Conditions-cadres et bonnes pratiques en matière de cybersécurité chez Axis

Janvier 2025, version 1.2

AXIS COMMUNICATIONS

Table des matières

1. Introduction

Les clients des secteurs de l'information, de la technologie et de la sécurité doivent avoir l'assurance que les solutions mises en œuvre dans leur entreprise sont sûres et fiables. Les systèmes et les données doivent être accessibles, mais uniquement aux utilisateurs autorisés, et les appareils doivent pouvoir fonctionner sur le réseau sans intrusion ni exposition involontaire à des menaces. La solution doit fonctionner de la façon dont elle a été conçue et comme prévu, avec le maintien de son intégrité et de ses fonctionnalités.

Mais dans le même temps, les menaces envers la sécurité sont omniprésentes. De nouvelles menaces apparaissent et leur nature change à chaque instant.

Axis Communications s'engage résolument en faveur de la sécurité et a mis en place des processus et des procédures pour gérer de façon continue la sécurité et les risques qui y sont liés. Tous les collaborateurs sont sensibilisés à la sécurité et invités à faire preuve de prudence.

Ce document a pour but de vous donner un aperçu du cadre et des bonnes pratiques en matière de cybersécurité chez Axis. Ces pratiques visent une approche systématique pour protéger la confidentialité, l'intégrité et la disponibilité de nos actifs.

2. Conditions-cadres de cybersécurité

Le système de gestion de la sécurité de l'information (SGSI) d'Axis est à la base du cadre de cybersécurité. Le SGSI est basé sur les exigences de la norme ISO 27001:2023 et facilite l'amélioration et le suivi continus de l'engagement d'Axis en matière de sécurité. Le SGSI est certifié selon la norme ISO 27001:2023 pour le champ d'application défini dans le certificat.

Dans le cadre du SGSI, Axis a mis en place un cadre de contrôle de la cybersécurité basé sur les contrôles de la norme ISO 27002. Le SGSI et les contrôles de sécurité correspondants font l'objet d'un audit annuel par un organisme de certification externe agréé afin de démontrer la conformité à la norme ISO 27001. En outre, Axis effectue des audits internes du SGSI conformément au plan d'audit interne annuel décidé par la direction.

2.1 Politique en matière de sécurité de l'information

La politique en matière de sécurité de l'information d'Axis définit l'orientation générale de l'engagement d'Axis en matière de sécurité. La politique en matière de sécurité de l'information est obligatoire et doit être respectée par tous les collaborateurs, les travailleurs occasionnels et les consultants, ainsi que par la direction et les membres du conseil d'administration.

La politique en matière de sécurité de l'information est complétée par des documents plus détaillés, comme des directives, des routines et la sécurité de base d'Axis (voir chapitre 3 pour plus de détails). La politique en matière de sécurité de l'information et les autres documents sont revus chaque année et/ou sont mis à jour en cas de modification de la stratégie globale ou de changement dans l'environnement Axis.

2.2 Rôles et responsabilités

De multiples rôles sont responsables de l'amélioration continue de la sécurité dans l'ensemble de l'organisation. Axis encourage une approche collaborative de la sécurité et insiste sur le fait que tous les collaborateurs ont un rôle important à jouer. Parmi les rôles et les organisations qui se consacrent à la sécurité, on peut citer, entre autres :

> Chief Information Officer (CIO)
  - Assume la responsabilité globale de la sécurité de l'information et de la protection de la vie privée au sein d'Axis.
  - Fait partie de l'équipe de direction de l'entreprise et est chargé de faire rapport au conseil d'administration sur les questions liées à la sécurité

> Équipe de Management du SGSI
  - Supervise le SGSI

> Équipe en charge du respect de la confidentialité
  - Point de contact pour les questions liées à la protection de la vie privée au sein de l'entreprise

> Gouvernance IT
  - Développe en permanence une méthodologie et une structure pour le SGSI d'Axis

> Software Security Group (SSG)
  - Le SSG est la principale entité de contact interne pour les organisations de développement en ce qui concerne les questions de sécurité.
  - Est responsable du Modèle de développement de la sécurité d'Axis (ASDM), un cadre qui définit les activités utilisées par Axis pour développer des logiciels plus sûrs
  - L'ASDM est la composante de développement sécurisé au sein du SGSI

> Security Operations Center (SOC)
  - Surveillance 24/7/365 pour détecter les cybermenaces et y répondre

3. Sécurité de base chez Axis

La Sécurité de base chez Axis est la référence pour toutes les exigences de sécurité chez Axis, et constitue un élément clé de la politique de sécurité de l'information d'Axis.

Pour établir la Sécurité de base, Axis a défini plusieurs domaines en s'appuyant sur des cadres de sécurité mondialement reconnus tels que la norme ISO 27001/2, NIST SP 800-53, ainsi que sur des exigences réglementaires telles que le RGPD. Vous trouverez ci-dessous une description globale des domaines et des pratiques appliquées.

3.1 Gestion des actifs et classification des informations

Les informations sont très précieuses pour Axis en tant qu'organisation et doivent être protégées de façon appropriée. Axis gère ses actifs en tenant des inventaires et en classant les actifs en fonction de leur criticité. Les directives relatives à la gestion des actifs comprennent un système de classification des actifs avec des niveaux de classification définis. La classification des actifs est une condition préalable à une protection efficace de la confidentialité, de l'intégrité et de la disponibilité des actifs.

Les actifs identifiés se voient attribuer un propriétaire opérationnel et technique, et cette propriété est documentée dans l'inventaire des actifs. Les propriétaires désignés sont responsables du travail continu d'inventaire et de classification des actifs.

3.2 Sauvegarde et récupération des données

Les procédures de sauvegarde et de récupération sont conçues pour protéger contre la perte de données et pour permettre une récupération suffisante des données. Les sauvegardes sont effectuées au moins une fois par jour, en fonction des exigences de disponibilité des données, et toutes les sauvegardes sont stockées dans un espace de stockage secondaire.

Des tests de restauration des sauvegardes sont effectués périodiquement à l'aide des solutions techniques et des outils disponibles.

3.3 Continuité des activités (Business continuity management – BCM)

La continuité des activités (Business continuity management – BCM) fait partie intégrante d'Axis et diverses mesures sont mises en œuvre pour assurer la continuité des activités. Les données sont stockées dans des centres de données primaires et secondaires situés dans des lieux géographiques différents afin de garantir la redondance. Les actifs sont documentés dans un registre des actifs avec des classifications de criticité et des exigences sur l'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO).

Des plans de communication sont mis en place pour la communication interne en cas de problèmes avec un impact potentiel sur la continuité des activités. La communication externe est gérée via la page d'état d'Axis sur status.axis.com.

3.4 Cryptographie, gestion des clés et des certificats

Des exigences ont été définies pour une utilisation et une gestion appropriées et efficaces des clés cryptographiques et des certificats afin de garantir la sécurité des communications et du stockage des informations.

Dans la mesure du possible, Axis suit les recommandations de la norme FIPS 140-3 (IEC/ISO 19790:2012) pour la sélection des algorithmes, avec une préférence pour les algorithmes suivants :

> Chiffrement des données en mouvement (TLS / mTLS) – RSA 2048 et plus récent
> Chiffrement des données au repos – AES 256
> Signature numérique – RSA 2048 et plus récent, ECDSA p256 et plus récent avec SHA256 et plus récent

3.5 Gestion des identités et des accès

La gestion des identités et des accès (Identity and access management – IAM) consiste à limiter l'accès aux composants physiques et logiques aux seuls utilisateurs autorisés. Axis a mis en œuvre de nombreux contrôles et pratiques en matière de sécurité liés à l'IAM, à la fois préventifs et de détection. Quelques exemples de contrôles de sécurité :

> Processus d'enregistrement/désenregistrement des utilisateurs avec des flux d'approbation définis
> Processus automatisé de désinscription/désactivation du compte des collaborateurs sortants dans l'Active Directory
> Application du principe de moindre privilège
> Authentification à plusieurs facteurs (Multi-factor authentication – MFA)
> Évaluation périodique des accès des utilisateurs
> Enregistrement et suivi des accès et des activités des utilisateurs
> Gestion des comptes privilégiés
> Single sign-on
> Gestion des accès à distance (y compris VPN avec MFA)
> Séparation des fonctions

3.6 Gestion des incidents

La gestion des incidents est essentielle pour la continuité des activités et Axis a défini un processus de gestion des incidents afin de minimiser l'impact potentiel d'un incident sur les activités et les parties prenantes. Cela inclut la détection, la communication, la coordination, l'atténuation et la résolution de l'incident, ainsi que l'apprentissage à partir des incidents passés afin de favoriser l'amélioration continue.

Axis surveille activement les systèmes et les services à l'aide d'outils automatisés afin de détecter les anomalies et autres indications d'incidents potentiels. Pour répondre aux incidents 24/24, 7 j/7 et 365 j/an, Axis a mis en place un Security Operations Center (SOC). Le SOC est responsable de la surveillance continue des problèmes de sécurité et se tient prêt à agir en cas d'identification d'une anomalie, d'une alarme ou d'une vulnérabilité de type « zero-day ».

Les incidents sont classés en fonction de l'impact potentiel sur l'entreprise, remontés en conséquence et suivis dans le système de gestion des incidents jusqu'à leur résolution. Un rapport d'incident est établi pour tous les incidents majeurs afin de clarifier la cause première et de faciliter l'amélioration continue du dispositif de sécurité.

Les incidents liés à la protection de la vie privée et les violations potentielles sont gérés selon une routine de gestion des violations de la vie privée. Cette routine comprend des canaux de communication, des voies d'escalade de l'information, des évaluations et de la documentation. Elle est établie sur la base des lois et règlements applicables en matière de protection de la vie privée, principalement le RGPD.

Les informations externes relatives aux incidents et à l'état des services Axis sont disponibles sur status.axis.com.

3.7 Sécurité informatique des opérations

La sécurité informatique des opérations consiste à disposer de processus, de procédures et de contrôles pour protéger l'environnement informatique opérationnel en matière de confidentialité, d'intégrité et de disponibilité. Au sein d'Axis, cela comprend, par exemple, la gestion des clients et des serveurs, la gestion des changements selon un processus structuré et systématique, et la gestion de la configuration selon les meilleures pratiques et les guides de renforcement de la sécurité.

La gestion des correctifs est également un élément essentiel de la sécurité informatique et s'inscrit dans le cadre d'un processus défini de gestion du cycle de vie.

3.8 Sécurité du réseau

Diverses mesures ont été mises en œuvre pour protéger les communications du réseau, assurer le contrôle des accès et permettre la sécurité opérationnelle.

Quelques exemples de contrôles de sécurité :

> Accès au réseau basé sur les rôles
> Obligation de disposer d'un certificat (IEEE 802.1X) pour accéder au réseau de l'entreprise
> Segmentation du réseau
> La communication entre les segments doit respecter la politique de pare-feu.
> Les clients connectés aux réseaux de production doivent disposer d'une protection de leur point d'accès
> L'accès au réseau à distance nécessite une connexion par VPN avec authentification à plusieurs facteurs.
> Surveillance proactive du trafic et des équipements du réseau
> Les équipements de réseau envoient des notifications qui sont consignées dans un journal stocké de façon centralisée
> Les modifications apportées à l'équipement du réseau sont enregistrées

3.9 Sécurité personnelle

La sécurité personnelle consiste à s'assurer que les collaborateurs et le personnel externe (consultants et sous-traitants) comprennent leurs responsabilités et sont compétents pour remplir les fonctions qui leur sont attribuées.

Lors du processus de recrutement, des directives sont définies en matière de sécurité et de sûreté. Cela inclut la vérification des références et des antécédents, en fonction de la législation locale et de la criticité de la fonction.

Le processus comprend également des mesures de sécurité pendant et après l'occupation, comme l'intégration (octroi de l'accès physique et logique), les accords de non-divulgation, la sensibilisation et la formation, et la fin de service (suppression de l'accès physique et logique lorsqu'un utilisateur quitte l'entreprise).

3.10 Sécurité physique

Des procédures et des routines sont définies pour maintenir la sécurité physique, créer un environnement sûr et sécurisé pour toutes les personnes qui travaillent ou visitent les locaux d'Axis, et pour protéger les locaux, les actifs et les personnes d'Axis.

Une carte d'accès et un code PIN sont nécessaires pour entrer dans les locaux d'Axis, et toute personne se trouvant dans les locaux doit porter visiblement un badge d'identification Axis. Tous les accès aux locaux sont consignés, et les journaux sont stockés de façon centralisée. Des caméras de surveillance sont installées dans l'ensemble des locaux.

Les visiteurs doivent toujours s'enregistrer à la réception d'Axis et présenter une pièce d'identité au collaborateur de la réception/du service desk. Lors de leur enregistrement, les visiteurs reçoivent un badge visiteur qu'ils doivent toujours porter de façon visible. Ils sont toujours escortés lorsqu'ils se trouvent dans les locaux d'Axis.

Les locaux d'Axis sont divisés en différentes zones de sécurité et l'accès aux zones restreintes est limité au personnel autorisé.

3.11 Protection de la vie privée

Axis veille à ce que des garanties et des mécanismes soient mis en place pour protéger les données personnelles des collaborateurs, des partenaires et des clients. La confiance et une marque forte sont au cœur de notre stratégie, et nous nous engageons à entretenir des relations transparentes avec les clients finaux. Nous conservons leurs informations, mais nous respectons toujours leur droit au contrôle total de leurs données, conformément aux réglementations et aux contrats applicables.

Les principes fondamentaux suivants s'appliquent lors de la collecte et du traitement des données à caractère personnel :

> Raisonnable et légal
> Dans la mesure où cela est nécessaire
> Dans un but légitime
> Traitement adéquat, pertinent et nécessaire par rapport à l'objectif poursuivi

De plus amples informations sur nos procédures en matière de protection de la vie privée sont disponibles sur www.axis.com/privacy

3.12 Travail à distance

Axis a défini des règles et des procédures de sécurité pour sécuriser les appareils utilisés pour le télétravail, par exemple en cas de déplacement ou de télétravail. Cela couvre les systèmes et les processus utilisés pour garantir un travail effectué de façon sûre et conforme, avec une séparation distincte entre l'utilisation professionnelle et non professionnelle.

La formation de sensibilisation à la sécurité et la politique « d'utilisation acceptable » aident les collaborateurs. Pour accéder aux systèmes et ressources internes lorsqu'il travaille en dehors du bureau, chaque utilisateur doit s'authentifier via une connexion VPN avec authentification à plusieurs facteurs.

Les appareils clients et mobiles sont cryptés. Les appareils mobiles sont gérés au moyen d'une solution de gestion des appareils mobiles (MDM) qui permet d'effacer les données à distance si nécessaire.

3.13 Gestion des risques

La gestion des risques s'effectue selon un cycle annuel de gestion des risques, géré par la gouvernance d'entreprise et couvrant tous les domaines d'activité, y compris la sécurité. Le cycle de gestion des risques comprend l'évaluation des risques, l'analyse des risques et le suivi des risques. L'analyse des risques est présentée à l'équipe de direction d'Axis, au comité d'audit et au conseil d'administration.

Dans le cadre du cycle de gestion des risques de l'entreprise, des directives pour l'évaluation des risques liés à la sécurité de l'information sont définies et appliquées dans le cadre du SGSI. Il s'agit d'évaluer et d'atténuer en permanence les risques par les propriétaires des systèmes et les responsables des risques dans l'ensemble de l'organisation. Les risques identifiés sont évalués et, en fonction de leur niveau, remontés à un échelon supérieur selon une matrice d'évaluation des risques. Le CIO est responsable de la notification des risques à la direction et au conseil d'administration.

L'approche, la méthodologie et la mise en œuvre de l'évaluation des risques en matière de sécurité de l'information font l'objet d'un audit externe annuel dans le cadre du processus de certification ISO 27001.

3.14 Développement sécurisé

Pour permettre le développement sécurisé de ses produits et services, Axis a défini et mis en œuvre le modèle de développement de sécurité Axis (ASDM). Les principaux objectifs de l'ASDM sont les suivants :

> Faire de la sécurité des logiciels une partie intégrante des activités de développement des logiciels Axis
> Réduire les risques commerciaux liés à la sécurité pour les clients d'Axis
> Répondre à la demande croissante des clients et des partenaires en matière de sécurité
> Réduire potentiellement les coûts grâce à la détection et à la résolution précoces des problèmes.

Le champ d'application de l'ASDM englobe tous les logiciels Axis inclus dans les produits et solutions Axis. Pour plus de détails sur l'ASDM, consultez help.axis.com/axis-security-development-model

3.15 Sensibilisation à la sécurité et formation

Axis a mis au point un programme de sensibilisation à la sécurité afin de former en permanence ses collaborateurs à la prévention et à l'atténuation des menaces à la sécurité.

Le programme de sensibilisation comprend une formation de sensibilisation à la sécurité liée à la politique de sécurité de l'information et aux meilleures pratiques en matière de sécurité. La formation de sensibilisation est obligatoire pour tous les représentants d'Axis.

Le programme comprend également une formation à la sûreté et à la sécurité physique. La formation est obligatoire pour tous les collaborateurs et sous-traitants qui accèdent aux locaux d'Axis, et doit être effectuée avant que la personne ne reçoive une carte d'accès aux locaux.

Une formation supplémentaire à la sécurité est dispensée, en fonction du rôle et des responsabilités de l'organisation ; par exemple, l'ASDM pour les développeurs (voir point 3.14 ci-dessus) et une sensibilisation spécifique pour les propriétaires de systèmes.

3.16 Acquisition de systèmes et gestion des fournisseurs

Un contrôle des fournisseurs est effectué avant la conclusion d'un accord. Il s'agit notamment d'évaluer le fournisseur potentiel selon un modèle d'évaluation comprenant un examen juridique, une évaluation de la sécurité et une évaluation de la protection de la vie privée. Les gestionnaires de contrats et le service juridique sont les principaux responsables du contrôle des fournisseurs. Ils consultent également divers experts au sein de l'organisation, par exemple des spécialistes de la sécurité.

Chaque fournisseur a un gestionnaire de contrat, qui a la responsabilité globale du suivi des livraisons du fournisseur, du respect des exigences du contrat et de l'évaluation périodique de la sécurité du fournisseur.

Les systèmes et les services qui sont ou seront achetés sont évalués pour s'assurer qu'ils sont conformes aux exigences d'Axis et qu'ils n'exposent pas Axis ou ses partenaires à des risques inacceptables. Les directives relatives à l'acquisition de systèmes répondent à ces exigences et doivent être appliquées lorsqu'un nouveau système ou service est envisagé.

3.17 Threat intelligence

La Threat intelligence est la collecte d'informations concernant l'apparition et l'évaluation des menaces numériques et physiques, ainsi que des acteurs de la menace, afin d'aider à contrer les attaques potentielles et les événements préjudiciables survenant dans le cyberespace.

L'Intelligence Analysis et la Threat intelligence sont effectués en permanence et via de multiples sources différentes.

Axis pratique la Threat intelligence, à la fois en ce qui concerne la surveillance des vulnérabilités de type « zero-day » et faisant preuve de proactivité en matière de Threat intelligence, par exemple en participant à des communautés dédiées à la sécurité.

3.18 Gestion des vulnérabilités et protection contre les logiciels malveillants

Des procédures de gestion des vulnérabilités et de protection contre les logiciels malveillants sont définies pour garantir l'utilisation d'outils et de méthodes appropriés afin d'évaluer les vulnérabilités et les codes malveillants dans les systèmes ou les applications, et d'y remédier. Axis utilise divers outils d'analyse pour évaluer en permanence les vulnérabilités internes et externes de son environnement informatique. Les vulnérabilités sont classées selon le système CVSS (Common Vulnerability Scoring System) et classées par ordre de priorité en fonction de leur criticité.

Les appareils connectés au réseau de production sont protégés et surveillés par une solution de pointe de détection et de réponse des points d'accès.

En ce qui concerne la gestion des vulnérabilités pour nos produits, Axis applique le modèle de développement de sécurité Axis (voir point 3.14 ci-dessus) aux logiciels pour le cycle de vie du produit. Axis est une autorité CNA agréée (Common Vulnerability and Exposures Numbering Authority), et divulgue les vulnérabilités de façon transparente, conformément au cadre établi dans le programme CVE. Pour plus de détails sur la sécurité des produits et la gestion des vulnérabilités, consultez
www.axis.com/support/cybersecurity/vulnerability-management et
help.axis.com/axis-vulnerability-management-policy

4. Certifications et conformité

Axis se conforme à toute une série d'exigences réglementaires, ainsi qu'à des cadres et des normes choisies de façon stratégique. Ces exigences, cadres et normes constituent une garantie de notre engagement en faveur de la sécurité de l'information, de la protection de la vie privée et d'autres domaines importants pour Axis et ses partenaires.

Une vue d'ensemble actualisée des certifications et des certificats de conformité est disponible sur : www.axis.com/compliance

À propos d'Axis Communications

En améliorant la sûreté, la sécurité, l'efficacité opérationnelle et l'intelligence économique, Axis contribue à un monde plus sûr et plus intelligent. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 5000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.