Regelwerkversion	**9-0**	Vertraulichkeitsklassifikation	**SBB Intern**
gültig ab	**27.03.2017**	Eigner	**P-OES / IT-SR**
		Betroffene Prozesse	
		verfügbare Sprachen	**DE, FR, IT**

Betroffene Divisionen	**Infrastruktur, Personenverkehr, Cargo, Immobilien, Konzern**
Spezifische Empfänger / Verteiler	**A2-A4, A20**
Ersatz für	**Regelwerkversion 8-0**
Zuordnung	**Gemäß Ziffer 1.4.1 / 1.4.2 / 1.4.3**

Security Handbuch SBB

Änderungsverzeichnis

Version	Kapitel	Änderung
9-0	4.6 4.8 4.15 4.16 4.17	Ergänzung Inhalt integraler Bestellprozess, Einbindung der Unterkapitel, Falluntersuchungsstelle und Compliance-Meldestelle. Ergänzung Kapitel Betriebskriminalität und Entführungsalarmsystem (fedpol). Planungsrichtlinien für Gebäude und Anlagen / Transport und Aufbewahrung von Werten (Anforderungen Versicherungsmanagement).
8-0	4.12.2	Anpassung bezüglich Anzeigepraxis, Schaden- und Strafrechtzentrum.
7-0	Alle	Straffung der Inhalte; Reduktion auf Grundsätze und Ziele mit Delegationsnorm für weiterführende Regelungen.

1. Einleitung

1.1. Geltungsbereich und Verbindlichkeit

Das vorliegende Dokument ist ein Steuerungs- und Regelungssystem im Sinn von organisatorischen und fachlichen Strukturen/Inhalten. Es enthält unternehmensweit gültige Vorgaben und Richtlinien, die den Sicherheitsstandard der SBB im Bereich Security festlegen. Das Security Handbuch (K 030.1) basiert auf den Grundsätzen des VR SBB zu Safety und Security (Z 018.1) sowie der Weisung Security SBB (K 018.3).

Das K 030.1 und die weiterführenden bzw. verlinkten Dokumente und Prozesse sind für alle Mitarbeitenden der Divisionen P, I, G, IM, der Konzernbereiche sowie für beauftragte Dritte verbindlich anzuwenden. Dies gilt im Grundsatz auch für die Tochtergesellschaften der SBB, soweit sie von der SBB AG oder von SBB Cargo AG kontrolliert werden. Bei den Beteiligungsgesellschaften sorgen die Linienverantwortlichen sowie die Vertreter der SBB in den Organen der Gesellschaft im Rahmen ihrer Zuständigkeit für die Einhaltung der jeweils geltenden Vorgaben und soweit sinnvoll für eine Angleichung an die Regelungen der SBB.

Kann die Richtlinie bei Gemeinschaftsunternehmen (50% - 50% Joint Venture) nicht durchgesetzt werden, ist ein gleichwertiger Sicherheitsstandard zu gewährleisten (die Standards vergleichbarer Unternehmen im Bereich Transport und Logistik sowie die internationalen Standards gemäss ISO 27000 ff. und ISO 22301).

Die Nichteinhaltung der in dieser Weisung vorgegebenen Richtlinien kann für die Mitarbeitenden der SBB arbeitsrechtliche Konsequenzen nach sich ziehen. Diese Bestimmungen sind sowohl für Mitarbeitende mit OR- als auch für Mitarbeitende mit GAV-Vertrag anwendbar. Die Verantwortung für externe Mitarbeitende und Lieferanten liegt bei den zuständigen Linienverantwortlichen.

1.2. Grundlagen und Zielsetzungen

1.2.1. Grundlagen

Der Verwaltungsrat und die Konzernleitung der SBB erteilen in den Grundsätzen des VR SBB zu Safety und Security (Z 018.1) sowie der Weisung Security SBB (K 018.3) den Auftrag zur Wahrung der öffentlichen Sicherheit sowie der Informations- und elektronischen ICT-Security. Nebst der Definition des bestehenden Sicherheitsniveaus wird dessen Erhaltung und Verbesserung angeordnet. Deshalb ist aufgrund dieser Fachbereichsrichtlinie ein Sicherheitsmanagementsystem zu errichten.

Der Verwaltungsrat benennt die zuständigen Stellen mit den zugehörigen Aufgaben, Kompetenzen sowie Verantwortungen und beschreibt grob das Reporting und die Kontrollen zur Steuerung des Bereiches Security. Diese Weisung wird im Bereich Informationssicherheit / ICT Security durch ein Framework konkretisiert, welches diverse weiterführende Policies, Konzepte, Bereichskonzepte, Weisungen und Richtlinien beinhaltet. Die Sicherheitslage wird mindesten jährlich im Sicherheitsbericht zuhanden des CEO rapportiert.

1.2.2. Ziele dieser Weisung

Das K 030.1 beinhaltet folgende Zielsetzungen:

- Die Weisung ist die Basis um ein einheitliches, wirtschaftliches und zeitgerechtes Sicherheitsniveau im Bereich Security bei den SBB sicherzustellen.
- Es regelt die Minimalanforderungen an bauliche, technische, prozessuale und organisatorische Massnahmen im Bereich Security, um für weiterführende Dokumentationen im Bereich Sicherheit eine Verbindlichkeit zu erreichen.
- Es ist ein Grundlagendokument für Beauftragte und Verantwortliche, welche Tätigkeiten im Bereich Security planen oder ausführen müssen.

1.2.3. Auszüge und bereichsspezifische Anweisungen

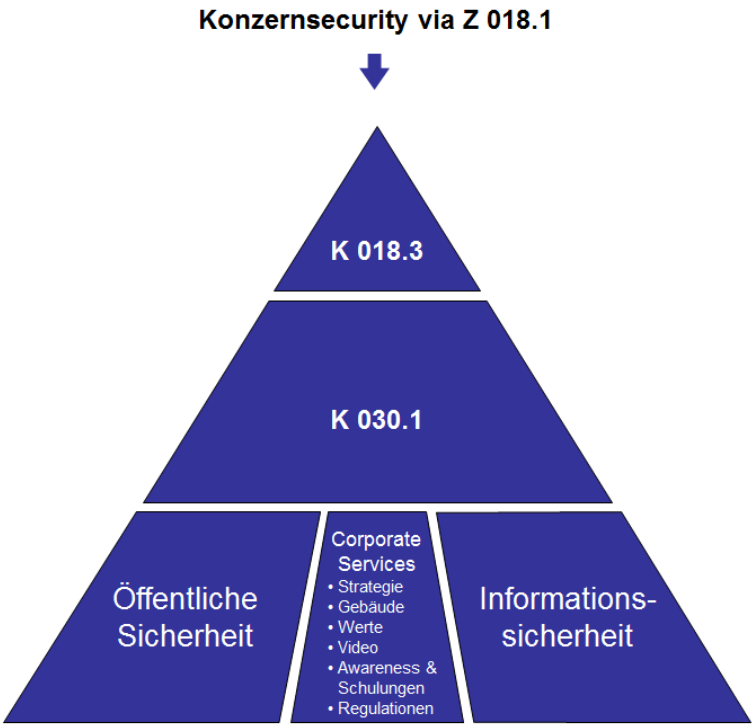
Zur Ausübung einer bestimmten sicherheitsrelevanten Tätigkeit ist meist nicht nur diese Weisung ausreichend. Oftmals sind detailliertere fachliche Handlungsanweisungen zu den jeweiligen Themenbereichen vorhanden oder notwendig, welche ebenfalls zu berücksichtigen sind. Die Verantwortung für das Erstellen und aktuell halten von weiterführenden bereichsspezifischen Anweisungen liegt in der Linie. Die bereichsspezifischen Anforderungen dürfen übergeordneten Regelungen oder Regelungen der Fachführungen Öffentliche Sicherheit und Informationssicherheit / ICT-Security nicht widersprechen, sondern nur konkretisieren oder verschärfen.

1.3. Begriffe und Definitionen

Die weiterführenden Beschreibungen und Erläuterungen zu den verwendeten Begriffen werden im Glossar der SBB beschrieben.

1.4. Abhängigkeit / Stellung zu anderen Dokumenten

Die Struktur des Security Regelwerks ist wie folgt aufgebaut:



Zu dieser Weisung K 030.1 (Security Handbuch) gibt es übergeordnete, mitgeltende und konkretisierende Regelungen in den Bereichen Öffentliche Sicherheit, Informationssicherheit und überschneidende Themen im Bereich Corporate Services. Letztere müssen nicht unbedingt in Form einer offiziellen Weisung gemäss Regelwerk erstellt sein.

1.4.1. Übergeordnete Regelungen

Das Security Handbuch der SBB basiert auf folgenden übergeordneten Grundlagen:

- Z 018.1: Grundsätze des Verwaltungsrates der SBB zu Safety und Security vom 27.09.2007
- K 018.3: Weisung Security SBB vom 15.11.2016
- K 600.0 Verhaltenskodex SBB («Code of Conduct»)

1.4.2. Mitgeltende Regelungen

Neben dem Security Handbuch der SBB gelten folgende Weisungen als mitgeltend:

- K 014.1 Compliance Policy SBB
- K 015.1 Risk Policy SBB
- K 015.3 Business Continuity Management (BCM) Policy SBB
- K 040.1 Datenschutz
- K 201.1 Regelung interner Zuständigkeiten und Verantwortungen für die operative Sicherheit (Safety & Security) bei der SBB AG
- K 232.0 Sicherheitsplanung im Hochbau

- K 250.0 Umgang mit sicherheitsrelevanten Änderungen
- K 400.16 Klassifikation von Informationen/Daten
- K 400.20 IT Governance
- K 400.22 ICT Security & Risk Management
- K 400.7 Weisung zur Informatiksteuerung im Bereich ICT Security & Risk für Industrieanwendungen

1.4.3. Konkretisierende untergeordnete Regelungen

- K 232.1 Fachspezifische Ausführungsbestimmungen zur Richtlinie K 232.0
- K 250.1 Fachspezifische Ausführungsbestimmungen zum Umgang mit sicherheitsrelevanten Änderungen
- R P 20006085 Führung der Tochtergesellschaften von SBB Personenverkehr im Bereich Security
- I-00024 Ausführungsbestimmung Risikomanagement Infrastruktur
- I-00025 Ausführungsbestimmung Risikomanagement in Investitionsprojekten
- I-00026 Ausführungsbestimmung Business Continuity Management Infrastruktur
- Weiterführende Regelungen gemäss den Kapiteln 2 und 4.

2. Security Grundsätze

2.1. Basisgrundsätze gemäss übergeordneter Regelungen

- Soweit rechtliche Vorgaben und anerkannte Standards bestehen, sind diese einzuhalten, die Compliance ist sicherzustellen.
- Die SBB strebt den Erhalt und wo möglich, die kontinuierliche Verbesserung des Sicherheitsniveaus an.
- Security ist Teil der unternehmerischen Fürsorgepflicht gegenüber unseren Mitarbeitenden und Kunden. Der Schutz der physischen und psychischen Integrität von Mitarbeitenden und Reisenden hat hohe Priorität.
- Die Linienverantwortlichen sind für den Erhalt des bestehenden Sicherheitsniveaus in ihrem Tätigkeitsbereich verantwortlich und ergreifen bei Abweichungen die erforderlichen Massnahmen. Sind verschiedene gleichwertige Massnahmen möglich, erfolgt die Wahl der Massnahme aufgrund einer Risikobeurteilung und einer Kosten-Nutzen Analyse.
- Security-Prävention steht im Zentrum und ist Teil unternehmerischen Denkens und Handelns.
- Security erfordert eine bereichsübergreifende Zusammenarbeit bei der SBB sowie mit externen Partnern. Synergiepotenziale sind konsequent zu nutzen.
- Durch Darstellung unserer Erfolge auf dem Gebiet der Security schaffen wir Vertrauen in die Sicherheit der Bahn.
- Die technischen Elemente sind so einzusetzen, damit sie den grösstmöglichen Nutzen für die Sicherheit erzielen. Technologische Innovationen schaffen zusätzlich Vertrauen.
- Die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen ist entsprechend ihrer Klassifikation zu gewährleisten. Deshalb müssen alle Informationen der SBB gemäss ihrem Verwendungszweck entsprechend klassifiziert werden.
- Bestmögliche Verhinderung von ungewollten Manipulationen oder „Angriffen“, welche Einfluss auf die Sicherheit von Informationen (Daten) der SBB haben.
- Die Betreiber von ICT der/oder für die SBB stellen je nach notwendigem Schutzbedarf die geschäftlich geforderten Informationen und die damit verbundene Verfügbarkeit der ICT Systeme sicher.
- Ein standardisiertes Informations- und ICT Risk Management sorgt für eine frühzeitige Erkennung und Bewertung von Gefahren und die Definition, Umsetzung und Überwachung der Massnahmen, d.h. eine Reduktion von Risiken bzw. schädigenden Ereignissen in Häufigkeit und Auswirkung auf ein vertretbares Mass.
- Security Massnahmen helfen mit, das Image der SBB zu erhalten und zu verbessern.
- Jeder Mitarbeitende ist für die Security mitverantwortlich.
- Die zur Umsetzung der Grundsätze notwendigen Ressourcen sind durch die Divisionen / Konzernbereiche zur Verfügung zu stellen.

2.2. Risk Management Security

Aktuell sind namentlich 2 Security-Risiken auf Stufe Konzern deponiert: a) Terroranschlag und b) Aggressionen im Bahnperimeter, welche mit der bestehenden Security-Architektur nicht mehr bewältigt werden können. Überdies betreibt P-OES fortlaufend integrales Risk Management im Rahmen der Lagebeurteilung und führt themenbezogen ein Massnahmencontrolling.

In der Informationssicherheit / ICT Security gilt die Weisung K 400.41 ICT Risk Management Policy SBB.

2.3. Security Standards

2.3.1. Öffentliche Sicherheit

Die SBB hat im Bereich der öffentlichen Sicherheit im Minimum die Vorgaben des Bundes und die in den Grundsätzen des Verwaltungsrats zu Safety und Security sowie die in der Fachbereichsrichtlinie Security definierte Sicherheitsvorgabe anzuwenden.

Die Massnahmen orientieren sich an diesen Standards sowie den Vorgaben des Bereiches P-OES:

- Kunden / Reisende: Die subjektive Sicherheit entspricht mindestens dem Sicherheitsgefühl im öffentlichen Raum.
- Bahnhöfe: Sichere, attraktive Bahnhöfe ermöglichen eine hohe Aufenthaltsqualität und erhöhen damit die Kundenzufriedenheit.
- Personal: Die Sicherheit der Mitarbeitenden erhöht deren Motivation, welche wiederum einen Einfluss auf die Servicequalität hat.
- Infrastruktur: Die Unversehrtheit und Verfügbarkeit der Infrastruktur erhöhen die Sicherheit, Kundenpünktlichkeit und das Konzernimage.
- Rollmaterial: Die Unversehrtheit und Verfügbarkeit des Rollmaterials fördert eine hohe Reisequalität, die Sicherheit der Lieferkette, die Kundenpünktlichkeit und das Konzernimage der SBB.
- Events / Grossanlässe: Die Sicherheit ist bei Grossanlässen für alle sichergestellt.

2.3.2. Informationssicherheit / ICT Security

Die SBB hat im Bereich der Informations- und ICT-Security – im Minimum – die in der Fachbereichsrichtlinie definierte Sicherheitsvorgabe bzw. Regelung des internationalen Standards/Norm ISO 27000 ff. (aktuellste Version) festgelegt. Die Massnahmen orientieren sich an deren Standards sowie den Vorgaben des Bereiches IT-SR. Die ICT Security Massnahmen sind aufgrund des technischen Fortschritts und neuer Gefährdungen laufend zu überprüfen und nötigenfalls anzupassen. Als Ergänzung zu diesem Security Handbuch sind unter Berücksichtigung der Standards weiterführende Security Vorgaben etabliert. Diese beschreiben grundlegende Rahmenbedingungen und Anforderungen an die verschiedenen Themenbereiche der Informations- und ICT Security des Unternehmens.

2.4. Security Management Systeme

Für das Security-Management, v.a. im Rahmen von Lagebeurteilung und Massnahmenplanung, ist ein gesichertes Zahlenmaterial und Steuersysteme von grosser Wichtigkeit. Neben reinen Statistikdaten (objektive Sicherheit) werden - um möglichst präzise Aussagen in Bezug auf die Lagebeurteilung machen zu können - auch Informationen über das subjektive Sicherheitsempfinden von Mitarbeitenden und Kunden miteinbezogen.

Das übergeordnete Ziel der Security Management Systeme ist es, auf Stufe Gesamtunternehmung einen Überblick über das sicherheitsrelevante Geschehen im Bereich Security zu schaffen. Dazu werden Informationen beschafft, erfasst und anschliessend ausgewertet bzw. analysiert. . Aufgrund der Analysen werden Konsequenzen abgeleitet und der Handlungsbedarf mit zielführenden Massnahmen definiert. Massnahmen werden im baulichen, technischen und organisatorischen Bereich getroffen. Speziell wird darauf geachtet, dass auch präventive Massnahmen ergriffen werden.

Im Rahmen des Controllings wird beurteilt, ob die Security-Ziele erreicht wurden. Darauf basierend wird der weitere Handlungsbedarf abgeleitet. Dieser Abgleich ist integraler Bestandteil des Risk Managements Security sowie des ICT Risk Managements.

Die bei den SBB anzuwendenden Security Management Systeme legen fest, mit welchen Instrumenten und Methoden das Management die auf Security und Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (regelt, plant, einsetzt, durchführt, überwacht und verbessert). Zur Ermittlung der objektiven Sicherheit wird u.a. auf die ESQ-Datenbank (Ereignisse Sicherheit & Qualität) zurückgegriffen.

2.5. Dokumentation und Meldung von Sicherheitsereignissen

Alle Security-Ereignisse müssen von den Mitarbeitenden der Divisionen und Konzernbereiche rasch möglichst (innerhalb 24 Stunden) in den offiziell dafür vorgesehenen Datenbanken (ESQ) erfasst werden. Der Meldeweg (wer meldet wann, was, wem) vom Feststellen eines Security-Ereignisses zur Erfassungsstelle sowie das Kontrollwesen müssen in den Organisationseinheiten der Divisionen und Konzernbereichen benutzerspezifisch geregelt werden (Linienaufgabe). Die Mitarbeitenden sind entsprechend zu sensibilisieren und zu instruieren.

2.6. Kommunikation zur Security

Jegliche kritische Kommunikation zum Thema Security – insbesondere zu Ereigniszahlen Security - ist je nach Aufgabenbereich durch den Leiter Öffentliche Sicherheit bzw. den Chief Information Security Officer (CISO) zu bewilligen. Für die „normale“ interne Kommunikation bezüglich Fragen der Security sind die Divisionen und Konzernbereiche in Ihrem Bereich selber zuständig.

Für die kritische interne und die gesamte externe Kommunikation von Security-Aspekten, insbesondere der Umgang mit Medienschaffenden, ist grundsätzlich der Konzernbereich Kommunikation zuständig und verantwortlich. Bei der Kommunikation gegen aussen betreiben die SBB bezüglich Security-Ereignissen eine zurückhaltende Informationspolitik, damit die von den Tätern erwünschte Publizität nicht eintritt und keine Nachahmungstäter animiert werden. Anfragen von Journalisten sind immer an den Konzernbereich Kommunikation, die Kommunikationsbereiche der Divisionen oder an eine der regionalen Medienstellen der SBB weiterzuleiten.

2.7. Waffentragverbot

Den Mitarbeitenden ist es grundsätzlich untersagt, während der Arbeitszeit Waffen gemäss eidgenössischer Waffenverordnung zu tragen. Für die Transportpolizei sowie für

den Objektschutz ist das Tragen und der Einsatz von Waffen speziell geregelt[1]. Grundsatzfragen sind an die Öffentliche Sicherheit oder an die Security-Beauftragten der Divisionen zu richten.

Themengebiet	Wer	Ablage
Waffentragverbot	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll?func=ll&objId=27306445&objAction=browse

3. Organisation und Geschäftsordnung

3.1. Fachliche Zuständigkeitsbereiche

3.1.1. Öffentliche Sicherheit (Public)-Security

Die Öffentliche Sicherheit setzt sich für den Erhalt und die kontinuierliche Verbesserung des Sicherheitsniveaus zum Schutz von Kunden, Mitarbeitenden und Dritten ein . Dies u. a. durch eine laufende Lagebeurteilung und die Festlegung von verbindlichen Security-Zielen, welche die Security-Kultur im gesamten Konzern fördert. .

P-OES beschäftigt sich im Rahmen der Konzernaufgabe mit der Konzeption und Koordination baulicher, technischer und organisatorischer Security-Massnahmen für die Divisionen und Konzernbereiche. Zwischen P-OES und den Security-Beauftragten der Divisionen findet eine enge Abstimmung statt (keine Fachführung).

3.1.2. Informationssicherheit / ICT-Security

Die Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken mit Bezug auf die Informationsverarbeitung. Sie hat den Schutz von Informationen zum Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die ICT Sicherheit beschäftigt sich hauptsächlich mit dem Schutz elektronisch gespeicherter Informationen sowie deren Verarbeitung und Übertragung (Kommunikation). Hierbei sind die klassischen Grundwerte der Informations- und ICT-Security „Vertraulichkeit, Integrität und Verfügbarkeit“ die Grundlagen für ihren Schutz. ICT-Security wird als Teilgebiet der Informationssicherheit behandelt.

Die Fachführung durch ICT Security ermöglicht eine weitgehend homogene Sicht und Behandlung der ICT Risikolandschaft für die bei den SBB eingesetzten informationsverarbeitenden Einrichtungen. Daher werden bei den grundsätzlichen Vorgaben der ICT Security keinerlei Unterscheidungen zwischen den Geschäftsanwendungen sowie den Industrieanwendungen (einschliesslich aller bahnspezifischen Anwendungen) vorgenommen. Für alle informationsverarbeitenden Einrichtungen gilt, dass die aktuellste Version des ISO 27000 ff. im Sinne einer homogenen Basis einzuhalten und bei Bedarf zu ergänzen ist. Aufgrund hoheitlicher (gesetzlicher) Vorgaben sowie den besonderen funktionalen Anforderungen an Industrieanwendungen ist es aber auch sinnvoll, konkrete Anforderungen dieser Anwendungen getrennt von den Geschäftsanwendungen SBB zu behandeln.

[1] Die Angehörigen der Transportpolizei benötigen in Ausübung des bewaffneten Dienstes keine Waffentragbewilligung (Waffengesetz G 514.54, Art 2). Für den Objektschutz gelten die normalen gesetzlichen Grundlagen des Waffengesetzes, eine Waffenprüfung sowie ein Waffentragschein sind zwingend notwendig.

Die Richtlinie zur Informatiksteuerung im Bereich ICT Security & Risk (K 400.22) wird daher durch Weisung zur Informatiksteuerung im Bereich ICT Security & Risk für Industrieanwendungen (K 400.7) ergänzt.

Ausgehend von diesen beiden Regelungen werden weiterführende verbindliche Vorgaben erstellt.

Die Betriebsverantwortlichen der Linie sind für die Einhaltung der Sicherheit und Umsetzung der Sicherheitsvorgaben verantwortlich.

3.1.3. Abgrenzung zur Krisenorganisation - Security bei Ereignissen

Normale Lage

Es gelten die Prozesse und Strukturen gemäss Organisations- und Geschäftsreglement (OGR).

Erhöhte Risikolage durch Grossanlässe oder *diffuser Bedrohung*

Es besteht ein erhöhter Informationsbedarf und Koordinationsaufwand bei der Security. In diesem Fall wird durch die Öffentliche Sicherheit ein Lagezentrum betrieben. Das Security Lagezentrum SELAZ wird in diesem Fall in das Lagezentrum integriert. Je nach Bedarf werden weitere interne und externe Stellen miteinbezogen. Es gelten die Prozesse und Strukturen gemäss Organisations- und Geschäftsreglement (OGR).

Krisenlage

Der SBB-Krisenstab übernimmt die Verantwortung für die Geschäftstätigkeit, sofern die normalen Prozesse und Strukturen für eine erfolgreiche, zeitgerechte Bewältigung nicht mehr genügen. Der Bereich Security ist im Krisenstab integriert.

3.2. Aufgaben und Kompetenzen

3.2.1. Aufgaben Öffentliche Sicherheit

Auf Stufe Konzern steht P-OES dem CEO zur Steuerung, Koordinierung und Kontrolle der öffentlichen Sicherheit zur Verfügung. Die Konzernaufgabe der Organisationseinheit Öffentliche Sicherheit beinhaltet:

- den Betrieb eines bereichsübergreifenden Securitymanagementsystems entlang der Gremienstruktur und Erlass des Security Handbuches K 030.1. Dieses enthält die unternehmensweit gültigen Anweisungen und Richtlinien, welche die minimalen Anforderungen festlegen.
- Erstellen des Securityprogramms (Ziele & Massnahmen) in Zusammenarbeit mit den Divisionen (Besteller) entlang der MUP-Periode.
- Sammeln, Bewerten und Auswerten von externen und internen Informationen zur Sicherheitslage und -entwicklung.
- Führung Risk Management Security und Terrorprävention.
- Führung der Konzernfachstellen Betriebskriminalität, Fälschung und Betrug, Video und Sicherheit Fantransporte sowie Verantwortung eines Bedrohungsmanagements.
- Fachlich Steuern, Informieren und Beraten der Security-Beauftragten der Divisionen.
- Erarbeiten von Sicherheitskonzepten in Abstimmung mit den betroffenen Geschäftsbereichen sowie Mitwirken an übergreifenden Sicherheitskonzepten (Safety / Security).
- Herbeiführen von zeitkritischen Entscheidungen für die Abwehr von Gefahren und Wiederherstellung des Regelzustandes.

- Vertreten der Interessen der SBB in Security-Angelegenheiten gegenüber Behörden, Verbänden und internationalen Securityorganisationen der Bahnen.
- Unterstützen der Konzernkommunikation bei der Öffentlichkeitsarbeit in Security-Fragen.
- Berichterstattung an den CEO und die KL SBB.

3.2.2. Aufgaben Informationssicherheit / ICT Security

Auf Stufe Konzern steht das ICT Security & Risk Management (IT-SR) dem CEO zur Steuerung, Koordinierung und Kontrolle der Information und ICT Security zur Verfügung. Konkret geht es um

- den Betrieb eines bereichsübergreifenden Sicherheitsmanagementsystems (ISMS) und den Erlass der entsprechenden Teile des Security Handbuchs K 030.1. Diese enthalten die unternehmensweit gültigen Anweisungen und Richtlinien, welche die minimalen Anforderungen festlegen.
- die konzernweite fachliche Führung des ICT Security & Risk Managements inkl. Initialisierung, Erstellung und Nachführung von Vorgaben, Strategien, Konzepten, Aktionsplänen, Merkblättern und Sicherheitsregeln.
- die Erstellung des ICT Security Programms mit Zielen und Massnahmen.
- die Auswertung und Beurteilung von externen und internen Informationen zur Informationssicherheitslage (z.B. Provider, MELANI, etc.).
- das Vertreten der Interessen der SBB in Information- und ICT Security-Angelegenheiten gegenüber Behörden, Verbänden sowie nationalen und internationalen Security Organisationen der Bahnen.
- die Unterstützung der Konzernkommunikation bei der Öffentlichkeitsarbeit im Bereich der Thematik Informationssicherheit bzw. ICT Security.
- die Koordination und Beauftragung von allen ICT (Security) Audits.
- die Führung *(als einzige Abteilung bei der SBB)* einer ICT Forensik Abteilung.
- die Erarbeitung von Präventionskonzepten, Kommunikations- und Sensibilisierungskonzepten (inkl. der Durchführung von konzernweiten Awareness Kampagnen).
- die Führung des IT Continuity Managements (IT Notfall-Managements) und Mitglied im SBB Krisenstab.
- die Berichterstattung an den CEO und die KL SBB.

3.2.3. Aufgaben Divisionen / Konzernbereiche

Die Divisionen und Konzernbereiche sind verantwortlich für die Security (inkl. der Informationssicherheit) in ihrem Bereich und stellen die notwendigen Mittel zur Verfügung. Die zuständige Organisationseinheit (Linie) ist verantwortlich für die Einhaltung der in den Weisungen definierten Security-Vorgaben. Zur Unterstützung der Linie setzen die Divisionen Security-Beauftragte ein.

Die Hauptaufgaben der Security-Beauftragten sind:

- Unterstützung bei der Gefahrenabwehr entsprechend den speziellen Erfordernissen der ihnen zugeordneten Divisionen unter Berücksichtigung der Security-Standards.

- Einleiten von Massnahmen zur Verbesserung des subjektiven Sicherheitsempfindens der Reisenden, Kunden und Mitarbeitenden in Abstimmung mit der Öffentlichen Sicherheit und/oder IT-SR.
- Regelmässiges Auswerten der Sicherheitslage und Erarbeiten von Vorschlägen für lageangepasste Massnahmen an die Öffentliche Sicherheit, an Informations- und ICT Security und an das eigene Management.
- Erarbeiten von Sicherheitskonzepten (Security) für alle Arten von Anlagen / Systeme des Geschäftsbereiches unter Zugrundelegung konzerneinheitlicher Sicherheitsstandards und Mitwirkung an übergreifenden Sicherheitskonzepten.
- Zusammenarbeit mit den Organisationseinheiten des Geschäftsbereiches, mit den anderen Geschäftsfeldern sowie mit der Öffentlichen Sicherheit und / oder IT-SR auf zentraler Ebene in Security-Angelegenheiten.
- Zusammenarbeit mit Sicherheitsbehörden und Sicherheits- und Ordnungsdiensten in ressortbezogenen Angelegenheiten.
- Fachbezogene Umsetzung von Security-Massnahmen im Verantwortungsbereich.
- In Arbeitsgruppen und Fachgremien mit sicherheitsspezifischen Aufgaben und Schnittstellen zur ICT sind Vertreter der Information und ICT-Security angemessen zu beteiligen.

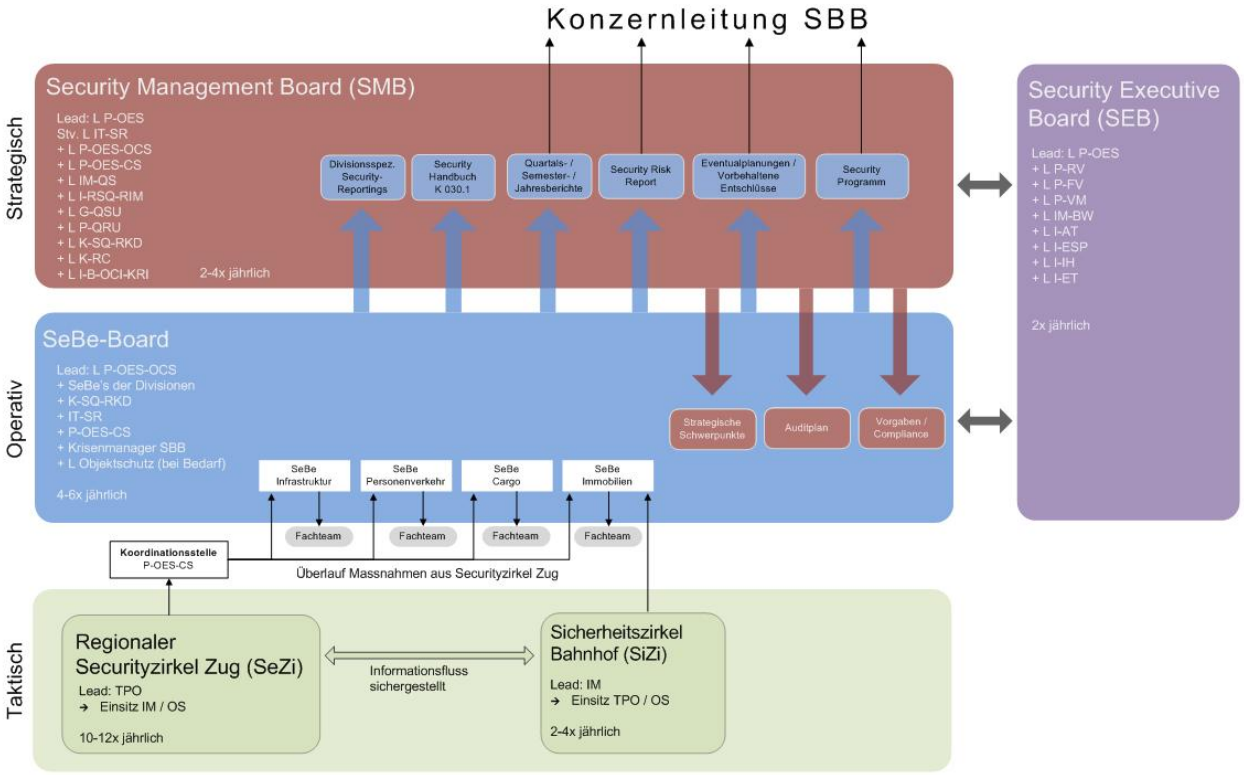
3.2.4. Aufgaben von ICT Betriebseinheiten (z.B. SBB IT & SBB Telecom)

Einleiten von Massnahmen, v.a. technischer Art (inkl. der Erstellung der detaillierten Spezifikationen) zur Verbesserung der Erstellungs- und / oder betrieblichen Sicherheit von Prozessen, Systemen, Netzen in Abstimmung mit ICT Security & Risk Management. Die operativen Entwicklungs- und Betriebseinheiten haben dafür die notwendigen Ressourcen bereitzustellen.

3.3. Gremien (Plattformen)

Die nachfolgende Gremienstruktur Security wurde am 25.02.2014 durch den Lagerapport Security (bis dato höchstes Security-Fachgremium der SBB) verabschiedet. Zur einheitlichen, durchgehenden und nachvollziehbaren Führung sowie Umsetzung der Security im Unternehmen sind basierend auf den Handlungsebenen verschiedene Gremien aufgesetzt. Der Hauptdrehpunkt bzw. das Hauptkoordinationsgremium in der Security, welches die strategischen Ziele und lagebedingten operativen Tätigkeiten koordiniert, ist das Board der Security-Beauftragten (SeBe-Board).

Die Handlungsebenen und Aufgaben setzen sich wie folgt zusammen:



Zur Schaffung eines SBB-weiten einheitlichen Sicherheitsstandards sowie zur Koordination eines konzerneinheitlichen Vorgehens bei Security Regulationen (inkl. gängiger Normen und Standards), Strategien, Programmen und Audits wird das Security Management Board (SMB) eingesetzt. Das SMB ist das oberste Fachgremium der SBB, welches sich mit allen grundlegenden strategischen Fragen der Security befasst. Ziel des Gremiums ist die verbindliche Sicherung der Grundlagen eines konzerneinheitlichen Vorgehens hinsichtlich aller Aktivitäten im Bereich Security. Über dieses Gremium finden nötigenfalls die übergreifenden Absprachen und Themenzuordnungen mit der Safety (analog ZSQA) statt. Die Ausarbeitung normativer Vorgaben, Strategien sowie Einzelaufgaben und strategische Programme (Security Programm) werden an das SeBe-Board zur Steuerung, Koordination und Umsetzung übergeben. Die taktische Umsetzung der Security obliegt den regionalen Securityzirkeln "Zug" sowie den Sicherheitszirkeln an ausgewählten Bahnhöfen. Auf operativer und taktischer Stufe können bei Bedarf permanente oder befristete Fachgremien zur Bearbeitung spezifischer Fragestellungen eingesetzt werden.

Im Bereich Informationssicherheit / ICT Security entscheidet der CISO oder der CIO der SBB, welche Themen durch welches Gremium oder durch welche Organisationseinheit behandelt und/oder freigeben werden.

3.4. Notfallstab Security

Im Rahmen des SBB Krisenmanagements und unter Einbezug der Security-Gremienstruktur betreibt P-OES einen Notfallstab Security. Der Notfallstab Security setzt sich zusammen aus dem Operation Center Security (Securitylage und konzernweite Massnahmen) und dem Führungsstab SBB Transportpolizei (operatives Polizeigeschäft).

3.5. Integraler Security-Bestellprozess

Mit der KL BV „Integraler Bestellprozess Onesecurity“ vom 26.11.2013 wurde u.a. eine integrale Sicherheitsplanung, Leistungsbestellung und Sourcing-Strategie beschlossen.

Die Sicherheitsplanung wird lageorientiert getrieben und geht von bestellerorientierten Zielbildern aus. Sie verknüpft bauliche, technische, organisatorische und personelle Massnahmen zu ganzheitlichen Security-Lösungen. Um Redundanzen zu vermeiden, werden die Bestellungen für Leistungen von Einsatzkräften zentral über die SBB Transportpolizei abgewickelt. Ausnahme bilden die Leistungen der SECURITRANS, die aufgrund des überwiegenden Safety-/Objektschutzanteils an Bahnhöfen weiterhin von Immobilien direkt mandatiert werden. Unter Führung der SBB Transportpolizei werden die Leistungen aller Einsatzkräfte im SBB-Perimeter integral geplant. Dadurch soll verhindert werden, dass Security-Leistungen mehrfach oder überlappend bestellt werden (Ressourcenallokation).

4. Regelungsbereiche Security

4.1. Überblick über alle fachlichen Regelungsbereiche

In den folgenden Kapiteln werden fachliche Grundsätze, Ziele und weiterführende Regelungen zu einzelnen Themengebiete festgelegt.

Kapitel	Themengebiet
4.2	Verhaltensrichtlinien
4.3	Informationssicherheit / ICT-Security
4.4	ICT Forensik
4.5	Videosysteme
4.6	Fachstelle Betriebskriminalität
4.7	Fachstelle Fälschung und Betrug
4.8	Planungsrichtlinien für Gebäude und Anlagen
4.9	Schliesssysteme und Zutrittsregelung
4.10	Notfallkonzept Gebäude
4.11	Bombendrohung / Bombenalarm / verdächtige Gegenstände
4.12	Vandalismus und Sabotage
4.13	Sicherheit Betriebs- und Fahrpersonal
4.14	Transportpolizei
4.15	Nationales Entführungsalarmsystem (fedpol)
4.16	Externe Sicherheitsdienstleister
4.17	Transport und Aufbewahrung von Werten
4.18	Sicherung von Transporten gefährlicher Güter

4.2. Verhaltensrichtlinien

4.2.1. Grundsätze

In der Planung von Sicherheitsmassnahmen im Bereich Security steht der Personenschutz im Vordergrund. Die Wahrung der eigenen Sicherheit hat immer Priorität (Unternehmensphilosophie). Klassische Beispiele für Risiken, bei denen das leibliche Wohlergehen der Mitarbeitenden, aber auch von Reisende gefährdet sein kann, sind Raubdelikte, Drohungen und Nötigungen, Körperverletzungsdelikte und Ähnliches. Um solche Risiken möglichst niedrig zu halten, sind Verhaltensempfehlungen präventiv und reaktiv (rückwirkend) angebracht.

Mit sinnvollen und zeitgemässen Verhaltensempfehlungen sollen Angriffe gegen das Leben und die körperliche Unversehrtheit der Mitarbeitenden, schlussendlich aber auch von Reisenden, verhindert oder zumindest erschwert werden.

Neben der Gestaltung des Arbeitsplatzes sowie baulichen und technischen Schutzeinrichtungen werden auch der Sicherheit in Arbeitsabläufen grosses Gewicht beigemessen (Arbeitsgesetz / GAV).

Die Verhaltensschulung der Mitarbeitenden in Bezug auf:

- Motivation
- Stärkung des Sicherheitsbewusstseins
- Kenntnis der relevanten Sicherheitsvorschriften
- Kenntnis der örtlichen Sicherheitsmassnahmen
- Kenntnis der aktuellen Risiken und Gefahren
- Kenntnis der eigenen Möglichkeiten in aussergewöhnlichen Situationen

ist ein laufender Prozess im Bereich Security.

4.2.2. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Arbeitsbeginn / Arbeitsschluss	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120859
Verhalten in sensiblen Räumlichkeiten / Gebäuden	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120856
Verhalten in Kassenstellen	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120865
Billettautomaten / Entwerter / Schliessfachanlagen und Münzwechselautomaten	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120858
Bewirtschaftung von Geldausgabeautomaten	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120861
Umgang mit Wertpapier	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120862
Alarmdisposition in Kassenstellen	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120857
Kassenstellen-Audits	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120864

4.3. Informationssicherheit / ICT Security

4.3.1. Grundsätze

Informationen und Daten dürfen grundsätzlich nur für den Zweck, für den sie bestimmt sind, verwendet werden.

- Die Sorgfalt, der Aufwand für den Umgang mit und die Aufbewahrung von Informationen richten sich nach den Risiken von Informationsabflüssen und Informationsverlusten. Dies betrifft neben der externen auch die interne Weitergabe von Informationen.
- Informationssicherheit betrifft alle Aspekte der Kommunikation. Sie verpflichtet auch in nicht geregelten Situationen Informationen zu schützen in analoger Anwendung der in diesem Reglement verankerten Vorgaben.
- Betrifft die Informationssicherheit Interessen des Datenschutzes, so ist besondere Sorgfalt geboten. Vor allem sind diesbezüglich nur Technologien (Software) zu verwenden, mit welchen die Vorgaben des Datenschutzes eingehalten werden können.

Der Einsatz von ICT-Systemen sowie die Bearbeitung elektronischer Daten muss innerhalb der gesetzlichen, vertraglichen und internen Bestimmungen erfolgen. Es darf weder gegen Rechte und Ansprüche von Mitarbeitenden und Dritten, noch gegen Rechtsvorschriften verstossen werden. Bei der elektronischen Bearbeitung von Informationen und der Benutzung von ICT Systemen sind insbesondere das Datenschutzgesetz (DSG) und das Urheberrechtsgesetz (URG) sowie die Tatbestände bezüglich Datenmissbrauchgemäss Strafgesetzbuch (StGB) sowie spezielle Nutzungsrechtsbestimmungen zu beachten.

Das Sicherheitsbewusstsein der Mitarbeitenden und ihre Bereitschaft, ihren Beitrag zum Erreichen und Erhalten des Sicherheitsstandards zu leisten, sind Voraussetzungen für den Unternehmenserfolg. Ihre kritische Aufmerksamkeit und ihr eigenverantwortliches Handeln sind die wirksamsten Sicherheitsmassnahmen. Sämtliche Mitarbeitenden sind für die Sicherheit verantwortlich und verpflichtet, durch ihr eigenverantwortliches Verhalten ihren Anteil zur Informationssicherheit zu leisten. Sie kennen die Sicherheitsziele der SBB und handeln nach diesen.

Die dauerhafte Unternehmenssicherheit wird unterstützt durch organisatorische, personelle, prozessorientierte und technische Massnahmen. Durch das Bearbeiten von Informationen dürfen keine Persönlichkeitsrechte verletzt werden. Die SBB begegnet der Verbreitung von rassistischem Gedankengut, Gewaltdarstellungen und Pornographie sowie anderen illegalen Inhalten konsequent und umfassend.

4.3.2. Ziele

Die SBB verfolgt folgende generellen Informationssicherheitsziele:

- Um die Dienstleistungen gegenüber Kunden und Partnern erbringen zu können, wird im Rahmen der Sicherheitsvorgaben und des Vertretbaren die geschäftlich geforderte Verfügbarkeit der Informationen sichergestellt.
- Die Integrität, die Konsistenz und der Schutz von Information sind entsprechend ihrer Klassifikation zu gewährleisten. Deshalb sind alle Informationen der SBB entsprechend ihrem Verwendungszweck zu klassifizieren. Die Klassifikation muss regelmässig und nach relevanten Veränderungen durch den Informationseigner überprüft werden.
- Ein standardisiertes Information Risk Management sorgt für eine frühzeitige Erkennung und Bewertung von Gefahren und definiert die Umsetzung sowie Überwachung der Massnahmen.

- Ein einheitliches Vorgehen bei Betriebsstörungen sorgt für ein schnellstmögliches Zurückkehren in den normalen Betriebszustand. Für den Fall des Auftretens katastrophaler Ereignisse werden adäquate Massnahmen vorbereitet, die eine Sicherstellung der Geschäftstätigkeit innerhalb von 24 Stunden und bis zur Rückkehr zum normalen Betriebszustand gewährleisten.
- Informationssicherheits-Massnahmen helfen mit, das Image der SBB zu erhalten und zu verbessern.
- Für ICT-Systeme der operativen Bahnbetriebsführung, die sicherheitsrelevante Aufgaben übernehmen, sowie für Steuerungssysteme im Bahnbetrieb und der Energieversorgung gelten zusätzlich spezielle und ergänzende Weisungen und Richtlinien, welche jedoch den Informationssicherheitsgrundsätzen der SBB, den Standards nicht widersprechen bzw. diese Sicherheitsbestimmungen nicht unterschreiten dürfen (siehe Kapitel 3.1.2).
- Die Informationssicherheits-Massnahmen sind aufgrund des technischen Fortschritts und neuer Gefährdungen laufend anzupassen.

4.3.3. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
ICT Risk Management	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132397
ICT Risk Management Policy	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll?func=doc.Fetch&nodeid=26248840
Anlagewertmanagement	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132403
Personalsicherheit	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132401
Physische und umfeldbedingte Sicherheit	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132394
Kommunikations- und Betriebsmanagement	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132396
Zugangskontrollen	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132395
Systembeschaffung, -entwicklung und -wartung	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132399
Vorfall Management in der Informationssicherheit	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132398
Unternehmenskontinuitätsmanagement	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132404
Erfüllung Compliance / Audits und Reviews	IT-SR	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132400

4.4. ICT Forensik

4.4.1. Grundsätze

Der Einsatz von ICT-Systemen sowie die Bearbeitung von elektronischen / digitalen Daten hat innerhalb der gesetzlichen, vertraglichen und internen Bestimmungen zu erfolgen. Mit der immer weiteren Digitalisierung der Geschäftsprozesse nehmen auch die Gefahrenbereiche immer mehr zu. Die ICT Forensik des ICT Security & Risk Managements (IT-SR) unterstützt hier und stellt federführend sicher, dass elektronische / digitale Evidence[2] bei intern oder extern gemeldeten Vorfällen korrekt erhoben wird, die Compliance sichergestellt werden kann und Security Incidents / Weisungsverstösse untersucht und Massnahmen getroffen werden können. In der Regel sind dies Gesetzes-, Vertrags- oder Weisungsverstösse im Zusammenhang mit ICT Systemen.

Die Untersuchung dieser Verstösse erfordern die Anwendung von Methoden und Verfahren der ICT Forensik.

4.4.2. Ziele / Aufgabe

- ICT Forensik, als Bereich innerhalb ICT Security & Risk Management, arbeitet über definierte Schnittstellen und Prozesse mit den entsprechenden Fachbereichen, insbesondere der Fachstelle Betriebskriminalität, zusammen.
- Es wird gewährleistet, dass elektronische / digitale Evidence so erhoben / sichergestellt wird, dass diese gerichtsverwertbar ist und dort im Beweisverfahren als Beweis anerkannt wird. Der Bereich ICT Security & Risk Management (IT-SR) verfügt dazu über die notwendigen Berechtigungen.
- Die ICT Forensik hilft den Fachbereichen der SBB bei der Aufarbeitung von Vorfällen, die mittels ICT Systemen begangen wurden. In einer direkten Zusammenarbeit mit dem Strafrechtzentrum und Arbeitsrecht ist sichergestellt, dass Fristen bei externen Untersuchungen und Rahmenbedingungen aus Arbeitsverträgen eingehalten werden.
- Erkenntnisse aus den Untersuchungen der ICT Forensik werden mit dem Fachbereich besprochen und wo nötig mit Abklärungen im Fachbereich abgestimmt / zusammengeführt. Das weitere Vorgehen wird dann gemeinsam definiert.

4.4.3. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch K 030.1:

Themengebiet	Wer	Ablage
Organisation, Aufgaben, Kompetenzen und Verantwortlichkeiten der ICT Forensik.	IT-SR	*https://dms.sbb.ch/OTCS/llisapi.dll/open/26415356*

[2] Unter Evidence werden Spuren verstanden, die auch vor Gericht gebraucht werden können und auf nachvollziehbare / wiederholbare Form erhoben wurden.

4.5. Videosysteme

4.5.1. Grundsätze

Die SBB setzt die Videoüberwachung gemäss Geltungsbereich der Videoüberwachungsverordnung des öffentlichen Verkehr (VüV-ÖV) angemessen und verhältnismässig zum Schutz von Personen und Werten innerhalb der Infrastruktur (Bauten, Anlagen, Einrichtungen) und in Schienenfahrzeugen der SBB ein. Sie gehört als integraler Bestandteil zu einem ausgewogenen, verhältnismässigen Securitykonzept. Im Vordergrund steht die Prävention. Die Videoaufzeichnung ermöglicht bei Vorfällen, Ermittlungsansätze zu liefern. Die vollständige Compliance mit den gesetzlichen Vorschriften und den internen Richtlinien muss erfüllt sein. Die SBB ist gegenüber dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hinsichtlich Aufzeichnungsdauer und Nutzer jederzeit auskunftsfähig.

4.5.2. Ziele

Die Installation für Securityzwecke muss in jedem Fall, basierend auf einer Risikodefinition und –analyse, in einem Einsatzkonzept dargelegt und begründet werden. Videoüberwachungssysteme, welche die Safety und betrieblichen Ziele erreichen sollen, sind in einem Einsatzkonzept, ohne Risikodefinition und –analyse, darzulegen und zu begründen.

- Security-Ziele:
  - Personenschutz (Mitarbeitende, Reisende, Kunden und deren Sachen)
  - Objektschutz (Rollmaterial, Gebäudesicherheit, technische Anlagen, Vandalismus, Littering, Zutrittskontrollen, etc.)
  - Wertschutz (Diebstahl von Waren / Güter, Geldbestände, Wertgegenstände in Verkaufsanlagen), Schutz von Automaten (Billettautomaten, Bancomaten, Geldwechsler etc.), Schalter, Reisezentren
  - Steuerung Kundenströme / Kundenlenkung (Einsatzplanung bei Grossereignissen)
- Safety-Ziele sind z.B.:
  Entgleisungen und Zusammenstösse verhindern, Unfälle Reisender und Dritter verhindern (Perron, Gleisüberschreitungen, etc.), Arbeitsunfälle verhindern, Tunnelsicherheit erhöhen, Anlagen- und Gebäudeverfügbarkeit (z.B. Brandschutz), Ladegutverluste und die Überwachung von technischen Abläufen (z.B. Schutz vor Naturrisiken, Kraftwerkeinläufe, Schienenmessungen).
- Betriebliche Ziele sind:
  Betriebsführung, Zugsabfertigung, Kundenlenkung / Fahrgastzählungen und Unterstützen der Ereignisdienste zur Bewältigung von Ereignissen

4.5.3. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Video Policy	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132365
Planungs- und Betriebsrichtlinie Videosysteme	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132364
Vorlage Einsatzkonzept	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll?func=ll&objId=29540383&objAction=browse
Vorlage Risikobeurteilung & -analyse	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll?func=ll&objId=29542296&objAction=browse

4.6. Fachstelle Betriebskriminalität

4.6.1. Grundsätze

In Zusammenarbeit mit der Falluntersuchungsstelle SBB führt die Fachstelle Betriebskriminalität bei Verdacht auf betriebsinterne kriminelle Handlungen Ermittlungen durch und definiert dadurch Massnahmen zur Schliessung von Sicherheitslücken.

Zudem ist die Fachstelle für das Bedrohungsmanagement zuständig. Zum Management von Konflikt-, Bedrohung- und Gewaltsituationen braucht es eine Bündelung von Fachwissen, eine interprofessionelle Vernetzung und eine klare Verteilung von Verantwortlichkeiten.

Anonyme Hinweise über illegale Tätigkeiten können der Compliance-Meldestelle http://compliance.sbb.ch weitergeleitet werden. Gemeldete Vorfälle werden nach einem standardisierten Prozess entgegengenommen und untersucht. Alle gelieferten Informationen, einschließlich der Identität des Hinweisgebers, werden streng vertraulich behandelt. Meldungen können auch anonym abgegeben werden.

4.6.2. Ziele

Beweissicherung und Durchführung interner Ermittlungen. Massnahmendefinition zur Schliessung von erkannten Sicherheitslücken & Koordination bei Drohungen gegenüber exponierten Abteilungen und Führungskräften (bspw. HR, etc.).

4.6.3. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Organisation, Aufgaben, Kompetenzen und Verantwortlichkeiten der Fachstelle Betriebskriminalität	P-OES	*https://dms.sbb.ch/OTCS/llisapi.dll/open/25120849*
Compliance Meldestelle	K-RC-CCO	*https://dms.sbb.ch/OTCS/llisapi.dll/open/45702392*
Schaden- und Strafrechtzentrum SBB Falluntersuchungsstelle	F-VMT-SZ	*https://dms.sbb.ch/OTCS/llisapi.dll/open/58218430*

4.7. Fachstelle Fälschung und Betrug

4.7.1. Grundsätze

Mit Hilfsmitteln wie Multifunktionsgeräten, Farbfotokopierern, Scannern und EDV-Verarbeitungsprogrammen sowie einer Vielzahl von Druckmöglichkeiten stellen potenzielle Straftäter qualitativ gute Fälschungen von Formularen, Dokumenten, Zahlungsmitteln oder Fahrausweisen her (bei der Kontrolle ist der „erste Eindruck“ einer Fälschung meistens gut).

Weiterführende Informationen zum Thema Fälschungen und Betrug:

- Infoportal öV
- Checklisten ZP
- Intranet-Seite P-OES, Corporate Security, Fälschung / Betrug

4.7.2. Ziele

Qualifizierte Straftaten im Bereich Urkundenfälschung / Betrug (Fahrausweise, Grundkartenausweise, persönliche Ausweise, Checks), Geldfälschung (Noten und Hartgeld) sowie betrügerischer Missbrauch von Fahrausweisen, Grundkartenausweisen und persönlichen Ausweisen werden bei der Fachstelle Fälschung / Betrug (P-OES) zentral bearbeitet.
Das weitere Vorgehen wird in enger Zusammenarbeit mit dem Schaden- und Strafrechtzentrum, P-VM, P-VS und der zentralen Einnahmensicherung (ZES) koordiniert. Eine Strafanzeige erfolgt ausschliesslich durch das Strafrechtzentrum.

4.7.3. Weiterführende Regelungen

Themengebiet	Wer	Ablage
Vorschriften über die Zahlungsmittel, V 545	P-VS	http://infoportal.sbb.ch/content/infoportal/de/desktop/home/angebote-und-tarife.tarifsystem.html/tarife/2471.html
Checkliste für die Fahrausweiskontrolle, Tarif 690	VöV	http://infoportal.sbb.ch/content/infoportal/de/desktop/home/angebote-und-tarife.tarifsystem.html/angebote/6076.html
Handbuch Fahrausweiskontrolle, Tarif 695	VöV	http://infoportal.sbb.ch/content/infoportal/de/desktop/home/angebote-und-tarife.tarifsystem.html/angebote/695-handbuch-fur-die-fahrausweiskontrolle/5063.0.html

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Fahrausweisfälschungen	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132455
Falschgeld	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132454

4.8. Planungsrichtlinien für Gebäude und Anlagen

4.8.1. Grundsätze

Die erfolgreiche Integration aller Sicherheitsaspekte in Bau- und Umbauprojekten bedingt ein systematisches Herleiten der erforderlichen Schutzmassnahmen. Die Voraussetzung dafür ist das rechtzeitige Einbinden der Sicherheitsaspekte schon zu Beginn des Planungsprozesses. Nur so kann ein Kosten-/Nutzen-optimiertes, den Schutzbedürfnissen entsprechendes Sicherheitsniveau erzielt werden.

Die detaillierte Vorgehensweise, entsprechend nach den Bauphasen nach SIA 112 ist in der Weisung K 232.1 – Fachspezifische Ausführungsbestimmungen zur Richtlinie K 232.0 „Sicherheitsplanung im Hochbau“ (Neubau, Umbau, Instandsetzung und Umnutzung) erläutert. Die Berücksichtigung der nachfolgenden Planungsgrundsätze bezüglich baulicher, technischer und organisatorischer Schutzmassnahmen müssen für Neu- und Umbauprojekte eingehalten werden. Das Versicherungsmanagement SBB verlangt einen adäquaten Schutz der versicherten Sachen. Werden diese Bestimmungen nicht eingehalten, kann der Versicherer die Entschädigung kürzen oder verweigern. Die Grundlage dazu bildet das vorliegende Regelwerk. Kompetenz zur Beurteilung der Adäquanz i. S. Security wurde vom Versicherungsmanagement an P-OES delegiert.

1. Frühzeitige Sicherheitsplanung
   Diese erfolgt auf Basis der mit den Sicherheitsspezialisten ausgearbeiteten Rahmenbedingungen. Die Sicherheitsvorgaben mit ihren Schutzmassnahmen (inkl. Schliesssystem) werden nahtlos in ein Gesamtkonzept (Bau-, Umbauprojekt) integriert und müssen bereits ab der ersten Planungsphase Bestandteil der Pflichtenhefte / Vorgaben (Architekten- und/oder Ingenieurwettbewerb) sein.
2. Schutzziele nach Risiken bestimmen
   Der Gebäudeeigentümer ist verantwortlich für die Risikobeurteilung gemäss den Methoden und Instrumenten zur Durchführung einer Risikoanalyse, und leitet risikoorientierte Schutzziele und Massnahmen ab. Im Vorfeld von Studien und / oder Vorprojekten sind die Fachführungen der Divisionen (Risk, Safety, Security) und ggf. P-OES beizuziehen.
3. Grundsatz der Prävention
   Übergeordnetes Ziel ist es, Schäden gar nicht erst entstehen zu lassen.
4. Vollständigkeit und Ausgewogenheit der Schutzmassnahmen
   Die Schutzmassnahmen für ein Objekt müssen aufeinander abgestimmt sein und eine nahtlose Kette bilden (keine Sicherheitslücken, keine unerwünschten Redundanzen).
5. Wirtschaftlichkeit
   Die Betrachtung der finanziellen Aspekte (Kosten / Nutzen) eines Schutzkonzeptes muss auch die Folgekosten für Personal, Wartung, Betrieb und mögliche Nachrüstungen beinhalten.
6. Schutzzonen
   Die Schutzzonen eines Objektes sind von aussen nach innen so zu gestalten, dass sie in ihrer Schutzwirkung aufeinander aufbauen und sich wechselseitig ergänzen.
7. Reduktion der Abhängigkeiten
   Nutzungen mit sehr hohen Sicherheitsansprüchen sind möglichst in sich geschlossen (autark) zu planen (vgl. Schutzzonenübertritte), damit sie von allgemein zugänglichen Zonen isoliert betrieben werden können.

8. Konsistenz der Schutzmassnahmen
   Bauliche, technische und organisatorische Massnahmen müssen aufeinander so abgestimmt werden, dass Widersprüche im Schutzkonzept ausgeschlossen werden.
9. Akzeptanz
   Die Massnahmen müssen von Internen als auch von Externen als zumutbar und notwendig empfunden und im Grundsatz akzeptiert werden. Dies setzt eine enge Zusammenarbeit mit den Stakeholdern voraus.
10. Antizipation von Entwicklungen
    Da sich die Anforderungen an die Sicherheit permanent ändern, sind bekannte Entwicklungen sowohl bezüglich der Nutzersituation als auch der Risiken bei Planung, Bau und Betrieb zu berücksichtigen.

4.8.2. Ziele

- Personenschutz
  Der Schutz der Gesundheit und des Lebens der sich in den nicht öffentlich zugänglichen Bereichen von Gebäuden und Mietobjekten aufhaltenden Menschen.
- Gebäude- und Anlagenschutz
  Der Schutz der Bauten / Anlagen / Einrichtungen (innen und aussen), der Werte und der Informationen / Daten sowie der Betriebsabläufe vor aktiven und passiven Gefahren (Kriminalität / Brandfälle).
- Sicherstellung der Verfügbarkeit
  Schutz der bahnrelevanten Installationen zur Gewährung der Verfügbarkeit der Bahninfrastruktur.
- Wahrung Image SBB.

4.8.3. Weiterführende Regelungen

Zu beachten ist die Regelung 232.0 “Sicherheitsplanung im Hochbau”, deren Ausführungsbestimmungen 232.1 sowie Weisungen und Dokumente der Safety.

Folgende Security-Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Planungsgrundsätze	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132442
Schutzzonen	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132439
Methoden und Instrumente zur Durchführung einer Risikoanalyse	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132440
Weitere Hilfsmittel und Übergangsbestimmungen	P-OES-CS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132443

4.9. Schliesssysteme und Zutrittsregelung

4.9.1. Grundsätze

Für Schliesssysteme von Objekten gelten einerseits die gesetzlichen Vorschriften wie Brandschutznormen der Vereinigung kantonaler Feuerversicherungen (VKF) respektive Gebäudeversicherungen und andererseits die spezifischen Anforderungen des Nutzers für Objekte und Räumlichkeiten. Hauptsächliche Gebäudeeigentümer bei den SBB sind die Divisionen Infrastruktur (I) und Immobilien (IM). Die generellen Verantwortlichkeiten, welche die Gebäudesicherheit betreffen, sind mit der Weisung R K 201.1 geregelt.

Gebäude Eigentümerfunktion

Der Gebäudeeigentümer definiert das Schliesskonzept, stellt die Gebäudeschliessung, und im Rahmen des Mietverhältnisses dem Nutzer ein Schliesssystem für den Mietperimeter zur Verfügung. Das Schliesssystem entspricht in der Regel den Anforderungen des entsprechenden Gebäudes (gilt auch für die Aussenhülle).

Gebäude Nutzerfunktion

Der Nutzer definiert die Zutrittsregelung in seinen (gemieteten) Bereich und ist, sofern er auf den Einsatz eines eigenen Produktes besteht, für die Umsetzung und Finanzierung selber verantwortlich. Übersteigen die Anforderungen an die Schliesssysteme spezieller Nutzerbereiche diejenigen der vom Gebäudeeigentümer definiert sind, ist der Nutzer für die entsprechende Auftragserteilung an den Gebäudeeigentümer verantwortlich und trägt die Kosten.

4.9.2. Ziele

Durch die Festlegung von Mindeststandards für die Gebäudeschliessung werden inakzeptable Risiken für Personen, Sachwerte, Informationen so weit als möglich ausgeschlossen und die Verfügbarkeit des Bahnbetriebes gewährleistet.

4.9.3. Weiterführende Regelungen

Themengebiet	Wer	Ablage
Zuständigkeiten Schliesssysteme Infrastruktur	I-ET	https://dms.sbb.ch/LivelinkDt/livelink.exe?func=doc.Fetch&nodeid=4158591
Gebäudeschliessung SBB Immobilien	IM-BW	https://dms.sbb.ch/LivelinkDt/livelink.exe?func=doc.Fetch&nodeid=9020327

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Mindestanforderungen an das Schliesssystem	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132428
Zutrittsregelung	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132427
Personal- und Partnerausweise	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132429

4.10. Notfallkonzept Gebäude

4.10.1. Grundsätze

Aussergewöhnliche Situationen / „Notfälle“ ereignen sich meist unvermittelt und fordern rasches Handeln. In Gebäuden und Mietobjekten mit grossen Menschenansammlungen wie grossen Bahnhöfen, Verwaltungsgebäuden usw. der SBB müssen die Menschenrettung und die Schadensbekämpfung vorbereitet und funktionstüchtig sein. Deshalb ist für jedes Objekt ein Notfallblatt zu erstellen. Wo nötig (z.B. unübersichtliche, komplexe Gebäude) ist zusätzlich ein Fluchtwegplan zu erstellen.

Der Gebäudesicherheitskoordinator sorgt für die Notfallorganisation gemäss R K 201.1. In der Notfallorganisation sind die notwendigen Rollen und Aufgaben objektspezifisch geregelt.

Im Rahmen der Erstellung des Notfallkonzeptes sind minimal folgende Verhaltensregeln zu erstellen:

- Verhalten im Brandfall
- Verhalten bei medizinischem Notfall
- Verhalten bei Evakuation
- Verhalten bei krimineller Bedrohung

4.10.2. Ziele

Die objektspezifische Dokumentation von sicherheitsrelevanten Aspekten unterstützt präventiv die Schadensminimierung im Ereignisfall.

Vorlagen, Checklisten und Hilfsmittel sind im Intranet unter folgendem Link abrufbar

http://intranet.sbb.ch/de/Themen/Sicherheit/Alle/Safety/Gebaeudesicherheit/Notfallkonzept/Seiten/default.aspx

4.11. Bombendrohung / Bombenalarm / verdächtige Gegenstände

4.11.1. Grundsätze

- Jede Drohung ist grundsätzlich ernst zu nehmen
- Ruhe bewahren – Panik vermeiden – Drohung/Erpressung ernst nehmen
- Aufmerksam zuhören – Notizen machen (wer, was, wo, womit, wie, wann, warum)
- Beweisstücke (Droh- oder Erpresserschreiben) in Couvert legen (Spurenschutz)
- Gefährdeten Personenkreis nach Möglichkeit eruieren und informieren
- Sofort Polizei und/oder Notrufnummer der Transportpolizei 0800 117 117 kontaktieren

Gegenstände / Gepäckstücke gelten als verdächtig, wenn sie aufgrund ihres Aussehens, ihrer Beschaffenheit, ihrer Position in der Umgebung und/oder äusserer Umstände (z.B. Grossereignis, erhöhte Bedrohungslage) den Verdacht erwecken, dass diese zum Zwecke des Angriffs auf Leib und Leben von Menschen oder der Zerstörung von Anlagen positioniert wurden. Befragen Sie die Personen, die in der Nähe stehen:

- Gehört dieses Gepäckstück Ihnen? Sahen Sie, wer es zurückgelassen hat?
- Wie lange befindet sich der Gegenstand oder das Gepäckstück schon dort?

Nur wenn kein begründeter Verdacht besteht, kann der Gegenstand als Fundsache behandelt werden. Im Vordergrund steht immer ihre eigene Sicherheit. Am verdächtigen Gegenstand / Gepäckstück dürfen keinerlei Manipulationen vorgenommen werden.

- nicht berühren / nicht öffnen / nicht verlagern oder transportieren / nicht abdecken
- in unmittelbarer Nähe nicht rauchen und nicht telefonieren (Funkenüberschlag)

Die Feststellung eines verdächtigen Gegenstandes / Gepäckstückes ist immer und unverzüglich der Einsatzleitzentrale der SBB Transportpolizei – 0800 117 117 - mitzuteilen. Diese alarmiert die weiteren Stellen via direkte Zugangskanäle (Polizei, BZ, usw.).

Ausschliesslich und endgültig entscheidet die Polizei über die Gefährlichkeit eines verdächtigen Gegenstandes. Es gilt das Prinzip: Die SBB beschreibt – die Polizei bewertet. Der Polizei ist die Situation vor Ort möglichst präzise zu beschreiben, um sie für die Anordnung geeigneter Massnahmen zu unterstützen.

Informationen an die Medien haben ausschliesslich über KOM zu erfolgen.

4.11.2. Ziele

- Früherkennen von Gefahren und vermeiden von Schäden
- Durch eine strukturierte und ruhige Handlungsweise Paniksituationen verhindern

4.11.3. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Checkliste verdächtige Gegenstände	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25129043
Meldeprozess verdächtige Gegenstände	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25132380
Checkliste Bombendrohung	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25131117

4.12. Vandalismus und Sabotage

4.12.1. Definition

Unter Vandalismus wird die gewaltsame Beschädigung und Zerstörung von Geräten, Maschinen, Infrastruktur, usw. verstanden.

Unter Sabotage wird gezielter Vandalismus zur Erreichung eines bestimmten (oft politischen) Ziels verstanden.

4.12.2. Grundsätze

Begründete divisionale Abweichungen der nachfolgenden Grundsätze sind nur nach Rücksprache mit der Öffentlichen Sicherheit möglich.

Allgemein:

Die Auswirkungen von Sachbeschädigungen und Sabotageaktionen haben einen negativen Einfluss auf das Image der SBB und verursachen jährlich wiederkehrende hohe Kosten. Grundsätzlich werden daher Sprayereien auf Bahnareal sowie an und in Fahrzeugen nicht toleriert und schnellstmöglich beseitigt.

Kommunikation:

Bei der externen Kommunikation betreiben die SBB bezüglich Vandalismusschäden eine zurückhaltende Informationspolitik, damit die von den Tätern erwünschte Publizität nicht eintritt und keine Nachahmungstäter animiert werden.

Baulich:

Im Rahmen der Umgebungsgestaltung ist natürlichen Methoden wie z.B. Bauwerksbegrünung den Vorzug zu geben. Massnahmen gegen Vandalismus sind in Um- und Neubauprojekten von Anbeginn weg in der Planung zu berücksichtigen. Bei Oberflächenbehandlungen (Schutzanstrich, Reinigung, Entfernung) sind wenn immer möglich ökologisch unbedenkliche Produkte anzuwenden.

Fahrzeuge:

Bei der Beschaffung von Rollmaterial sind die Aussenwände und die Fahrgasträume möglichst so zu beschaffen, dass sie mit handelsüblichen Reinigungsmitteln ohne speziellen Aufwand von Vandalismusschäden aller Art gereinigt werden können.

Beseitigung:

Sprayereien und Sachbeschädigungen an Gebäuden, Rollmaterial, Anlagen und Einrichtungen werden möglichst schnell repariert, bzw. entfernt. Betroffenes Rollmaterial im Personenverkehr wird so rasch als möglich ausgesetzt und repariert. Betroffenes Rollmaterial im Güterverkehr wird so rasch als möglich ausgesetzt und repariert, sofern betriebsrelevante Teile in ihrer Funktion beeinträchtigt sind.

Strafrecht:

Ermittelte Täter werden straf- und zivilrechtlich zur Verantwortung gezogen. Gegen eine unbekannte Täterschaft wird ab einer Schadensumme von CHF 1000.- Anzeige erstattet. Sind die Erfolgsaussichten die Täterschaft zu ermitteln äußerst gering, so kann auf eine Anzeige verzichtet werden, sofern die Schadensumme CHF 10`000 nicht überschreitet. Die betroffenen Bereiche wenden sich hierzu an das Strafrechtzentrum.

4.12.3. Ziele

Mit einem konzernweit abgestimmten Vorgehen werden die Schäden reduziert und eine möglichst hohe präventive Wirkung in der objektiven und subjektiven Sicherheit erzielt.

Die Umsetzung von Massnahmen liegt in der Verantwortung der Linie. Divisionen und Organisationseinheiten nehmen ihre Verantwortung bezüglich Prävention und Schadensbeseitigung wahr.

4.12.4. Weiterführende Regelungen

P-OP-QSU

Sprayereien an Schienenfahrzeugen / Vandalismus an Schienenfahrzeugen / P-Event-Züge – Vandalismus-Schäden

Video-Auswertungen für Vandalismus-Schäden

http://sharepointapps.sbb.ch/apps/sapdms/GetSapDoc.aspx?LANGU=de&DOKNR=20142210&TEILDOKNR=000

G-AM-FT

Sprayereien / Vandalismus an Rollmaterial „SBB Cargo“

https://dms.sbb.ch/livelinkdt/livelink.exe/fetch/4085881/4085898/livelink.exe/4857740/D%20G-32655_DE?func=doc.Fetch&nodeid=4857740

G-F-SVC

Sachbeschädigungen / Beschädigung von Transportgut SBB Cargo

http://intranet.sbb.ch/de/Themen/Finanzielles/Alle/Versicherungen/Documents/SZ/Arbeitsablauf_Sachbeschaedigung.pdf

IM-CL

Sprayereien an Immobilien

http://filer.sbb.ch/IMKOM/INET/Prozesstool%20MEGA/DE/pages/ecd848674f467709.htm

IM-BW

Vandalismus an Gebäuden / -einrichtungen, Immobilien

http://filer.sbb.ch/IMKOM/INET/Prozesstool%20MEGA/DE/pages/ecd82c864f46715e.htm

Übrige Schäden an Gebäuden / -einrichtungen, Immobilien

http://filer.sbb.ch/IMKOM/INET/Prozesstool%20MEGA/DE/pages/ecd8106c4f460bbf.htm

I-F-ZC

http://intranet.sbb.ch/de/themen/finanzielles/infrastruktur/finanzen_infrastruktur/schadenfallmanagement-infrastruktur/Seiten/Default.aspx

I-ESP-FFM

Sprayereien an Dienstwagen und Fahrzeuge Infrastruktur

\\filer23\i-net2310L\Public\i-se.F6413\FZM\Strasse\D\Meldeablauf_bei_Personen_Fahrzeugschaeden_d.pdf

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Vandalismus an Billettautomaten / Entwertern / Schliessfächern	P-VS	*https://dms.sbb.ch/OTCS/llisapi.dll/open/25120846*

4.13. Sicherheit Betriebs- und Fahrpersonal

4.13.1. Grundsätze

Dem Betriebs- und Fahrpersonal werden im Rahmen Ihrer Tätigkeiten auch Aufgaben im Bereich Security übertragen. Das sicherheitsbewusste Handeln und Denken muss deshalb sichergestellt sein. Bestehende Sicherheitsmängel oder Risiken müssen rasch erkannt und richtig behoben werden können. Eine adäquate Ausbildung ist deshalb unumgänglich.

Die Security-Bestimmungen sind verbindlich in Tarifen für alle Transportunternehmen sowie in den jeweiligen Reglementen, Weisungen und Checklisten geregelt.

4.13.2. Ziele

In Ausnahmesituationen wie Aggressionen, Vandalismus oder bei der Feststellung von Betrügen können die Betroffenen situativ eine richtige Entscheidung treffen.

4.13.3. Weiterführende Regelungen

Themengebiet	Wer	Ablage
Handbuch Zugpersonal	P-VM	*http://intranet.sbb.ch/de/themen/berufe/personenverkehr/zugpersonal/links-zugpersonal/Seiten/Links-Zugpersonal.aspx*

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Polizeigrossintervention	P-OES	*https://dms.sbb.ch/OTCS/llisapi.dll/open/25120843*

4.14. Transportpolizei

4.14.1. Grundsätze

Die Transportpolizei (TPO) ist vom Gesetzgeber mit den sicherheitspolizeilichen Aufgaben im öffentlichen Verkehr beauftragt worden. Das Bundesgesetz über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr BGST (SR 745.2) regelt die Aufgaben und Kompetenzen der TPO.

Angehörige der TPO verfügen über ein eidgenössisches Fähigkeitszeugnis oder ein Zertifikat als Polizist und sind amtlich in die Pflicht genommen. Sie stellen die Aufrechterhaltung der Ruhe und Ordnung auf Arealen und Liegenschaften des öffentlichen Verkehrs sowie der Sicherheit der Kunden und des Personals sicher. Die TPO wird durch P-OES geführt. Die operativen Einsatzplanungen werden durch das Kommando sichergestellt.

Die TPO sorgt kundenorientiert für die Aufrechterhaltung von Sicherheit und Ordnung und setzt das Hausrecht konsequent durch. Sie trägt durch Prävention und andere geeignete Massnahmen zur Verhütung von Straftaten und Unfällen bei. Insbesondere nimmt sie die Aufgabe einer präventiven Sicherheitspolizei wahr und erfüllt Aufgaben gemäss dem Bundesgesetz über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr BGST (SR 745.2). Im Rahmen von Kooperationen mit Sicherheitsorganen des Bundes, der Kantone sowie der Gemeinden trägt sie entscheidend zur Erhöhung der Sicherheit von Kunden und Personal bei. Durch eine enge Zusammenarbeit mit den operativen Mitteln der SBB (u.a. Zugpersonal, Ereignismanagement I / P, Clean, Objektschutz, Programm RailFair, etc.) nutzt sie Synergien mit grösstmöglichem Nutzen für das Unternehmen.

4.14.2. Ziele

Die unterschiedlichen Herausforderungen verlangen, dass die TPO nach einem flexiblen Einsatzkonzept agiert. Dazu gehören:

- Präventive Präsenz durch Patrouillentätigkeit in Bahnhöfen, Zügen und Bahnareal.
- Lagegerechte Schwerpunktkontrollen.
- Führung und Einsatz von Spezialformationen (Sicherheitsdienst, Diensthunde, Observation, Personenschutz).
- Begleitung von Event-Zügen (Sport- und Grossanlässe) mit Konfliktpotential gemäss Security-Eventkalender.
- Lückenlose Erreichbarkeit über die Einsatzleitzentrale.
- Nutzung der modernen, technischen Möglichkeiten (Videodatensicherung, Auswertung und Auslagerung). Die Gesamtkoordination obliegt der Einsatzleitzentrale.
- Enge Zusammenarbeit mit städtischen und kantonalen Polizeikorps sowie anderen Sicherheitsorganen und I-B-INT.

Die Leistungen richten sich nach den verpflichtenden gesetzlichen Aufgaben und den Vorgaben der SBB, vertreten durch P-OES.

4.14.3. Weiterführende Regelungen

Themengebiet	Wer	Ablage
Leistungsgruppen und Ziele	P-OES	*https://dms.sbb.ch/OTCS/llisapi.dll/open/25132371*
Bestellung von TPO-Leistungen bei Events (ohne Fantransporte)	P-OES	*https://dms.sbb.ch/OTCS/llisapi.dll/open/25132372*
Benutzung der öffentlichen Bereiche des Areals der SBB	IM-BW	*https://dms.sbb.ch/LivelinkDt/livelink.exe?func=doc.Fetch&nodeid=14259845*

4.15. Nationales Entführungsalarmsystem (fedpol)

4.15.1. Grundsätze

Die SBB beteiligt sich als Konventionspartner am landesweiten Entführungsalarmsystem, um entführte minderjährige Personen aufzufinden. Beim Entführungsalarmsystem werden möglichst rasch landesweit genaue Informationen über eine Entführung verbreitet, um nützliche Hinweise aus der Bevölkerung zu erlangen. Die Verbreitungsmittel sind sehr weit gefächert und schliessen u. a. sämtliche elektronischen Medien, Webinstrumente, elektronische Autobahnanzeigetafeln, öffentliche Transportunternehmen, Grenzübergänge und Flughäfen mit ein.

4.15.2. Alarmauslösung

Ausgelöst wird die Suche von einer zuständigen Behörde des betreffenden Kantons, dies in enger Zusammenarbeit mit der Polizei und den Bundesbehörden. Die Einsatzzentrale Bundespolizei (EZ fedpol) schickt die Alarmmeldung per E-Mail an die Einsatzzentrale der Transportpolizei (TPO). Der entgegengenommene Alarm wird durch die ELZ TPO an das OCP (Operation Center Personenverkehr), die Netzleitung (I-BF), den Objektschutz, das Verkaufspersonal und die Patrouillen der TPO weitergeleitet. OCP und Netzleitung sorgen anschliessend für eine Weiterleitung des Alarms innerhalb ihrer Divisionen. Sobald der Alarm ausgelöst worden ist, wird die Entführungsmeldung während mehreren Stunden auf verschiedenen Kanälen verbreitet. Im Rahmen dieser Alarmierung wird eine Hotline-Nummer eingeblendet, über welche die Polizei entsprechende Hinweise der Bevölkerung entgegennehmen kann.

4.16. Externe Sicherheitsdienstleister

4.16.1 Grundsatz

Die SBB berücksichtigen nur private Sicherheitsdienste, die im Einklang mit den Konzernzielen, Unternehmenswerten und Compliance-Anforderungen der SBB arbeiten.

4.16.2 Arten von Sicherheitsdienstleistern

<u>Sicherheitsdienstleister mit hoheitlichen Kompetenzen gemäss BGST</u>

Ein privater Sicherheitsdienstleister, der im Auftrag der SBB Leistungen im öffentlich zugänglichen Bahnbetriebsgebiet und in den Fahrzeugen im Rahmen des BGST ausführen will, hat folgende Anforderungen zu erfüllen:

- Zulassung durch das Bundesamt für Verkehr gemäss BGST. (Bewilligungen für private Sicherheitsdienste, die im Auftrag der SBB Leistungen erbringen wollen, werden für die SBB beim Bundesamt für Verkehr ausschliesslich durch die SBB Transportpolizei gestellt);
- Erfahrung im Security-Bereich (Referenzaufträge / Referenzobjekte vorhanden);
- Einhaltung der branchenüblichen Gesamtarbeitsverträge;
- Gewährung der ortsüblichen Arbeitsbedingungen;
- Einsatz von Personal das über die notwendige Ausbildung, insbesondere über Erfahrung im Umgang mit Menschen (Kundenkontakt) verfügt und sich in der ortsüblichen Sprache einwandfrei verständigen kann;
- Mitgliedschaft beim Verband Schweizerischer Sicherheitsdienstleistungs-Unternehmen (VSSU);
- Verbot der Unterakkordanz.

Sicherheitsdienstleister ohne Kompetenzen gemäss BGST

Für private Organisationen, die im Auftrag der SBB Sicherheitsdienstleistungen ausserhalb des Anwendungsbereiches des BGST ausführen wollen, richten sich die Anforderungen nach den Bedürfnissen, die sich aus dem Auftrag ergeben. Sie haben zudem die folgenden Anforderungen zu erfüllen

- Erfahrung im Security-Bereich (Referenzaufträge / Referenzobjekte vorhanden);
- Einhaltung der branchenüblichen Gesamtarbeitsverträge;
- Gewährung der ortsüblichen Arbeitsbedingungen;
- Einsatz von Personal das für den geplanten Einsatz ausgebildet ist;
- Mitgliedschaft beim Verband Schweizerischer Sicherheitsdienstleistungs-Unternehmen (VSSU).

4.16.3 Einsatzrahmen externer Sicherheitsdienstleister

Die SBB Security-Organisation unterscheidet bezüglich externer privater Organisationen, die Sicherheitsdienstleitungen für die SBB erbringen, zwischen Aufträgen im Rahmen des BGST und den übrigen Aufträgen, die nicht im Rahmen des BGST erfolgen:

Aufträge im öffentlichen Bahnbetriebsgebiet mit Kompetenzen gemäss BGST	**Aufträge ohne Kompetenzen gemäss BGST**
Beispiele: Begleitung kritische Frühzüge, Einsatz im Kontext der Sicherheitsorganisation ZVV, Einsatz bei integralen Dispositiven im Kontext von Events mit Gewaltpotenzial.	Schutz von Promotionen / Standaktionen an Bahnhöfen, Einsatz zu Gunsten von IM-Mietern an Bahnhöfen, Berondung von Bürogebäuden, Überwachung von nicht der Öffentlichkeit gewidmeten Infrastrukturanlagen. Für Überwachungen im Safety-Bereich gelten die Regelungen der SBB Safety-Organisation.
Bestellung durch Divisionen / Dimensionierer über integralen Bestellprozess bei P-OES / P-OES-TPO auf Basis der abgeschlossenen LV/SLA oder lagebedingten Einzelaufträgen.	Bestellung/Auftragserteilung durch IM-Mieter, Veranstalter/Promotoren, Gebäudeeigentümer.
Einsatzverantwortung: SBB Transportpolizei.	Einsatzverantwortung: Auftraggeber bzw. Veranstalter.
Einsatzplanung und –führung: SBB Transportpolizei.	Einsatzplanung: Auftraggeber bzw. Veranstalter.
Kompetenz zu hoheitlichem Handeln (neben der Möglichkeit, sich auf die Jedermannsrechte abzustützen).	Verfügen nur über die Jedermannsrechte und die durch den Auftraggeber übertragen Kompetenzen zur Durchsetzung des Hausrechtes in den nichtöffentlichen Bereichen.
Einsatzbefugnisse gemäß Art. 3 und 4 ff. des Bundesgesetzes über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr (BGST).	Einsatzbefugnisse gemäß Umschreibung im Auftrag: Durchsetzung der Hausordnung. Vorbehalten bleiben in allen Fällen das Notwehrrecht bei Angriffen (Notwehr, Art. 14 ff. StGB) und die Jedermannsrechte bei Verbrechen und Vergehen (Vorläufige Festnahme, Art. 218 StPO).
Die Einsatzkräfte sind mit gelben Leuchtwesten gemäß Vorgaben der Transportpolizei ausgerüstet.	Ausrüstung & Uniform nach Maßgabe des Auftraggebers . Zur optischen Unterscheidung von den gemäss BGST eingesetzten Kräften dürfen keine gelben Leuchtwesten getragen werden.
Einsatzraum: Bahnhöfe, Züge, d.h. öffentlicher Bereich der Transportunternehmung (vorbehalten bleiben Zusatzaufträge auch in den nicht öffentlichen Bereichen).	Einsatzraum gemäß Auftrag.
Nur private Sicherheitsdienste mit Zulassung BAV.	Keine Zulassung BAV notwendig.
Verbot der Unterakkordanz.	Keine Auflagen gemäß BGST.

4.16.1. Weiterführende Regelungen

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Pflichtenheft und Ausrüstung	P-OES	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120838
Benutzung der öffentlichen Bereiche des Areals der SBB	IM-BW	https://dms.sbb.ch/LivelinkDt/livelink.exe?func=doc.Fetch&nodeid=14259845

4.17. Transport und Aufbewahrung von Werten

4.17.1. Grundsätze

In der Planung von Sicherheitsmassnahmen im Bereich Werttransporte wird dem Schutz von Menschen höhere Priorität beigemessen als dem Schutz von Werten (Billettpapier, Zahlungsmittel, etc.). Klassische Beispiele für Risiken, bei denen Werte das leibliche Wohlergehen der Mitarbeitenden, von Reisenden aber auch das Image der SBB gefährdet sein kann, sind Diebstähle (Trickdiebstähle), Raubdelikte und Delikte gegen Leib & Leben. Um solche Risiken möglichst niedrig zu halten, sind organisatorische Massnahmen, aber auch Verhaltensrichtlinien für Wertboten, die Wartung von Billettautomaten, den Versand von Wertsendungen, etc. angebracht.

Das Versicherungsmanagement SBB verlangt einen adäquaten Schutz der versicherten Sachen. Werden diese Bestimmungen nicht eingehalten, kann der Versicherer die Entschädigung kürzen oder verweigern. Die Grundlage dazu bildet das vorliegende Regelwerk. Kompetenz zur Beurteilung der Adäquanz i. S. Security wurde vom Versicherungsmanagement an P-OES delegiert.

4.17.2. Ziele

Durch ganzheitliche Sicherheitsmassnahmen (baulich, technisch, organisatorisch, personell) wird der Schutz von Menschen und Werten garantiert.

4.17.3. Weiterführende Regelungen

Themengebiet	Wer	Ablage
Leerung / Wartung von Kassenautomaten Park + Rail	IM-CL	https://dms.sbb.ch/OTCS/llisapi.dll?func=ll&objAction=download&objId=14530466

Folgende Dokumente erhalten ihre Legitimation aufgrund Delegation durch das Security Handbuch R K 030.1:

Themengebiet	Wer	Ablage
Geldtransporte	P-VS	https://dms.sbb.ch/OTCS/llisapi.dll/open/25120837

4.18. Sicherung von Transporten gefährlicher Güter

4.18.1. Grundsätze

Für den Transport von Gefahrgut ist die Gefahrgut-Gesetzgebung des RID massgeblich (internationale Vorschriften für die Beförderung von gefährlichen Gütern auf dem Verkehrsträger Schiene). In Ziffer 1.10 des RID werden minimale Anforderungen an die Sicherung vorgeschrieben, um den Diebstahl oder Missbrauch gefährlicher Güter, durch den Personen, Güter oder die Umwelt gefährdet werden können, zu minimieren.

Nach den gesetzlichen Bestimmungen des RID sind durch die jeweiligen Infrastrukturbetreiberinnen und EVU für ihren Tätigkeitsbereich Sicherungspläne inkl. der dazugehörenden Massnahmen zu führen. Insbesondere ist auch die Überwachung / Bewachung abgestellter Gefahrgutwagen zu regeln. Auf dem Netz der SBB verantwortet I-B die Sicherungspläne infrastrukturseitig. SBB Cargo erstellt und pflegt den Sicherungsplan für die Verkehrsunternehmung SBB Cargo. Andere Netzzugängerinnen erstellen die entsprechenden Sicherungspläne in eigener Verantwortung.

Der Inhalt der Sicherungspläne SBB Cargo und Infrastruktur sind „vertraulich“ klassiert und nur gegen Nachweis der Berechtigung einsehbar. Im Regelwerk SBB ist eine entsprechende Hinterlegung erfolgt; Suchbegriff „Sicherungsplan“.

4.18.2. Ziele

Sicherung von Gefahrguttransporten zur Minimierung von Diebstahl oder Missbrauch gefährlicher Güter, bei welchen Personen, Güter oder die Umwelt gefährdet werden können.

4.18.3. Weiterführende Regelungen

Themengebiet	Wer	Ablage
Sicherungsplan nach RID 1.10	G-QSU	Vertraulich. Auskunft bei G-QSU
D I-30059 Beförderung gefährlicher Güter	G-QSU	*http://intranet.sbb.ch/de/themen/richtlinien-und-vorschriften/alle/regelwerk-sbb/Seiten/Default.aspx*
D I-50026 Vorgaben von I-B zum Transport gefährlicher Güter und anderer wassergefährdenden Flüssigkeiten.	G-QSU	*http://intranet.sbb.ch/de/themen/richtlinien-und-vorschriften/alle/regelwerk-sbb/Seiten/Default.aspx*

P-OES

sig. Simon Jungo

Leiter Öffentliche Sicherheit

IT-SR

sig. Marcus Griesser

Leiter Security & Risk Management