Instruction de sécurité

SA-02101-C1 Règlement de sécurité physique pour les espaces de bureau

Swisscom SA

Group Security
Case postale
3050 Berne

Version	Date	Personne	Modifications apportées/remarques
0.1	11.03.2022	Claudio Passafaro	Version préliminaire
0.2	20.10.2022	Claudio Passafaro	Remaniement
0.3	24.11.2022	Claudio Passafaro	Remaniement
0.4	30.11.2022	Claudio Passafaro	Remaniement
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: 11.03.2022

Créateur: Passafaro Claudio
Va à: conformément à 2 Champ d'application

Sommaire

1 Terminologie

[1] Clean desk policy; directive sur la manière de laisser son poste de travail en cas d'absence.

[2] Wirecenter; locaux contenant des serveurs pour des applications logicielles de bureau exclusivement.

2 Champ d'application

[3] Le présent règlement concerne les espaces de bureaux utilisés par Swisscom. Il s'applique à la fois aux bâtiments dont Swisscom est propriétaire et à ceux qu'elle loue.

[4] Le présent règlement ne concerne pas explicitement:

- Les locaux loués pour des Wirecenter
- Les locaux avec des infrastructures techniques, p. ex. serveurs, utilisées pour l'exploitation des télécommunications. L'accès auxdits locaux doit être géré exclusivement par Swisscom, des dispositions séparées s'appliquent.
- Bâtiment Central Office, des dispositions séparées s'appliquent.

3 Clarification préalable

[5] Il convient de clarifier en amont le besoin de protection requis pour les activités et l'utilisation prévues. Il revient aux futurs utilisateurs (division opérationnelle) de s'assurer que le besoin de protection est correctement déterminé et déclaré.

[6] Le besoin de protection peut augmenter selon les points suivants (liste non exhaustive):

- Présence régulière de personnes particulièrement exposées
- Forte concentration d'infrastructures et d'équipements de valeur
- Traitement de données et d'informations particulièrement sensibles
- Importance accrue pour le maintien de l'exploitation

[7] La division opérationnelle qui met les espaces à disposition doit s'assurer que la capacité de protection physique correspond au besoin de protection déclaré. De plus, il convient de vérifier si le bâtiment ou les espaces sont également pertinents à long terme pour les utilisations prévisibles. Des espaces inadaptés peuvent nécessiter des mesures de sécurité supplémentaires, à prendre en compte dans l'analyse de rentabilité.

[8] En cas de changement d'usage ou de modification des informations traitées sur l'espace, il incombe aux utilisateurs (division opérationnelle) de vérifier le besoin de protection et de déclarer un ajustement si nécessaire.

3.1 Aucun besoin de protection particulier

[9] Les dispositions au point 4 Protection de base s'appliquent.

3.2 Locaux avec exigences SL2

[10] Les normes de sécurité minimales selon «Security Services – Use Cases – Contrôle d'intégrité – Dispositions de protection physique pour les locaux avec exigences SL2» s'appliquent.

3.3 Besoin de protection accru

[11] Il convient d'élaborer un concept de sécurité basé sur les risques, qui servira de référence pour le concept de protection.

4 Protection de base

4.1 Accès ordinaire

[12] L'accès ordinaire du personnel Swisscom aux espaces Swisscom passe par le système de gestion des accès de Swisscom. Cela garantit à Swisscom de pouvoir gérer les autorisations de façon efficiente.

[13] L'accès ordinaire pour les prestataires FM par exemple s'effectue aussi de préférence via le système de gestion des accès de Swisscom. Toutefois, ces accès peuvent aussi être gérés par un système interne, notamment celui du propriétaire. À cet effet, les dispositions relatives aux systèmes tiers de contrôle d'accès (point 5) sont à prendre en compte.

4.2 Accès extraordinaire

[14] Des événements extraordinaires ou la nécessité de limiter des dommages peuvent exiger que le propriétaire ou ses prestataires disposent d'un accès d'urgence. Le processus d'accès d'urgence nécessaire ou les moyens d'accès (p. ex. clés physiques) doivent être élaborés sur le plan technique et/ou organisationnel de façon à consigner leur utilisation.

[15] L'usage d'un deuxième système tiers de contrôle des accès, incluant les espaces Swisscom, est autorisé à des fins exceptionnelles. À cet effet, les dispositions relatives aux systèmes tiers de contrôle d'accès (point 4.4) sont à prendre en compte.

[16] Si une installation de détection des dangers surveille en tout ou partie les espaces Swisscom et que celle-ci alerte des services d'urgence publics (p. ex. pompiers), il sera alors choisi un système auquel seuls les pompiers, le cas échéant Swisscom, ont accès. Les moyens d'accès pour ce type d'intervention seront interdits aux tiers, y compris le propriétaire. Si un service d'intervention privé est impliqué comme détenteur de clés, un accord contractuel sera conclu avec Swisscom pour imposer par écrit au prestataire des obligations de diligence, de responsabilité, d'annonce en cas de perte et de conservation en lieu sûr.

4.3 Sécurité physique

[17] Les espaces Swisscom doivent être fermés de chaque côté et les murs, fenêtres et portes doivent être conçus de manière à empêcher toute intrusion non autorisée sans être remarquée.

[18] Les portes séparant des zones communes de l'espace Swisscom doivent de façon générale être équipées d'une fermeture automatique ainsi que d'une surveillance électrique. Le dispositif doit intégrer un contact de verrouillage et un capteur magnétique connectés en série. Si la porte n'est pas fermée dans le temps imparti, une alarme à distance doit se déclencher.

[19] Les ascenseurs ne doivent pas ouvrir directement sur des espaces Swisscom. S'il est impossible de faire autrement, il convient de prévoir dans l'idéal des portes d'entrée avec système de contrôle d'accès Swisscom.

[20] Pour les espaces loués, Swisscom reçoit une liste (plan de fermeture) de toutes les clés mécaniques ou mécatroniques qui permettent d'accéder aux espaces Swisscom. L'usage prévu pour chacune desdites clés est déclaré et leur traçabilité est documentée. En principe, Swisscom utilise son propre système de fermeture pour les espaces en location.

4.4 Systèmes de contrôle d'accès non Swisscom

[21] Les systèmes de contrôle d'accès non Swisscom ne sont autorisés qu'à titre exceptionnel et requièrent l'approbation de Group Security.

[22] Ils doivent être gérés par un système de gestion qui consigne en détail les accès.

[23] Les protocoles d'accès sont à conserver pendant au moins 6 mois.

[24] Les droits d'accès valables pour les espaces Swisscom qui y sont gérés doivent être contrôlés et assainis selon une méthode adaptée et à un intervalle approprié, afin de garantir que toute personne n'ayant plus besoin desdits droits n'est plus autorisée à y accéder.

[25] Toutes les personnes autorisées sur les espaces Swisscom et dans les systèmes de sécurité pertinents doivent être soumises à un contrôle de sécurité régulier (extrait du casier judiciaire et du registre des poursuites) et une déclaration de confidentialité de chaque personne mentionnée sera exigée et conservée.

[26] Swisscom est autorisée à consulter les protocoles d'accès et les journaux de contrôle.

4.5 Alimentation électrique des dispositifs de sécurité

[27] L'alimentation électrique des dispositifs de sécurité doit suivre les dispositions légales. Il n'y a pas d'autres exigences opérationnelles.

[28] Les dispositifs de sécurité suivants, le cas échéant, doivent rester en service même en cas de coupure de courant (liste non exhaustive).

- Installations de détection des dangers, systèmes d'alarme de l'entreprise, systèmes de gestion des bâtiments et de sécurité
- Systèmes d'aspiration de fumée
- Systèmes d'évacuation
- Systèmes de contrôle d'accès
- Systèmes de vidéosurveillance
- Éclairage de sécurité, éclairage des sorties de secours
- Portes battantes, portes coulissantes, portails, sas, en particulier le long des voies d'évacuation

[29] La fonctionnalité doit être garantie soit mécaniquement, soit au moyen d'une ASI, d'une batterie ou d'un générateur de secours.

5 Sites à l'étranger

5.1 Exception

[30] Les dispositions du point 4 ne s'appliquent pas aux sites à l'étranger.

5.2 Systèmes de contrôle d'accès non Swisscom à l'étranger

[31] L'utilisation de systèmes de contrôle d'accès non Swisscom est tolérée, une approbation de Group Security est nécessaire. Les conditions suivantes s'appliquent:

- Le système de contrôle d'accès doit consigner en détail tous les accès.
- Les données sont à conserver durant un délai suffisant.
- Un concept écrit doit être élaboré et présenté à Swisscom.

5.3 Clean desk policy

[32] L'application du point 5.2 requiert de déclarer et d'instaurer une clean desk policy dans les espaces Swisscom concernés. Cette politique doit être définie par écrit avec des instructions d'action concrètes. Elle doit contenir au minimum les points suivants:

- Les informations professionnelles doivent être rangées avant que la personne ne quitte son poste de travail.
- Les documents physiques contenant des informations professionnelles doivent être conservés en lieu sûr fermé à clé.

6 Droits de contrôle et de consultation

6.1 Droit d'audit

[33] Swisscom se réserve un droit d'audit afin de contrôler le respect des accords contractuels, l'intégrité et le niveau de sécurité des solutions (techniques) choisies pour les contrôles d'accès et le renforcement physique de la périphérie.

6.2 Droit de consultation

[34] Swisscom se réserve le droit de consulter les journaux de dysfonctionnement, d'alarme et d'accès des systèmes d'accès et d'alarme dans les espaces loués afin de contrôler les événements pertinents en matière de sécurité.

6.3 Obligation de soutien

[35] Le bailleur s'engage à soutenir Swisscom en qualité de partenaire dans les cas décrits aux points 6.1 et 6.2 ci-dessus et à fournir en intégralité et en temps voulu les documents nécessaires dans un format lisible.

7 Autorisations

[36] Seuls les membres des départements de sécurité de Swisscom (Suisse) SA sont autorisés à demander et à consulter les données d'accès ou d'autres enregistrements de sécurité (CCTV, etc.).

[37] Les données d'accès et les enregistrements de sécurité peuvent être consultés par l'équipe d'exploitation du système en question pour une première évaluation. Toute transmission d'informations en interne ou en externe nécessite l'analyse et l'approbation de Group Security (GSE-PHY).

8 Informations contractuelles

[38] Les dispositions de sécurité sont à convenir avec le propriétaire dans le contrat de location, à savoir:

- Droits de contrôle et de consultation, y compris désignation des personnes autorisées par Swisscom conformément au point 5.
- Dispositions de diligence et de sécurité relatives aux moyens d'accès physiques et électroniques selon les points 4.2 et 4.4 ou bien le point 5.2 pour les sites à l'étranger.

9 Information sur le document

Le présent règlement de sécurité définit le cadre de la sécurité physique sur les espaces de bureau. Il contient des mesures pour une protection de base, définit les responsabilités concernant l'identification du besoin de protection spécifique et l'application à l'étranger.

9.1 «Version 1»

Doc ID	SA-02101-C1 Règlement de sécurité physique pour les espaces de bureau
Classification	C1 Public
Scope of application	Swisscom SA
Issue date	11.03.2022
Statut	realeased
Document subject	Instruction de sécurité
Related	LLV-SYS-007/ LLV-SYS-008/ LLV-SYS-009/ LLV-SYS-023/ LLV-DAT-012/ LLV-IAM-039/ LLV-IAM-056/ LLV-IAM-057