nstruction de sécurité

SA-02159-C1–Concept de protection des biens du groupe

Swisscom SA

Group Security
Case postale
3050 Berne

Version	Date	Personne	Modifications apportées/remarques
0.1	05.04.2022	Claudio Passafaro	–
0.2	14.10.2022	Claudio Passafaro	Modifications mineures
0.9	09.12.2022	Daniel Zysset	Traduit et finalisé
1.0	09.12.2022	Thomas Dummermuth	Vérification/libération

Responsable: SiBe Brand-Objektschutz
Éditeur: SiBe Brand-Objektschutz
Création:05.04.2022
Créateur: Passafaro Claudio
Va à: conformément à 1.2 Champ d'application

Sommaire

1 Introduction 3

1.1 But et objet du document 3
1.2 Champ d'application 3

2 Concept 3

2.1 Mesures 4
2.2 Objectifs de la protection 4
2.3 Mise en œuvre des objectifs de protection 4
2.4 Principes de la protection des biens 5

3 Minimum Security Standards 6

3.1 Objectifs de protection légaux 6
3.2 Bâtiment 6
3.3 Protection du périmètre 6
3.4 Vidéosurveillance 6
3.5 Organisation 6
3.6 Détection des intrusions 6
3.7 Contrôle, inspection et maintenance 6
3.8 Documentation 7

4 Soutien 7

4.1 Contrôles 7
4.2 Conseils généraux sur la protection des biens 7

5 Information sur le document 8

5.1 «Version 1» 8

1 Introduction

1.1 But et objet du document

[1] La sécurité revêt une importance cruciale pour Swisscom.

[2] Le présent document décrit la mise en œuvre de la Security Policy édictée par le responsable Group Security en ce qui concerne la protection des biens. Il définit à cet effet le niveau d'ambition, les objectifs de protection et les exigences minimales.

[3] Le document constitue la référence pour garantir un niveau de sécurité adéquat dans l'ensemble du groupe Swisscom et pour évaluer et mettre en œuvre des mesures appropriées.

1.2 Champ d'application

[4] Le présent document s'applique à Swisscom SA dans son intégralité, comprenant l'ensemble des sociétés du groupe, divisions commerciales et divisions du groupe ayant leur siège en Suisse et à l'étranger. Le terme Swisscom est utilisé pour désigner les unités suivantes: divisions commerciales et du groupe de Swisscom SA et Swisscom (Suisse) SA.

[5] La conformité des locaux existants est à contrôler. En cas de lacunes, des améliorations seront apportées selon une priorité basée sur les risques.

[6] Les nouveaux concepts de protection pour des biens spécifiques (solutions globales) doivent être soumis à Group Security pour vérification. Ils seront étudiés au cas par cas.

2 Concept

[7] Chaque situation étant spécifique, il n'existe pas de concept unique de protection des biens. La procédure de base est la suivante:

- Déterminer les menaces et les biens à protéger
- Déterminer les risques
- Déduire les objectifs de protection spécifiques
- Définir la politique de sécurité ou le dispositif de sécurité (stratégie de défense/surveillance et d'intervention)

[8] La présente approche vise à:

- Évaluer les risques de façon objective et spécifique à l'entreprise
- Définir des mesures conformes aux objectifs de protection, à partir de critères clairs et compréhensibles
- Établir une base pour des mesures de sécurité équilibrées et optimisées sur le plan économique
- Élaborer un concept de sécurité modulaire et orienté sur les groupes cibles
- Établir des bases d'audit pour le contrôle périodique des mesures de sécurité prises

2.1 Mesures

[9] Tous les bâtiments et/ou locaux doivent être classés selon leur besoin de protection et être protégés par un concept ou des mesures de protection des biens appropriés.

[10] Un tel concept écrit comprend au minimum:

- Appréciation et évaluation des risques
- Exigences opérationnelles (acceptation du risque et objectifs de protection)
- Dispositif de sécurité (mesures de sécurité)

2.2 Objectifs de la protection

[11] Pour Swisscom, les objectifs supérieurs suivants de la gestion de la sécurité revêtent une importance capitale (ils s'appuient sur la Swisscom Security Policy):

- Protection des personnes
- Protection des informations
- Protection des biens matériels
- Protection de la performance de l'entreprise

[12] Concernant la protection des biens, lesdits objectifs sont subdivisés et priorisés comme suit:

- Vie et santé du personnel et des personnes qui se trouvent dans nos locaux
- Actifs de l'entreprise
- Savoir-faire de l'entreprise
- Processus d'affaires, communication, IT et infrastructure
- Environnement
- Réputation
- Propriétés adjacentes

2.3 Mise en œuvre des objectifs de protection

[13] À partir des résultats de l'évaluation des risques, les mesures de protection des biens sont analysées au cas par cas. Elles visent à empêcher les événements de sécurité (actes de malveillance, délits et autres situations indésirables). De plus, les incidents ainsi que les dommages conséquents doivent pouvoir être limités et maîtrisés.

[14] Les risques peuvent être évités, réduits, écartés ou absorbés.

[15] Une analyse des risques permet de déterminer et d'évaluer les mesures de défense, de surveillance et d'intervention nécessaires. Des mesures doivent être prises pour réduire les risques à un niveau acceptable. Possibilités:

[16] Dissuader – l'auteur potentiel doit être dissuadé de poursuivre son action en découvrant de façon inattendue des mesures ou réactions visant à prévenir les dommages.

[17] Décourager – l'auteur potentiel doit être **découragé** de poursuivre son action par des obstacles.

[18] Retarder – l'auteur potentiel doit être retardé dans son action pour permettre à la réaction de prévention des dommages d'être efficace dans une large probabilité.

[19] Empêcher – l'auteur potentiel doit être empêché dans son action jusqu'à ce qu'une réaction de prévention des dommages puisse être mise en œuvre avec certitude.

[20] Détecter – les événements de sécurité doivent être détectés dans un délai raisonnable afin de déclencher des réactions de prévention et de réduction des dommages.

[21] Intervenir – les événements de sécurité nécessitent une **intervention** pour prévenir ou réduire les dommages.

2.4 Principes de la protection des biens

[22] Une **effraction** sur la périphérie du bâtiment (portes, fenêtres et enceinte du bâtiment) doit être entravée de façon à pouvoir détecter avec une large probabilité les tentatives d'effraction.

[23] Le **vol** de biens, marchandises et équipements d'exploitation doit être entravé et, dans le cas d'informations et de biens sensibles, ne pas pouvoir passer inaperçu.

[24] Pour les bâtiments comportant des dangers particuliers ou ayant une présence des personnes importante, une **évacuation** immédiate doit être garantie dans un délai de 15 minutes en cas de scénarios présentant un potentiel de risque en restant dans le bâtiment.

[25] Les **actes de sabotage** ne doivent avoir sur l'activité aucun impact grave dépassant la valeur définie des objectifs généraux de protection pour la perte d'exploitation et les dommages matériels.

[26] L'**accès** au bâtiment hors des heures de travail doit être contrôlé et consigné à toutes les entrées, de manière à empêcher tout accès non autorisé.

[27] L'**accès** au bâtiment pendant les heures de travail doit être contrôlé et consigné à toutes les entrées, de manière à empêcher tout accès non autorisé.

[28] Il convient de garantir l'**absence de toute personne non autorisée dans le bâtiment**.

[29] Les **dommages** prévisibles **causés par les éléments naturels** (cartes de risques) sont à empêcher par des mesures de protection.

[30] Partout où cela est possible, des mesures préventives contre les **agressions** doivent être mises en œuvre. Après un tel événement, une prise en charge professionnelle des personnes concernées doit être assurée.

[31] L'**espionnage** doit être empêché par des mesures proportionnées, en particulier dans les lieux présentant un risque particulier à cet égard.

3 Minimum Security Standards

3.1 Objectifs de protection légaux

[32] Il convient de s'assurer que toutes les exigences légales en vigueur localement (lois, autorisations, directives et normes) sont respectées.

3.2 Bâtiment

[33] Le bâtiment doit pouvoir résister aux conditions météorologiques locales. L'accès non autorisé doit pouvoir être évité dans la mesure du possible.

3.3 Protection du périmètre

[34] Les limites de propriété ou, en dernier recours, les passages entre des zones publiques ou mixtes et des zones internes doivent présenter des fermetures physiques clairement identifiables.

3.4 Vidéosurveillance

[35] Si un système de vidéosurveillance s'avère nécessaire conformément à l'analyse des risques, les enregistrements correspondants doivent être indexés en fonction des événements.

[36] Un concept écrit définissant les paramètres pertinents est nécessaire.

[37] Les dispositions légales en vigueur en matière de protection des données doivent être respectées. En Suisse, il s'agit de la loi fédérale sur la protection des données RS 235.1.

3.5 Organisation

[38] Lorsque des entreprises et des personnes accomplissent des missions de sécurité, les tâches et obligations correspondantes sont à documenter par écrit et doivent être signées par le mandataire responsable.

3.6 Détection des intrusions

[39] Si un système d'alarme anti-intrusion s'avère nécessaire conformément à l'analyse des risques, il convient de s'assurer que les messages d'alerte sont suivis et documentés.

3.7 Contrôle, inspection et maintenance

[40] Il convient de garantir que tous les équipements, installations et systèmes de sécurité sont régulièrement inspectés, testés et entretenus. Les installations mises hors service pour entretien, réparation ou contrôle doivent être remises en service aussitôt après.

3.8 Documentation

[41] Le concept de protection et, le cas échéant, les analyses de risques sont à tenir à jour et à contrôler à intervalles définis. Les concepts de protection, en tout ou partie, doivent être disponibles et accessibles aux personnes en charge de la protection des biens.

4 Soutien

4.1 Contrôles

[42] Group Security réalise des contrôles sur les sites selon une approche basée sur les risques. Les sites s'engagent à contacter Group Security en cas de changements pertinents sur des sites importants pour l'entreprise.

4.2 Conseils généraux sur la protection des biens

[43] Group Security peut être contacté en qualité de centre de compétence afin d'obtenir des conseils et une assistance. Un soutien sur la méthode d'évaluation des risques en vue de déterminer la sécurité appropriée est assuré par GSE-SEL.

5 Information sur le document

Le présent document décrit la mise en œuvre de la Security Policy en ce qui concerne la protection des biens. Il définit à cet effet le niveau d'ambition, les objectifs de protection et les exigences minimales.

Le document constitue la référence pour garantir un niveau de sécurité adéquat dans l'ensemble du groupe Swisscom et pour évaluer et mettre en œuvre des mesures appropriées.

5.1 «Version 1»

Doc ID	SA-02159-C1-Concept de protection des biens du groupe
Classification	C1 Public
Scope of application	Swisscom SA
Issue date	05.04.2022
Statut	released
Document subject	Instruction de sécurité
Related LLV	LLV-IAM-032/ LLV-SYS-002/ LLV-SYS-003/ LLV-SYS-006/ LLV-IAM-068/ LLV-SYS-024/ LLV-ANA-002/ LLV-ANA-010