Instruction de sécurité

SA Photographies et enregistrements vidéo

Swisscom SA

Group Security
Case postale
3050 Berne

Version	Date	Personne	Modifications apportées/remarques
0.5	20.08.2022	André Papageorgiu	Ébauche
0.6	25.08.2022	Claudio Passafaro	Finalisation pour consultation
0.7	19.10.2022	Daniel Zysset	Mise en forme et structure
0.8	10.11.2022	Claudio Passafaro	Incorporation des derniers retours
0.9	09.12.2022	Daniel Zysset	Traduit et finalisé
1.0	09.12.2022	Thomas Dummermuth	Vérification/libération
1.0	01.05.2023	Daniel Zysset	Petits ajustements formels effectués

Responsable: SiBe Brand-Objektschutz
Éditeur: SiBe Brand-Objektschutz
Création: 20.08.2022
Créateur: Passafaro Claudio
Va à: conformément à 1.1 Champ d'application

Table des matières

1 Introduction

[1] Swisscom est une entreprise de télécommunications notoire. La sécurité est d'une importance capitale pour Swisscom qui, partant, considère aussi le sérieux et la fiabilité comme des qualités cruciales. Étant la plus grande entreprise de télécommunications de Suisse, nous ne sommes pas seulement la cible privilégiée des attaques, notre infrastructure aussi intéresse les criminels et les services de renseignements dans la mesure où elle peut leur servir à accéder aux données de tiers voire de nos clients. Aujourd'hui, les pirates ne se contentent plus de lancer des attaques en ligne, de plus en plus d'entre elles sont en effet précédées par ce qu'on appelle de l'ingénierie sociale afin d'augmenter leurs chances de réussite.

[2] L'ingénierie sociale est un processus visant à obtenir des informations en exploitant le comportement humain – lesquelles sont ensuite utilisées pour les escroqueries les plus diverses. En l'occurrence, les qualités humaines telles que la confiance, la serviabilité, la peur ou le respect de l'autorité sont instrumentalisées dans le but d'accéder à des informations confidentielles, d'introduire subrepticement des programmes malveillants ou de désactiver des fonctions de sécurité.

[3] Les caractéristiques centrales des attaques faisant appel à l'ingénierie sociale sont l'usurpation d'identité et la tromperie sur l'intention des auteurs. Pour ce faire, ceux-ci se servent d'informations internes à l'entreprise concernant les personnes, les fonctions, les sites, les processus, le jargon de la société, etc.

[4] Les auteurs ciblent comme première source d'information les données qui sont accessibles publiquement, telles que les photos et les vidéos publiées sur Internet et les réseaux sociaux.

1.1 Champ d'application

[5] Ce document s'applique à l'ensemble de Swisscom (Suisse) SA, avec toutes les divisions commerciales[1] et du groupe basées[2] en Suisse et à l'étranger, ci-après dénommées Swisscom.

[6] Les sociétés du groupe mettent en place leur propre gestion de la sécurité ou se joignent à la gestion de la sécurité de Swisscom. La responsabilité de la sécurité reste du ressort de la société du groupe. La décision relève de la responsabilité de la société du groupe et est soutenue par Group Security.

[7] La présente instruction de sécurité régit la gestion des photographies et enregistrements vidéo des collaboratrices et collaborateurs Swisscom sur l'ensemble des surfaces utilisées par Swisscom.

[8] Elle s'applique de plus aux filiales et à leurs collaboratrices et collaborateurs, ainsi qu'aux mandataires qui pénètrent sur les surfaces utilisées par Swisscom. En revanche, elle ne s'applique pas aux surfaces et aux bâtiments de ces derniers.

[9] Elle s'applique en complément de dispositions légales telles que, par exemple, celles sur la protection de la personnalité et des données.

[1] Les secteurs d'activité comprennent Retail Customers ("B2C"), Business Customers ("B2B") et IT, Network & Infrastructure ("INI").

[2] Parmi les divisions du groupe, on trouve le Group Business Steering ("GBS"), le Group Human Resources ("GHR"), le Group Communications & Responsibility ("GCR") et le Group Security & Corporate Affairs ("GSA").

1.2 Documents de référence

[1] Directive Sécurité

[2] Security-Policy

[3] Loi fédérale sur la protection des données (LPD) 235.1

1.3 Objectif de la protection

[10] Le but est de s'assurer, pour les photographies et les enregistrements vidéo, que:

- la protection des informations secrètes et confidentielles est garantie,
- la diffusion incontrôlée d'informations secrètes et confidentielles est empêchée, et
- le public dispose d'un accès limité aux procédures, rôles et informations internes à l'entreprise.

2 Dispositions

2.1 Dispositions générales

[11] Sur la base du besoin en protection local, chaque exploitant de surfaces peut édicter des interdictions générales de prendre des photos et d'enregistrer des vidéos ainsi que des processus de dérogation.

[12] Il ne faut jamais révéler d'informations personnelles, confidentielles ou secrètes concernant Swisscom, les collaboratrices et collaborateurs, les clients ou les partenaires.

[13] Seules des informations classées publiques (C1) doivent être publiées.

[14] Les citations, y compris celles fidèles au sens, doivent uniquement être rapportées avec l'accord de la source originale. Les droits de propriété intellectuelle sont à préserver.

[15] Les communiqués et prises de position officiels de Swisscom sont du ressort exclusif du service médias. Si des journalistes te contactent au sujet d'une de tes publications, renvoie-les vers le service médias.

2.2 Photographies et enregistrements vidéo à des fins d'utilisation interne

[16] Les enregistrements reposant sur une finalité interne sont autorisés. Par exemple à des fins de formation ou de documentation des défauts (liste non exhaustive).

[17] Les enregistrements non destinés à être publiés doivent être classés au minimum C2 et traités comme tels.

[18] Les enregistrements doivent uniquement contenir des informations relevant de la finalité concrète.

[19] Une fois que la finalité cesse, les enregistrements doivent être supprimés ou stockés selon leur classification.

[20] L'accès aux enregistrements doit être réduit au minimum.

2.3 Photographies et enregistrements vidéo à des fins d'utilisation externe

[21] Swisscom est active sur différentes plateformes de réseaux sociaux depuis 2009. Quand des photographies ou des enregistrements vidéo de biens, installations ou shops de Swisscom, ainsi que de personnes s'y trouvant, doivent être publiés sur des canaux publics ou privés, les règles de sécurité suivantes doivent être observées:

[22] Avant la publication, il faut obtenir l'accord de l'utilisateur ou de l'exploitant de la surface, de l'installation ou du bâtiment. L'interlocuteur pour les surfaces et installations est le Value Stream Manager du Value Stream Basic Infrastructure, et pour les bâtiments c'est le Security Agent du Corporate Real Estate Management.

[23] Principe du Need to know: il ne faut pas révéler plus d'informations que cela est absolument nécessaire.

[24] Les adresses et les prises de vue en extérieur permettant une localisation exacte sont à éviter pour les bâtiments d'infrastructure, à moins qu'il ne s'agisse de sites publiquement connus.

[25] Les dispositifs de sécurité ne doivent pas être montrés ou, si nécessaire, sans référence concrète à un site et sans domaine d'application concret chez Swisscom.

[26] Les personnes identifiables ne doivent pas être photographiées ou filmées et montrées sans leur consentement.

[27] Présenter le moins possible de collaboratrices et collaborateurs avec leurs noms et fonctions.

[28] Éviter de montrer des noms de produit ou de marque d'infrastructure, ainsi que des numéros IP et autres numéros de référence techniques (informations réseau, noms de routeur ou de commutateur).

[29] Aucun nom de client (logo, nom, adresse, etc.) ne doit être mentionné ou montré.

[30] Vérifie avec soin la prise de vue avant de la publier. Tu en es responsable. Garde en tête qu'une fois publiés sur Internet, tous les contenus y restent accessibles pour l'éternité.

3 Exécution

[31] Les exploitants des bâtiments et des surfaces appliquent la présente instruction de sécurité. Notamment, ils évaluent les demandes d'enregistrements photo et vidéo, et délivrent les autorisations et conditions correspondantes.

[32] Group Security – Physical Security surveille la mise en œuvre de la présente instruction de sécurité et aide les exploitants à son interprétation.

4 Information sur le document

La présente instruction de sécurité régit la gestion des photographies et enregistrements vidéo des collaboratrices et collaborateurs Swisscom sur l'ensemble des surfaces utilisées par Swisscom

4.1 «Version 1.0»

Doc ID	SECDOC-111
Titel	SA Photographies et enregistrements vidéo
Classification	C1 Public
Scope of application	Swisscom SA
Issue date	20.08.2022
Statut	released
Document subject	Instruction de sécurité
Related LLV	LLV-DAT-001, LLV-DAT-003, LLV-DAT-004, LLV-DAT-005,