

Sicherheitsanweisung

SA-02143-C1 Film- und Fotoaufnahmen

Swisscom AG

Group Security

Postfach

3050 Bern

| Version | Datum | Person | Vorgenommene Anpassungen/Bemerkungen |
|---------|------------|-------------------|--------------------------------------|
| 0.5 | 20.08.2022 | André Papageorgiu | Entwurf |
| 0.6 | 25.08.2022 | Claudio Passafaro | Finalisierung für Vernehmlassung |
| 0.7 | 19.10.2022 | Daniel Zysset | Formatierung und Struktur |
| 0.8 | 10.11.2022 | Claudio Passafaro | Letzte Rückmeldungen eingepflegt |
| 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: 20.08.2022

Ersteller: Passafaro Claudio

Geht an: gemäss 1.1 Geltungsbereich

Inhalt

| | | |
|----------|--|----------|
| 1 | Einleitung | 3 |
| 1.1 | Geltungsbereich | 3 |
| 1.2 | Referenzierte Dokumente | 3 |
| 1.3 | Schutzziel | 3 |
| 2 | Bestimmungen | 4 |
| 2.1 | Allgemeine Bestimmungen | 4 |
| 2.2 | Foto- und Filmaufnahmen zur innerbetrieblichen Verwendung | 4 |
| 2.3 | Foto- und Filmaufnahmen zur ausserbetrieblichen Verwendung | 4 |
| 3 | Vollzug | 5 |
| 4 | Dokument Information | 6 |
| 4.1 | «Version 1.0» | 6 |

1 Einleitung

¹ Swisscom ist ein bekanntes Telekommunikationsunternehmen. Sicherheit hat für Swisscom einen zentralen Stellenwert und damit sind auch Vertrauenswürdigkeit und Zuverlässigkeit zentrale Qualitätsattribute. Als grösstes Telekommunikationsunternehmen der Schweiz sind wir nicht nur als primäres Angriffsziel attraktiv, unsere Infrastruktur ist für Kriminelle oder Nachrichtendienste auch als Sprungbrett interessant, um an Daten von Dritten beziehungsweise unserer Kunden zu gelangen. Hackerangriffe erfolgen nicht mehr ausschliesslich online, zunehmend wird für erfolgreiches Hacking vorgängig sogenanntes Social Engineering betrieben.

² Social Engineering ist ein Verfahren, um mittels Ausnutzen menschlichen Verhaltens an Informationen zu gelangen, die letztlich für verschiedenste Betrugsmaschinen verwendet werden. Dabei werden menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft, Angst oder Respekt vor Autorität ausgenutzt, um an vertrauliche Informationen zu gelangen, unbewusst Schadsoftware einzuschleusen oder Sicherheitsfunktionen ausser Kraft zu setzen.

³ Zentrales Merkmal bei Angriffen mithilfe Social Engineering ist die Täuschung über die Identität und die Absicht der Täterschaft. Dabei verwendet die Täterschaft betriebsinterne Informationen zu Personen, Funktionen, Standorte, Prozesse, Firmenslang usw.

⁴ Als primäre Informationsquelle nutzt die Täterschaft gezielt öffentlich zugängliche Quellen wie Fotos und Filme, die in sozialen Netzwerken oder im Internet publiziert wurden.

1.1 Geltungsbereich

⁵ Die vorliegende Sicherheitsanweisung regelt den Umgang mit Film- und Fotoaufnahmen durch Swisscom-Mitarbeitende und auf sämtlichen von Swisscom genutzten Flächen.

⁶ Sie gilt zudem für Tochtergesellschaften mit deren Mitarbeitenden sowie für Auftragnehmer, die von Swisscom genutzte Flächen betreten. Sie gilt hingegen nicht für deren Flächen und Gebäude.

⁷ Sie gilt ergänzend zu gesetzlichen Bestimmungen wie beispielsweise für den Daten- und Persönlichkeitsschutz.

1.2 Referenzierte Dokumente

⁸ Das Security Framework Swisscom befindet sich auf einem eigenen SharePoint.

[1][Direktive-Sicherheit](#)

[2][SE-POL-01428-C2-Security-Policy](#)

[3][Schweizerisches Bundesgesetz über den Datenschutz \(DSG\) 235.1](#)

1.3 Schutzziel

⁹ Bei Film- und Fotoaufnahmen ist sichergestellt, dass:

- der Schutz vertraulicher und geheimer Informationen gewährleistet ist,
- die unkontrollierte Verbreitung vertraulicher und geheimer Informationen verhindert wird und

- der öffentliche Einblick in unternehmensinterne Abläufe, Rollen und Informationen begrenzt wird.

2 Bestimmungen

2.1 Allgemeine Bestimmungen

- ¹⁰ Jeder Betreiber von Flächen kann aufgrund des lokalen Schutzbedarfs generelle Film- und Fotoverbote und Ausnahmegewilligungsprozesse erlassen.
- ¹¹ Es sind keine persönlichen, vertraulichen oder geheimen Informationen preiszugeben, die Swisscom, Mitarbeitenden, Kunden oder Partnern gehören.
- ¹² Nur als öffentlich klassifizierte Informationen (C1) dürfen veröffentlicht werden.
- ¹³ Zitate, auch sinngemässe, sind nur mit Einverständnis der Originalquelle zu machen. Die Rechte an geistigem Eigentum sind zu wahren.
- ¹⁴ Offizielle Mitteilungen und Stellungnahmen von Swisscom sind dem Mediendienst zu überlassen. Falls sich Journalisten wegen eines Eintrags bei dir melden, verweise sie an den Mediendienst.

2.2 Foto- und Filmaufnahmen zur innerbetrieblichen Verwendung

- ¹⁵ Aufnahmen, denen ein innerbetrieblicher Verwendungszweck zugrunde liegt, sind zulässig. Beispielsweise für Schulungszwecke oder Mängelerfassung (nicht abschliessende Aufzählung).
- ¹⁶ Aufnahmen, welche nicht für die Veröffentlichung vorgesehen sind, sind mindestens mit C2 zu klassifizieren und zu behandeln.
- ¹⁷ Aufnahmen dürfen nur die für den konkreten Verwendungszweck relevante Informationen enthalten.
- ¹⁸ Entfällt der Verwendungszweck, so sind die Aufnahmen zu löschen bzw. entsprechend ihrer Klassifizierung abzulegen.
- ¹⁹ Der Zugriff auf die Aufnahmen ist auf das Minimum zu beschränken.

2.3 Foto- und Filmaufnahmen zur ausserbetrieblichen Verwendung

- ²⁰ Swisscom ist seit 2009 auf diversen Social-Media-Plattformen aktiv. Wenn Foto- oder Filmaufnahmen von Swisscomliegenschaften, -anlagen, -shops sowie dort befindlicher Personen auf öffentlichen oder privaten Kanälen publiziert werden sollen, sind folgende Sicherheitsregeln zu beachten:
- ²¹ Vor der Publikation ist vom Nutzer bzw. Betreiber der Fläche, der Anlage oder des Gebäudes eine Einwilligung einzuholen. Die Ansprechperson für die Flächen und Anlagen ist der Value Stream Manager vom Value Stream Basic Infrastruktur und von den Gebäuden der Security Agent von Corporate Real Estate Management.
- ²² Need to know-Prinzip: Es sind nur so viele Informationen preiszugeben wie unbedingt notwendig.
- ²³ Adressen und Aufnahmen im Freien, die eine örtlich exakte Zuordnung erlauben, sind bei Infrastrukturbauten zu vermeiden – ausser es handelt sich um öffentlich bekannte Standorte.

²⁴ Sicherheitseinrichtungen sind nicht zu zeigen oder – wenn nötig – ohne konkreten Bezug zu einem Standort und ohne konkreten Einsatzbereich bei Swisscom.

²⁵ Erkennbare Personen dürfen nicht ohne deren Einverständnis aufgenommen und gezeigt werden.

²⁶ So wenig Mitarbeitende mit Namen und Funktion vorstellen wie möglich.

²⁷ Vermeiden, Marken- und Produktnamen von Infrastruktur sowie IP- und andere technische Zuordnungsnummern zu zeigen (Netzwerkinformationen, Router- oder Switchnamen).

²⁸ Es dürfen keine Kundennamen (Firmenlogos, Namen, Adressen etc.) genannt oder gezeigt werden.

²⁹ Prüfe die Aufnahme sorgfältig, bevor du sie veröffentlichst. Du bist dafür verantwortlich. Beachte, dass einmal im Internet publizierte Inhalte grundsätzlich permanent öffentlich zugänglich bleiben.

3 Vollzug

³⁰ Die Betreiber von Gebäuden und Flächen wenden diese Sicherheitsanweisung an. Namentlich beurteilen sie Gesuche für Film- und Fotoaufnahmen und erteilen entsprechende Einwilligungen und Auflagen.

³¹ Group Security - Physical Security überwacht die Umsetzung dieser Sicherheitsanweisung und unterstützt die Betreiber in der Auslegung.

4 Dokument Information

Dieses Dokument regelt den Umgang mit Film- und Fotoaufnahmen durch Swisscom-Mitarbeitende auf sämtlichen von Swisscom genutzten Flächen

4.1 «Version 1.0»

| | |
|-----------------------------|---|
| Doc ID | SA-02143-C2 Film und Fotoaufnahmen Sicherheitsanweisung |
| Classification | C1 Public |
| Scope of application | Swisscom AG |
| Issue date | 20.08.2022 |
| Status | released |
| Document subject | Sicherheitsanweisung |
| Related LLV | LLV-DAT-001 , LLV-DAT-003 , LLV-DAT-004 , LLV-DAT-005 , |