Sécurité et confidentialité de l'information

Définitions

(MNM DEF)

TABLE DES MATIERES

1. Introduction

Le présent document fait partie intégrante des normes minimales relatives à la sécurité et à la confidentialité de l'information dans la sécurité sociale. Il est destiné aux responsables, aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de la sécurité sociale (IPSS).

Dans un souci de cohérence de la terminologie et des concepts utilisés dans tous les documents de politique, toutes les définitions relatives à la sécurité et à la confidentialité de l'information sont centralisées dans ce document.

2. Définitions

A

Analyse d'impact relative à la protection des données : analyse de parties de processus et de l'impact que peut y entraîner une interruption des activités.

Appareils mobiles : terme général employé pour désigner les smartphones, tablettes, notebooks et autres ordinateurs portables.

Applications critiques : sans les applications critiques, une organisation n'est pas en mesure d'exécuter les activités quotidiennes.

Authentification à deux facteurs (TOTP) : méthode d'authentification utilisant une combinaison de deux moyens différents pour confirmer l'identité de l'utilisateur (ex. retirer de l'argent par le biais d'une carte bancaire et d'un code PIN).

Autorisation : détermination des actions que l'utilisateur peut exécuter dans une application ou un système.

C

Clé compromise : clé dont il est impossible de garantir qu'elle est utilisable exclusivement par des personnes autorisées.

Confidentialité de l'information : fait que des informations ne soient pas mises à disposition ou ouvertes à des processus, des entités ou des individus non autorisés.

Conseiller en sécurité : responsable de la tenue à jour et du développement de la stratégie de sécurisation de l'organisation conformément à la législation en vigueur et aux normes minimales sur lesquelles se base l'organisation. Il rend formellement compte à la direction une fois par an.

Convention : accord écrit entre les organisations et un tiers sur des travaux, des livraisons et des services fournis par des tiers à l'organisation et/ou inversement.

D

Déclassification : suppression de la classification précédemment accordée à l'information, de sorte que l'information est librement accessible.

Déni de service : situation dans laquelle un système informatique est malencontreusement indisponible pour la prestation de services attendue.

Destruction : s'assurer que toute trace de données ou d'informations a été éliminée d'un support de données ou que le support de données même est suffisamment détruit et que les données ou informations de la même source ne peuvent pas à nouveau être rendues visibles ou lisibles. La destruction de documents, par exemple, peut se faire au moyen d'une déchiqueteuse ou en rassemblant les données dans des containers spéciaux, dont le contenu est détruit par une firme spécialisée. La destruction de données originales n'est possible qu'après en avoir averti le propriétaire et compte tenu des dispositions légales y afférentes. L'acte de destruction doit faire l'objet d'une autorisation.

Disponibilité de l'information : fait que l'information est accessible et utilisable à la demande d'une entité compétente.

Données : information électronique traitée ou stockée sur des systèmes d'information.

Données internes : toutes les données qui ne peuvent être utilisées qu'au sein de l'organisation. Ces données ne peuvent être rendues publiques sans l'accord préalable d'un membre du personnel compétent de l'organisation.

Données sensibles : données classifiées comme telles par leur propriétaire. De manière générale, les données sensibles ne peuvent pas être communiquées au public, mais exclusivement à la personne ou à l'entreprise concernées. En fonction de la classification, ces données sensibles sont clairement définies, soumises à des règles d'utilisation et utilisées par un groupe relativement restreint de collaborateurs.

Données sensibles à caractère personnel : dans cette politique, les données sont considérées comme "sensibles" sur la base des articles 6 (qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle), 7 (santé) et 8 (litiges) de la loi du 8/12/1992 (loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel). Tant qu'il n'y a pas de contradiction avec la législation en la matière, le propriétaire des données peut décider de considérer des données à caractère personnel, autres que celles explicitement indiquées dans la législation susmentionnée, comme "données non sensibles à caractère personnel".

Droits d'accès privilégiés : droits d'accès nécessaires pour introduire des modifications dans le modèle RBAC ou pour exécuter des modifications sur le système (administration système).

E

Environnement à haut risque : environnement exposé à un grand risque sur le plan de la sécurité de l'information. Exemple : environnement qui génère un trafic de données sur un réseau public (comme une connexion VPN).

Espaces sécurisés : espaces physiquement protégés (ex. data centers).

Évaluation des risques : ensemble de procédures visant à identifier, analyser et évaluer des risques.

Événement de sécurité de l'information : changement observé dans le fonctionnement normal d'un système, d'un environnement, d'un processus ou d'une personne, en relation avec une violation potentielle de la sécurité de l'information, l'échec des mesures de contrôle, une situation inédite qui peut être pertinente dans le cadre de la sécurité de l'information.

F

(Digital) Forensics : concernant des procès, des enquêtes judiciaires.

G

Gestion de la continuité business (Business Continuity Management : BCM) : la gestion de la continuité business a pour but de protéger les processus business (activités business) contre les interruptions et, en cas d'interruption, de veiller à une réaction positive et efficace.

Gestion de la continuité ICT : la gestion de la continuité ICT garantit que les technologies de l'information et de la communication ainsi que les services sont protégés et peuvent être restaurés à la fois à des niveaux prédéfinis et dans des délais exigés par le business. La gestion de la continuité ICT soutient le processus général de gestion de la continuité business (Business Continuity Management (BCM)) d'une organisation.

Gestionnaire opérationnel de l'information : un gestionnaire opérationnel de l'information est un individu ou un département, désigné soit par l'organisation, soit par le propriétaire des processus, qui est responsable de l'implémentation et de la gestion opérationnelle des mesures de sécurité nécessaires en fonction du niveau de classification défini par le propriétaire des processus. Dans la pratique, un gestionnaire opérationnel de l'information peut être un administrateur système, un développeur d'applications, un responsable de la gestion des bâtiments...

Gestion relationnelle : gestion de la relation avec un tiers qui a (ou aura) accès à l'information et/ou aux ressources d'information de l'organisation et/ou livre (livrera) des informations et/ou des ressources d'information à l'organisation.

I

Incident de sécurité de l'information : un ou plusieurs événements non désirés liés à la sécurité de l'information présentant un risque significatif de perturber la prestation de services de l'organisation et de compromettre la sécurité de l'information.

Information : l'information est une ressource qui, comme toute autre ressource importante, doit être protégée/sécurisée adéquatement. L'information peut prendre différentes formes, notamment écrite, imprimée, électronique ou orale.

Informations/données confidentielles : dans la classification des données, toutes les catégories doivent être considérées comme confidentielles, à l'exception des données internes de l'entreprise et des données publiques. Il est à noter que certaines données d'entreprise internes, bien que pas vraiment confidentielles, sont quand même sécurisées un minimum.

Intégrité de l'information : fait que l'exactitude et l'exhaustivité de l'information sont protégées.

L

Liste de distribution : liste des personnes auxquelles un document peut être envoyé ou communiqué en tout ou en partie. Il peut d'agir de personnes individuelles physiques ou de groupes de personnes qui se distinguent par une caractéristique vérifiable particulière.

M

Matrice de sécurité : modèle utilisé pour gérer les droits d'accès sur la base des autorisations, rôles et fonctions pour les applications.

Mesures de gestion : mesures prises pour assurer l'intégrité, la confidentialité et la disponibilité de l'information.

Mobile device management (MDM) : software permettant, à distance, d'éteindre ou de bloquer des appareils ou encore d'en effacer des données.

Moyen d'information : tout élément/moyen utile à l'organisation pour créer, recevoir, traiter, stocker, distribuer, envoyer, dupliquer et détruire de l'information ; information pouvant être stockée sur différents supports d'information et dans différents systèmes d'information.

P

Patch : adaptation/mise à jour soit d'un logiciel existant sur la base d'un code de programme pour corriger et/ou améliorer des lacunes ou des erreurs, soit d'une machine réseau et/ou d'un câblage réseau.

Périmètre logique : barrière au niveau des systèmes d'information, qui empêche l'intrusion de personnes ou d'applications non autorisées. L'existence d'un périmètre logique exige donc la vérification de l'identité, le contrôle de l'autorisation et le filtrage des données.

Périmètre physique : barrière physique bloquant l'accès aux personnes non autorisées. L'existence d'un périmètre physique s'accompagne donc de l'octroi d'un accès à des personnes autorisées. Diverses formes sont possibles, telles qu'une clé ou un système de badge. Dans le cadre de cette politique, on part du principe que le périmètre physique est suffisamment sécurisé contre une intrusion par des personnes non autorisées.

Privacy Risk Assessment (PRA) : voir l'analyse d'impact relative à la protection des données.

Procédures : elles soutiennent les documents politiques spécifiques en traduisant les politiques concernées en tâches opérationnelles spécifiques (détermination de la sécurisation).

Profil de risque : résultat de l'analyse des risques de l'organisation. Dans l'analyse des risques, les risques sont déterminés sur la base de l'impact et de la probabilité de menaces à la sécurité de l'information. Tous les risques confondus constituent le profil de risque de l'organisation.

Propriétaire de l'information : l'information doit être attribuée à un "propriétaire" qui connaît l'utilisation et la valeur de l'information pour l'organisation, nécessaire pour déterminer le niveau de classification de l'information. Un "propriétaire" de l'information est chargé de :

- protéger l'information
- déterminer la valeur de l'information pour l'organisation
- déterminer le niveau de classification de l'information
- labelliser l'information
- appliquer les mesures de gestion nécessaires sur la base de la classification

Un "propriétaire" de l'information ne détient toutefois aucun droit de propriété au sens strictement juridique du terme.

Propriétaire de rôle : responsable d'un rôle dans le modèle RBAC, composé d'un lot spécifique d'autorisations et associé à une ou plusieurs fonctions.

Propriétaire système : responsable d'un ou plusieurs systèmes d'information placés sous la gestion de l'organisation.

R

Recovery Point Objective (RPO) : délai maximal durant lequel la perte de données est acceptable.

Recovery Time Objective (RTO) : délai dans lequel des systèmes et des données doivent être restaurés à un point antérieurement constaté à la suite de la panne d'un système.

Respect : le non-respect de ces politiques peut entraîner de graves risques à la sécurité concernant la confidentialité, l'intégrité et la disponibilité des données (sensibles), ainsi que l'image et la réputation de l'organisation. Le non-respect de la politique et des procédures y afférentes peut conduire à des sanctions, voire à des poursuites judiciaires.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre (Source RGPD)

Risque : chance ("probabilité") qu'une certaine menace se produise avec un certain impact ("gravité") en conséquence.

Risque inhérent : probabilité d'un impact négatif en l'absence de mesures de protection.

Risque résiduel : probabilité d'un impact négatif, en dépit des règles prises pour influencer (limiter) le risque (inhérent).

RGPD UE : Règlement général européen sur la protection des données.

Role-based access control (RBAC) : méthode permettant d'organiser de façon efficace et efficiente un contrôle d'accès pour des systèmes d'information, où les utilisateurs sont associés à des fonctions business prédéfinies, qui consistent en divers rôles, dont chacun détient un lot spécifique d'autorisations.

S

Sécurité de l'information : protection de l'information contre un large éventail de menaces. L'intégrité, la confidentialité et la disponibilité de l'information sont trois aspects fondamentaux dans ce contexte.

Session active : environnement en ligne spécifique dans lequel un utilisateur travaille avec son application/transaction. Un utilisateur peut travailler simultanément dans plusieurs environnements (ou sessions) en ligne.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (source RGPD).

Stockage : conservation de données sur un support (moyen de stockage). Un traitement peut être effectué à partir du stockage.

Security Incident & Event management (SIEM) : terme employé pour désigner des produits et services logiciels qui centralisent des données sur des événements et des incidents pour ensuite les analyser.

Security Incident Response Team (SIRT) : équipe de collaborateurs appelée à agir lorsque certains incidents de sécurité de l'information se produisent. En fonction du type d'incident de sécurité de l'information, cette équipe peut chaque fois être composée de différentes personnes.

Support analogique : un support analogique permet de sauvegarder des données sous forme non numérique. Le support analogique le plus répandu est le papier.

Support numérique : lorsque des données sont sauvegardées de façon électronique (représentation des données sous forme binaire), on parle d'un support numérique.

Systèmes d'utilisateurs : tous les systèmes attribués à un utilisateur individuel et utilisés exclusivement par cette personne.

Système de détection d'intrusion : système automatisé qui détecte les tentatives ou les cas d'accès non autorisé à un système d'information ou un réseau.

Système de prévention d'intrusion : système automatisé qui bloque les tentatives ou les cas d'accès non autorisé à un réseau.

Systèmes informatiques ou d'information critiques : sur la base d'une analyse des risques, il faut déterminer si un système informatique ou d'information doit être considéré comme critique. Le caractère critique doit être considéré sur la base de l'importance d'un système informatique ou d'information dans la garantie de la confidentialité, de l'intégrité ou de la disponibilité des données et de la prestation de services IT.

Systèmes d'information : tous les réseaux et systèmes ICT, applications incluses, gérés par l'organisation.

T

Tiers : personne ou organisation étrangère à l'organisation, qui travaille pour ou avec l'organisation ou livre des biens ou des services, à l'exception des clients (ex. citoyens, entreprises). Un tiers de première ligne est le tiers avec lequel l'organisation négocie et conclut un contrat directement.

Token : moyen d'authentification utilisé pour contrôler l'identité de l'utilisateur. Un token comporte généralement des séries de chiffres qui font partie d'un mot de passe (ex. token que peuvent demander des citoyens, token électronique délivré aux collaborateurs de l'organisation).

Traitement : toute opération ou ensemble d'opérations concernant des informations, effectué(e) ou non en recourant à des procédures automatisées, comme la collecte, l'enregistrement, l'ordonnancement, la conservation, la mise à jour, la modification, la demande, la consultation, l'utilisation, la fourniture via envoi ou diffusion ou la mise à disposition, la compilation ou la mise en relation d'une quelconque autre façon, de même que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

Transaction : échange automatique de données entre systèmes IT sans intervention d'un utilisateur. Exemple : échange de données avec d'autres institutions publiques.

Transport : le transport physique de données désigne le déplacement du support (analogique ou numérique) ou le déplacement du matériel dans lequel serait intégré ce support. Implicitement, il est alors aussi automatiquement question de moyen de stockage mobile. Le transport électronique désigne la copie ou le traitement de données via un réseau de télécommunication. Le transport électronique concerne exclusivement des données numériques. Le transport électronique se caractérise par le fait que l'on ne déplace pas le moyen de stockage même, mais une copie des données.

U

Utilisateurs de systèmes d'information : tous les collaborateurs internes et externes, services et applications automatisés, parties externes (ex. autres organisations) et clients (ex. individus, entreprises, institutions).

Usurpation d'adresse : technique permettant d'usurper des adresses IP afin de contourner les pare-feux.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2017		V2017	Intégration EU GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si des erreurs ou des problèmes sont constatés à la lecture du présent document, vous êtes prié en tant que lecteur de transmettre au conseiller en sécurité de la sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'institution une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement à vos données de contact.

***** FIN DU DOCUMENT *****