Instruction de sécurité

SA Base pour les concepts de protection

Swisscom SA

Group Security
Case postale
3050 Berne

Version	Date	Personne	Modifications apportées/remarques
0.1	29.03.2023	Claudio Passafaro	Création
0.2	04.04.2023	Daniel Zysset	Remaniement
1.0	24.05.2023	Claudio Passafaro	Validation

Responsable: resp. séc. Protection d'objet contre les incendies

Éditeur: resp. séc. Protection d'objet contre les incendies

Créateur: Passafaro Claudio, GSE-PHY

Création: 29.03.2023

Va à: conformément à 1.2 Champ d'application

Table des matières

1 Introduction

1.1 Contexte

[1] Une grande partie des bureaux et des bâtiments d'exploitation de Swisscom peuvent être construits et exploités selon des concepts standards.

[2] Lorsque des surfaces ou des bâtiments présentent un besoin de protection particulier, celui-ci doit être établi sur la base de critères de gestion des risques et d'objectifs de protection, en impliquant les utilisateurs des surfaces concernées. Un concept de protection spécifique à l'objet doit être élaboré sur la base de cette analyse.

[3] Les concepts de protection spécifiques à un objet doivent être vérifiés par Group Security.

[4] Le présent document comprend le catalogue des risques Sécurité physique, qui est utilisé pour l'analyse des risques, l'évaluation des risques et la classification des mesures, pour toutes les études de risques portant sur l'intérieur et l'extérieur des bâtiments et locaux de Swisscom SA. Il sert à homogénéiser l'évaluation des risques.

1.2 Champ d'application

[5] Le présent document s'applique à Swisscom (Suisse) SA dans son intégralité, comprenant l'ensemble des divisions commerciales[1] et divisions du groupe[2] ayant leur siège en Suisse et à l'étranger, ci-après dénommée Swisscom.

[6] Les sociétés du groupe mettent en place leur propre gestion de la sécurité ou s'associent à celle de Swisscom. La responsabilité de la sécurité reste du ressort de la société du groupe. La décision revient à la société du groupe et est soutenue par Group Security.

1.3 Documents de référence

[1] Directive Sécurité

[2] Security-Policy

[1] Les segments incluent Retail Customers («B2C»), Business Customers («B2B»), ainsi que IT, Network & Infrastructure («INI»)

[2] Les divisions du groupe incluent Group Business Steering («GBS»), Group Human Resources («GHR»), Group Communications & Responsibility («GCR») et Group Security & Corporate Affairs («GSA»)

2 Besoin et capacité de protection des bâtiments et des surfaces

2.1 Besoin de protection

[7] La classe de protection du conteneur de protection «bâtiment ou surface» dépend de la classe de dommage la plus élevée des objets à protéger qu'il contient (ou devra contenir).

OBJET À PROTÉGER	Classification	Classes			
Informations	Confidentialité	C1 - Public	C2 - General	C3 - Confidential	C4 - Strictly Confidential
	Intégrité	I1 - None	I2 - Basic	I3 - Medium	I4 - High
Objets matériels	Valeur monétaire	M1 - None	M2 - Basic	M3 - Medium	M4 - High

CONTENEUR DE PROTECTION	Qualification	Classes			
Espace ou surface	*Niveau de protection*	*None*	*Basic*	*Medium*	*High*
	Confidentialité	pcC1	pcC2	pcC3	pcC4
	Intégrité	pcI1	pcI2	pcI3	pcI4
	Valeur monétaire	pcM1	pcM2	pcM3	pcM4

2.2 Facteurs d'évaluation

Pour les installations TIC, les locaux de vente, les bureaux et les locaux d'archivage, ainsi que pour les salles de conférence, la confidentialité C1-C4 est en général le critère déterminant.

2.3 Évaluation des objectifs de protection sur la base des risques

[8] Un concept de sécurité se compose d'une série de mesures de sécurité coordonnées entre elles, dont la combinaison permet d'obtenir l'effet de protection souhaité. Il peut comprendre des mesures constructives, techniques, organisationnelles et d'assurance.

[9] Ces mesures sont le fruit d'une évaluation des risques. À cette occasion, les dangers associés aux objectifs de protection sont identifiés et évalués individuellement. Cette évaluation constitue finalement la base des mesures qui seront déduites en vue d'être inscrites dans le concept de sécurité.

L'objectif de l'analyse est d'obtenir une vue d'ensemble aussi complète que possible de tous les dangers et de prendre des mesures proportionnées.

2.3.1 Démarche

[10] L'analyse des risques comprend les étapes présentées dans le tableau ci-après.

[11] Il convient en principe se suivre les dispositions prévues par le règlement d'exécution de la gestion des risques (lien: Ausführungsreglement Risikomanagement_01052022.pdf (swisscom.com)). Cela concerne notamment les dispositions relatives à l'acceptation des risques.

La réalisation de l'analyse des risques peut s'inspirer des recommandations de la directive «Risk Impact Assessment» (lien: Risk Impact Assessment Weisung_DE.pdf (swisscom.com)).

Étape	Table des matières	Résultat
Recensement des objectifs de protection	Il convient tout d'abord de déterminer à quels objectifs de protection les mesures doivent répondre. Les principaux objectifs de sécurité de Swisscom sont définis dans la Security Policy (chapitre 3). En parallèle, il peut y avoir des exigences légales ou spécifiques aux clients devant être prises en compte au cas par cas.	Les objectifs de protection sont connus.
Identification des risques	Les dangers associés aux objectifs de protection sont identifiés. Le catalogue des risques figurant au point 3.1 fournit une vue d'ensemble des dangers potentiels. Les dangers ayant un effet négatif prévisible sur les objectifs de protection sont enregistrés en tant que risques.	Les risques associés aux objectifs de protection sont identifiés.
Évaluation des risques	Les risques recensés sont évalués individuellement en termes de probabilité de survenance et d'impact.	Les risques sont évalués.
Identification de mesures de gestion des risques	Cette étape consiste à prendre des mesures appropriées en fonction du niveau de risque. En règle générale, il s'agira de mesures de réduction des risques. Il est toutefois aussi possible d'accepter un risque. À cet égard, il convient de suivre le processus de gestion des risques de l'unité organisationnelle concernée.	Des mesures de gestion des risques sont définies.
Documentation des résultats	La dernière étape consiste à consigner les résultats dans le concept de sécurité.	Concept de sécurité

3 Analyse des risques

[12] Le catalogue des risques peut être consulté au point 0. Il décrit les risques ayant un impact sur les objets à protéger de Swisscom, ainsi que leur pertinence et leur délimitation pour le domaine de la sécurité physique.

[13] Le catalogue peut être utilisé pour les analyses de risques dans le domaine de la sécurité physique, l'évaluation des risques identifiés et la définition de mesures.

[14] Les objectifs de protection spécifiques sont répertoriés au point 0,

- pour les risques actifs, c'est-à-dire les risques provoqués par des actions intentionnelles et ciblées contre des objets ou des personnes,
- pour les risques passifs, c'est-à-dire les risques causés par une défaillance humaine ou technique, ou par des phénomènes naturels.

[15] Remarques: les objectifs de protection sont mentionnés lorsque des mesures pouvant être prises dans le cadre de la sécurité physique contribuent à atteindre ces objectifs de protection. Si des recoupements partiels avec la sécurité des informations sont possibles, les objectifs de protection de cette dernière ne sont toutefois en aucun cas couverts intégralement.

3.1 Catalogue des risques

Identificateur = <Numéro>Rphy (Rphy= «Risque physique»)

					Risque affectant les objets à protéger												
			Pertinent pour la sécurité physique		Protection des personnes			Protection des biens immatériels			Protection des biens matériels			Protection de la performance de l' entreprise		
N°	Risque	Description du risque	J	N	Clients	Collaborateurs	Partenaires	Informations	Savoir-faire	Propriété intellectuelle	Bâtiments	Installations	Mobilier / argent	Réputation	Produits	Environnement
	Dépendance vis-à-vis de collaborateurs et de tiers	Constitution inconsciente ou intentionnelle de connaissances chez des individus ou des tiers dont la défaillance/le départ (accident, maladie, etc.) peut entraver ou empêcher la continuité de l'exploitation d'installations et de systèmes, et/ou l'exécution de processus importants.		X					•							
	Menace de violence physique	Diffusion de messages sérieux ou de fausses déclarations (par téléphone ou par écrit) dans le but d'exercer des pressions et/ou de perturber ou de paralyser temporairement l'activité de l'entreprise.	X		•	•	•									
		Menaces contre l'intégrité physique d'individus et/ou de leur environnement personnel proche.	X		•	•	•							•		
		Mettre une personne ou un groupe de personnes en incapacité de résister, en usant de violence, de menaces graves ou de toute autre manière, afin de s'octroyer un avantage pécuniaire illégitime.	X		•	•	•									
	Agression contre des personnes	Agression violente (physique ou avec arme) contre une ou plusieurs personnes.	X		•	•	•									
	Attentat/acte de terrorisme	Attaque planifiée contre un individu, un groupe de personnes ou une infrastructure/un bâtiment, à l'aide d'une arme ou d'explosifs, dans le but de tuer.	X		•	•	•	•	•		•	•	•	•		
	Chute d'objets volants sur des ouvrages	Impact d'un avion ou de parties d'un avion sur des édifices.	X		•	•	•	•	•		•	•	•	•		
	Défaillance des installations de sécurité	Panne temporaire ou prolongée des installations de sécurité (p. ex. système de détection d'incendie et d'intrusion, système de contrôle d'accès).	X								•	•	•			

Identificateur = <Numéro>Rphy (Rphy= «Risque physique»)

					Risque affectant les objets à protéger												
			Pertinent pour la sécurité physique		Protection des personnes			Protection des biens immatériels			Protection des biens matériels			Protection de la performance de l' entreprise		
N°	Risque	Description du risque	J	N	Clients	Collaborateurs	Partenaires	Informations	Savoir-faire	Propriété intellectuelle	Bâtiments	Installations	Mobilier / argent	Réputation	Produits	Environnement
	Panne d'installations techniques essentielles à l'exploitation	Défaillance temporaire ou prolongée d'installations techniques essentielles à l'exploitation (ASI, répartiteur principal à basse tension, système de contrôle, installations de climatisation et de réfrigération, etc.)	X					•			•	•			•	
	Panne des installations de télécommunicatio n	Défaillance temporaire ou prolongée des installations de télécommunications.		X				•				•			•	
	Panne des systèmes IT et réseau	Défaillance temporaire ou prolongée des systèmes IT essentiels à l'exploitation.		X				•			•	•			•	
		Défaillance temporaire ou prolongée des systèmes réseau (WAN/LAN) essentiels à l'exploitation.		X				•			•	•			•	
	Défaillance de l'approvisionneme nt en ressources	Panne temporaire ou prolongée de l'approvisionnement en électricité (48 V ou 220 V), en eau, en chauffage urbain, en gaz, ainsi que des réseaux de télécommunications.	X					•			•	•			•	
	Escroquerie/falsific ation/abus de confiance	Manœuvres ou manipulations visant à obtenir un avantage financier ou matériel pour soi-même ou pour des tiers.		X										•		
	Corruption	Offrir, promettre, donner ou faire parvenir un cadeau (matériel/immatériel) ou un autre avantage à une personne pour qu'elle déroge aux obligations de sa profession ou de sa fonction.		X										•		
	Alerte à la bombe	Diffusion de messages sérieux ou de fausses déclarations (par téléphone ou par écrit) dans le but d'exercer des pressions et/ou de perturber ou de paralyser temporairement l'activité de l'entreprise.	X		•	•	•				•	•	•	•		
		Menaces contre l'intégrité physique des personnes.	X		•	•	•							•		

Identificateur = <Numéro>Rphy (Rphy= «Risque physique»)

					Risque affectant les objets à protéger												
			Pertinent pour la sécurité physique		Protection des personnes			Protection des biens immatériels			Protection des biens matériels			Protection de la performance de l' entreprise		
N°	Risque	Description du risque	J	N	Clients	Collaborateurs	Partenaires	Informations	Savoir-faire	Propriété intellectuelle	Bâtiments	Installations	Mobilier / argent	Réputation	Produits	Environnement
	Incendie	Incendie involontaire dû à une défaillance humaine ou technique ou à des phénomènes naturels.	X		•	•	•	•			•	•	•			
	Incendie criminel	Incendie intentionnel (l'incendie criminel est une forme particulière de sabotage).	X		•	•	•	•			•	•	•			
	Manifestation	Expression publique et collective de l'opinion de nombreuses personnes sur un terrain public ou privé.	X								•	•	•	•		
	Occupation	Occupation pacifique ou violente (non autorisée) d'un bâtiment/d'une partie de bâtiment par les employés ou par des personnes extérieures (violation de domicile).	X		•	•	•				•	•		•		
	Vol	Détournement de valeurs matérielles ou immatérielles sans s'être préalablement introduit dans un bâtiment de force.	X					•	•	•	•	•	•			
	Catastrophes naturelles	Événements naturels (p. ex. tempête, inondation, foudre, tremblement de terre) entraînant des destructions.	X		•	•	•	•			•	•	•	•	•	•
	Cambriolage	Intrusion par la force dans un bâtiment ou un local fermé à clé, ou ouverture forcée d'un contenant fermé à clé pour s'approprier de manière illicite des biens matériels ou immatériels, ou pour préparer des actes criminels.	X					•	•	•	•	•	•	•		
	Épidémie/ intoxication	Intoxication d'individus ou de groupes de personnes par l'émission de substances nocives ou hautement toxiques, de l'intérieur ou de l'extérieur, par l'air ou par des substances gazeuses dans l'air, ou par la consommation ou l'utilisation de l'eau (lavage), ou à la suite d'un contact physique avec des objets/matériaux empoisonnés ou des personnes infectées.	X		•	•	•	•	•		•			•		
	Chantage	Mettre une personne ou un groupe de personnes en incapacité de résister, en usant de violence, de menaces graves ou de toute autre manière, afin de s'assurer un avantage pécuniaire illégitime.		X	•	•	•	•		•			•	•		

Identificateur = <Numéro>Rphy (Rphy= «Risque physique»)

					Risque affectant les objets à protéger												
			Pertinent pour la sécurité physique		Protection des personnes			Protection des biens immatériels			Protection des biens matériels			Protection de la performance de l' entreprise		
N°	Risque	Description du risque	J	N	Clients	Collaborateurs	Partenaires	Informations	Savoir-faire	Propriété intellectuelle	Bâtiments	Installations	Mobilier / argent	Réputation	Produits	Environnement
	Coercition	Contraindre une personne ou un groupe de personnes à faire, ne pas faire ou tolérer quelque chose, par la violence ou la menace de dommages sérieux ou de toute autre restriction de sa capacité d'action.		X	•	•	•	•		•			•	•		
	Enlèvement	Séquestration de personnes dans le but d'imposer des exigences, associée à l'usage de violence physique et psychique. Les auteurs et les endroits dans lesquels les personnes enlevées sont détenues sont inconnus.		X	•	•	•							•		
	Explosion	Réaction chimique foudroyante, accompagnée d'une onde de choc, d'une grande puissance destructrice, souvent suivie d'un incendie.	X		•	•	•	•	•		•	•	•	•	•	•
	Prise d'otages	Séquestration de personnes dans le but de faire valoir des revendications par la menace ou le recours direct à la violence.		X	•	•	•				•		•	•		
	Vol d'identité	Vol et utilisation de l'identité d'un collaborateur ou de l'entreprise Swisscom.	X					•	•	•			•	•		
	Fuite d'informations	Divulgation involontaire ou par négligence d'informations sensibles.		X				•	•	•				•		
	Vol d'informations	Appropriation illicite d'informations sous forme physique et/ou électronique ou de supports de données.		X				•	•	•				•		
	Manipulation d'informations	Falsification (insertion, modification ou effacement) d'informations enregistrées sous forme électronique ou sur des supports de données non électroniques tels que papier, film ou support sonore.		X				•	•	•				•		
	Perte d'informations	Destruction ou perte d'informations (électroniques/physiques) classifiées ou nécessaires à l'entreprise (données/dossiers/supports de données).		X				•	•	•				•		
	Contamination de produits de consommation et	Intoxication volontaire ou involontaire de produits de consommation et de denrées alimentaires au moyen de produits chimiques ou d'autres substances dangereuses pour la santé.		X	•	•	•									•

Identificateur = <Numéro>Rphy (Rphy= «Risque physique»)

					Risque affectant les objets à protéger												
			Pertinent pour la sécurité physique		Protection des personnes			Protection des biens immatériels			Protection des biens matériels			Protection de la performance de l' entreprise		
N°	Risque	Description du risque	J	N	Clients	Collaborateurs	Partenaires	Informations	Savoir-faire	Propriété intellectuelle	Bâtiments	Installations	Mobilier / argent	Réputation	Produits	Environnement
	de denrées alimentaires															
	Pollution radioactive	Contamination radioactive de l'environnement (homme, animal, sol, eau, air, faune, etc.)		X	•	•	•				•	•				•
	Braquage	Imposition de revendications pour l'obtention de biens matériels/immatériels par l'usage direct de la force. L'agression est généralement planifiée et survient de manière inattendue.	X		•	•	•	•		•	•	•	•	•		
	Sabotage	Atteinte délibérée et planifiée à la marche de l'entreprise par l'endommagement/la mise hors service de parties de bâtiments ou d'installations importantes pour l'activité.	X			•		•	•	•	•	•	•		•	
	Espionnage/écoute de systèmes de communication	Appropriation illégale d'informations (écoute, copie, photographie, etc.), généralement sur une longue période, sans laisser de traces.	X					•	•	•				•	•	
	Grève	Refus collectif des employés d'exécuter certaines activités ou opérations en guise de mesure de lutte pour faire valoir des revendications.		X		•								•	•	
	Surtension	Augmentation momentanée de la tension dans le réseau pouvant endommager et/ou détruire des appareils électriques ou électroniques (p. ex. foudre, fluctuations de courant dans le réseau).	X			•		•			•	•			•	
	Libération accidentelle de substances toxiques ou inflammables (accident chimique)	Contamination de l'environnement par des substances toxiques, agressives/corrosives ou inflammables/explosives sous forme liquide, solide ou gazeuse (p. ex. locaux pour batteries/ASI, installations diesel, stations-service essence et diesel, locaux de produits de nettoyage dans des grands bâtiments, etc.)	X		•	•	•				•	•				•
	Vandalisme/dégradation de biens	Dommages volontaires, mais pas nécessairement ciblés, à des parties du bâtiment ou à des installations techniques.	X								•	•		•		

Identificateur = <Numéro>Rphy (Rphy= «Risque physique»)

					Risque affectant les objets à protéger												
			Pertinent pour la sécurité physique		Protection des personnes			Protection des biens immatériels			Protection des biens matériels			Protection de la performance de l' entreprise		
N°	Risque	Description du risque	J	N	Clients	Collaborateurs	Partenaires	Informations	Savoir-faire	Propriété intellectuelle	Bâtiments	Installations	Mobilier / argent	Réputation	Produits	Environnement
	Dégâts liés à l'eau	Endommagement ou destruction involontaire de biens matériels et immatériels par l'eau (p. ex. rupture de canalisation) ou par des infiltrations d'eau (nappe phréatique, eau d'extinction, etc.)	X								•	•	•	•		•

3.2 Objectifs de protection spécifiques selon la typologie des risques

N°	Risque	Objectifs de protection pouvant être atteints par des mesures de sécurité physique ***Objectifs de protection pouvant être atteints par d'autres mesures (non physiques)***	Action sur
Risques **actifs** – Risques provoqués par des actions intentionnelles et ciblées contre des objets ou des personnes.			
	Menace de violence physique	**Réduction au minimum** – La mise en danger physique de personnes et l'impact sur le fonctionnement de Swisscom d'une alerte à la bombe sont minimes.	Rphy02 Rphy03 Rphy04
		Réalisme – Une évaluation réaliste de la situation et une action adaptée à la situation sont garanties à tout moment. Toutes les mesures de fouille des bâtiments sont préparées de façon optimale.	Rphy02 Rphy03 Rphy04
		Prévention de la panique – Les situations de panique sont autant que possible évitées. Une éventuelle évacuation peut être effectuée rapidement et en toute sécurité.	Rphy02 Rphy03 Rphy04
	Agression contre des personnes	**Entrave** – Les attaques contre les personnes par des tiers/visiteurs sont plus difficiles à l'intérieur des bâtiments.	Rphy05
		Délai d'intervention – En cas d'événement, les forces d'intervention externes sont sur place dans les plus brefs délais.	Rphy05
	Escroquerie/falsification/abus de confiance	**Détection** – L'escroquerie/les tentatives de falsification et les abus de confiance sont, dans la mesure du possible, détectés dans un délai raisonnable.	Rphy14
		Enquête – En cas de suspicion ou de constatation d'escroquerie/falsification ou d'abus de confiance, une enquête est immédiatement menée afin de limiter les dommages et d'identifier les auteurs.	Rphy14
	Incendie criminel	**Prévention** – Des efforts sont entrepris pour prévenir les incendies criminels.	Rphy19
		Entrave – Il est très difficile de lancer ou d'introduire des engins incendiaires dans les bâtiments.	Rphy19
	Manifestation / Occupation	**Information** – Le responsable de la sécurité est rapidement informé des manifestations prévues ou en cours qui sont susceptibles de compromettre le fonctionnement de l'entreprise et prend des contre-mesures.	Rphy20 Rphy21
		Entrave – Si elle ne peut être empêchée, une occupation doit être fortement compliquée et avoir des effets limités.	Rphy20 Rphy21
	Vol	**Manque d'intérêt** – Les vols doivent d'emblée apparaître comme peu intéressants.	Rphy22
		Entrave – Les vols par effraction doivent dans la mesure du possible être évités.	Rphy22
		Climat de travail – Une ambiance de travail agréable et une bonne politique du personnel limitent considérablement les risques de vol par le personnel interne.	Rphy22
		Prévention – Le personnel est sensibilisé à la prévention des vols.	Rphy22
	Cambriolage	**Inutile** – Les tentatives d'effraction doivent sembler inutiles.	Rphy24

N°	Risque	Objectifs de protection pouvant être atteints par des mesures de sécurité physique ***Objectifs de protection pouvant être atteints par d'autres mesures (non physiques)***	Action sur
		Entrave – Les cambriolages sont difficiles pendant les heures de travail et très difficiles en dehors des heures de travail.	Rphy24
		Détection – Les tentatives d'effraction dans des locaux présentant des exigences de sécurité élevées (zone 4: zone de sécurité) sont immédiatement détectées, signalées et retardées par des mesures structurelles, de façon à permettre à la police d'intervenir à temps.	Rphy24
		Proportionnalité – Les tentatives d'effraction dans les bâtiments doivent être entravées (structurellement) et détectées (d'un point de vue organisationnel et technique) grâce à des mesures appropriées, adaptées au degré de protection. Dans les bâtiments nécessitant une protection élevée, une surveillance de l'enveloppe extérieure est nécessaire (p. ex. en cas de bris de verre).	Rphy24
	Vol d'identité	**Limitation des risques** – Le risque de vol et d'usurpation de l'identité d'un collaborateur ou de l'entreprise Swisscom doit être limité par les mesures préventives mises en place.	Rphy31
	Vol d'informations	***Protection contre l'effacement des traces*** *– La protection des informations de l'entreprise et des clients sous forme électronique ou physique est assurée par l'impossibilité de voler des informations et des supports d'information sans laisser de traces.*	Rphy33
	Manipulation d'informations	***Mesures préventives*** *– La probabilité de manipulation d'informations doit être limitée par la mise en place de mesures préventives.*	Rphy34
		Consignation *– L'accès aux données est réglementé et fait l'objet d'une consignation pour les données importantes.*	Rphy34
		Sauvegarde des données *– La sauvegarde et l'externalisation des données sont assurées pour tous les systèmes informatiques et effectuées régulièrement.*	Rphy34
		Vérification des droits d'accès *– Les droits d'accès sont vérifiés au moins une fois par an et validés par le supérieur hiérarchique.*	Rphy34
	Braquage	**Manque d'intérêt** – Les braquages pendant les heures de travail et en dehors sont entravés et doivent apparaître d'emblée comme peu intéressants.	Rphy38
		Possibilité de rétractation – Il est garanti que le moins de personnes possible seront mises en danger en cas d'agression (possibilité de rétractation pour l'agresseur).	Rphy38
		Alerte et intervention – L'alerte des forces d'intervention est assurée à tout moment en cas d'agression.	Rphy38
		Faible préjudice financier – Le butin est dans tous les cas inférieur à la somme assurée.	Rphy38
		Conditions préalables à la recherche – Il est garanti qu'après une agression, les conditions préalables à une recherche fructueuse sont remplies.	Rphy38
	Sabotage	**Possibilité limitée** – Les possibilités de sabotage par des tiers ou par les propres collaborateurs sont fortement limitées, tant à l'intérieur qu'à l'extérieur des bâtiments.	Rphy39
		Protection appropriée – Les systèmes/dispositifs essentiels à la sécurité des bâtiments sont protégés de façon appropriée contre le sabotage.	Rphy39

N°	Risque	Objectifs de protection pouvant être atteints par des mesures de sécurité physique ***Objectifs de protection pouvant être atteints par d'autres mesures (non physiques)***	Action sur
		Protection contre la projection d'objets – La projection d'objets ou le déversement de liquides (p. ex. des engins incendiaires) dans les ouvertures particulièrement exposées de l'enveloppe extérieure (p. ex. les ouvertures de ventilation) est entravée.	Rphy39
		Politique du personnel et ambiance de travail *– Une politique du personnel progressiste et une ambiance de travail agréable réduisent fortement le risque de sabotage par les propres collaborateurs.*	Rphy39
	Espionnage/écoute de systèmes de communication	**Détectabilité** – L'espionnage, c'est-à-dire la collecte d'informations sur une longue période sans que cela soit remarqué, doit être contré par des mesures appropriées. Il est notamment garanti qu'une collecte d'informations non autorisée sera détectée dans un délai raisonnable et ne pourra pas se prolonger.	Rphy40
		Siphonnage et manipulation de câbles – Des mesures structurelles et techniques restreignent considérablement les possibilités de mise sur écoute de lignes de communication. Les manipulations de lignes sont détectées.	Rphy40
		Locaux à protéger – Les locaux à protéger particulièrement (p. ex. locaux de la direction) doivent être protégés par des mesures supplémentaires appropriées (p. ex. protection visuelle et phonique, protection contre les émissions des écrans, etc.). Les exigences doivent être déterminées au préalable par une analyse des risques ciblée.	Rphy40
	Vandalisme / dégradation de biens	**Manque d'intérêt** – Les actes de vandalisme sont difficiles à commettre tant à l'intérieur qu'à l'extérieur des bâtiments et semblent peu intéressants.	Rphy44
		Mesures rapides – Les actes de vandalisme sont constatés au plus tard le jour ouvrable suivant. Des mesures appropriées sont immédiatement prises.	Rphy44
Risques passifs – Risques causés par une défaillance humaine ou technique, ou par des phénomènes naturels.			
	Dépendance vis-à-vis de collaborateurs et de tiers	***Documentation*** *– Tous les équipements techniques, installations et équipements d'exploitation importants pour l'activité de l'entreprise sont documentés par écrit pendant toute leur durée d'exploitation et jusqu'à leur remplacement, ce qui garantit que leur maintenance peut être assurée en toute indépendance par des tiers.*	Rphy01
		Dépendances *– Les dépendances vis-à-vis de collaborateurs et de tiers sont connues. En fonction du degré de dépendance, des dispositions sont prises afin de disposer de possibilités de remplacement/d'évitement dans un délai raisonnable.*	Rphy01
		Savoir-faire *– Le savoir-faire propre à l'entreprise est documenté, sécurisé en conséquence et externalisé en double, indépendamment des documentations et enregistrements de collaborateurs individuels.*	Rphy01
	Chute d'objets volants	**Risque résiduel** – La mise en danger de personnes et la destruction de bâtiments par un crash d'avion ou autre sont acceptées en tant que risques résiduels.	Rphy07
	Panne d'installations techniques essentielles à l'exploitation	**Prévention** – Le risque de défaillance d'installations techniques importantes pour l'exploitation est dans une large mesure évité et surveillé en conséquence.	Rphy09
		Infrastructures – Les infrastructures techniques telles que le chauffage, la climatisation et la ventilation doivent être planifiées de manière à garantir la continuité de l'exploitation. Lorsque c'est nécessaire, des installations redondantes	Rphy09

N°	Risque	Objectifs de protection pouvant être atteints par des mesures de sécurité physique ***Objectifs de protection pouvant être atteints par d'autres mesures (non physiques)***	Action sur
		ou des possibilités de commutation/substitution sont prévues et installées ou préparées.	
		Compétences – Les compétences et les responsabilités en matière de planification, d'exploitation, de maintenance et de contrôle des infrastructures techniques sont clairement définies.	Rphy09
	Panne technique (systèmes IT et réseau)	***Hors périmètre*** *– La défaillance des systèmes IT ne relève pas de la sécurité physique, mais est traitée dans le cadre du Business Continuity Management ou du Desaster Recovery Planning.*	Rphy11
	Défaillance des installations de sécurité	**Disponibilité** – La disponibilité des installations techniques de sécurité est maintenue à un niveau élevé. Les pannes et les dysfonctionnements des installations de sécurité sont immédiatement signalés par des signaux visuels et sonores à un endroit centralisé.	Rphy08
		Protection – Les installations de sécurité sont protégées contre le sabotage et les manipulations.	Rphy08
		Compétences – Les compétences et les responsabilités en matière de planification, d'exploitation, de maintenance et de contrôle des installations de sécurité sont clairement définies.	Rphy08
	Défaillance des installations de télécommunications	***Hors périmètre*** *– La défaillance des installations de télécommunications ne relève pas de la sécurité physique, mais est traitée dans le cadre du Business Continuity Management ou du Desaster Recovery Planning*	Rphy10
	Défaillance de l'approvisionnement en ressources	**Fonctionnement des composants des voies d'évacuation** – Le fonctionnement de l'éclairage de secours et des composants techniques des voies d'évacuation est garanti en cas de panne de courant.	Rphy13
		Temps d'arrêt – Les équipements, systèmes et installations techniques importants pour un fonctionnement ininterrompu et sans faille sont définis. Leur temps d'arrêt maximal autorisé est fixé.	Rphy13
		Détection et résolution – Les incidents techniques sont rapidement identifiés et résolus en fonction de leur urgence.	Rphy13
		Redondance – Des alimentations et des systèmes de distribution redondants (p. ex. électricité, eau, gaz) sont disponibles dans la mesure où ils alimentent des installations essentielles à l'exploitation.	Rphy13
	Incendie	**Sauvetage en temps utile** – Indépendamment du lieu et de l'heure d'un début d'incendie, toutes les personnes peuvent se sauver à temps.	Rphy18
		Probabilité minimum – La probabilité d'un début d'incendie est limitée au minimum.	Rphy18
		Détection précoce – Un début d'incendie est détecté le plus tôt possible et automatiquement signalé.	Rphy18
		Compartiments coupe-feu – Les compartiments coupe-feu sont formés et leur taille est limitée au minimum nécessaire à l'exploitation.	Rphy18
		Émissions limitées – La fumée et les gaz émanant de l'incendie restent confinés dans le compartiment coupe-feu concerné.	Rphy18

N°	Risque	Objectifs de protection pouvant être atteints par des mesures de sécurité physique ***Objectifs de protection pouvant être atteints par d'autres mesures (non physiques)***	Action sur
		Alerte – L'alerte rapide des pompiers en cas d'incendie est assurée à tout moment. Les voies d'intervention correspondantes sont désignées et restent accessibles à tout moment.	Rphy18
		Lutte contre l'incendie – Tous les collaborateurs sont régulièrement formés à la lutte contre l'incendie (exercices pratiques).	Rphy18
		Prévention des incendies – Pour la prévention des incendies, des rondes de contrôle sont effectuées à intervalles réguliers et leurs résultats sont consignés. Les améliorations appropriées sont mises en œuvre au plus vite.	Rphy18
		Détection des fuites – Une fuite de combustible (chauffage) est rapidement détectée et automatiquement signalée.	Rphy18
		Limitation des dommages – En cas d'incendie, l'ampleur des dommages est limitée au minimum.	Rphy18
		Prescriptions légales – La protection incendie doit être assurée conformément aux prescriptions légales.	Rphy18
		Protection des câbles – Les installations de câbles électriques importantes pour l'exploitation (courant fort et courant faible / lignes de données) sont protégées contre les effets d'un incendie.	Rphy18
		***Pertinence** – Un incendie ne menace pas l'existence de Swisscom. En particulier, les centres de calcul et les centres techniques essentiels à l'activité sont encore opérationnels après un incendie (partiel) ou sont couverts grâce à une redondance appropriée.*	Rphy18
	Libération accidentelle de substances toxiques ou inflammables / accident chimique	**Protection chimique** – La pénétration dans les bâtiments de substances nocives ou destructrices présentes dans l'atmosphère est entravée par des mesures organisationnelles appropriées et des dispositifs techniques conformes à l'état actuel de la technique.	Rphy43
		Préparation organisationnelle – Des mesures organisationnelles appropriées sont prises en cas d'événement.	Rphy43
	Catastrophes naturelles	**Constructions neuves** – Les nouvelles constructions doivent prendre en compte les prescriptions techniques et structurelles en vigueur contre les phénomènes naturels.	Rphy23
	Explosion	**Limitation** – Les risques d'explosion sont en grande partie limités.	Rphy29
		Détection précoce – Une fuite de gaz est détectée à temps.	Rphy29
	Fuite d'informations	***Prévention** – La fuite accidentelle et involontaire d'informations et la falsification d'informations sont empêchées autant que possible ou sont détectées et immédiatement stoppées. Tous les collaborateurs sont formés sur l'utilisation appropriée des systèmes de communication bureautiques, des supports de données et des données (prévention des pertes de données).*	Rphy32
		Entrave – Des mesures de sécurité spéciales relevant des techniques de construction et d'organisation compliquent la fuite d'informations (sur support papier ou électronique) dans les archives, les conteneurs et les systèmes concernés.	Rphy32

N°	Risque	Objectifs de protection pouvant être atteints par des mesures de sécurité physique ***Objectifs de protection pouvant être atteints par d'autres mesures (non physiques)***	Action sur
		Destruction appropriée *– Une destruction appropriée des supports de données et d'informations est garantie.*	Rphy32
	Perte d'informations	***Règlement*** *– La sauvegarde des informations, leur stockage, leur externalisation et leur destruction sont gérés pour chaque corpus d'informations en fonction de la disponibilité requise. Et ce, indépendamment du type de support de données (disques durs, USB, bandes, papier, etc.) sur lequel les informations sont stockées.*	Rphy35
		Droits d'accès *– L'accès et l'utilisation des informations sont réglementés de manière à garantir la confidentialité, l'intégrité et la disponibilité des informations.*	Rphy35
	Surtension	**Limitation** – Les effets des surtensions sont limités.	Rphy42
		Prévention des dommages – Les dommages causés par la foudre sont en grande partie évités.	Rphy42
		Protection CEM – Tous les systèmes électroniques sont protégés contre les dommages dus aux surtensions et aux interférences (CEM).	Rphy42
	Dégâts liés à l'eau	**Détection précoce** – La détection précoce d'éventuels dégâts des eaux est assurée.	Rphy45
		Limitation des dommages – Les dommages causés par les infiltrations d'eau sont réduits au minimum.	Rphy45
		Protection contre les ruptures de canalisations – Un cheminement ciblé des conduites d'eau doit éviter que les centres de données et les centres techniques ne soient endommagés ou détruits par l'eau en cas de rupture de canalisation. Les conduites d'eau à l'intérieur des locaux abritant des infrastructures vitales ou critiques (centres de calcul, centres de techniques, centrales ASI, etc.) doivent être évitées ou isolées.	Rphy45

4 Dispositions transitoires

[16] La présente instruction de sécurité s'applique aux constructions nouvelles et transformées à compter de la Release Date.

5 Informations sur le document

[17] Le présent document comprend le catalogue des risques Sécurité physique, qui est utilisé pour l'analyse des risques, l'évaluation des risques et la classification des mesures, pour toutes les études de risques portant sur l'intérieur et l'extérieur des bâtiments et locaux de Swisscom SA. Il sert à homogénéiser l'évaluation des risques.

5.1 «Version 1»

Doc ID	SECDOC-103
Title	SA Base pour les concepts de protection
Classification	C2 General
Scope of application	Swisscom SA
Issue date	29.03.2023
Status	realeased
Document subject	Instruction de sécurité
Related	LLV-SYS-008/ LLV-SYS-009