Sicherheitsanweisung

SA Grundlage für Schutzkonzepte

Swisscom AG

Group Security
Postfach
3050 Bern

Version	Datum	Person	Vorgenommene Anpassungen/Bemerkungen
0.1	29.03.2023	Claudio Passafaro	Erstellung
0.2	04.04.2023	Daniel Zysset	Überarbeitung
1.0	24.05.2023	Claudio Passafaro	Freigabe

Verantwortlich: SiBe Brand-Objektschutz
Herausgeber: SiBe Brand-Objektschutz
Erstellung: 29.03.2023
Ersteller: Passafaro Claudio, GSE-PHY
Geht an: gemäss 1.2 Geltungsbereich

Inhalt

1 Einleitung 3

1.1 Ausgangslage 3
1.2 Geltungsbereich 3
1.3 Referenzierte Dokumente 3

2 Schutzbedarf und Schutzfähigkeit von Gebäuden und Flächen 4

2.1 Schutzbedarf 4
2.2 Bewertungsfaktoren 4
2.3 Risikobasierte Schutzzielbetrachtung 4
2.3.1 Vorgehensweise 5

3 Risikobetrachtung 6

3.1 Risikokatalog 7
3.2 Spezifische Schutzziele nach Risiko-Typisierung 12

4 Übergangsbestimmungen 18

5 Dokument Information 18

5.1 «Version 1» 18

1 Einleitung

1.1 Ausgangslage

[1] Ein Grossteil der Büro- und Betriebsgebäude von Swisscom können gemäss Standardkonzepten gebaut und betrieben werden.

[2] Wo Flächen oder Gebäude einen besonderen Schutzbedarf aufweisen, muss dieser Schutzbedarf auf der Grundlage eines Risikomanagements und anhand von Schutzzielen unter Einbezug der Flächennutzer ermittelt werden. Darauf basierend ist ein objektspezifisches Schutzkonzept zu erstellen.

[3] Objektspezifische Schutzkonzepte müssen von Group Security geprüft werden.

[4] Das vorliegende Dokument umfasst den Risikokatalog Physische Sicherheit, der für die Risikoanalyse, die Bewertung von Risiken und die Einstufung von Massnahmen herangezogen wird, für alle Risikobetrachtungen in und an Gebäuden und Räumlichkeiten von Swisscom AG. Er dient der Homogenisierung von Risikoeinschätzungen.

1.2 Geltungsbereich

[5] Dieses Dokument gilt für die gesamte Swisscom (Schweiz) AG, mit allen Geschäfts[1]- und Konzernbereichen[2] mit Sitz im In- und Ausland folgend Swisscom genannt.

[6] Die Konzerngesellschaften bauen ein eigenes Security Management auf oder schliessen sich dem Security Management der Swisscom an. Die Verantwortung für die Security liegt weiterhin bei der Konzerngesellschaft. Der Entscheid liegt in der Verantwortung der Konzerngesellschaft und wird von Group Security unterstützt

1.3 Referenzierte Dokumente

[1] Direktive-Sicherheit

[2] Security-Policy

[1] Zu den Geschäftsbereichen zählen Retail Customers („B2C"), Business Customers („B2B") sowie IT, Network & Infrastructure („INI")

[2] Zu den Konzernbereichen zählen Group Business Steering („GBS"), Group Human Resources („GHR"), Group Communications & Responsibility („GCR") und Group Security & Corporate Affairs („GSA")

2 Schutzbedarf und Schutzfähigkeit von Gebäuden und Flächen

2.1 Schutzbedarf

[7] Die Schutzklasse des Schutzcontainers Gebäude oder Fläche richtet sich nach der höchsten Schadensklasse der darin enthaltenen (oder vorgesehenen) Schutzobjekte.

SCHUTZOBJEKT	Klassifizierung	Klassen			
Informationen	Vertraulichkeit	C1 - Public	C2 - General	C3 - Confidential	C4 - Strictly Confidential
	Integrität	I1 - None	I2 - Basic	I3 - Medium	I4 - High
Materielle Objekte	Geldwert	M1 - None	M2 - Basic	M3 - Medium	M4 - High

SCHUTZCONTAINER	Qualifizierung	Klassen			
Raum od. Fläche	*Schutzlevel*	*None*	*Basic*	*Medium*	*High*
	Vertraulichkeit	pcC1	pcC2	pcC3	pcC4
	Integrität	pcI1	pcI2	pcI3	pcI4
	Geldwert	pcM1	pcM2	pcM3	pcM4

2.2 Bewertungsfaktoren

Für ICT-Anlagen, Verkaufsräumlichkeiten, Büro- und Archivräumlichkeiten sowie für Konferenzräume ist in der Regel die Vertraulichkeit C1-C4 das massgebende Kriterium.

2.3 Risikobasierte Schutzzielbetrachtung

[8] Ein Sicherheitskonzept besteht aus einer Reihe von aufeinander abgestimmten Sicherheitsmassnahmen, die in ihrer Kombination die gewünschte Schutzwirkung ergeben. Es kann bauliche, technische, organisatorische und versicherungstechnische Massnahmen umfassen.

[9] Die Massnahmen ergeben sich aus einer Risikobetrachtung. Dabei werden Gefahren für die Schutzziele identifiziert und individuell bewertet. Diese Bewertung bildet schliesslich die Grundlage für die abzuleitenden Massnahmen, welche im Sicherheitskonzept festgehalten werden.

Das Ziel der Analyse ist es, eine möglichst vollständige Übersicht aller Gefahren zu erhalten und durch verhältnismässige Massnahmen zu adressieren

2.3.1 Vorgehensweise

[10] Die Risikoanalyse beinhaltet die in der folgenden Tabelle dargestellten Schritte.

[11] Grundsätzlich sind dabei die Regelungen des Ausführungsreglement Risikomanagement zu befolgen (Link: Ausführungsreglement Risikomanagement_01052022.pdf (swisscom.com). Dies betrifft insbesondere die Regelungen zur Risikoakzeptanz.

Für die Durchführung der Risikoanalyse kann eine Orientierung an den Empfehlungen der "Risk Impact Assessment Weisung" erfolgen (Link: Risk Impact Assessment Weisung_DE.pdf (swisscom.com)).

Schritt	Inhalt	Ergebnis
Erhebung Schutzziele	Zunächst muss erhoben werden, welche Schutzziele durch die Massnahmen erreicht werden sollen. Die wesentlichen Sicherheitsschutzziele der Swisscom sind in der Security Policy (Kapitel 3) definiert. Daneben kann es weitere gesetzliche oder Kundenanforderungen geben, die individuell berücksichtigt werden müssen.	Die Schutzziele sind bekannt.
Identifikation von Risiken	Die Gefahren für die Schutzziele werden identifiziert. Eine Übersicht möglicher Gefahren stellt der Risikokatalog unter Ziffer 3.1 dar. Gefahren, die eine erwartbar negative Auswirkung auf die Schutzziele haben, werden als Risiken erfasst.	Die Risiken für die Schutzziele sind bekannt.
Risikobewertung	Die erfassten Risiken werden individuell hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung bewertet.	Die Risiken sind bewertet.
Identifikation von Massnahmen zur Risikobehandlung	Im letzten Schritt werden für je nach Höhe des Risikos geeignete Massnahmen zur Behandlung getroffen. In der Regel wird es sich dabei um Massnahmen zur Risikoreduktion handeln. Es ist aber auch möglich, ein Risiko zu akzeptieren. Dabei gilt es, den Risikomanagementprozess der betreffenden Organisationseinheit zu befolgen.	Massnahmen zur Behandlung der Risiken sind definiert.
Dokumentation der Ergebnisse	Im letzten Schritt werden die Ergebnisse im Sicherheitskonzept festgehalten.	Sicherheitskonzept

3 Risikobetrachtung

[12] Unter Ziffer 3.1 ist der Risikokatalog aufgeführt. Es werden Risiken beschrieben, die einen Impact auf die Schutzobjekte von Swisscom besitzen, sowie deren Relevanz und Abgrenzung für den Betrachtungsbereich Physische Sicherheit.

[13] Der Katalog kann für Risikoanalysen im Bereich Physische Sicherheit, die Bewertung von identifizierten Risiken und die Festlegung von Massnahmen herangezogen werden.

[14] Unter Ziffer 3.2 werden die spezifischen Schutzziele aufgeführt,

- für aktive Risiken, also Risiken, die durch beabsichtigte und gezielt gegen Objekte oder Personen gerichtete Handlungen herbeigeführt werden
- für passive Risiken, also Risiken, die durch menschliches oder technisches Versagen oder durch Naturereignisse verursacht werden

[15] Hinweise: Die Schutzziele sind insofern aufgeführt, als dass Massnahmen, die im Rahmen physischer Sicherheit getroffen werden können, zur Erreichung dieser Schutzziele beitragen. Partiell kann es dabei zu Überschneidungen mit der Informationssicherheit kommen, deckt deren Schutzziele aber in keinem Fall vollständig ab.

3.1 Risikokatalog

Identifier = Rphy<Nummer> (Rphy="Risiko Physical")

					Risiko wirkt auf Schutzobjekte												
			Relevant für physische Sicherheit		Schutz der Personen			Schutz der immateriellen Werte			Schutz der materiellen Werte			Schutz der Unternehmensleistung		
No	**Risiko**	**Risikobeschreibung**	**J**	**N**	Kunden	Mitarbeitende	Partner	Informationen	KnowHow	geistiges Eigentum	Gebäude	Technische Anlagen	Mobilien/ Geld	Reputation	Produkte	Umwelt
Rphy01	Abhängigkeit von Mitarbeitenden und Dritten	Unbewusstes oder beabsichtigtes Schaffen von Wissen bei Einzelpersonen oder Drittpersonen, die bei Ausfall/ Ausscheiden (Unfall, Krankheit, o.ä.) insbesondere die Betriebskontinuität von Anlagen sowie Systemen und/ oder die Ausführung wichtiger Kernprozesse beeinträchtigen oder verhindern		X					•							
Rphy02	Androhung physischer Gewalt	Verbreitung von ernst gemeinten Meldungen oder Falschmeldungen (telefonisch oder schriftlich) zwecks Durchsetzung erpresserischer Forderungen und/ oder zur Störung bzw. vorübergehender Lahmlegung des Betriebes	X		•	•	•									
Rphy03		Drohungen gegen die körperliche Integrität von Einzelpersonen und/oder nahes persönliches Umfeld	X		•	•	•							•		
Rphy04		Eine Person oder Personengruppe durch Gewalt, Anwendung einer schweren Drohung oder auf eine andere Art und Weise widerstandsunfähig zu machen, um sich so einen unrechtmässigen Vermögensvorteil zu gewähren	X		•	•	•									
Rphy05	Angriff gegen Personen	Gewalttätiger (körperlich oder mit Waffe) Angriff auf eine oder mehrere Personen	X		•	•	•									
Rphy06	Attentat/Terrorakt	Geplanter Angriff auf eine Einzelperson, eine Personengruppe oder einer Infrastruktur/ einem Gebäude mit einer Waffe oder mittels Sprengstoffs, mit dem Ziel, diese zu töten	X		•	•	•	•	•		•	•	•	•		
Rphy07	Absturz von Flugkörpern auf Bauwerke	Aufprall eines Flugzeuges oder Teile davon auf Bauwerke	X		•	•	•	•	•		•	•	•	•		
Rphy08	Ausfall von Sicherheitsanlagen	Vorübergehender oder länger andauernder Ausfall der Sicherheitsanlagen (z.B. Brandmelde- und Einbruchmeldeanlage, Zutrittskontrollsystem)	X								•	•	•			

Identifier = Rphy<Nummer> (Rphy="Risiko Physical")

					Risiko wirkt auf Schutzobjekte												
			Relevant für physische Sicherheit		Schutz der Personen			Schutz der immateriellen Werte			Schutz der materiellen Werte				Schutz der Unternehmensleistung		
No	**Risiko**	**Risikobeschreibung**	**J**	**N**	Kunden	Mitarbeitende	Partner	Informationen	KnowHow	geistiges Eigentum	Gebäude	Technische Anlagen	Mobilien/ Geld	Reputation	Produkte	Umwelt
Rphy09	Ausfall von betriebswichtigen technischen Anlagen	Vorübergehender oder länger andauernder Ausfall der betriebswichtigen technischen Anlagen (USV, Niederspannungs-Hauptverteilung, Leitsystem, Klima- und Kälteanlagen, etc.)	X					•			•	•			•	
Rphy10	Ausfall von Telekommuni-kationsanlagen	Vorübergehender oder länger andauernder Ausfall der Telekommunikationsanlagen		X				•				•			•	
Rphy11	Ausfall von IT- und Netzwerksystemen	Vorübergehender oder länger andauernder Ausfall der betriebswichtigen IT-Systeme		X				•			•	•			•	
Rphy12		Vorübergehender oder länger andauernder Ausfall der Netzwerksysteme (WAN/ LAN)		X				•			•	•			•	
Rphy13	Ausfall der Versorgung mit Ressourcen	Vorübergehender oder länger andauernder Ausfall der Strom- (48V oder 220V), Wasser-, Fernwärme- und Gasversorgung sowie der Telekommunikationsnetze	X					•			•	•			•	
Rphy14	Betrug/Fälschung/ Veruntreuung	Machenschaften oder Manipulationen, um sich oder Dritten einen finanziellen oder materiellen Vorteil zu verschaffen		X										•		
Rphy15	Bestechung	Einer Person ein Geschenk (materiell/ immateriell) oder einen anderen Vorteil anbieten, versprechen, geben oder zukommen lassen, damit er seine Dienst- oder Amtspflicht verletzt		X										•		
Rphy16	Bombendrohung	Verbreitung von ernst gemeinten Meldungen oder Falschmeldungen (telefonisch oder schriftlich) zwecks Durchsetzung erpresserischer Forderungen und/oder zur Störung bzw. vorübergehender Lahmlegung des Betriebes.	X		•	•	•				•	•	•	•		
Rphy17		Drohungen gegen die körperliche Integrität von Personen.	X		•	•	•							•		
Rphy18	Brand	Unbeabsichtigtes Entstehen von Feuer durch menschliches oder technisches Versagen bzw. Naturereignisse	X		•	•	•	•			•	•	•			
Rphy19	Brandstiftung	Vorsätzlich gelegter Brand (Brandstiftung ist eine Sonderform der Sabotage)	X		•	•	•	•			•	•	•			

Identifier = Rphy<Nummer> (Rphy="Risiko Physical")

					Risiko wirkt auf Schutzobjekte												
			Relevant für physische Sicherheit		Schutz der Personen			Schutz der immateriellen Werte			Schutz der materiellen Werte				Schutz der Unternehmensleistung		
No	**Risiko**	**Risikobeschreibung**	**J**	**N**	Kunden	Mitarbeitende	Partner	Informationen	KnowHow	geistiges Eigentum	Gebäude	Technische Anlagen	Mobilien/ Geld	Reputation	Produkte	Umwelt
Rphy20	Demonstration	Öffentliche, gemeinsame Meinungsäusserung vieler Personen auf öffentlichem oder privatem Grund	X								•	•	•	•		
Rphy21	Besetzung	Friedliches oder gewaltsames (unbefugtes) Besetzen eines Gebäudes/ Gebäudeteiles durch Fremdpersonen (Hausfriedensbruch) oder eigenen Mitarbeitenden	X		•	•	•				•	•		•		
Rphy22	Diebstahl	Entwenden von materiellen oder immateriellen Werten, ohne zuvor gewaltsam in ein Gebäude eingedrungen zu sein	X					•	•	•	•	•	•			
Rphy23	Elementar-gewalten	Naturereignisse (z.B. Sturm, Hochwasser, Blitzschlag, Erdbeben) die Zerstörungen zur Folge haben	X		•	•	•	•			•	•	•	•	•	•
Rphy24	Einbruch	Gewaltsames Eindringen in ein Gebäude oder in einen verschlossenen Raum bzw. Aufbruch eines verschlossenen Behältnis zwecks widerrechtlichen Aneignens von materiellen oder immateriellen Werten oder zur Vorbereitung krimineller Handlungen	X					•	•	•	•	•	•	•		
Rphy25	Epidemie/ Vergiftung	Vergiftung von Einzelpersonen oder Personenmassen durch die Immission von gesundheitsschädigenden oder hoch toxischen Substanzen, von innen oder von aussen, über die Luft bzw. durch gasförmige Stoffe in der Luft oder durch den Genuss bzw. die Verwendung des Wassers (Waschen) oder infolge des körperlichen Kontaktes mit vergifteten Gegenständen/Materialien oder infizierten Personen.	X		•	•	•	•	•		•			•		
Rphy26	Erpressung	Eine Person oder Personengruppe durch Gewalt, Anwendung einer schweren Drohung oder auf eine andere Art und Weise widerstandsunfähig zu machen, um sich so einen unrechtmässigen Vermögensvorteil zu gewährleisten.		X	•	•	•	•		•			•	•		
Rphy27	Nötigung	Eine Person oder Personengruppe durch Gewalt oder Androhung ernstlicher Nachteile oder durch andere Beschränkung seiner/ihrer		X	•	•	•	•		•			•	•		

Identifier = Rphy<Nummer> (Rphy="Risiko Physical")

					Risiko wirkt auf Schutzobjekte												
			Relevant für physische Sicherheit		Schutz der Personen			Schutz der immateriellen Werte			Schutz der materiellen Werte					Schutz der Unternehmensleistung	
No	Risiko	Risikobeschreibung	J	N	Kunden	Mitarbeitende	Partner	Informationen	KnowHow	geistiges Eigentum	Gebäude	Technische Anlagen	Mobilien/ Geld	Reputation	Produkte	Umwelt
		Handlungsfähigkeit nötigen, etwas zu tun, zu unterlassen oder zu dulden.														
Rphy28	Entführung	Freiheitsberaubung von Personen zur Durchsetzung von Forderungen verbunden mit physischer und psychischer Gewaltanwendung. Täter und Lokalitäten, in welchen die Entführten gefangen gehalten werden, sind unbekannt.		X	•	•	•							•		
Rphy29	Explosion	Blitzartige, von einer Druckwelle begleitete, chemische Reaktion mit grosser Zerstörungskraft, oft mit nachfolgendem Brand	X		•	•	•	•	•		•	•	•	•	•	•
Rphy30	Geiselnahme	Freiheitsberaubung von Personen zur Durchsetzung von Forderungen mittels direkter Gewaltandrohung bzw. -anwendung		X	•	•	•				•		•	•		
Rphy31	Identitäts-diebstahl	Diebstahl und Verwendung einer Identität eines Mitarbeitenden oder des Unternehmens Swisscom	X					•	•	•			•	•		
Rphy32	Informations-abfluss	Unbeabsichtigte oder fahrlässige Weitergabe von sensitiven Informationen		X				•	•	•				•		
Rphy33	Informations-diebstahl	Widerrechtliches Aneignen von physischen und/oder elektronischen Informationen bzw. Datenträgern		X				•	•	•				•		
Rphy34	Informations-manipulation	Verfälschung (Einfügen, Ändern oder Löschen) von elektronisch aufgezeichneten Informationen oder solchen auf nicht elektronischen Datenträgern wie Papier, Film, Tonträger		X				•	•	•				•		
Rphy35	Informations-verlust	Vernichten oder Verlieren von klassifizierten oder betriebsnotwendigen (elektronische/physische) Informationen (Daten/Akten/Datenträger)		X				•	•	•				•		
Rphy36	Kontaminierung von Genuss- und Lebensmitteln	Vorsätzliche oder ungewollte Vergiftung von Genuss- und Lebensmitteln mittels Chemikalien oder anderen gesundheitsgefährdenden Substanzen		X	•	•	•									•
Rphy37	Radioaktive Verseuchung	Radioaktive Kontaminierung der Umwelt (Mensch, Tier, Boden, Wasser, Luft, Fauna etc.)		X	•	•	•				•	•				•

Identifier = Rphy<Nummer> (Rphy="Risiko Physical")

					Risiko wirkt auf Schutzobjekte											
			Relevant für physische Sicherheit		Schutz der Personen			Schutz der immateriellen Werte			Schutz der materiellen Werte			Schutz der Unternehmensleistung		
No	**Risiko**	**Risikobeschreibung**	**J**	**N**	Kunden	Mitarbeitende	Partner	Informationen	KnowHow	geistiges Eigentum	Gebäude	Technische Anlagen	Mobilien/ Geld	Reputation	Produkte	Umwelt
Rphy38	Raubüberfall	Durchsetzung von Forderungen zur Erlangung von materiellen/immateriellen Werten mittels direkter Gewaltanwendung. Der Überfall ist in der Regel geplant und tritt unerwartet ein.	X		•	•	•	•		•	•	•	•	•		
Rphy39	Sabotage	Vorsätzlich geplante, mutwillige Beeinträchtigung des Betriebsablaufs durch Beschädigung/Ausserbetriebsetzung von Gebäudeteilen oder betriebswichtigen Anlagen	X			•		•	•	•	•	•	•		•	
Rphy40	Spionage/Abhören von Kommunika-tionssystemen	Widerrechtliches Aneignen von Informationen (Abhören, Kopieren, Fotografieren, usw,) meist über längere Zeit ohne Spuren zu hinterlassen	X					•	•	•				•	•	
Rphy41	Streik	Gemeinschaftliche Weigerung der Mitarbeitenden gewisse Tätigkeiten oder Vorgänge auszuführen als Kampfmassnahme zur Erreichung von Forderungen		X		•								•	•	
Rphy42	Überspannung	Kurzzeitiger Spannungsanstieg im Netz, der elektrische bzw. elektronische Geräte beschädigen und/ oder zerstören kann (z.B. Blitz, Stromschwankungen Netz).	X			•		•			•	•			•	
Rphy43	Unbeabsichtigtes Freisetzen von to-xischen oder brennbaren Substanzen (Chemieunfall)	Kontaminierung der Umwelt durch toxische, aggressive/korrosive oder brennbare/explosive Substanzen in flüssiger, fester oder gasförmiger Form (z.B. Batterieräume/USV-Räume, Diesel-Anlagen, Tankstellen Benzin und Diesel, Putzmittelräume in Grossgebäuden, etc.)	X		•	•	•				•	•				•
Rphy44	Vandalismus/Sach beschädigung	Mutwillige, aber nicht unbedingt zielgerichtete Beschädigung von Gebäudeteilen oder technischen Installationen	X								•	•		•		
Rphy45	Wasserschaden	Unbeabsichtigte Beschädigung oder Zerstörung materieller und immaterieller Werte durch Wasser (z.B. Rohrbruch) oder eindringendes Wasser (Grundwasser, Löschwasser, etc.)	X								•	•	•	•		•

3.2 Spezifische Schutzziele nach Risiko-Typisierung

No.	Risiko	Schutzziele, mit Massnahmen physischer Sicherheit erreichbar *Schutzziele, die mit anderen (nicht-physischen) Massnahmen erreichbar sind*	Wirkt auf
Aktive Risiken - Risiken, die durch beabsichtigte und gezielt gegen Objekte oder Personen gerichtete Handlungen verursacht werden			
1-1	Androhung Phys. Gewalt	**Minimalität** - Die physische Gefährdung von Personen und die Auswirkung auf die Funktionsfähigkeit der Swisscom durch eine Bombendrohung sind minimal.	Rphy02 Rphy03 Rphy04
1-2		**Realismus** - Eine realistische Lagebeurteilung und ein situations-gerechtes Handeln sind jederzeit gewährleistet. Alle Massnahmen zur Gebäudedurchsuchung sind optimal vorbereitet.	Rphy02 Rphy03 Rphy04
1-3		**Panikverhinderung** - Paniksituationen werden möglichst verhindert. Eine eventuelle Evakuierung ist rasch und sicher durchführbar.	Rphy02 Rphy03 Rphy04
1-4	Angriff gegen Personen	**Erschwerung** - Angriffe gegen Personen durch Dritte/Besucher sind innerhalb der Gebäude erschwert.	Rphy05
1-5		**Interventionszeit** - Im Ereignisfall sind externe Interventionskräfte innerhalb kürzester Zeit zur Stelle.	Rphy05
1-6	Betrug/ Fälschung/ Veruntreuung	**Erkennbarkeit** - Betrug/Fälschungsversuche und Veruntreuung werden nach Möglichkeit innert nützlicher Frist erkannt	Rphy14
1-7		**Untersuchung** - Wird Betrug/ Fälschung oder Veruntreuung vermutet oder festgestellt, folgt umgehend eine Untersuchung zum Zweck der Schadenminimierung und zur Ermittlung der Täterschaft.	Rphy14
1-8	Brandstiftung	**Prävention** - Anstrengungen zur Prävention von Brandstiftungen werden unternommen	Rphy19
1-9		**Erschwerung** - Das Einwerfen oder Einbringen von Brandsätzen in die Gebäude ist stark erschwert	Rphy19
1-10	Demonstration/ Besetzung	**Orientierung** - Der Sicherheitsbeauftragte wird über geplante oder sich in Gang befindliche Demonstrationen, welche die Betriebsabläufe gefährden können, rasch orientiert und leitet Gegenmassnahmen ein	Rphy20 Rphy21
1-11		**Erschwerung** - Eine Besetzung soll, wenn nicht verhindert, doch stark erschwert sein und hat limitierte Auswirkungen	Rphy20 Rphy21
1-12	**Diebstahl**	**Unattraktivität** - Diebstähle müssen von vornherein als unattraktiv erscheinen	Rphy22
1-13		**Erschwerung** - Einschleichdiebstähle werden möglichst verhindert	Rphy22
1-14		**Arbeitsklima** - Das Diebstahlrisiko durch internes Personal ist durch ein gutes Arbeitsklima und eine gute Personalpolitik stark reduziert	Rphy22
1-15		**Prävention** - Das Personal ist für Diebstahlprävention sensibilisiert	Rphy22
1-16	**Einbruch**	**Aussichtslos** - Einbruchversuche müssen aussichtslos erscheinen	Rphy24

No.	Risiko	Schutzziele, mit Massnahmen physischer Sicherheit erreichbar ***Schutzziele, die mit anderen (nicht-physischen) Massnahmen erreichbar sind***	Wirkt auf
1-17		**Erschwernis**- Einbruchdiebstähle sind während den Arbeitszeiten erschwert und ausserhalb der Arbeitszeiten stark erschwert	Rphy24
1-18		**Detektion** - Einbruchversuche in Räume mit erhöhten Sicherheitsanforderungen (Zone 4: Sicherheitszone) werden sofort detektiert, weitergemeldet und durch bauliche Massnahmen so verzögert, dass eine rechtzeitige Intervention durch die Polizei gewährleistet ist	Rphy24
1-19		**Angemessenheit** - Einbruchversuche in Gebäude sind durch geeignete, dem Schutzgrad angemessene Massnahmen zu erschweren (baulich) und zu detektieren (organisatorisch, technisch). In Gebäuden mit hohem Schutzbedarf ist eine Aussenhautüberwachung (z.B. bzgl. Glasbruch) notwendig	Rphy24
1-20	**Identitätsdiebstahl**	**Risikominderung** - Das Risiko des Diebstahls und die Verwendung einer Identität eines Mitarbeitenden oder des Unternehmens Swisscom ist durch eingeführte präventive Massnahmen zu verringern.	Rphy31
1-21	**Informations-diebstahl**	***Schutz vor Spurlosigkeit*** *- Der Schutz von betrieblichen und kundenbezogenen Informationen in elektronischer oder physischer Form ist gewährleistet, indem der Diebstahl von Informationen und Informationsträgern nicht möglich ist ohne Spuren zu hinterlassen*	Rphy33
1-22	**Informations-manipulation**	***Präventive Massnahmen*** *- Die Wahrscheinlichkeit der Informationsmanipulation ist durch eingeführte präventive Massnahmen zu verkleinern*	Rphy34
1-23		***Protokollierung*** *- Der Zugriff auf Datenbestände ist geregelt und wird bei wichtigen Datenbeständen protokolliert*	Rphy34
1-24		***Datensicherung*** *- Die Datensicherung und Auslagerung ist für alle IT-Systeme geregelt und wird periodisch durchgeführt*	Rphy34
1-25		***Zugriffsberechtigungs-Prüfung*** *- Die Zugriffsberechtigungen werden mindestens einmal jährlich überprüft und durch den Linienvorgesetzten freigegeben*	Rphy34
1-26	**Raubüberfall**	**Unattraktivität** - Überfälle während und ausserhalb der Arbeitszeiten sind erschwert und müssen von vornherein als unattraktiv erscheinen	Rphy38
1-27		**Rückzugsmöglichkeit** - Es ist sichergestellt, dass bei einem Überfall möglichst wenige Personen gefährdet werden (Rückzugsmöglichkeit für Täter).	Rphy38
1-28		**Alarmierung und Intervention** - Die Alarmierung der Interventionskräfte bei Überfall ist jederzeit sichergestellt.	Rphy38
1-29		**Geringer finanzieller Schaden** - Die Beute ist in jedem Fall kleiner als die versicherte Summe	Rphy38
1-30		**Voraussetzung für Fahndung** - Es ist sichergestellt, dass nach einem Überfall die Voraussetzung für eine erfolgreiche Fahndung gegeben ist	Rphy38
1-31	**Sabotage**	**Eingeschränkte Möglichkeit** - Die Möglichkeiten für Sabotage-Anschläge durch Dritte oder eigene Mitarbeitende sind sowohl innerhalb als auch ausserhalb der Gebäude stark eingeschränkt.	Rphy39
1-32		**Angemessener Schutz** - Die für die Sicherheit der Gebäude wichtigen Sicherheitssysteme/-einrichtungen sind vor Sabotage angemessen geschützt	Rphy39

No.	Risiko	Schutzziele, mit Massnahmen physischer Sicherheit erreichbar ***Schutzziele, die mit anderen (nicht-physischen) Massnahmen erreichbar sind***	Wirkt auf
1-33		**Einwurfschutz** - Das Einwerfen von Gegenständen oder Eingiessen von Flüssigkeiten (z.B. Brandsätze) in besonders gefährdete Aussenhautdurchbrüche (z.B. Lüftungsöffnungen) ist erschwert	Rphy39
1-34		***Personalpolitik und Arbeitsklima*** *- Das Sabotagerisiko durch eigene Mitarbeitende ist durch eine fortschrittliche Personalpolitik und ein angenehmes Arbeitsklima stark reduziert*	Rphy39
1-35	**Spionage/ Abhören von Kommunikations-systemen**	**Auffälligkeit** - Spionage, also die Informationsbeschaffung über längere Zeit, ohne dass diese bemerkt wird, ist mit geeigneten Massnahmen zu begegnen. Insbesondere ist sichergestellt, dass eine unbefugte Informationsbeschaffung innert nützlicher Frist entdeckt wird und sich nicht über längere Zeit hinziehen kann.	Rphy40
1-36		**Anzapfen und Kabelmanipulation** - Das Anzapfen von Kommunikationsleitungen wird durch bauliche und technische Massnahmen stark eingeschränkt. Manipulationen an Leitungen werden entdeckt.	Rphy40
1-37		**Schützenswerte Räumlichkeiten** - Besonders schützenswerte Räumlichkeiten (z.B. Geschäftsleitung-Räume) sind durch weiterführende, angemessene Massnahmen (z.B. Sicht- und Schallschutz, Abstrahlschutz Bildschirme, etc.) abzusichern. Die Anforderungen sind vorgängig durch eine gezielte Risikoanalyse zu erheben.	Rphy40
1-38	**Vandalismus / Sachbeschädigung**	**Unattraktivität** - Vandalenakte sind innerhalb wie ausserhalb der Gebäude erschwert und erscheinen unattraktiv	Rphy44
1-39		**Rasche Massnahmen** - Vandalenakte werden spätestens am nachfolgenden Arbeitstag festgestellt. Entsprechende Massnahmen werden umgehend eingeleitet	Rphy44
Passive Risiken - Risiken, die durch menschliches oder technisches Versagen oder durch Naturereignisse verursacht werden			
1-40	**Abhängigkeit von Mitarbeitern und Dritten**	***Dokumentation*** *- Alle betriebswichtigen technischen Anlagen, Installationen und Betriebseinrichtungen sind während ihrer gesamten Betriebsdauer bis zum Ersatz schriftlich dokumentiert und gewährleisten dadurch eine unabhängige Wartbarkeit durch Dritte*	Rphy01
1-41		***Abhängigkeiten*** *- Abhängigkeiten von Mitarbeitenden und Dritten sind erkannt. Entsprechend dem Abhängigkeitsgrad sind Vorkehrungen für Ersatz-/ Ausweichmöglichkeiten getroffen und in angemessener Zeit verfügbar.*	Rphy01
1-42		***Knowhow*** *- Das betriebseigene Know-how ist unabhängig von Dokumentationen und Aufzeichnungen einzelner Mitarbeitenden dokumentiert, entsprechend gesichert und im Doppel ausgelagert.*	Rphy01
1-43	**Absturz von Flugkörpern**	**Restrisiko** - Die Gefährdung von Menschen und die Zerstörung von Gebäuden durch einen Flugzeugabsturz o.ä. wird als Restrisiko akzeptiert	Rphy07
1-44	**Ausfall betriebswichtiger technischer Anlagen**	**Vermeidung** - Ein möglicher Ausfall betriebswichtiger technischer Anlagen wird weitgehend vermieden und entsprechend überwacht	Rphy09
1-45		**Infrastruktur** - Die technischen Infrastrukturanlagen wie Heizung, Klima- und Lüftungsanlagen sind so zu planen, dass die Betriebskontinuität gewährleistet ist. Wo notwendig, sind redundante Anlagen respektive Umschaltmöglichkeiten und/oder Ausweichmöglichkeiten vorgesehen und installiert oder vorbereitet.	Rphy09

No.	Risiko	Schutzziele, mit Massnahmen physischer Sicherheit erreichbar *Schutzziele, die mit anderen (nicht-physischen) Massnahmen erreichbar sind*	Wirkt auf
1-46		**Zuständigkeit** - Die Zuständigkeiten und Verantwortlichkeiten für Planung, Betrieb, Wartung und Kontrolle von technischen Infrastrukturanlagen sind klar geregelt	Rphy09
1-47	**Ausfall von Technik (IT- und Netzwerksystemen)**	***Ausserhalb des Umfangs*** *- Der Ausfall von IT Systemen ist nicht Bestandteil der physischen Sicherheit, sondern wird im Rahmen des Business Continutity Managements bzw. Desaster Recovery Planning behandelt.*	Rphy11
1-48	**Ausfall von Sicherheitsanlagen**	**Verfügbarkeit** - Die Verfügbarkeit der technischen Sicherheitsanlagen ist auf hohem Niveau gehalten. Ausfälle und Störungen der Sicherheitsanlagen werden an einem zentralen Ort unverzüglich optisch und akustisch angezeigt	Rphy08
1-49		**Schutz** - Die Sicherheitsanlagen sind gegen Sabotage und Manipulation geschützt.	Rphy08
1-50		**Zuständigkeiten** - Die Zuständigkeiten und Verantwortlichkeiten für Planung, Betrieb, Wartung und Kontrolle von Sicherheitsanlagen sind klar geregelt.	Rphy08
1-51	**Ausfall von Telekommunikation sanlagen**	***Ausserhalb des Umfangs*** *- Der Ausfall von Telekommunikationsanlagen ist nicht Bestandteil der physischen Sicherheit, sondern wird im Rahmen des Business Continutity Managements bzw. Desaster Recovery Plannings behandelt*	Rphy10
1-52	**Ausfall der Versorgung mit Ressourcen**	**Funktion Fluchtwegkomponenten** - Die Funktion der für die Evakuierung notwendigen Notbeleuchtung und der technischen Fluchtwegkomponenten ist bei einem Stromausfall gewährleistet	Rphy13
1-53		**Ausfallzeiten** - Die für den ununterbrochenen und störungsfreien Betrieb wichtigen technischen Anlagen, Systeme und Installationen sind definiert. Deren maximal zulässige Ausfallzeit ist festgelegt	Rphy13
1-54		**Entdeckung und Behebung** - Technische Störungen werden rasch erkannt und entsprechend ihrer Dringlichkeit behoben	Rphy13
1-55		**Redundanz** - Redundante Einspeisungen und Verteilersysteme (z.B. Strom, Wasser, Gas) sind vorhanden, soweit diese betriebswichtigen Anlagen versorgen	Rphy13
1-56	**Brand**	**Rechtzeitige Rettung** - Unabhängig von Ort und Zeit eines Brandausbruches können sich alle Personen rechtzeitig retten	Rphy18
1-57		**Wahrscheinlichkeit minimiert** - Die Wahrscheinlichkeit eines Brandausbruches ist minimiert	Rphy18
1-58		**Früherkennung** - Ein Brandausbruch wird möglichst frühzeitig erkannt und automatisch gemeldet.	Rphy18
1-59		**Brandabschnitte** - Brandabschnitte sind gebildet, ihre Grösse ist auf das betrieblich notwendige Minimum beschränkt	Rphy18
1-60		**Emissionen eingeschränkt** - Rauch und Brandgase bleiben auf den betroffenen Brandabschnitt beschränkt	Rphy18
1-61		**Alarmierung** - Die frühzeitige Alarmierung der Feuerwehr im Brandfall ist jederzeit sichergestellt. Entsprechende Interventionswege sind bezeichnet und werden jederzeit freigehalten	Rphy18
1-62		**Brandbekämpfung** - Alle Mitarbeitenden werden regelmässig bezüglich Brandbekämpfung geschult (praktische Übungen).	Rphy18

No.	Risiko	Schutzziele, mit Massnahmen physischer Sicherheit erreichbar *Schutzziele, die mit anderen (nicht-physischen) Massnahmen erreichbar sind*	Wirkt auf
1-63		**Brandprävention** - Zur Brandprävention werden entsprechende periodische Kontrollgänge ausgeführt und deren Resultate festgehalten. Entsprechende Verbesserungen werden umgehend realisiert.	Rphy18
1-64		**Austrittserkennung** - Ein Austritt von Brennstoffen (Heizung) wird frühzeitig festgestellt und automatisch gemeldet	Rphy18
1-65		**Schadensminimierung** - Das Schadensausmass im Brandfall ist minimiert	Rphy18
1-66		**Gesetzliche Vorschriften** - Der Brandschutz ist gemäss den gesetzlichen Vorschriften einzuhalten	Rphy18
1-67		**Kabelschutz** - Betriebswichtige Elektrokabelinstallationen (Stark- und Schwachstrom/Datenleitungen) sind gegen Brandeinwirkung geschützt	Rphy18
1-68		***Relevanz*** *- Ein Brandfall bedroht die Existenz der Swisscom nicht. Insbesondere sind betriebswichtige Rechenzentren und Technikzentralen nach einem (Teil-)Brand noch funktionsfähig oder durch geeignete Redundanz abgedeckt*	Rphy18
1-69	**Unbeabsichtigtes Freisetzen von toxischen oder brennbaren Substanzen/Chemieunfall**	**Chemie-Schutz** - Das Eindringen von gesundheitsgefährdenden oder zerstörerischen Substanzen aus der Atmosphäre in die Gebäude ist durch entsprechende organisatorische Massnahmen und technischen Vorkehrungen gemäss neuestem Stand der Technik erschwert	Rphy43
1-70		**Organisatorisch Vorbereitet** - Für den Ereignisfall sind entsprechende organisatorische Massnahmen getroffen	Rphy43
1-71	**Elementargewalten**	**Neubauten** - Bei Neubauten sind entsprechende baulich-technische Vorschriften gegen Elementargewalten berücksichtigt	Rphy23
1-72	**Explosion**	**Reduktion** - Die Explosionsrisiken sind weitgehend reduziert	Rphy29
1-73		**Frühdetektion** - Ein Gasaustritt (z.B. Leck) wird frühzeitig festgestellt	Rphy29
1-74	**Informationsabfluss**	***Verhinderung*** *- Der versehentliche, unbeabsichtigte Informationsabfluss und die Informationsverfälschung sind soweit möglich verhindert bzw. werden festgestellt und umgehend unterbunden. Alle Mitarbeitenden sind über den sachgemässen Umgang mit Bürokommunikations-Systemen, Datenträgern und Daten instruiert (Vermeidung von Datenverlusten).*	Rphy32
1-75		**Erschwerung** - Spezielle baulich-technische und organisatorische Sicherheitsmassnahmen in den entsprechenden Archiven, Behältnissen und Systemen erschweren den Informationsabfluss bei Informationsträgern (in Papier- oder elektronischer Form).	Rphy32
1-76		***Sachgerechte Vernichtung*** *- Die sachgerechte Vernichtung von Daten- und Informationsträgern ist gewährleistet.*	Rphy32
1-77	**Informationsverlust**	***Regelung*** *- Informationssicherung, Lagerung, Auslagerung und Vernichtung sind für alle Informationsbestände nach Bedarf der Verfügbarkeit geregelt. Dabei ist es irrelevant, auf welchen Datenträger-Typen (Festplatten, USB, Tapes, Papier, etc.). die Informationen gespeichert sind*	Rphy35
1-78		***Zugangsgewährung*** *- Der Zugang und Zugriff auf Informationen ist geregelt, so dass die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen gewährleistet ist.*	Rphy35

No.	Risiko	Schutzziele, mit Massnahmen physischer Sicherheit erreichbar *Schutzziele, die mit anderen (nicht-physischen) Massnahmen erreichbar sind*	Wirkt auf
1-79	**Überspannung**	**Begrenzung** - Die Auswirkungen von Überspannungen sind begrenzt	Rphy42
1-80		**Schadensverhinderung** - Schäden durch Blitzeinschlag sind weitgehend verhindert	Rphy42
1-81		**EMV Schutz** - Alle elektronischen Systeme sind gegen Beschädigung durch Überspannung und Einwirkung von Störungen (EMV) geschützt	Rphy42
1-82	**Wasserschaden**	**Früherkennung** - Die Früherkennung von möglichen Wasserschäden ist sichergestellt	Rphy45
1-83		**Schadensminimierung** - Schäden durch Wassereinbrüche sind minimiert	Rphy45
1-84		**Schutz vor Leitungsbruch** - Mittels gezielter Führung von Wasserleitungen ist zu verhindern, dass Rechenzentren und Technikzentralen bei einem Leitungsbruch durch Wasser beschädigt bzw. zerstört werden. Wasserleitungen innerhalb von Räumlichkeiten mit betriebswichtiger oder kritischer Infrastruktur (RZ, TZ, USV-Zentralen, etc.) sind zu vermeiden oder abzuschotten	Rphy45

4 Übergangsbestimmungen

[16] Diese Sicherheitsanweisung ist bei Neu- und Umbauten ab Release Date anzuwenden.

5 Dokument Information

[17] Das vorliegende Dokument umfasst den Risikokatalog Physische Sicherheit, der für die Risikoanalyse, die Bewertung von Risiken und die Einstufung von Massnahmen herangezogen wird, für alle Risikobetrachtungen in und an Gebäuden und Räumlichkeiten von Swisscom AG. Er dient der Homogenisierung von Risikoeinschätzungen.

5.1 «Version 1»

Doc ID	SECDOC-103
Titel	SA Grundlage für Schutzkonzepte
Classification	C2 General
Scope of application	Swisscom AG
Issue date	29.03.2023
Status	realeased
Document subject	Sicherheitsanweisung
Related	LLV-SYS-008/ LLV-SYS-009