Regelwerkversion	**2-0**	Vertraulichkeitsklassifikation	**intern**
gültig ab	**01.11.2020**	Eigner	**IT-SR**
		Betroffene Prozesse	-
		verfügbare Sprachen	**DE, FR, IT**

Betroffene Divisionen	**Infrastruktur, Personenverkehr, Immobilien, Konzern**
Spezifische Empfänger / Verteiler	**LIDI-R: A2, A20**
Ersatz für	**Regelwerkversion 1-0**
Zuordnung	**K 018.4**

Umgang mit IT-Arbeitsmitteln und Geschäftsdaten

Inhalt

1. Allgemeines 2
1.1. Ausgangslage, Ziele 2
1.2. Geltungsbereich (Unternehmen, Anwender / Funktion) 2

2. Meine Arbeitsmittel 2
2.1. Umgang mit IT-Arbeitsmitteln 2
2.2. Passwörter 2
2.3. Nutzungsbestimmungen für spezifische IT-Arbeitsmittel 2

3. Umgang mit Informationen 3
3.1. Klassifikation 3
3.2. Vertraulichkeit und Geheimhaltung 4
3.3. Datenablage 4
3.4. Versand von Unterlagen 5
3.5. Mobile Datenträger 5

4. Sicherheitsrelevante Vorkommnisse 5

5. Software und Apps 5

6. Private Nutzung, Persönlichkeitsrechte und Überwachung 6
6.1. Private Nutzung 6
6.2. Persönlichkeitsrechte und Überwachung 6

Änderungsverzeichnis

Version	Kapitel	Änderung
2-0	3.1	Anpassungen für Azure Information Protection
1-0		Erstausgabe, Ersatz für K 400.5, K 400.8, K 400.9, K 400.33, K 400.43, K 400.44

1. Allgemeines

1.1. Ausgangslage, Ziele

Ein sorgfältiger Umgang mit IT-Arbeitsmitteln und Geschäftsdaten ist ein zentrales Element für den Schutz von Personendaten und vertraulichen Informationen sowie für den Schutz der Informatiksysteme und damit des gesamten Betriebs.

1.2. Geltungsbereich (Unternehmen, Anwender / Funktion)

Diese Vorgaben gelten für sämtliche Personen, welche IT-Arbeitsmittel und Geschäftsdaten der SBB AG oder der SBB Cargo AG nutzen.

2. Meine Arbeitsmittel

Für SBB Mitarbeitende werden IT-Arbeitsmittel für die Erfüllung der Arbeitsaufgaben grundsätzlich zur Verfügung gestellt. Mitarbeitende oder Mitarbeitende von Lieferanten und Partnern können aber auch eigene IT-Arbeitsmittel verwenden. Diese Arbeitsmittel werden als «Bring your own Device» oder kurz «BYOD» bezeichnet.

2.1. Umgang mit IT-Arbeitsmitteln

Du gehst mit den von der SBB zur Verfügung gestellten IT-Arbeitsmitteln sorgfältig um und schützt sie vor Schaden und Verlust.

Du lässt deine IT-Arbeitsmittel im Betriebszustand nicht unbeaufsichtigt. Beim Verlassen des Arbeitsplatzes sperrst du deine IT-Arbeitsmittel. Du verleihst deine IT-Arbeitsmittel mit Geschäftsdaten der SBB nicht an Dritte.

PC und Notebook kannst du jederzeit sperren durch drücken der **Windows + L-Taste** oder (**Control+Alt+Delete, Enter**). Auch Tablet und Smartphone kannst du mit der Ausschalttaste sperren.

2.2. Passwörter

Du hältst deine persönlichen Passwörter geheim und gibst sie nicht an andere Personen weiter. Dein Passwort gibst du unbeobachtet vor den Augen Dritter ein. Geschäftliche Passwörter dürfen nicht für private Dienste verwendet werden.

Die grösste Sicherheit bietet ein langes Passwort. Überlege dir also eine zufällige Aneinanderreihung von Wörtern. Diese Wortkombination kannst du dir gut merken und sie bereitet Hackern am meisten Schwierigkeiten.

2.3. Nutzungsbestimmungen für spezifische IT-Arbeitsmittel

Für bestimmte IT-Arbeitsmittel und IT-Dienste gibt es zusätzliche Nutzungsbestimmungen. Die entsprechenden Vorgaben erhältst du mit dem Gerät oder beim Aufschalten des jeweiligen Dienstes. Zudem sind die IT-Arbeitsmittel durch technische Massnahmen geschützt. Diese sogenannten „Gerätepolicies“ stellen einen Mindestschutz sicher (z.B. verlangt ein Smartphone zwingend einen Code und wird nach einer bestimmten Zeit gesperrt).

Technische Schutzmassnahmen darfst du nicht entfernen oder umgehen.

Beim Zugriff auf Geschäftsdaten mit privaten Geräten („BYOD“), welche nicht durch die SBB verwaltet werden, stellst du folgenden Mindestschutz sicher:

-Gerätepasswort mit mindestens 4 Ziffern

-Auto-Lock nach 5 Minuten

-Geräteverschlüsselung

-iOS: Löschung aller Daten (komplette Rückstellung auf Werkseinstellungen) nach zehnmaliger Falscheingabe des Gerätepassworts.

-Android: Löschung aller Daten im SBB Arbeitsbereich nach zehnmaliger Falscheingabe des Gerätepassworts.

Hier findest du alle Informationen zum Umgang mit mobilen Geräten; insbesondere bei Eintritt, Übertritt und internem Wechsel, Austritt, Geräte-Austausch und beim Einsatz eines privaten Geräts («BYOD»).

Weitere Nutzungsbedingungen beim Einsatz von privaten Geräten (« BYOD») für den Zugriff auf Office 365 findest du hier.

Die «Mobile Device Services» («MDS») berechtigen SBB Mitarbeitende, mit von SBB Informatik freigegebenen mobilen Geräten E-Mails, Kalendereinträge, Kontakte, Notizen und Aufgaben zu synchronisieren sowie mit den entsprechenden Apps («ICT-Selfcare», «Mitarbeitendenportal» etc.) auf das SBB Unternehmensnetzwerk zuzugreifen.

Du findest die Nutzungsbedingungen für den MDS-Dienst hier.

3. Umgang mit Informationen

3.1. Klassifikation

Geschäftsdaten umfassen Daten und Informationen, welche in Zusammenhang mit der SBB stehen. Dazu gehören Daten der SBB und von Kunden, Mitarbeitenden, Lieferanten und Geschäftspartnern.

Die Daten können beispielsweise vorliege in Form von Office-Dokumenten, E-Mails, Papierunterlagen, Personal-Dossiers und Rechnungen.

Du klassifizierst die von dir erstellten, bearbeiteten und abgelegten vertraulichen Geschäftsdaten zwingend als „C3 - Vertraulich“. Bei öffentlichen und internen Geschäftsdaten wird eine Klassifizierung empfohlen, ist aber nicht zwingend notwendig. Dennoch hilft sie, Missverständnisse zu vermeiden und leistet einen wichtigen Beitrag zur Einhaltung der Informationssicherheit.

Die Klassifikation sagt aus, wie wertvoll Daten sind und wer sie sehen darf.

Bei der SBB gibt es die folgenden Klassifikationsstufen hinsichtlich deren Vertraulichkeit:

1. Öffentlich sind Daten, die für die Öffentlichkeit erstellt wurden. Dazu gehören beispielsweise der Fahrplan, Verkaufsprospekte oder Medienmitteilungen. Es ist keine Beschriftung bezüglich Vertraulichkeit notwendig.
2. Intern sind Daten, welche für den internen Gebrauch und ausgewählte weitere Adressaten bestimmt sind. Dazu gehören interne Weisungen, das Telefonverzeichnis oder die Dienstadresse. Solche Informationen sind mit dem Vermerk „intern“ zu versehen.
3. Vertrauliche Daten sind besonders schützenswerte Daten. Dazu gehören beispielsweise Finanzreportings, Dokumentationen kritischer Technologien, Protokolle von VR, KL und GL-Sitzungen und besonders schützenswerte Personendaten. Auf Dokumente gehört immer der Vermerk „vertraulich“.

Weiterführende Links:

Detaillierte Ausführungen zur Klassifikation sind der Weisung zur Klassifikation zu entnehmen.

3.2. Vertraulichkeit und Geheimhaltung

Du behandelst Geschäftsdaten der SBB mit der notwendigen Sorgfalt. Auch interne Daten gehören nicht an die Öffentlichkeit. Innerhalb der SBB tauschen wir als «intern» klassifizierte Daten jedoch offen aus und nutzen nicht vertrauliche Daten zur übergreifenden Zusammenarbeit zum Wohle der SBB.

Der sorgfältige Umgang mit Geschäftsdaten ist ein wichtiges Element des Verhaltenscodex der SBB.

Vertrauliche geschäftliche Gespräche, Papierdokumente und mobile Datenträger sowie Inhalte auf deinem Bildschirm schützt du und bewahrst diese vor unberechtigtem Zugriff.

Einen Sichtschutzfilter für dein Notebook bekommst du im ICT-Serviceportal. Wähle Bestellportal und gib den Suchbegriff «Sichtschutz» ein. Du erhältst eine Auswahl von Sichtschutzfiltern für verschiedene Notebooktypen.

Nutze für vertrauliche Gespräche, wenn möglich, einen abschliessbaren Fokusraum. Ein Zugabteil und ein Restaurant sind keine Orte für vertrauliche Telefongespräche.

Lasse Papierdokumente und mobile Datenträger nicht offen herumliegen und trage insbesondere ausserhalb der Arbeitsräume sorge zu ihnen.

3.3. Datenablage

Geschäftsdaten legst du auf den von der SBB zur Verfügung gestellten Services ab (Sharepoint, OneDrive for Business, DMS, Filer etc.). Private Cloud-Services (private Dropbox oder iCloud) sind nicht zulässig für die Ablage von Geschäftsdaten. Daten mit der Klassifikationsstufe «vertraulich» dürfen nur auf gemanagten Geräten der SBB lokal gespeichert werden.

Du findest Informationen zur Datenablage in Sharepoint, OneDrive for Business und DMS auf der Seite des ICT-Workplace.

3.4. Versand von Unterlagen

Für den geschäftlichen E-Mail-Verkehr verwendest du die offiziellen SBB E-Mail-Systeme (Exchange/Outlook). Du leitest geschäftliche E-Mails nicht an private E-Mail-Adressen weiter.

Vertrauliche Informationen überträgst du grundsätzlich verschlüsselt. Sie dürfen ohne Zustimmung des Autors nicht an Externe weitergeleitet werden.

Weiterführende Vorgaben zum Umgang mit der elektronischen Kommunikation und zum Umgang mit sozialen Medien finden du hier: Verhaltensgrundsätze Elektronische Kommunikation und Social Media Guide

3.5. Mobile Datenträger

Mobile Datenträger sind nur für öffentliche Daten einzusetzen (z.B. grosses Firmen-Video, welches die Speicherkapazität überschreitet). Geschäftsdaten mit der Klassifikation «intern» oder «vertraulich» gehören auf die dafür vorgesehenen Geschäftsablagen (z.B. SharePoint oder das geschäftliche OneDrive). Zum Datenaustausch ist die Freigabefunktion zu verwenden.

Du kannst Geschäftsdaten nicht nur SBB intern, sondern auch mit Dritten mittels Sharepoint teilen. Wie das klappt, erfährst du in dieser Anleitung auf der Seite des ICT-Workplace.

4. Sicherheitsrelevante Vorkommnisse

Verlust oder Diebstahl von Geräten mit Geschäftsdaten, relevante Vorfälle im Bereich Informationssicherheit und allfällige Verstösse im Bereich Datenschutz meldest du umgehend dem ICT Service Desk (Telefon **+41 51 220 30 40**).

5. Software und Apps

Du verwendest zu Geschäftszwecken grundsätzlich Software, welche von der SBB beschafft und lizenziert wurde.

Wenn du nicht von der SBB bereitgestellte Software zu Geschäftszwecken verwendest (sowohl auf SBB Geräten wie auch auf BYOD-Geräten), so bist du dafür verantwortlich, dass die Software auch für geschäftliche Zwecke genutzt werden kann und korrekt lizenziert ist.

Zusätzliche Softwareprodukte können über das ICT-Serviceportal bestellt werden.

6. Private Nutzung, Persönlichkeitsrechte und Überwachung

6.1. Private Nutzung

ICT-Mittel, welche von der SBB zur Verfügung gestellt werden, sind primär für die geschäftliche Nutzung vorgesehen. Die Mitarbeitenden dürfen diese in angemessenem Rahmen und Umfang auch für private Zwecke nutzen.

Du öffnest keine Webseiten mit rechtswidrigen oder anstössigen Inhalten (sexistisch, rassistisch, extremistisch, pornographisch, unethisch, diffamierend). Hast du eine solche Seite irrtümlich geöffnet, schliesst du diese unverzüglich wieder.

Der Zugriff kann durch Arbeitsanweisungen im Rahmen der Verhältnismässigkeit eingeschränkt oder verboten werden, wenn die Person zum Beispiel mit Überwachungsfunktionen betraut ist.

Deine unmittelbar vorgesetzte Person kann die Nutzung des Internets im Rahmen der Verhältnismässigkeit einschränken oder verbieten, wenn ein begründeter Verdacht oder Gewissheit besteht, dass die private Nutzung das zulässige Mass überschreitet oder rechtswidrige respektive anstössige Seiten besucht werden.

Käufe und Bezüge von Dienstleistungen mit Mobile-Abonnementen z.B. per Mobilerechnung, kostenpflichtige SMS oder SMS-Pay für private Zwecke sind nicht erlaubt.

Detaillierte Informationen zur Bezahlung mit Smartphone (über ein Mobilabonnement der SBB) findest du im Beitrag: mit SBB Smartphone bezahlen.

6.2. Persönlichkeitsrechte und Überwachung

Zur Sicherstellung des Betriebs ist es teilweise notwendig, dass SBB IT-Arbeitsmittel überwacht werden.

Bei entsprechenden Überwachungs- und Auswertungsmassnahmen wird sichergestellt, dass alle gesetzlichen und internen Vorgaben, sowie die Vereinbarungen mit den Sozialpartnern eingehalten werden. Zudem wird sichergestellt, dass die Massnahmen einen möglichst geringen Eingriff in die Persönlichkeitsrechte darstellen.

Bei Überwachungsmassnahmen berücksichtigt die SBB das Verhältnismässigkeitsprinzip und verwendet nur diejenigen Auswertungs- und Überwachungsmassnahmen, welche für den angestrebten Zweck den geringsten Eingriff in die Persönlichkeitsrechte darstellen.

Weiterführende Informationen findest du in der Weisung K 155.1.

IT-SR-L
sig. Marcus Griesser
CISO

IT-SR
sig. Daniel Wild
Security and Risk Manager