Regelwerkversion	**2-0**	Vertraulichkeitsklassifikation	**intern**
gültig ab	**01.01.2013**	Eigner	**IT-SR**
letzte Review		Betroffene Prozesse	**Steuerung Informatik**
nächste Review		verfügbare Sprachen	**DE, FR, IT**

Betroffene Divisionen	**Infrastruktur, Personenverkehr, Cargo, Immobilien, Konzern**
Spezifische Empfänger / Verteiler	**-**
Ersatz für	**Ausgabedatum 01.04.2010 (V1-0)**

Richtlinie betreffend der zulässigen Nutzung des Internets, der e-Mail-Dienste und -Programme sowie dem Umgang mit der Informatik Hard-und Software

1. Allgemeines

1.1 Ausgangslage, Ziele

Diese Richtlinie regelt die Sachverhalte, welche ICT Security & Riskmanagement aufgrund einer ausdrücklichen Delegationsnorm in der Konzernweisung betreffend der zulässigen Nutzung des Internets sowie von E - Mail - Diensten und E - Mail - Programmen (K 400.8) sowie der Konzernweisung betreffend dem zulässigen Umgang mit der Informatik - Hard- und Software (K 400.9) regeln darf.

1.2 Geltungsbereich

Sie gilt für jede natürliche Person, welche die von der SBB AG, deren offiziellen Outsourcing - Partner (Provider) oder von der SBB Cargo AG zur Verfügung gestellte Informatik - Hard- und/oder Software oder das Internet, E-Mail-Dienste und E-Mail-Programme mittels eines lokalen oder eines Fern-Zugriffs nutzt.

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

1.2 Übergeordnete und zugehörige Dokumente

K 400.8 „Konzernweisung betreffend der zulässigen Nutzung des Internets sowie von E - Mail - Diensten und E - Mail – Programmen“

K 400.9 „Konzernweisung betreffend dem zulässigen Umgang mit der Informatik - Hard- und Software“

1.3 Begriffe und Abkürzungen

Es werden die folgenden Begriffe innerhalb der vorliegenden Richtlinie verwendet:

Begriff	Beschreibung
Account	Benutzerkonto
Attachment	Eine an ein E-Mail angehängte Datei
Benutzer	Nutzer/Nutzerin von Hard- und/oder Software, des Internets und/oder von E- Mail-Diensten und/oder E-Mail-Programmen
CISO	Chief Information Security Officer der SBB
NSM	Network Security Manager
Folder	Dateiordner
Handheld	Kleincomputer (Psion, Communicator oder ähnliche)
Hardware	Gesamtheit der Geräte und technischen Teile einer Datenverarbeitungsanlage
Hash	Verschlüsselungstechnische Prüfsumme über ein Dokument zur Sicherstellung der Integrität.
Hoax	E-Mail mit falschen Informationen (meist Viruswarnungen), häufig mit Aufforderung zum Weiterversand.
IT	Informationstechnologie. Elektronische Geräte zur Bearbeitung, Aufzeichnung, Speicherung und Sicherung von Daten.
JavaScript/ActiveX	Internetapplikationen zum Anzeigen spezieller Elemente des Internets
Login/Logout	An-/Abmeldungsmeldung zu Handen des IT-Systems
Weisung Nutzung Internet	Entspricht der Konzernweisung betreffend der zulässigen Nutzung des Internets sowie von E-Mail-Diensten und E-Mail-Programmen (R Z 400.8).

Weisung Umgang Hard- und Software	Entspricht der Konzernweisung betreffend dem zuläs-Sigen Umgang mit der Informatik-Hard- und Software (R Z 400.9)
Software	Sammelbegriff für die, auf einem Computer ablaufenden Programme
CISO	Chief Information Security Officer

2. Bestimmungen betreffend Software

2.1 Einsatz privater Software auf PC/Laptops (Ziff. 4.1, K 400.9)

Der Einsatz privater Software auf den von der SBB, ihrem Outsourcing-Partner (vergl. Ziff. 1, Abs. 1 Z 400.9) oder der SBB Cargo zur Verfügung gestellten PC/Laptops ist verboten. Ausnahmen können vom Vorgesetzten – nach Einholung der Zustimmung des Informatik-Supportdienstes und des CISO der SBB – genehmigt werden.

2.2 Installation/Deinstallation von Software (Ziff. 4.1, K 400.9)

Die Installationen und Deinstallationen von Software darf nur von den Informatik-Supportdiensten vorgenommen werden.

Die Installation von nicht von der SBB oder der SBB Cargo beschaffter Software ist verboten.

2.3 Zur Verfügung gestellte Software (Ziff. 4.1, K 400.9)

Allfällige, von der SBB oder der SBB Cargo zur Verfügung gestellte Software für private PC oder private Laptops darf nur für Zwecke der SBB oder der SBB Cargo verwendet werden. Diese Software muss nach Beendigung des Arbeits- bzw. Auftragsverhältnisses mit der SBB oder der SBB Cargo auf dem privaten PC oder dem privaten Laptop wieder gelöscht werden und darf nicht weiter genutzt werden.

2.4 Bedarf nach einer neuen oder andern Software (Ziff. 4.1 K 400.9)

Bei Bedarf nach einer neuen oder einer andern Software ist nach Rücksprache mit dem Vorgesetzten mit dem Informatik-Supportdienst Kontakt aufzunehmen.

2.5 Änderung der Konfigurationseinstellungen (Ziff. 4.1, K 400.9)

Der Benutzer darf die Konfigurationseinstellungen an der Software nicht ändern (z.B. die Sicherheitsstufe des Browsers oder die Prüfeinstellungen des Virusprogramms). Ist eine bestimmte Konfigurationseinstellung erwünscht, muss ein entsprechender Antrag des Vorgesetzten an den jeweiligen Softwareverantwortlichen - bei Sicherheitseinstellungen an den CISO - eingereicht werden.

2.6 Kopieren und Erteilen von Nutzungsrechten an Software (Ziff. 4.1, K 400.9)

Es ist verboten Software zu kopieren. Vorbehalten bleiben die Fälle, bei welchen dies rechtlich eindeutig (z.B. für Sicherungszwecke) zulässig ist und dies der hierzu zuständige Solution Center Leiter vorher bewilligt hat.

Es ist verboten natürlichen oder juristischen Personen Nutzungsrechte bzw. Unterlizenzen an Software zu erteilen, bei welchen die SBB oder die SBB Cargo weder über das diesbezügliche Urheberrecht verfügt, noch (insbes. vertraglich) berechtigt ist, diesbezügliche Nutzungsrechte bzw. Unterlizenzen zu gewähren. Im Zweifelsfall ist die rechtliche Zulässigkeit durch den zuständigen Rechtsdienst bei SBB IT vorgängig beurteilen zu lassen.

2.7 Grundsätze betreffend dem Umgang mit Passwörtern (Ziff. 4.1, K 400.9)

Das Passwort ermöglicht den Benutzern, ihre Identifikation durch das IT-System verifizieren zu lassen und Zugriff auf die für ihn vorgesehenen IT-Komponenten bzw. Informationen (Daten) zu erhalten.

Die Verbindung von Benutzeridentifikation und geheimgehaltenem Passwort verhindert, dass Dritte unter einer fremden Identifikation deren Zugriffsrechte und somit nicht autorisierten Zugriff auf IT-Komponenten erhalten.

Es ist unzulässig Passwörter Dritter zu knacken oder auch nur zu versuchen, Passwörter Dritter zu knacken.

Die Passwörter sind geheim zu halten und dürfen nur dem zulässigen Benutzer bekannt sein. Sie müssen unverzüglich geändert werden, sobald sie unautorisierten Personen bekannt sind.

Die Eingabe von Passwörtern hat unbeobachtet zu erfolgen. Hierzu hat das System bzw die Applikationen sicher zu stellen, dass die Passworteingabe verdeckt erfolgen kann.

Das Passwort muss aus mindestens 8 Zeichen bestehen und mindestens je ein Zeichen aus drei der folgenden Kategorien enthalten:

- Grossbuchstaben
- Kleinbuchstaben
- Zahlen
- Sonderzeichen

Passwörter dürfen nicht leicht zu erraten sein und sollten keine Verbindung zur Unternehmung, zu einer IT-Anwendung oder zum Benutzer aufweisen, wie z.B. Name, Vorname, Autonummer, Telefonnummer des Benutzers. Die Benutzung von Trivialpasswörtern (zB AAAAAAAA, 12345678, Wiederholung der

Benutzeridentifikation) ist zu unterlassen. Technisch begründete Abweichungen sind durch IT-SR zu bewilligen.

Voreingestellte Passwörter sind sofort zu ändern und Initialpasswörter für die Erstanmeldung an einem System sind nach dem erstmaligen Gebrauch durch individuelle Passwörter zu ersetzen.

Die persönlichen Passwörter sind regelmässig (in der Regel jeden Monat) durch neue zu ersetzen.

Wenn zwei im SBB-Netz stehende Systeme über Systemuser miteinander kommunizieren, kann die Service Koordination für das Passwort die Eigenschaften «never expires» und «user cannot change password» vergeben.

Die Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.

Passwörter von privilegierten Benutzern sind versiegelt an sicheren Orten zu hinterlegen, um bei Notfällen oder Abwesenheiten dieser Benutzer den Zugriff auf Systeme und Applikationen sicherzustellen. Die hinterlegten Passwörter müssen vom betreffenden Benutzer von der betreffenden Benutzerin stets aktualisiert werden. Der Umgang mit notfallmässigem Zugriff auf Administratorenrechte wird in A.1.8 geregelt.

2.8 Grundsätze betreffend dem Umgang mit Admin-Accounts

Weder Administratoren noch Anwender dürfen mit Admin-Accounts arbeiten. Administratoren müssen mit den persönlichen User-IDs, die mit den entsprechenden Admin-Rechten versehen sind, arbeiten, damit die Nachvollziehbarkeit ihrer Tätigkeiten gewährleistet ist.

Mit Admin-Accounts darf nur in Notfällen gearbeitet werden, wenn keiner der Administratoren eingesetzt werden kann.

Weitere Regelungen über den Umgang mit privilegierten Accounts finden sich in der Weisung K 400.11 „Privilegierte Accounts“.

3 Bestimmungen betreffend Hardware

3.1 Regelungsbereich

Nachfolgende Regelungen betreffen Arbeitsplatzrechner (PC) und mobile Endgeräte wie Laptops, Smartphones und dergleichen, soweit sich die Einzelvorschrift nicht explizit nur auf eine bestimmte Geräteart bezieht.

3.2 Standort (Ziffer 3 K 400.9)

Eine wesentliche Aenderung des Standortes des Arbeitsplatz-PC ist nur nach vorheriger Zustimmung des Informatik-Supportdienstes zulässig.

Mobile Endgeräte dürfen im Betriebszustand nicht unbeaufsichtigt gelassen werden.

3.3 Netzanschlüsse (Ziffer 3 K 400.9)

Aenderungen an der Netzkonfiguration dürfen nur durch den Informatik-Supportdienst vorgenommen werden

3.4 Modem (Ziffer 3 K 400.9)

Es dürfen von den Benutzern keine Modems installiert werden. Vorbehalten bleiben die Fälle, bei welchem eine Installation eines Modems durch den direkten Vorgesetzten beim CISO beantragt und durch diesen und den zuständigen DIO bewilligt worden ist. Liegt eine Bewilligung vor, ist das Modem durch I-TC zu installieren.

3.5 Remotezugriff via IPSec VPN von privaten PC/Laptops aus (Ziff. 4.4 K 400.9)

IPSec VPN wird für Wartungsarbeiten auf Systemebene/- konfigurationen, für Entwickler (Sourcecoderepositories, Test-/ Integrationsumgebungen) und Analysen im Rahmen von Incidents und Vorfällen eingesetzt. Dafür gilt folgende Regelung:

Die Herstellung einer IPSEC VPN-Verbindung mittels Remote-Access-Service (RAS) von privaten (d.h. nicht von der SBB zur Verfügung gestellten) PC oder Laptops aus ist nicht zulässig. Hiervon ausgenommen sind die durch den NSM und den CISO der SBB genehmigten Geräte mit Spezialsoftware, welche zur Wartung (z.B. von Netzwerkkomponenten oder IT-Serversystemen) benötigt werden.

Der Zugriff von privaten, nicht von der SBB zur Verfügung gestellten PCs oder Laptops via IT WORKPLACE RAS/IT WORKPLACE RAS für Dritte ist erlaubt.

3.6 Datensicherung und –ablage (Ziffer 3.4 und 4.1 K 400.9)

Mittels PC eingegebene Daten sind auf dem zugeteilten Serverbereich zu speichern. Mittels Laptop eingegebene Daten dürfen auch auf den Festplatten derselben gespeichert werden.

Erfasst der Benutzer Daten, welche auch von anderen Benutzer benötigt werden, so ist der Benutzer verpflichtet, diese Daten - wenn möglich - auf den Server zu überspielen. (Auf diese Weise können diese Daten im Rahmen des Server-Back up automatisch gesichert werden.)

Überspielt der Benutzer die Daten seines IT-Geräts nicht täglich auf den Server, so muss er selber ein periodisches Back up der Datensätze auf mobile Speichermedien durchführen. Diese müssen anschliessend beschriftet und sicher aufbewahrt werden. Der Benutzer wird über das Vorgehen durch den Informatik-Supportdienst informiert.

Daten ab externen Datenträgern (z.B. USB-Sticks, externe Festplatten) sind nach Möglichkeit zuerst auf Viren hin untersuchen zu lassen. Das Help Desk (Tel. Nr. 166) sowie der Informatik-Supportdienst unterstützen und beraten die Benutzer hierbei.

Der Benutzer muss sich über die Klassifikationsstufe der Daten vorgängig informieren und den Umgang des Gerätes dieser Stufe anpassen.

Als „vertraulich“ klassifizierte Daten müssen verschlüsselt gespeichert werden, sobald die entsprechende Infrastruktur zur Verfügung steht. Bis zu diesem Zeitpunkt dürfen keine solchen Daten auf den Mobilgeräten gespeichert werden.

Unberechtigten darf keine Einsicht in Personaldaten oder in als „vertraulich“ klassifizierte Daten gewährt werden.

Datenablagen bei Drittfirmen sind nur unter der Einhaltung des RfA-Ablaufs (Request for Architecture) und der Genehmigung des RfA-Boards gestattet, da es sich um mögliche unbekannte Auswirkungen auf die Sicherheit handelt.

3.7 Virenschutz (Ziff. 3.4 und 4.1 K 400.9)

Es dürfen nur PC und Laptops innerhalb der Räumlichkeiten der SBB oder der SBB Cargo benutzt werden, welche über ein automatisches Virenschutz-Update-System verfügen. Stellt der Benutzer fest, dass ein solches auf seinem PC oder Laptop nicht installiert ist, so hat er die für ihn zuständige Benutzerunterstützung hiervon in Kenntnis zu setzen.

Der Benutzer hat sicherzustellen, dass das die Betriebssystemsoftware den aktuellen Release-Stand SBB aufweist und mit den aktuellen Sicherheitspatches SBB versehen ist.

Wird ein Viren-Befall festgestellt oder vermutet, so ist der Help Desk bzw. die User-Unterstützung unverzüglich zu informieren. Gleichzeitig ist der Computer vom Netzwerk zu trennen. Das weitere Vorgehen wird vom Help Desk bzw. der User-Unterstützung angeordnet.

Der Ablauf des Viren-Prüf-Programms darf durch den Benutzer nicht abgebrochen werden.

Das installierte Virenschutzprogramm darf nicht deaktiviert werden und das Gerät muss regelmässig an das Netz angeschlossen werden, um ein Update der Virenschutz-Tabellen sicherzustellen.

Der Benutzer eines mobilen IT-Geräts kann zwecks Erhöhung des Virenschutzes das mobile IT-Gerät entweder dem lokalen Netzwerk anschliessen oder eine aktuelle Virenschutz-Software auf dem mobilen IT-Gerät installieren.

3.8 Virenschutz bei Remote Access – Verbindungen (Ziff. 3.4 und 4.1, K 400.9)

Jede Person, welche das Datenkommunikationsnetz der SBB via einer Remote-Access-Verbindung (nicht IT WORKPLACE–RAS) nutzt, hat mittels der Verwendung eines sich auf dem neuesten Stand befindlichen Virenschutzprogramms sicher zu stellen, dass der von ihr benutzte PC/Laptop - vor jeglicher Verbindung mit dem Datenkommunikations-Netz der SBB – mit Bestimmtheit keine Viren, Würmer und dergleichen aufweist.

Vermutet der Nutzer des Datenkommunikationsnetzes der SBB, dass das Datenkommunikationsnetz der SBB von dem von ihm benutzten PC/Laptop einen Virus/Wurm oder dergleichen zugestellt erhalten haben könnte, so meldet er dies umgehend der Organisationseinheit IT-SR der SBB.

IT-SR berät bestehende sowie zukünftige Nutzer des Datenkommunikationsnetzes der SBB hinsichtlich der Verwendung eines effizienten Virenschutzes-Programms.

3.9 Kommunikation über drahtlose öffentl. Netzwerke (Public GSM, Public WLAN) (Ziff. 3 und 4.1 K 400.9)

Sofern ein Verschlüsselungsmechanismus zur Verfügung steht, dürfen Daten nur verschlüsselt übertragen werden. In keinem Fall darf ein vorhandener Verschlüsselungsechanismus deaktiviert werden.

3.10 Anschluss an nicht unter Kontrolle der SBB stehende Netzwerke (z.B. Internet, private WLAN) (Ziff. 3 und 4. K 400.9)

Unter nicht in Kontrolle der SBB stehende Netzwerke sind Netzwerke anderer Organisationen wie Lieferanten, Kunden und dergleichen zu verstehen.

Der Anschluss von SBB-Geräten an solche Netzwerke ist verboten. Dies dient einerseits der Verhinderung des ungewollten Datenabflusses von SBB-Geräten an die fremde Netzwerkumgebung. Andererseits soll damit vermieden werden, dass ein Austausch von allfälligen Schadprogrammen zwischen dem fremden Netzwerk und den SBB-Geräten stattfindet.

Der Anschluss eines IT WORKPLACE-Gerätes an das Internet zwecks Einsatzes für IT WORKPLACE-RAS ist ausdrücklich erlaubt.

Vorbehalten bleiben Ausnahmebewilligungen des CISO der SBB..

3.11 Verlust und Diebstahl (Ziff. 3 und 4.1 K 400.9)

Bei Verlust/Diebstahl von SBB-Endgeräten ist der Verlust / Diebstahl sofort an die entsprechenden Stellen zu melden. Verluste von Geräten der Mobiltelefonie sind dem Supportcenter Mobiltelefonie zu melden. Der Verlust der anderen Geräte sind gemäss definiertem Prozess der IT Servicekoordination anzuzeigen.

3.12 Melden sicherheitsrelevanter Ereignissen und Risiken (Ziff. 3 und 4.1 K 400.9)

Jeder Nutzer von SBB-Endgeräten ist verpflichtet, Ereignisse, welche sicherheits-relevant sind, und/oder erkannte Risiken unverzüglich an den zuständigen Objekt-verantwortlichen (bei Projekten: Projektleiter, bei über IT WORKPLACE beschafften Geräten: Fachbus IT WORKPLACE (IT-OM-WUS-WDM)Zulässige Nutzung des Internets

4.1 Risikoreiche Nutzungen (Ziff. 3.1.3 K 400.8)

Bestellungen bzw. Auftragserteilungen via Internet unter Angabe der Kreditkarten-nummer sowie Finanzgeschäfte (z.B. Online-Wertpapierhandel, Telebanking) via Internet sind nach Möglichkeit zu unterlassen und werden weder von der SBB, noch von der SBB Cargo empfohlen. Der Benutzer anerkennt, dass solche Bestellungen/Auftragserteilungen und Finanzgeschäft-Transaktionen stets auf eigene Gefahr des Benutzers erfolgen und dass weder die SBB, (inkl. deren Tochtergesellschaften, mit ihr irgendwie verbundene Vereine, Stiftungen, etc.) noch die SBB Cargo (inkl. deren Tochtergesellschaften, mit ihr irgendwie verbundene Vereine, Stiftungen etc.) für daraus resultierende Schäden des Benutzers haftet.

4.2 Bekanntgabe von sensiblen Daten (Ziff. 3.1.3 K 400.8)

Firmeninterne Benutzer-IDs und Passwörter dürfen nicht im Internet veröffentlicht oder für Logins in externe Internet-Dienste (z.B. Private E-Mail-Konten, Member-Logins) verwendet werden.

Weder die SBB, noch die SBB Cargo gewährleisten, dass nicht nach dem neuesten Stand der Technik oder sonstwie korrekt verschlüsselte und mittels Internet übermittelte Pass-wörter, Benutzernamen, geheime oder vertrauliche Informationen usw. nicht von unbe-rechtigten Dritten gelesen werden können.

Die Geschäftsadresse, die geschäftliche E-Mail-Adresse sowie der Namen des Arbeitge-bers sollten nach Möglichkeit im Internet nicht preisgegeben werden.

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

5.1 Information und Unterstützung (Ziff. 4.4 K 400.8)

Im Falle von Problemen betreffend dem Umgang mit E-Mail – Diensten können sich die Benutzer und Benutzerinnen an das zuständige Help Desk oder den Informatik – Supportdienst wenden. Sollten sich Fragen betreffend der Sicherheit der übertragenen Informationen stellen, kann sich der Benutzer an den Informatik - Supportdienst, die Abteilung „Arbeitsplatz und Mail“ (IT-OM-WUS-WDM) der SBB oder im Falle von bedeutenden Sicherheitsbedenken direkt an den CISO wenden.

5.2 Verwendung von E-Mail-Systemen (Clients) (Ziff. 4.4 K 400.8)

Für den geschäftlichen E-Mail-Verkehr dürfen nur die dafür bestimmten und zugelassenen E-Mail Systeme und E-Mail Programme (z.B. Exchange/Outlook) verwendet werden. Ausnahmen hierzu können mit Einwilligung des Vorgesetzten beim CISO beantragt werden.

Die SBB AG ist berechtigt, den Gebrauch von allgemein zugänglichen E-Mail-Systemen (wie zB Hotmail, GMX, Yahoo) von PCs, Laptops oder PDAs aus, welche geschäftlichen Zwecken der SBB AG oder ihrer Tochtergesellschaften dienen, technisch zu unterbinden und den Gebrauch solcher allgemein zugänglicher E-Mail-Systeme im geschäftlichen Umfeld ganz oder teilweise zu verbieten.

5.3 Zurückhaltende Angabe der E-Mail-Adresse bei Spam-Gefahr (Ziff. 4.4 K 400.8)

Die Angabe der geschäftlichen E-Mail-Adresse für Newsgroups, Mailinglisten etc. ist untersagt, falls dadurch Massen-Mails mit reinem Werbecharakter ausgelöst werden.

5.4 Private E-Mails (Ziff. 4.4 K 400.8)

E-Mails mit rein privaten Inhalten sollten - nach Möglichkeit - von E-Mails mit rein geschäftlichen Inhalten unterschieden werden können. Deshalb sollte – bei E-Mails mit rein privaten Inhalten – nach Möglichkeit im Betreff, im Text oder als Attribut der Begriff „Privat“ ausdrücklich oder zumindest sinngemäss erwähnt werden. Jeder Benutzer hat sicher zu stellen, dass nach Möglichkeit auch eingehende, rein private E - Mails in der eingangs erwähnten Weise gekennzeichnet werden. Die lokale Speicherung/ Archivierung privater E-Mails ist zu unterlassen.

5.5 Anlagen/Attachments (Ziff. 4.4 K 400.8)

Aus Sicherheits- und Ressourcengründen dürfen die angefügten Dokumente/Dateien nicht mehr als 5 Megabytes beim Versand und 10 Megabytes beim Empfang umfassen.

Der Versand von sogenannten Joke-, Animations- und Musikdateien, Free- und/oder Shareware oder von Spielen mittels E-Mail ist verboten.

5.6 Versand von E-Mails (Ziff. 4.4 K 400.8)

Das Versenden ausführbarer Programme mittels E-Mail ist nicht erlaubt. Hiervon ausgenommen ist das für geschäftliche Zwecke erforderliche Versenden von ausführbaren Programmen mittels E-Mail nach Genehmigung durch den CISO.

E-Mails, welche an interne E-Mail-Adressen versandt wurden, dürfen nur nach vorhergehender Inhaltsprüfung an externe E-Mail-Adressen weitergeleitet werden, wobei E-Mails im vertraulichen Inhalten generell nicht an an externe E-Mail-Adressen weitergeleitet werden dürfen.

Eine automatisierte Weiterleitung von E-Mails an externe E-Mail-Adressen ist nicht zulässig.

5.7 Vertraulichkeit/Verschlüsselung (Ziff. 4.4 K 400.8)

Es dürfen keine (insbes. als vertraulich) klassifizierten Informationen (in Form von E-Mail und/oder E-Mail-Attachments) ungeschützt extern (aus dem SBB-Netz) versandt werden.

Für die Verschlüsselung dürfen nur die vom CISO der SBB freigegebenen Verfahren eingesetzt werden. Bei Fragen rund um die Verschlüsselungstechniken kann der Benutzer sich an die Informatik-Supportdienste wenden.

5.8 Digitale Signatur (Ziff. 4.4 K 400.8)

Digitale Signaturverfahren dürfen verwendet werden, um die Authentizität der übertragenen Informationen – soweit rechtlich zulässig - zu gewährleisten.

5.9 Der Empfang von E – Mails (Ziff. 4.4 K 400.8)

Der Posteingang (bzw. die Mailbox) ist vom Benutzer mindestens einmal täglich auf den Eingang von E-Mails hin zu überprüfen. Im übrigen gilt die Stellvertreter-Regelung gemäss B.2.16. Nicht mehr benötigte E-Mails sind zu löschen. Benutzer und Benutzerinnen, welche E-Mails von Arbeitnehmern der SBB oder der SBB Cargo mit rechtswidrigen oder anstössigen Inhalten erhalten, melden den Sachverhalt - unter Beilage eines Ausdrucks des erhaltenen E-Mails - ihrem Vorgesetzten.

5.10 E - Mail und Vertragsabschluss (Ziff. 4.4 K 400.8)

Verträge mittels E-Mail sind – nach Möglichkeit und soweit rechtlich zulässig - unter Verwendung einer digitalen Signatur abzuschliessen.

5.11 E - Mail - Attachments (Ziff. 4.4 Z 400.8 und Ziff. 5.1 K 400.8)

E-Mail-Attachments von nicht identifizierbaren Absendern oder von zweifelhafter Herkunft dürfen nicht geöffnet werden (Gefahr von Viren). Der Informatik-Supportdienst ist über das suspekte Attachment raschest möglich zu informieren.

5.12 Mittels E- Mail empfangene Programme (Ziff. 4.4 K 400.8)

Per Attachment übermittelte Programme, welche von einem dem Empfänger bekannten Absender stammen, dürfen zwar entgegengenommen, jedoch nicht ausgeführt und vom Benutzer bzw. der Benutzerin auf der von der SBB, der SBB Cargo oder deren Outsourcing - Partnern zur Verfügung gestellten Hardware installiert werden. Vorbehalten bleiben Ausnahmebewilligungen, welcher der Zustimmung des CISO sowie des zuständigen DIO bedürfen.

5.13 Mittels E- Mail empfangene Hoaxes (Ziff. 4.4 K 400.8)

E-Mails mit unzutreffenden Warnungen (meist vor Viren) und der Aufforderung zum Weiterversand sind durch die Benutzer zu ignorieren. Der Informatik-Supportdienst ist über den Erhalt von Hoaxes zu informieren.

5.14 Stellvertreter - Regelung (Ziffer 4.4 K 400.8)

Der Vorgesetzte bestimmt wer - im Falle einer längeren Abwesenheit des Benutzers – dessen eingehenden E-Mails zu lesen hat und löschen darf.

Der Benutzer/die Benutzerin muss den Stellvertreter in der Mailbox für die Dauer der Abwesenheit entsprechend für den Zugriff auf die Mails berechtigen.

5.15 Speicherung/Archivierung (Ziffer 4.4 K 400.8)

Aus Sicherheitsgründen dürfen E-Mails und deren Attachments nicht lokal mittels des E-Mail-Programms (z.B. Outlook) gespeichert oder archiviert werden.

5.16 Kontrolle (Ziffer 4.4 K 400.8)

IT-SR ist befugt den E - Mail - Verkehr hinsichtlich der Beachtung der Ziffer 4.1 der Weisung „Nutzung Internet“ stichprobenartig durch anonyme Kontrollen gemäss einem bestimmten Zeitplan für eine beschänkte Benutzungsdauer zu kontrollieren.

IT-SR hat sich – im Rahmen ihrer Kontrolle - an die jeweils aktuellen Bestimmungen des „Leitfadens über Internet und E-Mail-Ueberwachung am Arbeitsplatz“ des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu halten.

Wird ein Missbrauch festgestellt, kann eine personenbezogene Auswertung der Protokollierungen vorgenommen werden. Das Resultat der personenbezogenen Auswertung ist von IT-SR dem Vorgesetzten der fehlbaren Person zu melden. Der Vorgesetzte trifft die erforderlichen Führungsmassnahmen. Die zugeteilten Personalverantwortlichen stehen den Vorgesetzten beratend und unterstützend zur Verfügung.

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 ArbGV 3.)

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

6. Inkrafttreten

Diese Weisung tritt am 01.01.2013 in Kraft.

IT	IT-SR
Sig. Peter Kummer	Sig. Marcus Griesser
CIO	CISO

Änderungsverzeichnis

Version	Gültig ab	Kapitel	Änderung
2-0	01.01.2013	alle	Weisung in die aktuelle Vorlage des Regelwerkes übernommen,; formale Anpassungen. Wechsel von K-IT zu IT.