

| | | | |
|---|--|--|---|
| Regelwerkversion gültig ab | 3-0 01.08.2018 | Vertraulichkeitsklassifikation Eigner Betroffene Prozesse verfügbare Sprachen | intern IT-SR Steuerung Informatik DE, FR, IT |
| Betroffene Divisionen Spezifische Empfänger / Verteiler Ersatz für Zuordnung | Infrastruktur, Personenverkehr, Cargo, Immobilien, Konzern LIDI-R A2 Regelwerkversion Version 2-0 K 030.1 | | |

Konzernweisung betreffend die zulässige Nutzung des Internets sowie von E - Mail - Diensten und E - Mail - Programmen

| | |
|---|----------|
| Änderungsverzeichnis | 1 |
| 1. Allgemeines..... | 2 |
| 1.1. Ausgangslage, Ziele | 2 |
| 1.2. Geltungsbereich..... | 2 |
| 1.3. Übergeordnete und zugehörige Dokumente | 2 |
| 1.4. Begriffe und Abkürzungen | 2 |
| 2. Administrative Sicherungsmassnahmen..... | 2 |
| 3. Nutzung des Internets für private und geschäftliche Zwecke | 3 |
| 3.1. Zugriff auf Internet – Sites für geschäftliche Zwecke | 3 |
| 3.2. Zugriff auf Internet – Sites für private Zwecke | 3 |
| 3.3. Kontrolle der zulässigen Nutzung des Internets..... | 4 |
| 3.4. Technische Verunmöglichung eines Zugriffs auf bestimmte Internet-Inhalte | 4 |
| 3.5. Download von Software ab dem Internet und lokale Installation derselben | 5 |
| 3.6. Aufbrechen von verschlüsselten https-Verbindungen (SSL-Interception) | 5 |
| 4. Nutzung von E - Mail - Diensten und E - Mail - Programmen | 5 |
| 5. Sanktionen | 6 |
| 6. Verhältnis Richtlinie und Weisungen..... | 6 |

Änderungsverzeichnis

| Version | Kapitel | Änderung |
|---------|---------|--|
| 3-0 | 3.6 | Thema SSL-Interception neu eingefügt. |
| 2-0 | alle | Übernahme der Weisung in die aktuelle Vorlage des Regelwerks. Wechsel von K-IT zu IT. |

1. Allgemeines

1.1. Ausgangslage, Ziele

Diese Weisung regelt die zulässige Art der Nutzung des Internets, von E-Mail-Diensten und E-Mail-Programmen (wie insbes. Outlook/Exchange, Gratis-Internet-E-Mail-Dienste, Messenger-Dienste oder Outlook) durch natürliche Personen, welche mittels eines lokalen oder eines Fern-Zugriffs auf das Datenkommunikations-Netz der SBB das Internet, E-Mail-Dienste und/oder E-Mail-Programme nutzen können.

1.2. Geltungsbereich

Die Weisung ist verbindlich für die Arbeitnehmer und Arbeitnehmerinnen der SBB sowie der SBB Cargo. Sie ist jedoch auch verbindlich für Mitarbeiter weiterer juristischer Personen, sofern diese weiteren juristischen Personen ihren Mitarbeitern die im vorhergehenden Absatz erwähnten technischen Möglichkeiten zur Verfügung stellen sowie für beauftragte externe Mitarbeiter der SBB, der SBB Cargo sowie weiterer juristischer Personen, welche ebenfalls über die im vorhergehenden Absatz erwähnten technischen Möglichkeiten verfügen.

Sämtliche natürlichen Personen, welche den Bestimmungen dieser Weisung unterstehen, werden nachfolgend als „Benutzer“ bezeichnet, wobei der leichten Lesbarkeit wegen generell die männliche Form benützt wird aber die Vertreterinnen des weiblichen Geschlechts ebenfalls gemeint sind.

1.3. Übergeordnete und zugehörige Dokumente

K 030.1 „Securityhandbuch SBB“

1.4. Begriffe und Abkürzungen

2. Administrative Sicherungsmassnahmen

- 2.1 Der unmittelbare Vorgesetzte stellt gegenüber den ihm unterstellten Benutzern sicher, dass diese über die Existenz sowie die zentralen Bestimmungen dieser Weisung (inkl. der dazugehörenden Richtlinie betreffend der zulässigen Nutzung des Internets, der E-Mail-Dienste und –programme sowie dem Umgang mit Informatik Hard- und Software (R Z 400.5 - nachfolgend als „Richtlinie“ bezeichnet) informiert werden. Er weist darauf hin, dass die Weisung samt der dazugehörenden Richtlinie jederzeit im Intranet der SBB im SBB Regelwerk eingesehen und heruntergeladen werden kann.
- 2.2 Die weiteren juristischen Personen im Sinne der Ziff. 1, Abs. 2 dieser Weisung (z.B. Securitrans etc.) werden von der SBB AG durch geeignete Massnahmen verpflichtet diese Weisung ebenfalls auf deren Mitarbeiter sinngemäss anzuwenden.

3. Nutzung des Internets für private und geschäftliche Zwecke

3.1. Zugriff auf Internet – Sites für geschäftliche Zwecke

3.1.1 Die Nutzung des Internets für geschäftliche Zwecke durch die Benutzer ist – unter Vorbehalt der Ziffer 3.1.2 - zulässig.

3.1.2 Unzulässig ist jedoch:

Das Öffnen von Internet – Sites, von welchem der Benutzer weiss oder zumindest wissen müsste, dass sie rechtswidrige oder zumindest anstössige Inhalte (Sites mit insbes. sexistischen, rassistischen, extremistischen, pornographischen, unethischen oder diffamierenden Inhalten) aufweisen. Diese Inhalte dürfen weder gespeichert, noch (auf irgendeine Weise) an Dritte weitergegeben werden. Ist eine solche Site irrtümlich geöffnet worden, so ist sie unverzüglich (ohne deren Inhalte zu speichern oder weiter zu geben) wieder zu schliessen.

3.1.3 Die Richtlinie zu dieser Weisung kann die Verwendung des Internets für Finanztransaktionen sowie für Bestellungen/Auftragerteilungen mittels Kreditkarten regeln. Die Richtlinie kann auch Bestimmungen betreffend der Bekanntgabe sensibler Daten mittels des Internets enthalten.

3.2. Zugriff auf Internet – Sites für private Zwecke

3.2.1 Der Zugriff auf Internet - Sites für private Zwecke durch die Benutzer ist zulässig, sofern sich der Zugriff auf einen zeitlich geringfügigen Rahmen beschränkt. Vorbehalten bleiben jedoch die Bestimmungen der Ziffer 3.1.2. dieser Weisung, welche auch im Falle einer privaten Nutzung des Internets einzuhalten sind.

Beeinträchtigen Zugriffe auf gestattete Internet Sites die Verfügbarkeit des SBB-Netzes kann der CISO die Sperrung des entsprechenden Internetlinks anordnen.

3.2.2 Besitzt der unmittelbare Vorgesetzte des Benutzers jedoch einen begründeten Verdacht oder gar die Gewissheit, dass der Zugriff auf zulässige Internet – Sites das zulässige Mass übersteigt oder dass die ihm unterstellte Person Sites öffnet oder öffnen wird, welche nicht geöffnet werden dürfen (vergl. Ziffer 3.1.2), so ist er berechtigt, die private Nutzung des Internets des Benutzers einzuschränken oder gar zu verbieten. Diese Massnahme muss jedoch stets verhältnismässig sein. Sanktionen gemäss der Ziffer 5 dieser Weisung bleiben vorbehalten.

Der Zugriff auf das Internet kann im Rahmen von abteilungsinternen Arbeitsanweisungen verboten und unterbunden werden, wenn dies verhältnismässig ist.

Verhältnismässigkeit ist beispielsweise dort gegeben, wo für geschäftliche Zwecke kein Internetzugriff notwendig ist und/oder die Personen mit Überwachungsfunktionen betraut sind.

3.3. Kontrolle der zulässigen Nutzung des Internets

- 3.3.1. Die Organisationseinheit IT-Security & Risk Management der SBB (nachfolgend als „IT-SR“ abgekürzt) nimmt stichprobenartige, anonyme Kontrollen der Internet-Protokollierungen gemäss einem bestimmten Zeitplan für eine beschränkte Benutzungsdauer vor um zu überprüfen, ob gegen die Ziffer 3.1.2 dieser Konzernweisung verstossen wird.

Wird ein Missbrauch festgestellt, kann eine personenbezogene Auswertung der Protokollierungen vorgenommen werden. Das Resultat der personenbezogenen Auswertung ist von IT Sec & Risk dem unmittelbaren Vorgesetzten der fehlbaren Person sowie der Human-Ressources-Leitung der Division/des Zentralbereichs, für welche die fehlbare Person tätig ist, zu melden. Der unmittelbare Vorgesetzte trifft die erforderlichen Führungsmassnahmen. Die zugeteilten Personalverantwortlichen stehen den Vorgesetzten beratend und unterstützend zur Verfügung.

- 3.3.2 IT-SR hat sich – im Rahmen ihrer Kontrolle - an die jeweils aktuellen Bestimmungen des „Leitfadens über Internet und E-Mail Überwachung am Arbeitsplatz“ des Eidg. Datenschutzbeauftragten zu halten.

Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden. Sind Überwachungs- oder Kontrollsysteme aus andern Gründen erforderlich, sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden. (Art. 26 Vo.3 zum ArbG.)

- 3.3.3. Ist fraglich, ob eine Kontrolle rechtlich zulässig ist oder nicht, lässt sich IT-Sec & Risk vorgängig SBB – intern rechtlich beraten.

3.4. Technische Verunmöglichung eines Zugriffs auf bestimmte Internet-Inhalte

IT-Sec & Risk ist berechtigt und verpflichtet - zwecks Verhinderung technisch bedingter Schäden (z.B. Einschleusen von Viren) - rechtlich zulässige, technische Schutzmassnahmen einzusetzen. Diese technischen Schutzmassnahmen werden regelmässig dem neuesten Stand der Technik angepasst. IT-Sec & Risk ist jederzeit berechtigt, den Zugriff auf Internet-Sites,

welche den Bestimmungen der Ziffer 3.1.2 widersprechen oder den Interessen oder dem guten Ruf des Konzerns SBB schaden könnten, technisch zu verunmöglichen.

3.5. Download von Software ab dem Internet und lokale Installation derselben

Das Herunterladen und das anschliessende lokale Installieren von Software ab dem Internet ist nicht zulässig. Vorbehalten bleiben die Fälle, bei welchen der CISO der SBB dies ausnahmsweise aus zwingenden geschäftlichen Gründen zugelassen hat.

Weitere Ausführungsbestimmungen zu diesem Regelungsgegenstand sowie zum Herunterladen von Software-Codes können sich aus der Richtlinie zu dieser Weisung ergeben.

3.6. Aufbrechen von verschlüsselten https-Verbindungen (SSL-Interception)

Um Viren und Malware im verschlüsselten Datenverkehr zu erkennen und zu stoppen, werden verschlüsselte Verbindungen (https) durch einen Forward Proxy aufgebrochen und auf Schadstoffsoftware abgesucht. Anschliessend wird der Datenverkehr wieder verschlüsselt und dem Empfänger zugestellt. Der entschlüsselte Internetverkehr wird weder gespeichert noch personenbezogen ausgewertet. Geblockt werden ausserdem unerwünschte Internetseiten, Applikationen und Inhalte (Gewalt, Rassismus, Pornographie, Streaming-Dienste).

Nicht aufgebrochen wird die Verschlüsselung der Kommunikation mit dem Bund, mit Banken und anderen Providern, bei denen von einem erhöhten Sicherheitsstandard ausgegangen wird (Banken, Spitäler und Krankenkassen).

Diese Regeln gelten auch für mobile Anwender, welche von unterwegs oder zuhause aufs Internet zugreifen.

4. Nutzung von E - Mail - Diensten und E - Mail - Programmen

- 4.1. Der Versand von E-Mails (mit oder ohne Attachments) mit rechtswidrigen oder anstössigen Inhalten ist – ungeachtet der Verwendung des E-Mail-Dienstes oder des E-Mail-Programms (z.B. Internet-E-Mail-Dienste oder Outlook) und ob es sich um ein geschäftliches oder ein privates E-Mail handelt – verboten.
- 4.2. Die Nutzung von Voice- und Messenger – Diensten, die nicht von der SBB zur Verfügung gestellt werden (z.B. MSN – Messenger, Skype) sowie der Versand von elektronischen Massenwerbesendungen für private Zwecke ist verboten.
- 4.3. Im Falle des Erhalts von E-Mails aus elektronischen Massenwerbesendungen kann - zwecks zukünftiger Verunmöglichung des Erhalts von

Massenwerbesendungen - dies dem Informatik-Supportdienst (166) gemeldet werden.

- 4.4. Ergänzende Bestimmungen betreffend der Nutzung von E-Mail-Diensten und – Programmen können sich aus der Richtlinie zu dieser Weisung ergeben.

5. Sanktionen

- 5.1. Die Sanktionen im Falle der Verletzung der Bestimmungen dieser Weisung – jedoch insbesondere im Falle der Verletzung der Ziffern 3.1.2 oder 4.1 dieser Weisung - durch Arbeitnehmer der SBB, der SBB Cargo oder Arbeitnehmer einer weiteren juristischen Person (vergl. Ziff. 1, Abs. 2) ergeben sich aus dem arbeitsvertragsrechtlichen Rechtsverhältnis zu ihrem Arbeitgeber. (Eine krasse Verletzung der Ziff. 3.1.2 oder 4.1 kann bis zur fristlosen Entlassung führen.)
- 5.2. Sanktionen dürfen erst verhängt werden, wenn Gewissheit über die Identität des fehlbaren Arbeitnehmers besteht. Die Sanktionen müssen stets verhältnismässig sein. Liegt ein strafbares Verhalten vor, so entscheidet der hierzu zuständige Rechtsdienst – zusammen mit dem Leiter der Organisationseinheit der fehlbaren Person - ob eine Strafanzeige eingereicht wird.
- 5.3. Hat ein Mitarbeiter einer weiteren juristischen Person (im Sinne von Ziff. 1, Abs. 2 dieser Weisung) oder ein beauftragter externer Mitarbeiter der SBB, der SBB Cargo oder einer weiteren juristischen Person gegen die Bestimmungen dieser Weisung (inkl. der dazugehörenden Richtlinie) verstossen, so ergreift dessen Arbeit- bzw. Auftraggeber die ihm geeignet erscheinenden, verhältnismässigen Sanktionen gegenüber der fehlbaren Person.
- 5.4. Ist die fehlbare Person mit dem Unternehmen wirtschaftlich deckungsgleich, welche einen (beispielsweise: Informatik-Dienstleistungs-) Vertrag mit der SBB, der SBB Cargo oder einer weiteren juristischen Person im Sinne von Ziff. 1, Abs. 2 dieser Weisung abgeschlossen hat (Bsp.: Einzelfirma oder einer 1-Mann-AG) oder weigert sich das Unternehmen, verhältnismässige Sanktionen gemäss der Ziffer 5.3 gegenüber ihrem fehlbaren Angestellten oder Beauftragten zu erlassen, so überprüft die SBB, die SBB Cargo bzw. die weitere juristische Person im Sinne von Ziff. 1, Abs. 2 dieser Weisung ihre zukünftige Vergabepolitik hinsichtlich dieses Unternehmens und zieht daraus die erforderlichen, rechtlich zulässigen Konsequenzen.

6. Verhältnis Richtlinie und Weisungen

IT-Sec & Risk ist berechtigt, im Rahmen der ihr mittels dieser Weisung delegierten Kompetenz (vergl. Ziffern 3.1.3, 3.5 usw. dieser Weisung) Ausführungsbestimmungen betreffend der zulässigen Nutzung des Internets sowie

von E-Mail-Diensten und E-Mail-Programmen in der „Richtlinie betreffend der zulässigen Nutzung des Internets, der E-Mail-Dienste und –programme sowie dem Umgang mit der Informatik Hard- und Soft-ware“ zu erlassen.

Die Bestimmungen dieser Richtlinie dürfen jedoch nicht den Bestimmungen dieser Weisung widersprechen. Von IT-Sec & Risk erstellte Änderungen an der Richtlinie, welche sich aus einer Delegationsnorm dieser Weisung ergeben, werden vorgängig einer Rechtskontrolle unterzogen.

IT

Sig. Peter Kummer

CIO

IT-SR

Sig. Marcus Griesser

CISO