

| | | | |
|-----------------------------------|-----------|--|----------------------|
| Regelwerkversion | 3-0 | Vertraulichkeitsklassifikation | intern |
| gültig ab | 01.1.2013 | 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 01.11.2011 (V1-0) | |

Konzernweisung betreffend den zulässigen Umgang mit der Informatik - Hard- und Software

| | | |
|-----------|--|----------|
| 1. | Allgemeines | 3 |
| 1.1. | Ausgangslage, Ziele | 3 |
| 1.2. | Geltungsbereich | 3 |
| 1.3. | Übergeordnete und zugehörige Dokumente | 3 |
| 2. | Administrative Sicherungsmassnahmen | 3 |
| 3. | Bestimmungen betreffend der Hardware | 3 |
| 3.1. | Grundsätze betreffend den Einsatz von Hardware | 3 |
| 3.1.1. | Zulässiger Einsatz von Hardware | 3 |
| 3.1.2. | Unentgeltliche, längerfristige Ausleihe von Hardware | 4 |
| 3.1.3. | Nutzung des zur Verfügung gestellten PC, Laptops oder von Informatik-Hilfsmitteln für private Zwecke | 4 |
| 3.1.4. | Nutzung von privaten PC oder Laptop für geschäftliche Zwecke | 4 |
| 3.1.5. | Sperren der Arbeitsstation | 4 |
| 3.2. | Datenträger | 4 |
| 3.3. | Bestimmungen betreffend den mobilen IT-Geräten auf denen SBB-Daten verarbeitet werden | 5 |
| 3.3.1. | Bestimmungen betreffend temporär zur Verfügung gestellten mobilen IT-Geräten | 5 |
| 3.3.1.1. | Abgabe oder Rücknahme von zur Verfügung gestellten mobilen IT-Geräten | 5 |
| 3.3.1.2. | Schutz vor Diebstahl bei mobilen IT-Geräten | 5 |
| 3.3.1.3. | Transport | 5 |
| 3.3.1.4. | Verlust | 5 |
| 3.4. | Datensicherung, elektronischer Papierkorb, temporäre Ordner, automatische Speicherung | 5 |
| 3.5. | Änderungen | 5 |
| 4. | Bestimmungen betreffend der Software sowie Daten | 6 |
| 4.1. | Einsatz | 6 |
| 4.2. | Tests der Schutzmechanismen von Browserschnittstellen zu Anwendungen | 6 |
| 4.3. | Austritt eines Arbeitnehmers | 7 |



| | | |
|-----------|---|----------|
| 4.4. | Löschen von Daten friStlos entlassener, verstorbener verschollener oder freigestellter Arbeitnehmer | 8 |
| 4.5. | Bearbeitung von klassifizierten Daten sowie von Personendaten..... | 8 |
| 4.6. | Protokollierung | 8 |
| 4.7. | Kontrolle..... | 8 |
| 4.8. | Änderungen | 8 |
| 5. | Verhältnis zu anderen Weisungen..... | 8 |
| 6. | Inkrafttreten | 9 |
| | Änderungsverzeichnis | 9 |

1. Allgemeines

1.1. Ausgangslage, Ziele

Diese Weisung regelt die zulässige Art der Nutzung von Informatik-Hard- und/oder Software.

1.2. Geltungsbereich

Sie gilt für jede natürliche Person, welche die von der SBB deren offiziellen Outsourcing - Partner (Provider) oder von der SBB Cargo zur Verfügung gestellte Informatik - Hard- und/oder Software nutzt.

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 30.1 Securityhandbuch SBB

2. Administrative Sicherungsmassnahmen

Der unmittelbare Vorgesetzte stellt sicher, dass die ihm unterstellten Benutzer 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“ (K 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 herunter geladen werden kann.

3. Bestimmungen betreffend der Hardware

3.1. Grundsätze betreffend den Einsatz von Hardware

3.1.1. Zulässiger Einsatz von Hardware

Es darf bei der SBB und der SBB Cargo nur Hardware eingesetzt werden, welche von der SBB (bzw. von dessen Outsourcing – Partner) oder der SBB Cargo beschafft und dem Benutzer für deren Aufgabenerfüllung zur Verfügung gestellt worden ist.

Die SBB und die SBB Cargo sind berechtigt, mittels technischer oder organisatorischer Massnahmen bei der SBB oder der SBB Cargo unberechtigt eingesetzte Hardware zu eruieren und anschliessend aus dem Verkehr zu ziehen.

Die Hardware ist sorgfältig zu behandeln

3.1.2. Unentgeltliche, längerfristige Ausleihe von Hardware

Jegliche zwei Monate überschreitende, unentgeltliche Ausleihe von Hardware, welche der SBB oder der SBB Cargo durch den Outsourcing-Partner der SBB zur Verfügung gestellt worden ist und ausserhalb der Räumlichkeiten der SBB oder der SBB Cargo genutzt werden soll, bedarf der vorgängigen Zustimmung des zuständigen Divisionsleiters wobei – im Falle der Erteilung der Zustimmung des Divisionsleiters - ein schriftlicher Gebrauchsleihevertrag mit dem Dritten abzuschliessen ist und SBB IT Account Management über die entlehene Hardware (wem ist welche Hardware bis wann entliehen worden ?) zügig zu informieren ist.

3.1.3. Nutzung des zur Verfügung gestellten PC, Laptops oder von Informatik-Hilfsmitteln für private Zwecke

Die Nutzung des zur Verfügung gestellten PC, Laptops oder von Informatik-Hilfsmitteln (Scanner, CD-Brenner etc.) für private Zwecke während der Arbeitszeit ist nicht zulässig. Vorbehalten bleiben die Fälle, bei welchen dies der unmittelbare Vorgesetzte für eine kurze Zeit erlaubt hat.

Eine Nutzung des zur Verfügung gestellten PC, Laptops oder von Informatik – Hilfsmitteln für private Zwecke ausserhalb der Arbeitszeit ist in einem zeitlich beschränkten Rahmen zulässig, falls der unmittelbare Vorgesetzte dies nicht verboten hat.

3.1.4. Nutzung von privaten PC oder Laptop für geschäftliche Zwecke

Private PC/Laptop dürfen nur mit vorheriger schriftlicher Bewilligung des Operation Managements und ICT-Security & Risk Management (nachfolgend IT-SR genannt) nach einer Homologation gemäss K 400.30 mit dem Datenkommunikations-Netz der SBB verbunden werden. Vorbehalten bleiben die Fälle, bei welchen ein Remote-Access-Anschluss bewilligt worden ist und der Zugang zum Netz nicht von den Räumlichkeiten der SBB oder der SBB Cargo aus erfolgt.

3.1.5. Sperren der Arbeitsstation

Der PC sowie der Laptop ist spätestens beim Verlassen des Arbeitsplatzes automatisch sperren zu lassen (z.B. durch einen passwortgeschützten Bildschirmschoner), um unbefugten Personen jeglichen Zugriff zu verunmöglichen.

Im Falle längerer Nichtbenutzung des PC/Laptops sowie bei Arbeitsschluss hat der Benutzer sich abzumelden (log out) und den PC/Laptop herunterzufahren.

3.2. Datenträger

Datenträger (Disketten, CD-ROMs, Festplatten, Magnetbänder, Druck-Outputs) dürfen nicht so herumliegen, dass unbefugte Personen diese eventuell kopieren, einsehen oder entwenden könnten.

3.3. Bestimmungen betreffend den mobilen IT-Geräten auf denen SBB-Daten verarbeitet werden

3.3.1. Bestimmungen betreffend temporär zur Verfügung gestellten mobilen IT-Geräten.

3.3.1.1. Abgabe oder Rücknahme von zur Verfügung gestellten mobilen IT-Geräten

Die Organisationseinheiten der SBB und der SBB Cargo, welche mobile IT-Geräte aus-leihen, stellen sicher, dass eine geeignete Kontrolle der entliehenen Geräte erfolgt.

Der Benutzer des zur Verfügung gestellten mobilen IT-Geräts hat die durch ihn auf der Festplatte gespeicherten Daten vor der Rückgabe des mobilen IT-Geräts zu löschen. All-fällig noch vorhandene, die persönliche Nutzung betreffende Daten, sind nach der Rückgabe des mobilen IT-Geräts vom Help Desk (Service Desk) bzw. der User-Unterstützung zu löschen.

3.3.1.2. Schutz vor Diebstahl bei mobilen IT-Geräten

Der Benutzer eines mobilen IT-Geräts ist verpflichtet alles zu unternehmen, um das ihm zur Verfügung gestellte, mobile IT-Gerät vor einem möglichen Diebstahl zu schützen.

3.3.1.3. Transport

Tragbare IT-Geräte dürfen lediglich gut verpackt transportiert werden.

3.3.1.4. Verlust

Im Falle eines Verlusts oder eines Diebstahls eines zur Verfügung gestellten mobilen IT-Geräts der SBB, ihres Outsourcing- Partners oder der SBB Cargo, ist aufgrund des mögliche Datenverlustes auch der Bereich IT-SR umgehend über den Verlust/Diebstahl zu informieren, damit die möglichen und nötigen Schutzmassnahmen (wie z.B. Sperrung des Accounts usw.) ergriffen werden können.

3.4. Datensicherung, elektronischer Papierkorb, temporäre Ordner, automatische Speicherung

IT-SR ist berechtigt Regelungen betreffend der Datensicherung und –ablage, temporären Ordnern, der automatischen Speicherung und Virenschutz-Vorkehrungen in der Richtlinie zu dieser Weisung zu erlassen.

3.5. Änderungen

Änderungen an der zur Verfügung gestellten Hardware (inkl. den zur Verfügung gestellten Informatik-Hilfsmitteln) dürfen nur durch den Informatik-Supportdienst vorgenommen werden. Vorbehalten bleiben Ausnahmegewilligungen des Bereiches IT-SR, wobei die Letzteren jedoch den CISO über ihre erteilte Ausnahmegewilligung zu orientieren haben.

4. Bestimmungen betreffend der Software sowie Daten

4.1. Einsatz

Es darf nur von der SBB oder von der SBB Cargo zugelassene Software auf den Computern/Laptops der SBB oder der SBB Cargo verwendet werden. Die Liste der zugelassenen Software kann bei der zentralen Lizenzverwaltungsstelle der SBB IT bezogen oder beim entsprechenden Warenkorb (beispielsweise IT WORKPLACE-Warenkorb) in Erfahrung gebracht werden. Ergänzende Bestimmungen betreffend der Software können sich aus der Richtlinie zu dieser Weisung ergeben.

4.2. Tests der Schutzmechanismen von Browserschnittstellen zu Anwendungen

Anwendungen, die mit einem WEB-Browser aufgerufen werden können, sind präventiv gegen mögliche Angriffe zu schützen. Die Browserschnittstelle solcher Anwendungen ist vor Produktivsetzung auf die Widerstandsfähigkeit hin zu testen.

Betroffen sind alle Anwendungen, welche mit einem WEB-Browser bedient werden können und sich im SBB-Netz befinden.

Es betrifft ausserdem Anwendungen, die auf Systeme von Drittanbietern ausgelagert sind. Diese Anwendungen sind nach Best Practices bei der Entwicklung vor Angriffen zu schützen.

Vor Produktivsetzung sind die Schutzmechanismen solcher Anwendungen gegenüber Angriffen zu testen.

Produktive Anwendungen sind bei der Entwicklung von neuen Versionen zu testen, wenn Änderungen vorgenommen werden, die deren Zugang über den WEB-Browser betreffen, mindestens aber alle zwei Jahre

4.2.1 Eigenentwicklungen der SBB Informatik

Die TestFactory SBB wird beauftragt, diese Tests der Schutzmechanismen Browserschnittstellen vorzubereiten, auszuführen und auszuwerten.

Die Produktivsetzung der Anwendung bzw einer neuen Version darf nur durch Vorlage einer Bestätigung der operationellen Security SBB erfolgen.

4.2.2 Durch Drittanbieter entwickelte und betriebene Anwendungen

Drittanbieter, die solche Anwendungen für die SBB entwickeln und betreiben, müssen verpflichtet werden, einen Nachweis zu erbringen, dass sie die Schutzmechanismen gegenüber Angriffen über die WEB-Browser-Schnittstelle untersucht und bewertet haben. Sie können stattdessen auch die Anwendungen durch die Testfactory SBB untersuchen lassen.

Die Koordination der Nachweise obliegt der Testfactory SBB.

4.2.3 Reports

Die Testfactory SBB stellt der IT Security periodisch ein Reporting über die Tests der Anwendungen zur Verfügung.

4.2.4 Übergangsregelung

Anwendungen, die am 1. Januar 2012 bereits produktiv sind, müssen bezüglich der Schutzmechanismen nachträglich getestet werden.

Die Testfactory plant diese Untersuchung mit den betroffenen Applikationsverantwortlichen nach folgender Priorisierung:

1. Anwendungen, die aus dem Internet oder Business-Netz von aussen per WEB-Browser erreichbar sind, müssen bis zum 31.12.2012 getestet werden.
2. Intranetanwendungen, die vertrauliche Daten bearbeiten, und
3. alle übrigen Intranetanwendungen, die interne Daten bearbeiten, müssen bis zum 31.12.2013 getestet sein

4.3. Austritt eines Arbeitnehmers

Jeder aus der SBB oder der SBB Cargo austretende Arbeitnehmer ist verpflichtet, vier Wochen vor seinem Austritt – in Absprache mit seinem Vorgesetzten - den Ablageort für die Übernahme von lokal gespeicherten, weiter

zu verwendenden Daten und/oder Mails zu bestimmen. Rein private oder nicht mehr benötigte Daten sind hierbei zu löschen.

4.4. Löschen von Daten fristlos entlassener, verstorbener verschollener oder freigestellter Arbeitnehmer

Die Personalservices (Human Ressources) der SBB und der SBB Cargo machen die Angehörigen der verstorbenen/verschollenen Arbeitnehmer sowie die fristlos entlassenen oder freigestellten Arbeitnehmer darauf aufmerksam, dass diese der SBB bzw. der SBB Cargo ein Gesuch um Übergabe rein privater Daten innert eines Monats seitdem der betreffende Arbeitnehmer nicht mehr am Arbeitsplatz erschienen ist, stellen können. Sie informieren den Informatik-Supportdienst rechtzeitig über die Namen und Vornamen der fristlos entlassenen, verstorbenen, verschollenen oder freigestellten Arbeitnehmer sowie über den Beginn des Laufs der einmonatigen Frist.

4.5. Bearbeitung von klassifizierten Daten sowie von Personendaten

Falls geheime oder vertrauliche Daten oder Personendaten auf einem IT-Gerät bearbeitet werden, sind diese durch besondere technische Massnahmen vor einem möglichen Zugriff nicht berechtigter Personen zu schützen. Der Informatik-Supportdienst berät und unterstützt hierzu die betreffenden Benutzer.

4.6. Protokollierung

Es können – im Rahmen des rechtlich Zulässigen und ausschliesslich aus technischen IT-Sicherheitsgründen (d.h. insbesondere nicht zwecks Überwachung der Arbeitnehmer und Arbeitnehmerinnen) - von der Organisationseinheit IT-SR stichprobenartige, anonyme Kontrollen der Zugriffe auf Programme und Dateien gemäss einem bestimmten Zeit-plan für eine beschränkte Benutzungsdauer vorgenommen werden. Diese Daten werden ausschliesslich in anonymisierter Form gespeichert und werden nach Gebrauch umgehend gelöscht.

4.7. Kontrolle

IT-SR ist berechtigt Inhalte, welche das IT-System und die Netzwerke der SBB passieren, von einem Computer schematisch nach Inhalten abzusuchen, die auf Gefahren wie Viren, Würmer, Systemüberlastungen etc. hindeuten. Diese Vorgänge laufen gemäss den aktuellen technischen Möglichkeiten vollautomatisch ab. Diese Daten werden in anonymisierter Form gespeichert und nach dem Gebrauch umgehend gelöscht.

4.8. Änderungen

Änderungen an der zur Verfügung gestellten Software dürfen nur durch den Informatik-Supportdienst vorgenommen werden. Vorbehalten bleiben Ausnahmegewilligungen des CISO oder des CIO, welcher den CISO über die erteilte Ausnahmegewilligung orientiert.

5. Verhältnis zu anderen Weisungen

IT-SR ist berechtigt, im Rahmen der ihr mittels dieser Weisung delegierten Kompetenz (vergl. beispielsweise die Ziffer 4.1 dieser Weisung) Ausführungsbestimmungen betreffend dem zulässigen Umgang mit der Informatik Hard- und Software in der „Richtlinie betreffend der zulässigen

Nutzung des Internets, der E-Mail-Dienste und –programme sowie dem zulässigen Umgang mit der Informatik-Hard- und Software“ zu erlassen. Die Bestimmungen dieser Richtlinie dürfen jedoch nicht den Bestimmungen dieser Weisung widersprechen.

Von IT-SR erstellte Änderungen an der Richtlinie, welche sich aus einer Delegationsnorm dieser Weisung ergeben, werden vorgängig einer Rechtskontrolle unterzogen.

6. Inkrafttreten

Diese Weisung tritt per 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 aktuelle Vorlage des Regelwerkes übernommen und formale Aktualisierung von Funktionsbezeichnungen. Wechsel von K-IT zu IT. |
| | | | |
| | | | |