Sicherheitsanweisung

SA-02101-C1 Physische Sicherheitsvorgaben für Office-Flächen

Swisscom AG

Group Security
Postfach
3050 Bern

Version	Datum	Person	Vorgenommene Anpassungen/Bemerkungen
0.1	11.03.2022	Claudio Passafaro	Vorabzug
0.2	20.10.2022	Claudio Passafaro	Überarbeitung
0.3	24.11.2022	Claudio Passafaro	Überarbeitung
0.4	30.11.2022	Claudio Passafaro	Überarbeitung
0.9	09.12.2022	Daniel Zysset	Übersetzt und finalisiert
1.0	09.12.2022	Thomas Dummermuth	Prüfung/Freigabe

Verantwortlich: SiBe Brand-Objektschutz
Herausgeber: SiBe Brand-Objektschutz
Erstellung: 11.03.2022
Ersteller: Passafaro Claudio
Geht an: gemäss 2 Geltungsbereich

Inhalt

1 Begriffe

[1] Clean desk policy; Richtlinie, wie Mitarbeitende den Arbeitsplatz bei Abwesenheit zurücklassen müssen.

[2] Wirecenter; Räume, die Server für ausschliesslich Büro-Softwareanwendungen beinhalten

2 Geltungsbereich

[3] Diese Vorgabe betrifft von Swisscom genutzte Büroflächen. Sie gelten sowohl für Gebäude, die sich im Besitz der Swisscom befinden sowie auch für solche, die angemietet sind.

[4] Nicht unter diese Vorgabe fallen explizit:

- angemietete Räume für Wirecenter.
- Räume mit technischen Infrastrukturen wie Server, die dem Betrieb der Telekommunikation dienen. Der Zugang dazu muss exklusiv durch Swisscom verwaltet werden, es gelten separate Bestimmungen.
- Central Office-Gebäude, es gelten separate Bestimmungen.

3 Vorabklärung

[5] Es ist frühzeitig zu klären, welcher Schutzbedarf die vorgesehenen Tätigkeiten und Nutzung nach sich ziehen. Es liegt in der Verantwortung der künftigen Nutzerschaft (Geschäftsbereich), sicherzustellen, dass der Schutzbedarf korrekt ermittelt und deklariert wird.

[6] Der Schutzbedarf kann sich wegen folgender Punkte (nicht abschliessende Aufzählung) erhöhen:

- Regelmässige Anwesenheit besonders exponierter Personen
- Hohe Wertkonzentration von Infrastruktur und Einrichtung
- Umgang mit besonders schützenswerten Daten und Informationen
- Erhöhte Wichtigkeit für die Aufrechterhaltung des Betriebs

[7] Der Geschäftsbereich, der die Flächen zur Verfügung stellt, hat sicherzustellen, dass die Schutzfähigkeit der Fläche dem deklarierten Schutzbedarf entspricht. Zudem ist zu überprüfen, ob das Gebäude beziehungsweise die Flächen auch langfristig sinnvoll für die absehbaren Nutzungen ist. Unpassende Flächen können zusätzliche Sicherheitsmassnahmen erforderlich machen, was in die Wirtschaftlichkeitsbetrachtung einzubeziehen ist.

[8] Erfolgt eine Nutzungsänderung oder eine Änderung der auf der Fläche verarbeiteten Informationen, ist die Nutzerschaft (Geschäftsbereich) dafür verantwortlich, den Schutzbedarf zu überprüfen und gegebenenfalls eine Anpassung zu deklarieren.

3.1 Kein besonderer Schutzbedarf

[9] Es gelten die Bestimmungen gemäss Grundschutz Ziffer 4 umzusetzen.

3.2 Räume mit SL2-Anforderungen

[10] Die minimalen Sicherheitsstandards gemäss "Security Services – Use Cases – Integritätsprüfung - Physische Schutzbestimmungen für Räume mit SL2-Anforderungen" sind umzusetzen.

3.3 Erhöhter Schutzbedarf

[11] Ein risikobasiertes Sicherheitskonzept ist auszuarbeiten, aus dem ein darauf abgestimmtes Schutzkonzept abgeleitet wird.

4 Grundschutz

4.1 Ordentlicher Zutritt

[12] Der ordentliche Zutritt für Swisscom-Mitarbeitende zu den Swisscom-Flächen erfolgt über das Swisscom Zutritts-Managementsystem. So wird gewährleistet, dass Swisscom Berechtigungen effizient verwalten kann.

[13] Der ordentliche Zutritt für z.B. FM-Dienstleister erfolgt vorzugsweise ebenfalls über das Swisscom Zutritts-Managementsystem. Es ist aber auch zulässig, diese Zutritte über ein hauseigenes Zutrittskontrollsystem z.B. des Eigentümers zu verwalten. Hierzu sind die Bestimmungen für fremde Zutrittskontrollsysteme Ziffer 5 zu berücksichtigen.

4.2 Ausserordentlicher Zutritt

[14] Ausserordentliche Ereignisse oder zur Verminderung von Schäden können es erfordern, dass der Eigentümer oder deren Dienstleister sich einen Notzutritt verschaffen müssen. Der dafür erforderliche Notzutrittsprozess beziehungsweise Zutrittsmittel (wie physische Schlüssel) müssen technisch und/oder organisatorisch so ausgestaltet werden, dass die Behändigung eines entsprechenden Zutrittsmittel protokolliert wird.

[15] Der Einsatz eines zweiten, fremden Zutrittskontrollsystem, welches auch die Swisscom-Flächen umfassen, sind für ausserordentliche Zwecke zulässig. Hierzu sind die Bestimmungen für fremde Zutrittskontrollsysteme Ziffer 4.4 zu berücksichtigen.

[16] Überwacht eine Gefahrenmeldeanlage Teile der Swisscom-Fläche und alarmiert diese öffentliche Notfalldienste (wie die Feuerwehr), so ist hierfür ein System zu wählen, auf welches ausschliesslich die Feuerwehr, gegebenenfalls auch Swisscom, zugreifen kann. Auszuschliessen ist der Zugriff auf Interventionszutrittsmittel für sämtliche Dritte wie auch dem Eigentümer. Wird ein privater Interventionsdienst als Schlüsselträger eingebunden, so ist eine vertragliche Vereinbarung mit Swisscom erforderlich, welche dem Dienstleister Sorgfaltspflichten, Haftung, Meldepflicht bei Verlust und die sichere Aufbewahrung schriftlich auferlegen.

4.3 Physische Sicherheit

[17] Swisscom-Flächen müssen allseitig verschlossen sowie Wände, Fenster und Türen so beschaffen sein, dass ein unberechtigtes Eindringen nicht unbemerkt erfolgen kann.

[18] Türen, die von Allgemeinflächen zur Swisscom-Fläche führen, sind grundsätzlich mit automatischer Riegelauslösung und selbsttätig schliessend auszustatten sowie mit einer elektrischen Überwachung auszurüsten. Es ist je ein Riegelkontakt und ein Magnetsensor in Serie geschaltet einzubauen. Wird die Türe innerhalb einer definierten Zeit nicht geschlossen, ist eine Fernalarmierung auszulösen.

[19] Aufzugsanlagen dürfen nicht direkt in Swisscom-Flächen führen. Wenn sich dies nicht vermeiden lässt, sind vorzugsweise Vortüren mit Zutrittskontrollsystem Swisscom vorzusehen.

[20] Bei Mietflächen erhält Swisscom eine Auflistung (Schliessplan) sämtlicher mechanischer oder mechatronischer Schlüssel, welche den Zugang zu Swisscom-Flächen ermöglichen. Es wird für jeden dieser Schlüssel der Verwendungszweck deklariert und dokumentiert wie die Nachvollziehbarkeit der Verwendung dieser Schlüssel sichergestellt ist. Grundsätzlich verwendet Swisscom eine eigene Mieterschliessung.

4.4 Swisscom-fremde Zutrittskontrollsysteme

[21] Swisscom-fremde Zutrittskontrollsysteme werden nur in Ausnahmefällen zugelassen und erfordern die Bewilligung von Group Security.

[22] Fremde Zutrittskontrollsysteme müssen von einem Managementsystem verwaltet werden, welches die Zutritte nachvollziehbar registriert.

[23] Zutrittsprotokolle sind während mindestens 6 Monaten aufzubewahren.

[24] Die darauf verwalteten, für Swisscom-Flächen gültigen Zutrittsrechte müssen mit einer geeigneten Methodik und in einem geeigneten Intervall überprüft und bereinigt werden, um sicherzustellen, dass keine Personen, welche die Zutrittsrechte nicht mehr benötigen, weiterhin Zutrittsberechtigt sind.

[25] Sämtliche für Swisscom-Flächen berechtigte Personen und Zugriffsberechtigte auf sicherheitsrelevante Systeme sind einer regelmässigen Sicherheitsprüfung (Strafregisterauszug und Betreibungsregisterauszug) zu unterziehen und von jeder genannten Person ist eine Vertraulichkeitserklärung einzuverlangen und aufzubewahren.

[26] Swisscom ist berechtigt, Einsicht in Zutrittsprotokolle und Kontrolljournale zu nehmen.

4.5 Stromversorgung von Sicherheitseinrichtungen

[27] Die Stromversorgung von Sicherheitseinrichtungen hat gemäss gesetzlichen Bestimmungen zu erfolgen. Es werden keine darüberhinausgehenden betrieblichen Anforderungen gestellt.

[28] Folgende Sicherheitseinrichtungen müssen, sofern vorhanden, auch im Falle eines Stromunterbruchs in Betrieb bleiben (Aufzählung nicht abschliessend):

- Gefahrenmeldeanlagen, betriebliche Alarmmeldeanlagen, Gebäude- und Sicherheitsleitsysteme
- Rauch-Ansaugsysteme
- Evakuierungsanlagen
- Zutrittskontrollsysteme
- Videoüberwachungsanlagen
- Sicherheitsbeleuchtung, Notausgangsleuchten
- Drehtüren, Schiebetüren, Tore, Schleusen – insbesondere in Fluchtwegen

[29] Die Sicherstellung der Funktionalität ist entweder mechanisch, mittels USV, Batterie oder Notstromgenerator zu gewährleisten.

5 Standorte im Ausland

5.1 Ausnahme

[30] Für Standorte im Ausland gelten die Bestimmungen gemäss Ziffer 4 nicht.

5.2 Swisscom-fremde Zutrittskontrollsysteme im Ausland

[31] Der Einsatz Swisscom-fremder Zutrittskontrollsysteme wird toleriert, eine Bewilligung von Group Security ist erforderlich. Es gelten folgende Auflagen:

- Das Zutrittskontrollsystem muss alle Zutritte nachvollziehbar registrieren
- Daten sind für eine ausreichende Zeit aufzubewahren
- Es ist ein schriftliches Konzept zu verfassen und Swisscom vorzulegen

5.3 Clean desk policy

[32] Voraussetzung für die Anwendung von Ziffer 5.2 ist, dass in den entsprechenden Swisscom-Flächen eine clean desk policy deklariert und durchgesetzt wird. Die clean desk policy muss schriftlich mit konkreten Handlungsanweisungen festgelegt werden. Sie muss im Minimum folgende Punkte enthalten:

- Vor dem Verlassen des Arbeitsplatzes ist derselbe von geschäftlichen Informationen zu bereinigen.
- Physische Dokumente mit geschäftlichen Informationen müssen unter Verschluss verwahrt werden.

6 Kontroll- und Einsichtsrechte

6.1 Auditrecht

[33] Swisscom behält sich ein Auditrecht vor, um die Einhaltung vertraglicher Vereinbarungen, die Integrität und Sicherheitslevel der gewählten (technischen) Lösungen zur Zutrittskontrolle und physischen Härtung der Peripherie zu überprüfen.

6.2 Recht zur Einsichtnahme

[34] Swisscom behält sich die Einsichtnahme in Störungs-, Alarm- und Zutrittsjournale der Zutritts- und Alarmsysteme der angemieteten Flächen vor, um sicherheitsrelevante Ereignisse zu überprüfen.

6.3 Unterstützungspflicht

[35] Der Vermieter verpflichtet sich, Swisscom im Falle der gemäss vorangehenden Ziffern 6.1 und 6.2 partnerschaftlich zu unterstützen und die dafür erforderlichen Unterlagen lesbar, vollständig und zeitnah zur Verfügung zu stellen.

7 Berechtigungen

[36] Berechtigt zur Einforderung und Einsichtnahme in Zutrittsdaten oder weitere Sicherheitsaufzeichnungen (CCTV etc.) sind ausschliesslich Angehörige der Sicherheitsabteilungen von Swisscom (Schweiz) AG.

[37] Zutrittsdaten und Sicherheitsaufzeichnungen können vom jeweiligen Systembetreiberteam für eine Erstbeurteilung eingesehen werden. Eine Weitergabe intern wie extern erfordert eine Beurteilung und Freigabe durch Group Security (GSE-PHY).

8 Vertragliches

[38] Sicherheitsrelevante Bestimmungen sind im Mietvertrag mit dem Eigentümer zu vereinbaren, namentlich:

- Kontroll- und Einsichtsrechte inklusive Bezeichnung der Berechtigten seitens Swisscom gemäss Ziffer 5.
- Sorgfalts- und Sicherheitsbestimmungen zu physischen und elektronischen Zutrittsmitteln gemäss Ziffer 4.2 und Ziffer 4.4. beziehungsweise Ziffer 5.2 für Standorte im Ausland.

9 Dokument Information

Diese Sicherheitsvorgabe definiert den Rahmen für die physische Sicherheit auf Office-Flächen. Sie enthält Massnahmen für einen Grundschutz, definiert Verantwortlichkeiten bezüglich der Erkennung von besonderem Schutzbedarf und die Anwendung im Ausland.

9.1 «Version 1»

Doc ID	SA-02101-C1 Physische Sicherheitsvorgaben für Office-Flächen
Classification	C1 Public
Scope of application	Swisscom AG
Issue date	11.03.2022
Status	realeased
Document subject	Sicherheitsanweisung
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