Istruzioni sulla sicurezza

SA Sicurezza fisica per spazi adibiti a ufficio

Swisscom SA

Group Security
Casella postale
3050 Berna

Versione	Data	Persona	Modifiche apportate/Osservazioni
1.0	09.12.2022	Thomas Dummermuth	Collaudo/rilascio
1.1	09.07.2023	Claudio Passafaro	Disposizioni per l'estero integrate nella sezione 4

Responsabile: SiBe Brand-Objektschutz
Edito da: SiBe Brand-Objektschutz
Redazione: 09.07.2023
Creato da: Passafaro Claudio
Destinatari: v. 2 Campo di applicazione

Indice

1 Definizioni

[1] Clean desk policy: direttiva che specifica in che modo i collaboratori devono lasciare la postazione di lavoro durante le assenze.

[2] Wire center: locali che ospitano server destinati unicamente ad applicativi software da ufficio.

2 Campo di applicazione

[3] Le presenti istruzioni sono valide per gli spazi adibiti a ufficio utilizzati da Swisscom. Si applicano sia agli edifici di proprietà di Swisscom che a quelli in locazione.

[4] Sono esplicitamente esclusi dal campo di applicazione delle presenti istruzioni:

- i locali presi in locazione per wire center.
- i locali con infrastrutture tecniche come server funzionali all'esercizio della telecomunicazione. L'accesso a tali locali deve essere gestito esclusivamente da Swisscom e si applicano disposizioni separate.
- la sede Central Office, a cui si applicano disposizioni separate.

3 Accertamento preliminare

[5] Occorre accertare tempestivamente il livello di protezione necessario in funzione delle attività e dell'utilizzo previsti. È responsabilità della futura utenza (divisione operativa) accertarsi che il livello di protezione necessario venga determinato e dichiarato correttamente.

[6] Il livello di protezione necessario può aumentare in relazione ai fattori seguenti (elenco non esaustivo):

- Presenza regolare di persone particolarmente esposte
- Elevata concentrazione di valore con riferimento a infrastrutture e arredi
- Trattamento di dati e informazioni degni di particolare protezione
- Importanza elevata per la prosecuzione dell'attività operativa

[7] La divisione operativa che mette a disposizione gli spazi deve assicurare che la capacità di protezione degli stessi sia conforme al livello di protezione dichiarato. Inoltre, occorre verificare se l'edificio o gli spazi sono idonei agli utilizzi previsti anche a lungo termine. Gli spazi inadatti possono rendere necessarie misure di sicurezza supplementari di cui occorre tenere conto nella valutazione economica.

[8] Qualora venga modificato l'utilizzo o cambino le informazioni trattate in uno spazio, è responsabilità dell'utenza (divisione operativa) verificare il livello di protezione necessario ed eventualmente dichiarare una modifica.

3.1 Locali senza uno specifico livello di protezione necessario

[9] Si applicano le disposizioni previste per la protezione di base di cui al punto 4.

3.2 Locali con requisiti SL2

[10] Vanno rispettati gli standard di sicurezza minimi previsti da «Security Services – Use Cases – Verifica dell'integrità – Disposizioni di protezione fisica per locali con requisiti SL2».

3.3 Locali in cui è necessario un livello di protezione elevato

[11] Va messo a punto un piano di sicurezza basato sul rischio in funzione del quale viene elaborato un piano di protezione.

4 Protezione di base

4.1 Accesso ordinario

[12] L'accesso ordinario per i collaboratori Swisscom agli spazi Swisscom avviene attraverso il sistema di gestione degli accessi di Swisscom. In questo modo viene garantito che Swisscom possa gestire le autorizzazioni in modo efficiente.

[13] Anche l'accesso ordinario ad es. per fornitori di servizi FM avviene preferibilmente attraverso il sistema di gestione degli accessi di Swisscom. Tuttavia, è ammesso anche che gli stessi vengano gestiti per mezzo di un sistema per il controllo degli accessi installato nell'edificio, ad es. appartenente al proprietario dello stabile. A tal fine vanno osservate le disposizioni per sistemi di terzi per il controllo degli accessi di cui al punto 4.4.

4.2 Accesso straordinario

[14] In caso di eventi straordinari o a fini di riduzione di danni può rendersi necessario che il proprietario dello stabile o i suoi fornitori di servizi procedano a un accesso d'emergenza. Il processo di accesso d'emergenza e i mezzi di accesso (ad es. chiavi fisiche) a tal fine necessari devono essere tecnicamente e/o organizzativamente concepiti in modo tale che la consegna di uno di questi mezzi di accesso venga protocollata.

[15] Per finalità straordinarie è ammesso l'impiego di un ulteriore sistema di terzi per il controllo degli accessi che include anche gli spazi di Swisscom. A tal fine vanno osservate le disposizioni per sistemi di terzi per il controllo degli accessi di cui al punto 4.4.

[16] Se un impianto di segnalazione di pericolo sorveglia parti degli spazi di Swisscom e trasmette un allarme ai servizi pubblici di emergenza (come i pompieri), a tal fine va scelto un sistema a cui possano accedere esclusivamente i pompieri ed eventualmente anche Swisscom. L'accesso a mezzi di accesso per gli interventi deve essere precluso a tutti i terzi così come al proprietario dello stabile. Se le chiavi vengono affidate a un servizio d'intervento privato, il suo coinvolgimento rende necessario un accordo contrattuale con Swisscom che imponga in forma scritta al fornitore di servizi gli obblighi di diligenza, la responsabilità, l'obbligo di informare in caso di smarrimento e la conservazione sicura.

4.3 Sicurezza fisica

[17] Gli spazi di Swisscom devono essere chiusi su ogni lato; pareti, finestre e porte devono essere tali da impedire che un'intrusione non autorizzata possa passare inosservata.

[18] Le porte che conducono dagli spazi comuni agli spazi di Swisscom devono essere a chiusura e bloccaggio automatici, oltre a disporre di una sorveglianza elettrica. Su ogni porta vanno montati un contatto di sicurezza e un sensore magnetico in serie. Se la porta non viene chiusa entro un tempo prestabilito, si deve attivare un allarme a distanza.

[19] Gli impianti elevatori non possono condurre direttamente negli spazi di Swisscom. Qualora ciò sia inevitabile, va preferibilmente installata una porta al piano con sistema per il controllo degli accessi di Swisscom.

[20] Negli spazi in locazione, Swisscom riceve un elenco (piano di chiusura) di tutte le chiavi meccaniche o meccatroniche che consentono di accedere agli spazi di Swisscom. Per ognuna di queste chiavi viene dichiarata la destinazione d'uso e viene documentato in che modo è garantita la tracciabilità del suo utilizzo. In linea di massima, Swisscom utilizza una propria serratura a carico del locatario.

4.4 Sistemi di terzi per il controllo degli accessi

[21] I sistemi di controllo degli accessi non-Swisscom sono consentiti in casi eccezionali e richiedono l'approvazione del Group Security. A tal fine, è necessario redigere un progetto scritto, che contenga almeno le seguenti disposizioni, e sottoporlo alla Group Security.

[22] I sistemi di terzi per il controllo degli accessi devono essere gestiti da un sistema che registra gli accessi in modo tracciabile.

[23] I protocolli degli accessi devono essere conservati per almeno 6 mesi.

[24] I diritti di accesso validi per gli spazi di Swisscom e gestiti su tali sistemi devono essere verificati e corretti con una metodologia appropriata e a intervalli adeguati per assicurare che nessuna persona conservi il diritto di accesso pur non avendone più la necessità.

[25] Swisscom è autorizzata a consultare i protocolli degli accessi e i giornali di controllo.

[26] Una politica di clean desk viene dichiarata e applicata nelle aree Swisscom corrispondenti. La politica di pulizia delle scrivanie deve essere messa per iscritto con istruzioni specifiche per l'azione. Deve contenere almeno i seguenti punti:

- Prima di lasciare il posto di lavoro, deve essere ripulito dalle informazioni commerciali
- I documenti fisici contenenti informazioni aziendali devono essere conservati sottochiave

4.5 Alimentazione elettrica degli impianti di sicurezza

[27] L'alimentazione elettrica degli impianti di sicurezza deve avvenire nel rispetto delle disposizioni di legge. Non vengono definiti ulteriori requisiti aziendali.

[28] I seguenti impianti di sicurezza, ove presenti, devono rimanere operativi anche in caso di interruzione della corrente (elenco non esaustivo):

- Impianti di segnalazione di pericolo, impianti di allarme aziendali, sistemi BMS e LLL
- Sistemi di aspirazione del fumo
- Impianti di evacuazione
- Sistemi per il controllo degli accessi
- Impianti di videosorveglianza
- Illuminazione di sicurezza, indicazioni luminose delle uscite di emergenza

– Porte girevoli, porte scorrevoli, cancelli, bussole antirapina – in particolare lungo le vie di fuga

[29] Il funzionamento deve essere assicurato meccanicamente, mediante gruppo di continuità, batteria o generatore d'emergenza.

5 Diritti di controllo e di consultazione

5.1 Diritto di audit

[30] Swisscom si riserva un diritto di audit per verificare il rispetto degli accordi contrattuali, dell'integrità e del livello di sicurezza delle soluzioni (tecniche) selezionate per il controllo degli accessi e l'hardening fisico della periferia.

5.2 Diritto di consultazione

[31] Swisscom si riserva di consultare i giornali di panne, allarmi e accessi dei sistemi di accesso e di allarme degli spazi in locazione al fine di verificare eventi rilevanti per la sicurezza.

5.3 Obbligo di assistenza

[32] Il locatore si impegna ad assistere Swisscom in maniera collaborativa nei casi di cui ai precedenti punti 6.1 e 6.2 e a mettere a disposizione la documentazione a tal fine necessaria in modo leggibile, completo e celere.

6 Autorizzazioni

[33] Sono autorizzati a richiedere e consultare i dati sugli accessi o altre registrazioni di sicurezza (CCTV ecc.) esclusivamente le persone appartenenti ai reparti addetti alla sicurezza di Swisscom (Svizzera) SA.

[34] Ai fini di una prima valutazione, i dati sugli accessi e le registrazioni di sicurezza possono essere visionati dal team che gestisce il relativo sistema. Il loro inoltro all'interno o all'esterno dell'azienda è soggetto a valutazione e autorizzazione di Group Security (GSA-GSE-PHY).

7 Questioni contrattuali

[35] Le disposizioni rilevanti per la sicurezza devono essere pattuite in sede di contratto di locazione con il locatore, segnatamente:

- Diritti di controllo e di consultazione a inclusione dei nominativi delle persone autorizzate di Swisscom ai sensi del punto 5.
- Disposizioni in materia di diligenza e sicurezza riguardo ai mezzi di accesso fisici ed elettronici ai sensi del punto 4.2 e del punto 4.4 risp. del punto 5.2 per le sedi all'estero.

8 Informazioni sul documento

Le presenti istruzioni sulla sicurezza definiscono la base di riferimento per la sicurezza fisica negli spazi adibiti a ufficio. Esse riportano misure per una protezione di base, individuano le responsabilità per l'individuazione degli spazi in cui è necessario un livello di protezione particolare e ne disciplinano l'applicazione all'estero.

8.1 «Versione 1.1»

Doc ID	SECDOC-129
Titel	SA Sicurezza fisica per spazi adibiti a ufficio
Classificazione	C1 Public
Ambito di applicazione	Swisscom SA
Data di emissione	09.07.2023
Stato	realeased
Oggetto del documento	Istruzioni sulla sicurezza
Correlazioni	LLV-SYS-007/ LLV-SYS-008/ LLV-SYS-009/ LLV-SYS-023/ LLV-DAT-012/ LLV-IAM-039/ LLV-IAM-056/ LLV-IAM-057