, Beeinträchtigung der Verfügbarkeit von Systemen und Services sowie rechtlichen Konsequenzen. Um eine effiziente Sicherheit zu erreichen, ist es wichtig, dass alle Mitarbeiterinnen und Mitarbeiter ihren Teil dazu beitragen.

Geltungsbereich

Diese Weisung gilt für alle Mitarbeitende aller Unternehmen der BMS. Dies sind:

- BR Bauhandel AG
- Gétaz-Miauton SA
- Barrit Baubedarf AG
- Regusci Reco SA

Die Weisung ist dem Personalreglement angehängt. BMS ist dazu berechtigt, das vorliegende Reglement jederzeit zu ergänzen und abzuändern. Die jeweils gültige Version der ICT Weisung kann auf den jeweils gültigen BMS Kommunikationskanälen abgerufen oder bei der HR Abteilung oder dem Vorgesetzten eingeholt werden.

Verantwortung übernehmen

Unabhängig der Funktion oder hierarchischen Position bei BMS, kann der Mitarbeitende zu mehr Sicherheit beitragen, indem er/sie persönliche Verantwortung ernst nimmt.

Regelungen und Sicherheitsvorschriften kennen

Der Mitarbeitende hat sich mit dieser Weisung und anderen Sicherheitsvorschriften der BMS vertraut zu machen. Bei Fragen soll sich der Mitarbeitende an den IT Help Desk oder an seinen/ihren Vorgesetzten wenden.
BMS behält sich das Recht vor, allfällige Verstösse gegen diese Weisung gemäss dem Artikel 3.1 und 3.8 des Personalreglements Folge zu leisten.

Schwachstellen melden

Sind kritische Vorfälle aufgetreten oder werden Schwachstellen erkannt, so erwartet BMS von seinen Mitarbeitenden, dass diese sofort handeln, indem sie den IT Help Desk oder den Vorgesetzten PER TELEFON informieren. Achtung: Es dürfen z. B. Phishing-Versuche, Ransomware oder andere Bedrohungen nicht per E-Mail an den Helpdesk oder an eine andere Person im BMS-Netzwerk weitergeleitet werden. Die fehlerhafte Nachricht ist sofort zu löschen oder als SPAM zu bezeichnen. Wenn ein Virus bereits als unter Quarantäne gestellt gekennzeichnet ist,

müssen keine weiteren Maßnahmen ergriffen werden, bei Zweifel ist der IT Helpdesk per Telefon zu kontaktieren. Die Mitarbeitenden werden gebeten, erkannte oder vermutete Schwachstellen nicht selber auszutesten.

Arbeitskollegen unterstützen

Unterstützen Sie Arbeitskolleginnen und -kollegen, indem Sie auf erkannte Sicherheitsrisiken aufmerksam machen. Ein freundlicher Ratschlag hilft oft mehr als eine Vorschrift.

Umgang mit Software und Hardware

Private Hardware und Software
Es ist ausdrücklich verboten, private Geräte wie PCs/Notebooks oder Netzwerkgeräte in den BMS Unternehmen zu verwenden. Auch dürfen vertrauliche Informationen der BMS nicht auf persönlichen Geräten zu Hause verarbeitet oder gespeichert werden.

Ausgenommen von dieser Regelung sind

- Benutzer, welche eine schriftliche Bewilligung der IT Abteilung für den Betrieb ihrer privaten Geräte erhalten haben.
- Interne und externe Mitarbeiter oder Gäste, welche vom Gast Wireless-LAN Gebrauch machen.
- Die professionelle E-Mail- und Kalender Verzeichnissynchronisation mit privaten Smartphones und Tablets ist nur mit dem BMS Exchange-Konto erlaubt, nicht mit iCloud oder einem anderen privaten (Cloud-basierten oder nicht) Verzeichnis. Die Nutzer akzeptieren explizit, dass bei der Synchronisation Sicherheitsrichtlinien automatisch auf den Geräten konfiguriert werden.

Beschaffung, Installation und Entsorgung von Geräten und Software
Neue Hardware, Software und Dienste sind über die IT Abteilung zu beschaffen und zu installieren. Hierfür steht ein Formular für alle Mitarbeitenden im Astra-Selbstbedienungsportal auf dem BMS-Intranet zur Verfügung. Dieses Formular wird zur Genehmigung durch den direkten Vorgesetzten und HR beim IT-Department (über das Helpdesk) eingereicht, bevor es ein "Anfrage"-Ticket in unserem Ticketing-System auslöst (derzeit Helpline).
Dieses Prozedere gilt auch für Freeware (kostenlos frei erhältliche Software), Open-Source Produkte (kostenlos frei erhältlicher Quellcode) oder Cloud-Dienste. Die eingesetzten Softwares müssen ausnahmslos lizenziert sein. Zudem muss sichergestellt werden, dass die installierten Softwares nicht unrechtmässig kopiert werden. Private Softwares zu installieren ist verboten.

Alte Geräte werden oberflächlich gereinigt und **mitsamt aller Zubehör wie Ladegeräten, Tragetaschen, etc** der IT Abteilung zurückgegeben: Bei Laptops und Desktops setzt der IT-Support diese komplett neu auf, so dass alle Daten gelöscht werden. Private Dokumente dürfen vor der Abgabe auf ein USB-Stick gespeichert und vom Laptop/Desktops gelöscht werden. **iPhones sollten vollständig von jeglichem iCloud-Konto getrennt und komplett auf die Werkeinstellungen zurückgesetzt werden**, bevor sie an den IT-Support zurückgegeben werden. Wird dieser Schritt vor der Abgabe unterlassen, können dem Mitarbeitenden hierdurch entstandene Kosten in Rechnung gestellt werden.

Cloud Speicher
Speichern von Daten in privaten Cloud-Services wie Dropbox, OneDrive, Box, G-Drive und vergleichbare ist nicht erlaubt. Bedarfsfälle müssen der IT Abteilung gemeldet werden.

Hardware- und Software Störungen/ Diebstahl
Alle Störungen an Software und Geräten müssen umgehend dem Vorgesetzten und dem IT Help Desk gemeldet werden. Diebstahl von Software und Geräten muss als Erstes sofort der Polizei gemeldet werden. Der Nachweis der Anzeige (scan oder Originaldokument) ist mittels eines Tickets dem IT-Helpdesk vorzulegen (das Dokument wird für die Meldung an die Haftpflichtversicherung benötigt). Für vorsätzliche oder grobfahrlässige Schäden an Hard- oder Software können Mitarbeitende gemäss Artikel 3.1 und 3.8 des Personalreglements in die Verantwortung gezogen und sanktioniert werden.

Nutzung, Pflege und Reinigung der Geräte
Die BMS ICT Geräte sind gemäss den Instruktionen der IT Abteilung zu nutzen. Das Material darf nicht ohne die Zustimmung der IT Abteilung verändert werden, weder dauerhaft noch oberflächlich (zB mit Stickern). Jede abnormale Nutzung eines Geräts muss der IT Abteilung unverzüglich gemeldet werden.
Für die äusserliche Pflege und Reinigung der BMS Geräte sind die Mitarbeitenden selbst verantwortlich. Gut gepflegte Hardware lebt länger und ist weniger anfällig auf Störungen. Dabei gilt: Getränke und Esswaren gehören in sichere Entfernung zu Tastatur und Geräten.

Benutzung von Kommunikationsmitteln

Regelung für die Nutzung von Internet, E-Mail, Telefonie und Kommunikationen auf Beekeeper

- BMS stellt allen Mitarbeitenden mit Zugang zu IT-Geräten den Zugriff auf das Internet zu Geschäftszwecken zur Verfügung.

- Die Mitarbeitenden sind für ihr Handeln selbst verantwortlich. Der Zugriff auf das Internet wird mit einem Webfilter eingeschränkt; als Folge stehen nicht alle Dienste im Internet zur Verfügung. Verbotene Inhalte und solche, die BMS schaden können, werden gefiltert.

- Einschränkungen durch den Webfilter sind verbindlich und dürfen nicht umgangen werden.

- Das Herunterladen von gesetzlich verbotenem Material (insbesondere pornographische Darstellungen, extrem-politisches Material u.ä.) sowie Verletzungen des Copyrights sind verboten und können für den Benutzer zu strafrechtlichen Konsequenzen sowie zu Sanktionen nach dem BMS Personalreglement führen.

- Die gelegentliche Nutzung des Internets und des Geschäftstelefons (für Anruf) zu privaten Zwecken ist erlaubt. Die Produktivität des Mitarbeitenden während der Arbeitszeit darf dadurch nicht beeinträchtigt werden.

- Wird ein privates Smartphone auch als Geschäftstelefon genutzt, so gilt Folgendes:
    - Es sind keine privaten Cloud-Synchronisierungen erlaubt.
    - Das geschäftliche Verzeichnis darf NUR auf dem BMS Exchange-Server synchronisiert werden.
    - Es dürfen keine digitalen Aufnahmen (Videos, Fotos, Audios, etc) von BMS-Daten auf dem privaten (internen oder zusätzlichen) Speicher gespeichert werden.

- Die Benutzer erkennen mit dem Gebrauch des Internets ausdrücklich das Recht von BMS an, im Rahmen der gesetzlichen Grundlagen Datenverkehr aufzuzeichnen und im Rahmen des geltenden Datenschutzgesetzes auszuwerten.

- **Die Nutzung der Geschäfts- E-Mail zu privaten Zwecken ist nicht erlaubt.** Spätestens am letzten Arbeitstag werden das E-Mail-Konto des austretenden Mitarbeitenden sowie auch alle anderen IT-Konten und die Inbox gesichert und gesperrt. Nach einer gewissen Zeit werden die Konten gelöscht.
  E-Mail-Konten austretender oder für lange Zeit krankgeschriebener Mitarbeitenden, die keine Gelegenheit hatten, die laufenden Geschäfte an eine zuständige Person zu übergeben, können nach Zustimmung der Abteilung Legal & Compliance und unter 4-Augen-Prinzip nach Mails zu den laufenden Geschäften durchsucht werden. Sollten wider Erwarten private E-Mails bei der Suche aufkommen, so werden diese ohne Einsichtnahme ausgesondert.

- Die Überwachung des geschäftlichen E-Mailverkehrs erfolgt im Rahmen der entsprechenden gesetzlichen Bestimmungen. Folgendes Prozedere wird bei BMS befolgt:
  - Besteht ein ernsthafter Verdacht auf ein schwerwiegendes Fehlverhalten im Unternehmen, welches jedoch nicht auf eine bestimmte Person festgelegt werden kann, so muss die HR-Abteilung eine schriftliche Anfrage für eine generelle Überwachung an die IT-Abteilung richten. Die IT-Abteilung kann sodann eine allgemeine oberflächliche Überwachung in die Wege leiten. Die oberflächliche Überwachung deckt keine Identitäten auf.
  - Verstärkt sich der Verdacht nach der oberflächlichen Überwachung, so können gezieltere Untersuchungen durch die HR-Abteilung angeordnet werden.
  - Wird ein Mitarbeitender gezielt eines Fehlverhaltens verdächtigt, so kann dessen Benutzerkonto, nach schriftlicher Anfrage durch die HR-Abteilung, von der IT-Abteilung auf Nachweis des Fehlverhaltens durchsucht werden.
  - Mit «Privat» gekennzeichnete E-Mails und Dokumente oder E-Mails und Dokumente, welche klar privater Natur sind (zB ein Kosename im Betreff) werden von der IT-Abteilung nicht geöffnet.
  - Von der gezielten Durchsuchung ihres Kontos betroffene Mitarbeitende werden spätestens nach der Dursuchung darüber informiert.
  - Alle Dursuchungen durch die IT-Abteilung werden durch die Abteilung Legal & Compliance begleitet.

  Die arbeitsrechtlichen Konsequenzen können von einer Verwarnung bis zur fristlosen Entlassung reichen, je nach Schwere des aufgedeckten Missverhaltens.

- E-Mails unbekannter oder fragwürdiger Herkunft sollten sofort gelöscht werden. Auf keinen Fall sollten unbekannte oder nicht erwünschte angehängte Dateien geöffnet werden.

- Im Zweifelsfall ist vor dem Öffnen eines fragwürdigen Anhangs der IT Help Desk TELEFONISCH zu kontaktieren – das Weiterleiten von fragwürdigen Anhängen an den IT Help Desk ist zu unterlassen.

- Kreditkartennummern, Passwörter, Geheimcodes etc sind ausdrücklich nicht via E-Mail zu versenden.

- Kommunikationen auf Beekeeper. Es gelten folgende Nutzungsregeln:

- Wir setzen auf die Eigenverantwortung der Mitarbeitenden. Bei Unsicherheiten hat sich der Mitarbeitende an seinen Vorgesetzten oder an die Personalabteilung zu wenden.
- Bei der Nutzung von BMSmobile gelten die bestehenden Regeln betreffend die Verwendung von Mobiltelefonen.
- Alle auf BMSmobile publizierten Inhalte sind ausschliesslich für den internen Gebrauch bestimmt und dürfen nicht an Externe weitergeleitet werden.
- Ausdrücklich untersagt sind Beiträge mit rassistischem, sexistischem oder für einzelne Mitarbeitende bzw. Mitarbeitergruppen beleidigendem Inhalt. BMS behält sich vor, Beiträge/Inhalte, die dieser Regel widersprechen, zu löschen.
- BMSmobile ist nicht vor Kunden zu nutzen.

Weitere Informationen finden sich auf Beekeeper selbst unter https://bms.beekeeper.io/fairplay

<u>Folgende Handlungen sind explizit verboten:</u>

- Ein Verstoss gegen anwendbare Gesetze oder die guten Sitten
- Das Umgehen einer Sicherheitsvorkehrung der Informationsdienstleistung
- Das Verletzen eines gewerblichen Schutz-, Urheber-, Persönlichkeits-, und Eigentumsrecht oder eines sonstigen Rechts Dritter
- Die Übermittlung eines Inhaltes mit Malware (Viren, Trojanischen Pferden, Würmer, Spyware, Adware) oder sonstiger Programmierung, die Software beschädigen kann
- Das Benutzen einer Seite oder Ausführen einer Anwendung, die zu einer Beschädigung oder zu einem Funktionsausfall der Webseiten von BMS, insbesondere durch Veränderungen an der physikalischen oder logischen Struktur der Server oder des Netzes, führen können.
- Das Verteilen oder Aufschalten von unerwünschten, unaufgeforderten oder belästigenden Massen-Emails oder anderer Nachrichten, Werbeaktionen, externen Umfragen (ob webbasiert oder nicht), Werbungen oder sonstigen Aufforderungen;
- Ein Zugriff auf und oder eine Benutzung von Anwendungen, Systemen, Diensten, Tools, Daten, Konten, Netzwerken oder Inhalten ohne schriftliche Genehmigung oder zu unbeabsichtigten Zwecken
- Das Vornehmen einer Desaktivierung, Unterbrechung, Umgehung, Störung oder sonstigen Verletzung der Sicherheit der Webseiten
- Das Vornehmen eines Angriffs, eines Missbrauchs, einer Störung, eines Unterbruchs oder einer Ausbeutung von Nutzern, Systemen oder Diensten, einschliesslich aber nicht beschränkt auf Denial of Service (DoS), Überwachung, Crawling, Spamming, Verwendung von Bots oder Scripts
- Die Mitarbeitenden verpflichten sich auch, folgende Handlungen zu unterlassen:
  - Das Anzeigen, Senden, Empfangen oder Speichern von obszönem oder unangemessenem Inhalt;
  - Das bedrohen, belästigen, verfolgen, beweislose diffamieren oder betrügen einer natürlichen oder juristischen Person;

- Das direkte oder indirekte Bewerben, Fördern, Unterstützen oder Vermarkten von kommerziellen Produkten, Dienstleistungen, Lösungen oder anderen Technologien von Drittanbietern;
- Der Versuch, über unsere Webseiten und/oder Profiles personenbezogene Daten zu sammeln, zu speichern oder zu veröffentlichen ohne Wissen und Zustimmung des Betroffenen;
- Das Senden von trügerischen oder falschen quellenidentifizierenden Informationen, einschliesslich „Spoofing“ oder „Phishing“;
- Die Beteiligung in oder Förderung von illegalen oder kriminellen Aktivitäten wie Kinderpornographie, Glücksspiel oder Piraterie
- Das Genehmigen, Ermöglichen oder Ermutigen Dritter, eine der obengenannten Handlungen zu ergreifen

Der Umgang mit Daten

Es ist BMS ein besonderes Anliegen, dass wir als Unternehmen und somit unsere Mitarbeitenden mit den Ihnen anvertrauten Informationen und Daten sorgfältig umgehen.
Nicht nur, weil uns das Datenschutzgesetz und andere Vorschriften dazu verpflichten, sondern vor allem, weil uns der Persönlichkeitsschutz unserer Mitarbeitenden und Kunden am Herzen liegt.

Dabei spielt es keine Rolle, ob die Daten auf dem Papier stehen oder im Computer gespeichert sind.

In diesem Zusammenhang sind folgende Punkte einzuhalten:

Datenbearbeitung

Mit dem Benutzerkonto erhalten Sie Zugang zu kritischen und vertrauenswürdigen Unternehmensdaten. Die Einsicht, Bearbeitung und Speicherung dieser Daten ist ausschliesslich für Geschäftszwecke unabhängig des Ortes des Zugriffs (Büro oder Fernzugriff).

Die Einsicht, Bearbeitung und Speicherung von Daten ist ausschliesslich mit Geräten der Unternehmen von BMS erlaubt. Eine Ausnahme besteht für die Synchronisation von E-Mail- und Intranet-Daten.

Die Verantwortung für eine ordnungsgemässe Bearbeitung der Geschäftsdaten liegt immer bei den Mitarbeitenden selbst.

Vertrauliches wegschliessen

Papiere und andere Datenträger mit vertraulichen Informationen sollten nicht länger als nötig herumliegen und nach Gebrauch weggeschlossen werden.

Als vertraulich gelten jede Information und jedes Dokument, welches interne Gegebenheiten beschreibt oder für die Konkurrenz wertvoll sein könnte. Personalinformationen fallen ebenfalls unter diesen Grundsatz.

Sicherheit im Sitzungszimmer

Mitarbeitende sollen weder vertrauliche Arbeitspapiere noch jegliche vertraulichen Angaben auf Flipcharts und Whiteboards in Sitzungszimmern hinterlassen. Ebenso wenig gehört Vertrauliches in den Papierkorb.

Physische Daten sicher entsorgen
Vertrauliche Dokumente sind am Besten mit Hilfe eines Aktenvernichters zu vernichten oder zumindest verkleinern bis sie unleserlich sind.

Speichern von Daten
Daten sind nicht lokal auf dem Computer, sondern auf den zentralen Systemen zu speichern. Dort kann BMS gewährleisten, dass die hohen Anforderungen bezüglich Datenschutz und Datensicherheit korrekt umgesetzt werden und demzufolge die Arbeitsprodukte der Mitarbeitenden auch nach einem Neuaufsetzen oder Austausch eines Gerätes
noch vollständig vorhanden sind. Ansonsten gehen Daten bei einem Geräte-Defekt, Geräte Diebstahl oder einer Fehlmanipulation verloren.

Remote Access Zugang (VPN-Zugang)

- Jeder Remote Access VPN muss durch einen Vorgesetzten über das Ticketing-System beim IT Help Desk beantragt werden.

- Remote Access ist ausschliesslich mit 2-Faktor Authentisierung erlaubt. Die IT Services stellt dafür eine SmartphoneApp zur Authentisierung zur Verfügung. Auf BMS Laptops/Tablets ist der «Global Protect» VPN client installiert.

- Der VPN-Nutzer benötigt: Ein BMS Benutzerkonto, eine aktuelle Windows-Version, eine aktuelle Version der Citrix Workspace und eine gute Internetverbindung oder grosse Bandbreite falls mehrere bandbreitenverbrauchende Geräte (zB TV Box, Spielkonsole, etc) gleichzeitig angeschlossen sind.

- Bei Remote Access gelten die gleichen Regelungen für die Einsicht, Bearbeitung und Speicherung von Geschäftsdaten. Der VPN-Nutzer ist dafür verantwortlich, dass sein Computer auf dem neuesten Stand ist und geschützt wird (aktuelles Anti-virus, etc)

Die Sicherheit am Arbeitsplatz

In den Unternehmen der BMS gehen täglich zahlreiche externe Personen ein und aus: Kunden, Besucher, Handwerker, Techniker, Reinigungs- und Bewachungspersonal. Die Ordnung am Arbeitsplatz ist somit ein wichtiger Sicherheitspunkt.

Die Clean-Desk-Policy befolgen
Bei BMS gilt die „Clean-Desk-Policy“. Das bedeutet, dass bei längeren Unterbrüchen – spätestens beim täglichen Arbeitsschluss – sämtliche Unterlagen aufgeräumt werden müssen. Verlassen Mitarbeitende ihren Arbeitsplatz für längere Zeit, müssen vertrauliche Informationen auf Papier, Datenträger sowie Notebook und Tablet weggeschlossen werden.

Vorsicht bei unbekannten Personen
Türen sind sorgfältig zu verschliessen. In Gebäuden ohne Empfangsbereich gilt es, fremden Personen nur die Tür aufzuhalten, wenn man sich vergewissert hat, dass diese zutrittsberechtigt ist. Mitarbeitende sollen verdächtige Personen oder Vorkommnisse Ihren Vorgesetzten oder dem Gebäudeverantwortlichen melden.

Der Computer auf der Verkaufsfläche

In den BMS Filialen stehen Computer und Kassensysteme zum Teil auf den Verkaufsflächen, was

BMS verletzbar macht, weil jeder Kunde oder Besucher potentiellen Zugang zu den Geräten hat. Es gilt diesen potentiellen Zugang zu verunmöglichen:

- Durch das Aktivieren der Anmeldesperre (Ctrl-Alt-Delete) beim Verlassen des Arbeitsortes, auch wenn nur für eine kurze Zeitspanne
- Umsicht bei der Eingabe des Passwortes (keine anderen Personen in der Nähe mit ungehinderter Sicht auf den Bildschirm)
- Das Bedienen der BMS Geräte und Dienste findet nur durch Personen statt, die dem Personalreglement und dieser Weisung zugestimmt haben
- Kein unbeaufsichtigtes Arbeiten am PC von Besuchern und/oder Kunden – auch nicht für kurze Internetabfragen

Persönliches Benutzerkonto

Jeder Mitarbeitende hat sein eigenes Benutzerkonto
Es werden keine anderen Personen am eigenen Benutzerkonto zugelassen. Mitarbeitende sollen immer nur den eigenen Benutzerkonto verwenden. Ausnahmen gelten für generische Benutzerkonto, zum Beispiel in unseren Shops an der Verkaufstheke; dort dürfen bis zu drei Benutzer dasselbe generische Benutzerkonto verwenden.

Besteht die Vermutung, dass ein Benutzerkonto und das zugehörige Passwort von Dritten missbraucht wird oder wurde, so ist dies sofort der IT Abteilung über das IT Help Desk zu melden.

Computer sperren
Auch für kürzere Absenzen ist der Computer zu sperren (Ctrl + Alt + Del). Beim Verlassen des Arbeitsplatzes (Sitzungen, Mittagspausen, etc) haben sich die Mitarbeitenden abzumelden.

Der richtige Umgang mit dem Passwort

- Das zum Benutzerkonto gehörende Passwort soll nur der jeweilige Mitarbeitende kennen. Ein Password soll niemanden (auch nicht einem Vorgesetzten, einem IT-Supporter, dem IT Help Desk, einem HR-Mitarbeitenden, etc) weitergegeben werden.
- Das Passwort ist in regelmässigen Abständen zu wechseln aber spätestens nach einer Erinnerung durch das System. Es sollte jedes Mal eine völlig neue Kombination gewählt werden. Das Passwort sollte sich nicht auf den Mitarbeitenden selbst, dessen Abteilung oder Funktion beziehen.
- Das Passwort sollte unbeobachtet eingegeben werden. Ist dies nicht möglich, so ist es möglichst bald wieder zu ändern.
- Das Passwort sollte nie im BMS Gerät gespeichert werden.
- Das Passwort sollte nie auf einen Zettel niedergeschrieben werden, welches von Dritten eingesehen werden könnte

Die Wahl eines wirksamen Passwortes

Idealerweise ist ein Passwort zu wählen, welches einfach zu behalten, aber schwierig zu erraten ist. Dabei gilt es, Folgendes zu berücksichtigen:

So lieber nicht…

- Das Passwort soll keinen Bezug auf die eigene Person haben. Passwörter mit Familiennamen, Vornamen, Geburtsdaten der Kinder, Namen der Haustiere, Arbeit, Hobby sind einfach zu erraten!
- Es sollte auf Namen von Persönlichkeiten, Tieren, Comicfiguren, Automarken, Ortschaften, Regionen etc. verzichtet werden.
- Es sollten keine Begriffe, die in Wörterbüchern – egal welcher Sprache - aufgeführt sind, verwendet werden.
- Buchstabenreihen („ABCD“) oder aufeinander folgende Tastaturkombinationen („asdfg“) sind zu vermeiden.
- Passwörter sollen nicht nummeriert werden (Passwort 1, Passwort 2, Passwort 3).

…aber so!

- Muss mindestens 8 Ziffern lang sein.
- Muss mindestens Gross- und Kleinbuchstaben enthalten.
- Muss mindestens ein Sonderzeichen wie „!“, „#“ enthalten.
- Wir empfehlen folgende Buchstaben (welche nur in einigen Sprachen vorkommen) nicht zu verwenden: é à è ü ö ä ç
- Muss mindestens eine Zahl enthalten.
- Darf kein sprechendes Wort wie den eigenen Namen enthalten.
- Die letzten 5 Passwörter dürfen nicht verwendet werden.
- Eselsbrücken bei der Passwortwahl nutzen - ein Beispiel dafür:
  - Ausgangswort: privatpost
  - Gross-/Kleinschreibung: PrivaTPost
  - Einbringen von Zahlen: Pr1vaTP05t
  - Einbringen von Sonderzeichen: Pr1v@TP05t?

Betrügerische Datenerschleichung/ Social Engineering

Wirtschaftsspione, Hacker und andere Personen geben sich oft als jemand anderes aus, um sich durch geschickte Fragen nach internen Telefonnummern, Namen von Mitarbeitenden, Passwörtern oder ähnlichen Informationen Zugang zu den internen Systemen zu verschaffen. Dieses Vorgehen – Social Hacking genannt– umgeht alle technischen Sicherheitsvorkehrungen und zielt auf das schwächste Glied in der Sicherheitskette: den Menschen.

Misstrauisch sein

Der Mitarbeitende hat die Identität bei unbekannten Fragestellern zu prüfen und diese um eine schriftliche Anfrage zu bitten, wenn Auskunft über eine Person oder das Unternehmen gegeben werden sollen. Scheint sich jemand als IT-Mitarbeiter der BMS auszugeben, so ist der Höher aufzulegen und das IT Helpdesk umgehend über die auf BMSmobile angegebene Telefonnummer zu kontaktieren.

Verdächtige Vorfälle melden
Verdächtige Vorfälle sind sofort dem Vorgesetzten und dem IT Help Desk zu melden.

Notebooks und andere mobile Geräte

Dieben keine Chance geben
Notebook, Tablet oder Smartphone sind nie unbeaufsichtigt liegen zu lassen. Besondere Vorsicht gilt auf Bahnhöfen, im Zug selber oder an anderen öffentlichen Plätzen. Notebooks sind immer als Handgepäck mitzunehmen. Ein allfälliger Diebstahl muss unverzüglich bei der Polizei, beim Vorgesetzten, dem IT Help Desk und bei Legal zu melden.

Nur für geschäftlichen Gebrauch
Mobile Geräte sind ein Arbeitsinstrument für den geschäftlichen Gebrauch. Es dürfen keine anderen Personen damit arbeiten – auch keine Freunde und Familienmitglieder.

Zuhause und unterwegs
Diese Weisung gilt ebenfalls für den Gebrauch der mobilen Arbeitsgeräte, unabhängig von Ort und Zeit, Zuhause und unterwegs.

Inkraftsetzung

Diese Weisung tritt am 7. Juni 2021 in Kraft und ersetzt alle vorherigen Fassungen der ICT-Weisung und die sonstigen vorherigen ICT-relevanten Dokumente.