Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

Office fédéral de la communication OFCOM
Division services de télécommunication

4ème édition, février 2023

Lignes directrices relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication

Table des matières

1 Généralités 3
1.1 Champ d'application 3
1.2 Caractère et valeur du document 3
1.3 Références 3
1.4 Abréviations 4
1.5 Définitions 5
2 Lignes directrices 6
Annexe 1 7
Annexe 2 9

1 Généralités

1.1 Champ d'application

La loi sur les télécommunications (LTC) [1] a notamment pour but d'assurer que le trafic des télécommunications ne soit pas perturbé et que des services de télécommunication de qualité soient fournis aux particuliers ainsi qu'aux milieux économiques (art. 1 LTC [1]). Par définition, les télécommunications sont basées sur des parties de réseau qui communiquent entre elles, qui s'influencent et sont dépendantes les unes des autres. Il est dès lors important de disposer d'une compréhension commune du standard minimal en matière de sécurité. Les réseaux et les services de télécommunication ne sont finalement autant sûrs et disponibles que ne l'est l'élément le plus faible de l'ensemble.

Les présentes lignes directrices relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication ont pour objectif de préciser les attentes du législateur en matière de sécurité afin de favoriser l'interprétation commune des milieux concernés et assurer la confiance des utilisateurs. Par ailleurs, elles définissent un niveau minimal de sécurité que devrait mettre en œuvre tout fournisseur de services de télécommunication pour contribuer à la fiabilité et la disponibilité du système global de télécommunication national.

Les lignes directrices peuvent être mises en relation avec les dispositions relatives à la sécurité et à la disponibilité figurant à l'art. 48*a* de la LTC [1]. Elles ont un statut de recommandations et concernent les divers réseaux filaires et hertziens utilisés pour l'acheminement de la voix et des données dans des situations ordinaires.

Pour les concessionnaires de radiocommunication mobile exploitant des réseaux de radiocommunication mobile à partir de la cinquième génération ce sont cependant les dispositions figurant aux art. 96*e* et 96*g*, al. 1 de l'ordonnance sur les services de télécommunication (OST, RS 784.101.1) ainsi que les prescriptions techniques administratives (PTA) sur la sécurité des réseaux et des services exploités par les concessionnaires de radiocommunication mobile (RS 784.101.113/1.13) qui s'appliquent. Ces dernières reprennent les principes qui figurent dans les présentes lignes directrices.

1.2 Caractère et valeur du document

Pour l'élaboration du présent document, l'Office fédéral de la communication (OFCOM) a pris en compte les travaux des organismes de normalisation ainsi que les avis des milieux concernés, qui ont été exprimés au cours d'une consultation publique.

Dans un premier temps, ce document est publié sous la forme de lignes directrices. L'OFCOM ne procédera pas à l'évaluation de la conformité à ces dernières mais leur mise en œuvre est vivement recommandée.

A l'avenir, les recommandations contenues dans ce document pourraient être transformées, si besoin est, en prescriptions techniques et administratives obligatoires.

1.3 Références

[1] RS 784.10
Loi du 30 avril 1997 sur les télécommunications (LTC)

[2] ISO/IEC 27001:2013
Information technology - Security techniques - Information security management systems - Requirements

[3] ISO/IEC 27002:2013

Information technology – Code of Pratice for Information Security Controls

[4] ISO/IEC 27011:2016
Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

[5] ISO 22301:2019 Security and Resilience – Business Continuity Management Systems - Requirements

[6] ISO/IEC 27035-1:2016 Information Technology – Security Techniques - Information Security Incident Management – Part 1: Principles of Incident Management

[7] ISO/IEC 27035-2:2016 Information Technology – Security Techniques - Information Security Incident Management – Part 2: Guidelines to Plan and Prepare for Incident Response

Les recommandations de l' ITU-T (UIT-T) peuvent être obtenues auprès de l'Union internationale des télécommunications, Place des Nations, 1211 Genève 20 (www.itu.int).

Les normes de l'ISO peuvent être obtenues auprès du Secrétariat central de l'Organisation internationale de normalisation, 1, rue de Varembé, 1211 Genève (www.iso.ch)

Les documents de l'ETSI peuvent être obtenus auprès de ETSI, Institut européen des normes de télécommunication, 650 Rue des Lucioles, 06921 Sophia Antipolis, France (www.etsi.org)

Les textes de loi avec références RS sont publiés dans le recueil systématique des lois fédérales disponible sur le site internet www.fedlex.admin.ch et peuvent être obtenus auprès de OFCL, CH-3003 Bern.

1.4 Abréviations

ETSI	*European Telecommunications Standards Institute* – Institut européen des normes de télécommunication
FST	Fournisseurs de services de télécommunications
ICT	*Information and communication technology* – Technologie de l'information et de la communication
ISMS	*Information Security Management System* – Système de gestion de la sécurité de l'information
ISO	*International Organization for Standardization* - Organisation internationale de normalisation
ITU-T	*International Telecommunication Union - Telecommunication Standardization Sector* (UIT-T)
LTC	Loi sur les télécommunications
OFCOM	Office fédéral de la communication
UIT-T	Union internationale des télécommunications – Secteur de standardisation des télécommunications

1.5 Définitions

Disponibilité : Mettre l'information et les biens associés à disposition des utilisateurs autorisés lorsque cela est nécessaire.

Plan de continuité (*Business Continuity Plan*) : document dont l'objectif est de prévoir les moyens techniques, contractuels, organisationnels et humains pour préparer l'entreprise à réagir face à une crise.

Service de télécommunication : la transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication.

Système de gestion de la sécurité de l'information (*Information Security Management System*) : partie du système de gestion global qui se base sur les risques pour établir, mettre en œuvre, exploiter, surveiller, réviser, maintenir et améliorer la sécurité de l'information.

2 Lignes directrices

1) Tout FST[1] devrait développer, mettre en œuvre et réexaminer en continu un système de gestion de la sécurité de l'information (*Information Security Management System, ISMS*) conforme à la norme ISO/IEC 27001:2013 [2]. Il devrait de plus se référer aux normes ISO/IEC 27002:2013 [3] ou ISO/IEC 27011:2016 [4] pour le choix des contrôles prévus dans le cadre de l'ISMS (cf. annexe 1).

2) Dans le cadre de l'ISMS mis en œuvre, tout FST devrait mettre en œuvre un plan de gestion de la continuité opérationnelle (*Business Continuity Plan*) conforme à la norme ISO 22301:2019 [5].

3) Dans le cadre de l'ISMS mis en œuvre, tout FST devrait mettre en œuvre un plan de gestion des incidents de sécurité conforme aux normes ISO/IEC 27035-1:2016 [6] et ISO 27035-2:2016 [7].

4) Tout FST devrait s'assurer que ces procédures et son infrastructure soient conformes aux normes reconnues relatives à la sécurité de l'information et des infrastructures de télécommunication (cf. annexe 2).

Bienne, le 17 février 2023

OFFICE FÉDÉRAL DE LA COMMUNICATION

Le directeur :

Bernard Maissen

[1] La liste des FST dont l'ensemble desquels est concerné par ces lignes directrices, est disponible sur le site Internet de l'OFCOM sous https://www.bakom.admin.ch/bakom/fr/page-daccueil/telecommunication/fournisseurs-de-services-de-telecommunication/liste-des-fournisseurs-de-services-de-telecommunication-annonces.html

Annexe 1

Le système de gestion de la sécurité de l'information (*Information Security Management System*, ISMS)

Pour les sociétés fournissant des services dans le domaine de la société de l'information et des télécommunications, l'infrastructure ainsi que l'information que cette dernière génère ou prend en charge, sont des biens importants. Une gestion consciencieuse de la sécurité de ces derniers est indispensable afin de permettre à ces sociétés d'assurer la fiabilité de leurs activités commerciales et de donner ainsi confiance à leurs partenaires commerciaux.

Poursuivant cet objectif, la norme ISO/IEC 27001:2013 [2] décrit une méthode permettant l'élaboration, la mise en œuvre, la maîtrise et l'amélioration continuelle d'un système de gestion de la sécurité (*Information Security Management System*, ISMS). Ce document s'adresse aux directions d'entreprise et aux collaborateurs responsables de la gestion de la sécurité.

L'élaboration d'un ISMS est influencée par les objectifs, les besoins, les exigences ainsi que les risques liés aux activités de l'organisation considérée. Il dépend par ailleurs des technologies utilisées, de la clientèle de même que de la grandeur et de la structure de la société. Toute évolution de ces critères doit provoquer une adaptation du système de gestion de la sécurité.

La norme ISO/IEC 27001:2013 [2] est autant utilisée par les propres collaborateurs d'une organisation que par des évaluateurs externes mandatés. Une évaluation indépendante effectuée par un organisme de certification accrédité peut en effet conduire à une certification reconnue démontrant la capacité de la société en question à maîtriser la gestion de la sécurité.

Le modèle proposé par ce document suit le principe de l'amélioration continue qui prévoit les 4 phases récurrentes « *PLAN-DO-CHECK-ACT* » (PDCA). Ce modèle est également mis en œuvre dans le cadre d'autres systèmes de gestion à l'instar de la norme ISO 9001, laquelle a pour objectif la gestion de la qualité. Il présente l'avantage de pouvoir être appliqué à tous les ISMS indépendamment de la grandeur de l'organisation et de l'activité de cette dernière.

La phase de planification du modèle (*PLAN*) a pour but de définir le cadre du système de gestion de la sécurité. Elle requiert l'identification et l'évaluation des risques encourus par la société. Il est également question de définir une politique en matière de sécurité qui décrit les objectifs de la direction d'entreprise et tient compte des risques considérés pour définir le périmètre à sécuriser. En se référant aux documents ISO/IEC 27002:2013 [3] ou ISO/IEC 27011:2016 [4] l'organisation est par ailleurs tenue de choisir des contrôles adaptés à la politique définie et aux risques contre lesquels elle a choisi de se prémunir. La recommandation ITU-T X.1051 publiée par l'ISO avec la référence ISO/IEC 27011:2016 [4] est fortement inspirée de la norme ISO/IEC 27002:2013 [3] et s'applique plus particulièrement au domaine des télécommunications. Le choix des contrôles retenus doit ensuite être mentionné dans un document appelé « *Statement of applicability* ». Il appartient finalement à la direction d'entreprise de donner son accord quant aux procédures, aux objectifs de contrôle et aux risques résiduels qu'il n'est pas prévu de considérer.

La seconde phase (*DO*) préconise la mise en œuvre et l'exploitation des procédures et des contrôles planifiés.

La phase suivante (*CHECK*), prévoit la surveillance et l'évaluation des procédures et des contrôles mis en œuvre, en fonction de la politique en matière de sécurité, des objectifs de l'organisation et de l'expérience pratique. Cette analyse doit également prendre en compte l'évolution des technologies, de l'organisation et du contexte légal. Il est également question

de réévaluer l'importance des risques résiduels qui n'auraient pas été considérés et de prendre en compte tout fait constaté qui est susceptible d'avoir un impact sur la performance et l'efficacité de l'ISMS. En définitive, la direction d'entreprise est tenue d'approuver cette analyse.

La dernière phase (*ACT*) prévoit de mettre en œuvre des actions correctives et préventives basées sur les résultats de l'analyse effectuée au cours de la phase précédente afin d'assurer l'amélioration de l'ISMS. Cette phase requiert également d'informer toutes les parties concernées.

Les 4 phases précédemment décrites doivent être exécutées régulièrement afin d'assurer la l'amélioration continuelle du système de gestion de la sécurité et par là, sa fiabilité.

Annexe 2

Normes reconnues relatives à la sécurité de l'information et des infrastructures de télécommunication

Les lignes directrices relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication mentionnent (ch. 2, chiffre 4) que tout FST devrait s'assurer de la conformité de ses procédures et de son infrastructure aux normes reconnues relatives à la sécurité de l'information et des infrastructures de télécommunication.

Dans ce domaine, de nombreux documents de référence ont été élaborés notamment par l'Institut européen des normes de télécommunication (ETSI) et l'Union internationale des télécommunications (UIT-T). Leur application dépend toutefois de l'infrastructure mise en œuvre et des services proposés.

L'accès aux documents élaborés par les organismes de normalisation est possible par l'intermédiaire du site Internet de l'OFCOM https://www.bakom.admin.ch/bakom/fr/page-daccueil/telecommunication/fournisseurs-de-services-de-telecommunication/lignes-directrices-relatives-a-la-securite-et-a-la-disponibilite/normes-reconnues-relatives-a-la-securite-de-linformation-et-des-.html