Sicherheitsanweisung

# SA-02159-C1-Objektschutzkonzept Konzern

Swisscom AG

Group Security
Postfach
3050 Bern

| Version | Datum | Person | Vorgenommene Anpassungen/Bemerkungen |
|---|---|---|---|
| 0.1 | 05.04.2022 | Claudio Passafaro | - |
| 0.2 | 14.10.2022 | Claudio Passafaro | Geringfügige Bereinigung |
| 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: 05.04.2022
Ersteller: Passafaro Claudio
Geht an: gemäss 1.2 Geltungsbereich

## Inhalt

# 1 Einleitung

## 1.1 Ziel und Zweck des Dokuments

[1] Sicherheit hat für Swisscom einen zentralen Stellenwert.

[2] Im vorliegenden Dokument wird die Umsetzung der vom Leiter Group Security erlassenen Security Policy für den Bereich Objektschutz beschrieben. Zu diesem Zweck werden der Ambitionslevel, die Schutzziele und Mindestanforderungen festgelegt.

[3] Sie bildet die Grundlage, um ein angemessenes Sicherheitsniveau in der gesamten Swisscom-Gruppe zu gewährleisten und zur Bewertung und Umsetzung geeigneter Massnahmen.

## 1.2 Geltungsbereich

[4] Dieses Dokument gilt für die gesamte Swisscom AG, mit allen Konzerngesellschaften, Geschäfts- und Konzernbereichen mit Sitz im In- und Ausland. Der Begriff Swisscom wird für die folgenden Einheiten verwendet: Geschäfts- und Konzernbereiche der Swisscom AG und die Swisscom (Schweiz) AG.

[5] Bestehende Räumlichkeiten sind auf ihre Konformität zu überprüfen. Im Falle von Lücken, sind Verbesserungen gemäss risikobasierter Priorität vorzunehmen.

[6] Neue objektspezifische Objektschutzkonzepte (Gesamtlösungen) müssen der Group Security zur Überprüfung eingereicht werden. Sie werden von Fall zu Fall geprüft.

# 2 Konzept

[7] Da jede Gegebenheit einzigartig ist, gibt es kein einheitliches Objektschutzkonzept. Grundlegend ist wie folgt vorzugehen:

- Ermitteln der Bedrohungen und schützenswerten Objekte
- Ermitteln der Risiken
- Ableiten der spezifischen Schutzziele
- Festlegen der Sicherheitspolitik bzw. des Sicherheitsdispositivs (Abwehr-/ Überwachung- und Interventionsstrategie)

[8] Ziele dieses Ansatzes sind:

- Objektive, betriebsspezifische Beurteilung der Risiken
- Schutzzielorientierte Massnahmenfestlegungen anhand von nachvollziehbaren Kriterien
- Grundlage für wirtschaftlich optimierte, ausgewogene Sicherheitsmassnahmen
- Modular aufgebautes, zielgruppenorientiertes Sicherheitskonzept
- Auditierungsgrundlagen zur periodischen Kontrolle der getroffenen Sicherheitsmassnahmen

## 2.1 Massnahmen

[9] Alle Gebäude und/oder Räumlichkeiten sind bezüglich Schutzbedarf einzuordnen und mit einem angemessenen Objektschutzkonzept beziehungsweise Objektschutzmassnahmen zu schützen.

[10] Ein schriftliches Objektschutzkonzept umfasst im Minimum:

- Beurteilung und Bewertung der Risiken
- Betriebliche Anforderungen (Risikoakzeptanz und Schutzziele)
- Sicherheitsdispositiv (Sicherheitsmassnahmen)

## 2.2 Schutzziele

[11] Für Swisscom sind folgende übergeordnete Sicherheitsziele des Security Managements von zentraler Bedeutung (Grundlage bildet die Swisscom Security Policy):

- Schutz der Personen
- Schutz von Informationen
- Schutz der materiellen Werte
- Schutz der Unternehmensleistung

[12] Für den Objektschutz werden diese Schutzziele wie folgt weiter unterteilt und priorisiert:

- Leben und Gesundheit der Mitarbeitenden und Personen, die sich in unseren Räumlichkeiten aufhalten
- Vermögenswerte des Unternehmens
- Knowhow des Unternehmens
- Businessprozesse, Kommunikation, IT und Infrastruktur
- Umwelt
- Reputation
- Angrenzende Grundstücke

## 2.3 Schutzzielumsetzung

[13] Basierend auf den Ergebnissen der Risikobewertung werden Objektschutzmassnahmen von Fall zu Fall bewertet. Sie sollen dem Eintritt von Sicherheitsereignissen (böswillige Handlungen, Delikte und andere unerwünschte Zustände) vorbeugen. Ausserdem sollen die Vorfälle sowie die daraus resultierenden Schäden begrenzbar und beherrschbar werden.

[14] Risiken können vermieden, gemindert, abgewälzt oder selbst getragen werden.

[15] Anhand einer Risikoanalyse können erforderliche abwehrende, überwachende und intervenierende Massnahmen ermittelt und bewertet werden. Massnahmen sind vorzukehren, um die Risiken auf ein akzeptables Niveau zu senken. Möglichkeiten:

[16] Abschrecken – die potenzielle Täterschaft soll durch das Vorfinden unerwarteter schadenabwehrender Massnahmen oder Reaktionen von ihrem weiteren Handeln abgeschreckt werden.

[17] Abhalten – die potenzielle Täterschaft soll durch Erschwernisse vom weiteren Handeln abgehalten werden.

[18] Verzögern – Der potenziellen Täterschaft soll der Erfolg verzögert werden, damit die schadenabwehrende Reaktion mit hoher Wahrscheinlichkeit wirksam werden kann.

[19] Verhindern – Der potenziellen Täterschaft soll der Erfolg bis zum sicheren Wirksamwerden einer schadenabwehrenden Reaktion verhindert werden.

[20] Detektion – Sicherheitsereignisse sollen innert nützlicher Frist detektiert werden, um schadenabwehrende und schadenmindernde Reaktionen auszulösen.

[21] Intervention – Sicherheitsereignisse erfordern eine Intervention zur Schadenabwehr oder Schadenminderung.

## 2.4 Objektschutz-Leitsätze

[22] Ein Einbruch an der Gebäudeperipherie (Türen, Fenster und Gebäudehülle) soll erschwert werden, sodass Einbruchversuche mit grösster Wahrscheinlichkeit festgestellt werden können.

[23] Der Diebstahl von Werten, Waren und Betriebseinrichtungen soll erschwert werden und bei sensitiven Informationen und Werten, nicht unbemerkt erfolgen können.

[24] Für Gebäude mit besonderen Gefahren oder hohen Personenbelegungen muss eine sofortige Evakuation der Personen aus Gebäuden innerhalb von 15 Minuten gewährleistet werden, wenn Szenarien mit Gefährdungspotential beim Verbleib im Gebäude vorhanden sind.

[25] Sabotagehandlungen dürfen keine gravierenden Auswirkungen auf den Betrieb haben, die den definierten Wert der generellen Schutzziele für den Betriebsausfall und den Sachschaden übersteigen.

[26] Der Zutritt zum Gebäude ausserhalb der Arbeitszeit soll an allen Eingängen kontrolliert und registriert sein, sodass ein unberechtigter Eintritt verhindert werden kann.

[27] Der Zutritt zum Gebäude innerhalb der Arbeitszeit soll an allen Eingängen kontrolliert sein, sodass ein unberechtigter Eintritt verhindert werden kann.

[28] Es muss sichergestellt werden, dass sich keine unberechtigten Personen im Gebäude aufhalten.

[29] Vorhersehbare Elementarschäden (Gefahrenkarten) sind mit Schutzmassnahmen zu verhindern.

[30] Wo möglich, sind präventive Massnahmen gegen Überfall zu implementieren. Nach einem solchen Ereignis ist eine professionelle Betreuung Betroffener sicherzustellen.

[31] Spionage ist mit verhältnismässigen Massnahmen zu verhindern, insbesondere an Orten, die hierfür ein besonderes Risiko aufweisen.

# 3 Minimum Security Standards

## 3.1 Gesetzliche Schutzziele

[32] Es ist sicherzustellen, dass alle lokal geltenden gesetzlichen Anforderungen (Gesetze, Bewilligungsauflagen, Richtlinien und Standards) eingehalten werden.

## 3.2 Gebäude

[33] Das Gebäude muss ortsüblichen Witterungsbedingungen standhalten können. Unerlaubter Zutritt muss möglichst verhindert werden können.

## 3.3 Perimeter-Schutz

[34] An Liegenschaftsgrenzen beziehungsweise spätestens am Übergang von öffentlichen oder gemischten Zonen zu internen Zonen müssen klar erkennbare physische Abschlüsse aufweisen.

## 3.4 Videoüberwachung

[35] Sollte ein Videoüberwachungssystem in Übereinstimmung mit der Risikoanalyse notwendig sein, müssen deren Aufzeichnungen ereignisgesteuert indexiert werden.

[36] Ein schriftliches Konzept mit der Festlegung relevanter Parameter ist erforderlich.

[37] Die geltenden gesetzlichen Datenschutzbestimmungen sind einzuhalten, in der Schweiz das eidgenössische Datenschutzgesetz SR 235.1.

## 3.5 Organisatorisches

[38] Wo Unternehmen und Personen Sicherheitsaufgaben erbringen, sind die entsprechenden Aufgaben und Pflichten schriftlich zu dokumentieren und vom verantwortlichen Auftraggeber zu unterzeichnen.

## 3.6 Einbruchmeldeanlagen

[39] Sollte eine Einbruchmeldeanlage in Übereinstimmung mit der Risikoanalyse notwendig sein, muss sichergestellt werden, dass Alarmmeldungen verfolgt und dokumentiert werden.

## 3.7 Prüfung, Inspektion und Wartung

[40] Es ist sicherzustellen, dass alle Sicherheitseinrichtungen, -anlagen und -systeme regelmäßig überprüft, getestet und gewartet werden. Anlagen, wie wegen Wartung, Reparatur oder Prüfung ausser Betrieb gesetzt werden, müssen danach sofort wieder in Betrieb genommen werden.

## 3.8 Dokumentation

[41] Das Schutzkonzept sowie wo vorhanden Risikoanalysen sind auf dem neuesten Stand zu halten und in definierten Abständen zu überprüfen. Schutzkonzepte (oder Teile davon) sind für am Objektschutz Beteiligte verfügbar und zugänglich zu machen.

# 4 Unterstützung

## 4.1 Kontrollen

[42] Group Security führt Kontrollen an Standorten nach einem risikobasierten Ansatz durch. Es wird erwartet, dass sich die Standorte bei relevanten Änderungen an unternehmenswichtigen Standorten an Group Security wenden.

## 4.2 Allgemeine Objektschutzberatung

[43] Group Security kann als Kompetenzzentrum für Beratung und Unterstützung kontaktiert werden. Unterstützung bei der Methodik der Risikobewertung zur Bewertung der angemessenen Sicherheit wird durch GSE-SEL geleistet.

# 5 Dokument Information

Im vorliegenden Dokument wird die Umsetzung der Security Policy für den Bereich Objektschutz beschrieben. Zu diesem Zweck werden der Ambitionslevel, die Schutzziele und Mindestanforderungen festgelegt.

Sie bildet die Grundlage, um ein angemessenes Sicherheitsniveau in der gesamten Swisscom-Gruppe zu gewährleisten und zur Bewertung und Umsetzung geeigneter Massnahmen.

## 5.1 «Version 1»

| | |
|---|---|
| Doc ID | SA-02159-C1-Objektschutzkonzept Konzern |
| Classification | C1 Public |
| Scope of application | Swisscom AG |
| Issue date | 05.04.2022 |
| Status | released |
| sDocument subject | Sicherheitsanweisung |
| 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 |