Politique relative à la sécurité et la confidentialité de l'information

Classification des données

(BLD DATA)

TABLE DES MATIERES

1. Introduction

Le présent document fait partie intégrante de la méthodologie relative 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).

La sécurité de l'information désigne l'ensemble des mesures et procédures destinées à protéger l'information. Le but est de garantir la continuité, l'intégrité et la confidentialité de l'information et des systèmes d'information ainsi que de limiter les conséquences des éventuels incidents de sécurité.

Le niveau de protection de l'information est exprimé en niveaux de classification pour la disponibilité, l'intégrité et la confidentialité de l'information :

- Confidentialité : compétences et possibilités concernant la mutation, la copie, l'ajout, la destruction ou la prise de connaissance d'informations pour un groupe déterminé d'ayants droit. Niveaux distingués : non protégé, restreint, confidentiel, secret.
- Intégrité : conformité de l'information avec la réalité et non-altération ou destruction volontaire ou accidentelle d'informations (l'intégralité, la précision, l'exactitude/l'authenticité et la validité). Niveaux distingués : incertain, protégé, élevé et absolu.
- Disponibilité : accessibilité et utilisabilité de l'information. Niveaux distingués : pas nécessaire, nécessaire, important et essentiel.

L'attribution de niveaux de classification à l'information et aux systèmes d'information est importante, car elle permet d'indiquer le niveau de protection (exigé). Il est ainsi possible de déterminer les exigences valables et les mesures à prendre. Ceci est par exemple pertinent pour des administrateurs qui ne sont pas toujours au fait du contenu et donc de la valeur de l'information, mais qui sont bien supposés prendre des mesures de sécurité adéquates. Les facteurs suivants influencent les mesures de sécurité adéquates : points de départ, principes architecturaux, exigences de sécurité.

Une méthode de classification permet de déterminer combien de mesures sont nécessaires. Si la classification est plus élevée que "confidentiel", des mesures supplémentaires s'imposent. Parfois, ces mesures sont déjà reprises dans la procédure. Parfois, ces mesures supplémentaires ont déjà été élaborées dans le cadre d'une évaluation des risques réalisée par une autre institution ou l'institution réalise une pondération des risques via une évaluation des risques résultant en des mesures plus adéquates.

Ce document explique l'importance et la méthode de la classification de l'information.

2. Classification de l'information

Toute organisation souscrit à la politique suivante relative à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité :

1. L'institution doit appliquer la protection ou la classification de l'information prévue, en ce compris les mesures de protection de la sécurité et de la confidentialité de l'information suivant un schéma de classification interne conforme à la législation et à la réglementation internationale d'application en la matière[1], et doit utiliser le modèle de classification des données de la sécurité sociale en vue de l'échange mutuel de données entre les organisations relevant des institutions publiques de sécurité sociale. Si les principes décrits dans la législation et la réglementation diffèrent des principes du schéma de classification interne de l'institution, sans toutefois être en contradiction, la règle la plus stricte sera d'application. Si le schéma de classification interne de l'institution est en contradiction avec la législation et la réglementation en vigueur, la législation et la réglementation seront d'application.
2. L'institution doit établir, valider, implémenter, communiquer et maintenir des procédures et des registres adéquats pour la labellisation (étiquetage) et le traitement de l'ensemble des compilations d'information, des supports d'information et des systèmes d'information conformément au schéma de classification interne.
3. L'objet de la classification est l'information. La classification déterminée par le type d'information vaut également pour le niveau supérieur des systèmes d'information. C'est-à-dire que si un système traite des informations secrètes, le système entier sera considéré comme secret, à moins que des mesures n'aient été prises dans le système d'information pour ce niveau supérieur. Toutes les classifications de tous les systèmes critiques sont définies centralement par les propriétaires et doivent être contrôlées annuellement par le conseiller en sécurité de l'information (CISO) et/ou le délégué à la protection des données (DPO).
4. Le responsable du traitement de l'information[2] détermine le niveau de protection exigé (classification) sur la base du schéma de classification interne. S'il s'agit d'exigences légales, cela sera indiqué explicitement. Le responsable du traitement de l'information détermine qui a accès à quelle information.
5. Le responsable du traitement de l'information peut se faire aider par des experts pour la classification, par exemple le conseiller en sécurité de l'information (CISO) et/ou le délégué à la protection des données (DPO).
6. L'information peut être plus ou moins sensible ou critique. Pour certaines informations, un niveau additionnel de protection ou un traitement spécial peuvent être nécessaires. Si des mesures destinées à protéger adéquatement des parties de l'information système classifiée à un niveau supérieur ont été prises dans le système d'information, ce dernier peut être globalement positionné plus bas dans le tableau et ainsi par exemple encore tomber dans la norme.
7. Un niveau de classification le plus "bas" possible est visé. En effet, une classification trop élevée engendre des coûts inutiles. En outre, l'information doit en principe être disponible pour un maximum de personnes dans le cadre d'une administration transparente.
8. Les mesures de contrôle doivent être adaptées aux risques, sur la base des possibilités techniques et des coûts des mesures à prendre. Ceci en fonction de la situation. Plus sensible est l'information, ou plus grand est le risque suivant le contexte dans lequel elle est utilisée, plus lourdes sont les exigences au niveau de la sécurité de l'information. Globalement, si des mesures permettent d'augmenter la sécurité et la confidentialité moyennant de faibles coûts supplémentaires, elles peuvent être considérées comme "appropriées". Des mesures permettant d'augmenter la sécurité et la confidentialité ne sont plus considérées comme "appropriées" à partir du moment où le coût qu'elles nécessitent pour mitiger les risques est disproportionnellement élevé. Les risques et les mesures de contrôle doivent être en équilibre.

[1] Notamment la législation du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

[2] Il s'agit généralement du propriétaire du processus.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2007		V2007	Première version	10/10/2007	10/10/2007
2017		V2017	Intégration EU GDPR	07/03/2017	07/03/2017
2018		V2018	Update après contrôle du groupe de travail policy en 2017	09/01/2018	01/01/2019

Erreurs et oublis

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 plateforme eHealth une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement à vos données de contact.

Définitions

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 un document intitulé "Définitions relatives à la sécurité et à la confidentialité de l'information".

Annexe B : Références

Ci-dessous figurent les documents qui ont servi d'inspiration au présent document :

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 pages
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 pages
- ISO, "ISO/IEC 27010:2015 Information security management for inter-sector and inter-organizational communications", novembre 2015, 32 pages
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 pages
- ENISA, "Threat taxonomy: a tool for structuring threat information", janvier 2016, 23 pages
- NIST, SP800-60 volume II revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories", août 2008, 279 pages

Ci-dessous figurent des références aux sites web qui ont servi d'inspiration au présent document.

- http://www.iso.org/iso/iso27001
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=68427
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf
- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information
- https://www.cert.be/fr/het-traffic-light-protocol-tlp.html

Annexe C : Directives relatives à la classification de l'information

Application de la législation et de la réglementation

Directives
Toutes les données à caractère personnel sont protégées par la législation, indépendamment de tout système de classification explicite. Depuis le 27 avril 2016, les données à caractère personnel sont protégées par le Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[3]. Les principes de ce Règlement doivent être respectés, indépendamment du système de classification interne défini par l'institution.

Des procédures doivent être établies pour permettre à chaque citoyen de revendiquer le droit de consulter des documents administratifs conformément à la loi du 1er avril 1994 relative à la publicité de l'administration. Ces procédures doivent permettre d'évaluer des demandes d'accès et de refuser les demandes qui ne répondent pas aux conditions prescrites par la loi. En vertu de la loi du 1er avril 1994 relative à la publicité de l'administration, il peut être dérogé aux règles de classification internes et aux mesures de sécurité y afférentes, après vérification de la validité d'une demande d'accès à des documents administratifs. Cette dérogation n'est possible que sur la base d'une décision d'une personne ou d'un organe mandatés.

Pour des informations émanant d'autres pays ou d'institutions internationales établies en Belgique auxquelles a accès l'institution, l'institution doit agir "au nom de l'instance d'origine" ("propriétaire" de l'information). Dans les cas précités, l'institution doit appliquer les mesures de sécurité correspondant au niveau de classification de l'information concernée.

Classification de l'information créée par l'institution

Directives
L'institution doit classifier toutes les informations (et tous les moyens d'information) qui échappent à la réglementation ou la législation relatives à la classification. Il s'agit d'informations :

- créées par l'institution même
  et
  - soit stockées en son nom sur des supports analogiques ou numériques (en sa détention ou non)
  - soit déplacées physiquement ou échangées électroniquement sur n'importe quel support en son nom.

Les informations non classifiées explicitement seront considérées comme internes, de sorte que ces informations :

- peuvent circuler librement dans l'institution
- peuvent être communiquées uniquement au public ou à des tiers sur la base d'une procédure d'autorisation
- peuvent être communiquées à des contractants ou à des partenaires si elles sont nécessaires à l'exécution d'une mission et si leur protection est garantie
- les informations non classifiées relatives à des personnes ou à des organisations peuvent être communiquées exclusivement aux personnes et organisations concernées.

La classification doit exprimer l'importance de l'information pour l'institution en termes de valeur pour l'institution,
de criticité, de sensibilité (confidentialité, intégrité et disponibilité) et d'exigences légales et/ou contractuelles.
L'information doit dès lors être classifiée de telle sorte qu'elle bénéficie d'une protection adéquate.
Le responsable du traitement de l'information et des moyens d'information est responsable de la classification.

[3] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&qid=1484310282035&from=FR

Un schéma de classification, composé de différents niveaux de classification, doit être dressé et contenir des accords de classification ainsi que des critères pour le contrôle régulier de la classification. Le niveau de protection doit être déterminé sur la base d'une analyse des aspects de confidentialité, d'intégrité et de disponibilité ainsi que - si nécessaire - sur la base de critères supplémentaires.

Le schéma de classification doit être cohérent à travers toute l'organisation afin que chacun classifie l'information de la même manière et ait la même conception des mesures de protection et de l'application de la protection adéquate.

Aucune donnée ne peut être traitée sans l'accord du propriétaire des données ou sans une règle explicite autorisant le traitement des données[4].

Une institution qui traite des informations au moyen de systèmes d'information court certains risques étant donné que ces informations et systèmes d'information sont exposés à des menaces et à des problèmes internes et externes.
La réalisation d'une solide évaluation des risques aide à déterminer les risques encourus ainsi que leur importance. Cela permet ensuite de déterminer les mesures de sécurité à prendre pour réduire les risques à un niveau acceptable. Dans la traduction des risques en mesures notamment, la classification constitue un précieux instrument pour déterminer la gravité d'un risque et la portée d'une mesure. Le schéma de classification interne proposé peut être considéré comme une forme simplifiée d'évaluation des risques. Lors d'une évaluation des risques, les menaces et problèmes sont nommés et inventoriés. La probabilité de chaque menace et chaque problème est déterminée,
de même que le dommage qui pourrait être occasionné si une menace ou un problème devait se réaliser (le risque inhérent).
Le but d'une évaluation des risques est de déterminer comment les risques peuvent être maîtrisés ou réduits à un niveau acceptable, à savoir via des mesures de protection de l'information (le risque résiduel). Outre l'évaluation des risques est réalisée une analyse des coûts-bénéfices. Tous les risques ne peuvent ou ne doivent pas être couverts : lorsque les coûts des mesures destinées à limiter un risque sont plus élevés que le dommage qu'il est susceptible d'entraîner, il peut être décidé d'accepter le risque résiduel.
C'est le responsable du traitement de l'information qui détermine si la classification de l'information est correcte, mais aussi s'il est possible de déroger à l'argumentation des mesures associées à cette classification, parce que le risque résiduel est acceptable.

Labellisation de l'information

Directives

Les procédures de labellisation de l'information doivent recouvrir tant l'information que les moyens physiques et électroniques y afférents et préciser, en fonction du type de moyen, où et comment les labels doivent être apposés.
La labellisation doit refléter le schéma de classification et être respectée pour toutes les informations classifiées à un niveau plus élevé que "interne".
Les informations qui ne sont pas formellement classifiées sont considérées comme "internes".
Les “Disclaimers” (avis de non-responsabilité) doivent indiquer :

- si nécessaire, que les informations sont sensibles et, si elles ont été créées par l'institution, qu'elles sont la propriété de l'institution
- que les informations peuvent être lues uniquement par le(s) destinataire(s) indiqué(s)
- que les données ne peuvent pas être utilisées ou communiquées sans autorisation
- que la personne qui a indûment reçu les données doit en avertir l'expéditeur
- s'il s'agit d'informations (très) confidentielles envoyées par la poste, que seul le destinataire peut ouvrir l'enveloppe.

[4] Loi du 11 avril 1994 relative à la publicité de l'administration

Manipulation des moyens d'information

Directives

Des procédures doivent être établies pour la manipulation, le traitement, le stockage et la communication d'informations conformément à leur classification.

Les aspects suivants doivent être pris en considération lors de la manipulation des moyens d'information :

- restrictions d'accès en fonction du niveau de classification et fondées sur le principe "need-to-have" pour la tâche
- enregistrement des destinataires autorisés des moyens d'information
- protection des copies temporaires ou permanentes de l'information à un niveau conforme au niveau de protection de l'information originale
- marquage (labellisation) de toutes les copies des moyens d'information à l'attention du (des) destinataire(s) autorisé(s).
- stockage des moyens ICT conformément au niveau de classification et/ou aux spécifications produit du fournisseur

Les accords avec d'autres organisations externes avec lesquelles sont échangées des informations doivent comporter des procédures pour identifier la classification de l'information et interpréter les labels/niveaux de classification d'autres organisations. Même si des dénominations de classification issues d'un schéma de classification d'une autre organisation sont identiques ou comparables à celles de l'institution, cela ne signifie pas que la valeur qui y est accordée est identique ou comparable.

Annexe D : Modèles de schémas de classification de données

1. Le modèle de classification des informations de la sécurité sociale

Les informations sont caractérisées par les paramètres suivants

- le type de donnée: en fonction des domaines inhérents à la sécurité sociale auxquels la donnée appartient;
- la sensibilité: détermine en général l'impact de la perte ou de la diffusion des informations.

On distingue 5 classes de sensibilité:

- *Niveau 4 à titre d'information (Top secret - Très secret)*
  Tombent sous les niveaux « Top Secret » pour l'Europe et "Très secret" pour la Belgique, les données, le matériel, les technologies, ... dont la connaissance ou l'utilisation risque de compromettre sérieusement le fonctionnement de l'Europe ou de la Belgique.
  En raison de la cohérence avec la position des institutions en Europe ou en Belgique, ce niveau de classification n'est pas utilisé dans les institutions.
- *Niveau 3: secret (Secret – High Classified – très confidentiel)*
  Le niveau « Secret » est attribué lorsqu'un usage inadéquat des informations
  - est susceptible de nuire gravement aux intérêts essentiels de l'institution.
  - a un impact sur les droits relatifs à la vie privée d'un groupe significatif de personnes
- *Niveau 2: confidentiel (Classified)*
  Le niveau « Confidentiel » est attribué lorsqu'un usage inadéquat des informations (par exemple suite à une protection insuffisante des données)
  - est susceptible de nuire à un des intérêts de l'institution ou de compromettre le fonctionnement du service.
  - a un impact sur les droits relatifs à la vie privée d'un groupe de personnes ou de personnes vulnérables et/ou d'enfants
- *Niveau 1: limité (Sensitive unclassified)*
  Le niveau « Limité » est attribué lorsqu'un usage inadéquat des informations
  - est susceptible de nuire à un intérêt d'un service ou de compromettre le fonctionnement d'un fonctionnaire ou d'un groupe de personnes dans le cadre de leur fonction au sein de l'institution.
  - a un impact sur les droits relatifs à la vie privée d'un groupe limité (exprimé en un pourcentage) de personnes ou d'une personne individuelle
- *Niveau 0: non classé (Unclassified – public)*

  Ce niveau a pour conséquence que les informations peuvent être diffusées sans problème puisque cette diffusion ne compromet pas l'intérêt de l'institution, d'un service ou le fonctionnement d'un fonctionnaire ou d'un groupe de personnes dans le cadre de leur fonction au sein de l'institution.

Remarque : Les **« données sensibles »** sont des données avec une classe de sensibilité « confidentielle » ou supérieure.

On distingue les types de données (informations) suivants:

I. Données publiques

Sont considérées comme des données publiques toutes les données qui sont publiques, qui ont notoriété générale ou sont dénuées de contenu confidentiel. Tous les autres types de données sont par conséquent des « données non publiques ».

La classe de sensibilité par défaut de données publiques est « non classée ».

Exemples: site internet accessible au grand public, brochures papier ou vidéos sur les médias sociaux destinés aux citoyens.

II. Données internes

Les données internes sont l'ensemble des données dont l'utilisation doit se limiter en interne dans l'institution. Ces données ne sont pas destinées à une publication au grand public sans l'approbation préalable de la direction.

La classe de sensibilité par défaut de ces données est « limitée ».

Exemples: liste de téléphone interne, procès-verbal d'un groupe de projet.

III. Données d'entreprise confidentielles

Les données confidentielles de l'entreprise sont l'ensemble des données liées au fonctionnement de l'institution et qui ont un caractère confidentiel dans le contexte de l'institution - et éventuellement de partenaires spécifiques. Ces données ne peuvent pas être communiquées sans l'approbation préalable de la direction.

La classe de sensibilité par défaut de ces données est « confidentielle ».

Exemples de données confidentielles: rapport du comité de direction, tableaux de bord, estimations budgétaires, budget, listes d'hôpitaux, listes de professionnels des soins de santé, liste des présidents de CPAS, ...

Synonyme: données professionnelles

IV. Données à caractère personnel

Données relatives à une personnes physique identifiée ou identifiable. Toutes les données à caractère personnel ont un caractère confidentiel et sont soumises aux directives du Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. (1)

La classe de sensibilité par défaut de ces données est « confidentielle ».

(1) (réglementation RGPD) « données à caractère personnel »: toute information concernant une personne physique identifiée ou identifiable (« la personne concernée »); est réputée identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel un nom, un numéro d'identification, des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique;

V. Données sociales à caractère personnel

Les « données sociales à caractère personnel [(1)] » sont toutes les données à caractère personnel nécessaires à l'application de la sécurité sociale concernant une personne physique. Les données sociales qui ne constituent pas des données à caractère personnel doivent au moins être traitées comme des données confidentielles de l'entreprise.

La classe de sensibilité par défaut de ces données est « confidentielle ».

(1) Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, art. 2, 6°.

VI. Données médicales à caractère personnel

Les « données sociales à caractère personnel relatives à la santé » [(1)] sont toutes les données sociales à caractère personnel dont on peut déduire une information sur l'état antérieur, actuel ou futur de la santé, à l'exception des données purement administratives ou comptables relatives aux traitements ou aux soins médicaux. Le traitement, l'échange et la conservation de ces données doivent avoir lieu sous la surveillance et la responsabilité d'un médecin [(2)].

La classe de sensibilité de ces données est « secrète ».

(1) Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, art. 2, 7°

(2) Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, art. 26, § 1er

Remarque :

- Définition RGPD (art. 4): « données concernant la santé »: les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;
- Voir aussi note MEDSEC

VII. Données médicales à caractère administratif

Il s'agit des données purement administratives ou comptables de la loi du 21 août 2008 ou donc l'ensemble des données médicales qui ne font pas partie des « données médicales à caractère personnel » (voir aussi la ligne directrice BLD MEDSEC chapitre 2).

La classe de sensibilité par défaut de ces données est « confidentielle ».

VIII. Données classifiées (loi du 11/12/1998)

La loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité fixe les critères pour la classification des documents ayant trait à la protection du territoire, ainsi que les compétences et responsabilités des fonctionnaires habilités à les utiliser.

Les classes de sensibilité de ces données sont « très secrète », « secrète », « confidentielle ».

IX. Données privées

Cette catégorie spéciale concerne des données privées qui peuvent être enregistrées par des collaborateurs dans le réseau de l'institution, mais qui n'ont aucun rapport avec leurs activités professionnelles. Les données personnelles sont traitées selon les règles du Règlement relatif à la vie privée et du règlement interne de l'institution.

La classe de sensibilité par défaut de ces données est « confidentielle ».

Exemple: lettre à des fins privées, courriels privés, fichiers relatifs à la gestion de la carrière personnelle, lettre à des fins privées

X. Catégories spécifiques de données à caractère personnel

(Art. 9 du RGPD) Données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

La classe de sensibilité de ces données est « secrète ».

Synonyme: données à caractère personnel spécifiques

XI Données à caractère personnel relatives aux condamnations pénales et aux infractions

(Art. 10 RGPD) Données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes

La classe de sensibilité de ces données est « secrète ».

XII. Données d'entreprise très confidentielles

Les données d'entreprise très confidentielles sont toutes les données en rapport avec le fonctionnement de l'institution et qui ont un caractère très confidentiel dans le contexte de l'institution, et éventuellement de partenaires spécifiques.

La classe de sensibilité par défaut de ces données est « très confidentielle ».
Exemples de ces données très confidentielles: la configuration de l'infrastructure TIC dans les centres de données.

Remarque : **données sensibles à caractère personnel** est la dénomination commune pour les données médicales à caractère personnel, les catégories spécifiques de données à caractère personnel, les données relatives aux condamnations pénales et aux infractions.

Aperçu type de donnée et classe de sensibilité par défaut

Type de données (informations) groupes	Classe de sensibilité
1. DONNEES PUBLIQUES **I. Données publiques**	non classée
2. DONNEES INTERNES **II. Données internes**	limitée
3. DONNEES D'ENTREPRISE CONFIDENTIELLES **III. Données d'entreprise confidentielles**	confidentielle
4. DONNEES A CARACTERE PERSONNEL **IV. Données à caractère personnel**	confidentielle
5. DONNEES SOCIALES A CARACTERE PERSONNEL **V. Données sociales à caractère personnel)**	confidentielle
6. DONNEES SENSIBLES A CARACTERE PERSONNEL **VI. Données médicales à caractère personnel** **X Catégories spécifiques de données à caractère personnel** **XI Données à caractère personnel relatives aux condamnations pénales et aux infractions**	très confidentielle
7. DONNEES MEDICALES A CARACTERE ADMINISTRATIF **VII Données médicales à caractère administratif**	confidentielle
8. DONNEES CLASSIFIEES (loi du 11/12/1998) **VIII Données classifiées (loi du 11/12/1998)**	très secrète, secrète, confidentielle
9. DONNEES PRIVEES **IX Données privées**	confidentielle
10. DONNEES D'ENTREPRISE TRES CONFIDENTIELLES **XII. Données très confidentielles de l'entreprise**	très confidentielle

2. TLP

Ci-dessous suit un exemple de classification par type de données, propre au contexte de l'échange d'informations entre institutions.

Le "Traffic Light Protocol" (ou TLP en abrégé) a été conçu pour permettre et encourager un échange d'informations sûr et contrôlé. Le concept fondamental est, pour l'expéditeur, d'indiquer dans quelle mesure il souhaite que ses informations soient diffusées en dehors de leur destinataire.

Le protocole exige que l'expéditeur attribue un code couleur à chaque information qu'il envoie. Cette couleur indique si et comment cette information peut être diffusée. Celui qui reçoit des informations et considère que certaines de ces informations doivent pouvoir être diffusées à plus grande échelle doit demander l'autorisation explicite de l'expéditeur.

Le TLP procure un schéma simple et intuitif permettant d'indiquer quand et moyennant quelle confidentialité certaines informations peuvent être partagées dans une communauté. Le partage de ces informations génère une collaboration plus fréquente et efficace entre l'institution et ses partenaires.

Couleurs et signification :

ROUGE	**Informations destinées exclusivement aux destinataires immédiats** Exemple : seulement pour les participants à une réunion, le destinataire immédiat d'un sms, d'un e-mail ou d'une lettre.
AMBRE	**Informations destinées à une organisation, éventuellement limitées à certaines personnes de l'organisation** Exemple : des informations peuvent être diffusées dans l'organisation sur une base "need-to-know". L'expéditeur a le droit de définir les limites de la diffusion.
VERT	**Informations destinées à une communauté, mais à ne pas diffuser sur internet** Exemple : partage d'informations uniquement dans un secteur déterminé sans diffusion sur internet ou en dehors du secteur
BLANC	**Informations pouvant être diffusées librement et indéfiniment, pour autant que la diffusion ne soit pas contraires à la loi (exemple : loi sur les droits d'auteur)**

3. Sécurité de l'information

Ci-dessous suit un exemple de classification par type de critère de sécurité de l'information :

- confidentialité
- intégrité et
- disponibilité

Niveaux de confidentialité distingués :

- Non classé : informations accessibles au grand public. Il n'y a pas de violation de cette classification possible.
- Interne : informations qui peuvent ou doivent être accessibles à tout le personnel de l'institution. La confidentialité est faible. La violation de cette classification peut engendrer un dommage (in)direct quelconque.
- Confidentiel : informations accessibles uniquement à un groupe restreint de personnes. Les informations sont mises à disposition sur la base de la confiance. La violation de cette classification peut engendrer un sérieux dommage (in)direct.
- Secret : informations sensibles qui peuvent être accessibles uniquement au destinataire immédiat. La violation de cette classification peut engendrer un dommage (in)direct très élevé.

Niveau	Authentification	Autorisation	Monitoring	Sécurité / Confidentialité
Non classé	Non	Non	Non	Non
Interne	Authentification "de base" requise. Expiration de session après 15 minutes d'inactivité. Expiration de session absolue après 120 minutes.	Authentification requise (membre de l'organisation)	Détermination de l'authentification erronée répétitive et du moment. Conservation des données de monitoring pour	Validation de l'output. Chiffrement durant le transport en dehors du réseau de l'institution via une sécurisation du transport ou du message. Les copies de données doivent être protégées tout aussi bien.

Niveau	Authentification	Autorisation	Monitoring	Sécurité / Confidentialité
	Blocage d'identité après 3 tentatives d'authentification successives échouées Authentification "de base" nécessaire pour le déblocage.		une période de six mois.	Les données de l'environnement de production ne sont pas utilisées dans les environnements de développement, de test et d'acceptation, à moins qu'elles aient été anonymisées et que le propriétaire de l'information ait donné son accord.
Confidentiel	Authentification "moyenne" requise. Expiration de session après 15 minutes d'inactivité. Pour le client, expiration de session absolue après 120 minutes. Blocage d'identité après 3 tentatives d'authentification successives échouées Authentification "moyenne" nécessaire pour le déblocage.	Autorisation exigée (rôle spécifique)	Détermination de l'authentification erronée répétitive et du moment. Conservation des données de monitoring pour une période de deux ans.	Validation de l'output. Chiffrement durant le transport et aux étapes intermédiaires dans et en dehors du réseau de l'institution via sécurisation du message. Les copies de données doivent au minimum être protégées tout aussi bien. Réduction du nombre de copies à un minimum. Les données de l'environnement de production ne sont pas utilisées dans les environnements de développement, de test et d'acceptation, à moins qu'elles aient été anonymisées et que le propriétaire de l'information ait donné son accord.
Secret	Authentification "élevée" requise. Expiration de session après 15 minutes d'inactivité. Pour le client, expiration de session absolue après 120 minutes. Blocage d'identité après 3 tentatives d'authentification successives échouées. Authentification "élevée" nécessaire pour le déblocage. Pas de SSO autorisé.	Autorisation exigée (rôle spécifique)	Détermination de l'authentification correcte et erronée et du moment. Conservation des données de monitoring pour une période de dix ans.	Validation de l'output. Chiffrement durant le transport et aux étapes intermédiaires via sécurisation du message. Stockage chiffré des données. Réduire à un minimum le transport de données. Uniquement transport et stockage dans le réseau fixe de la Commune <nom de la commune>. Pas de copies autorisées sauf pour disponibilité. Les données de l'environnement de production ne sont pas utilisées dans des environnements DTA, à moins qu'elles aient été anonymisées et que le propriétaire de l'information ait donné son accord.

Niveaux d'intégrité :

- Pas sûr : cette information peut changer. Pas de protection supplémentaire de l'intégrité nécessaire. La violation de l'intégrité n'a pas de dommage en conséquence.
- Protégé : le processus métier qui utilise cette information autorise quelques erreurs (d'intégrité). Un niveau de sécurisation de base est nécessaire. La violation de cette classification peut engendrer un dommage (in)direct quelconque.
- Élevé : le processus métier qui utilise cette information autorise un très petit nombre d'erreurs (d'intégrité). La protection de l'intégrité est indispensable. La violation de cette classification peut engendrer un sérieux dommage (in)direct.
- Absolu : le processus métier qui utilise cette information n'autorise aucune erreur (d'intégrité). La violation de cette intégrité peut engendrer un dommage (in)direct très élevé.

Niveau	Authentification	Autorisation	Monitoring	Sécurité / Confidentialité
Pas sûr	Non	Non	Non	Non
Protégé	Authentification "de base" requise.	Autorisation exigée.	Détermination de l'authentification (correcte et erronée) et du moment. Détermination de l'input et de l'output pertinents d'un système ou service IT. Conservation des données de monitoring pour une période de six mois	Validation de l'input. Contrôle de la mutation durant le transport. Sécurité du transport et du message. Données : la version des données utilisées est connue. Après exécution d'un service, les données modifiées restent cohérentes.
Elevé	Authentification "moyenne" requise.	Autorisation exigée. Principe des quatre yeux exigé.	Détermination de l'authentification (correcte et erronée) et du moment. Détermination de l'input et de l'output pertinents d'un système ou service IT. Conservation des données de monitoring pour une période de maximum deux ans ou plus en cas de présomption d'incident de sécurité.	Validation de l'input. Contrôle de la mutation durant le transport. Sécurisation du message. Données : la version des données utilisées est connue. Modifications sur la source uniquement. Après exécution d'un service, les données modifiées restent cohérentes.
Absolu	Authentification "élevée" requise. Pas de SSO autorisé.	Autorisation exigée. Principe des quatre yeux exigé.	Détermination de l'authentification (correcte et erronée) et du moment. Détermination de l'input et de l'output pertinents d'un système ou service IT. Conservation des données de monitoring pour une période de minimum trois ans en cas de présomption d'incident de sécurité. Détermination de l'ancien état des données à modifier.	Validation de l'input. Contrôle de la mutation durant le transport. Sécurisation du message. L'information n'est pas stockée en dehors de la source (sauf pour disponibilité) et pas modifiée en dehors de la source. Après exécution d'un service, les données modifiées restent cohérentes.

Niveaux de disponibilité:

- Pas nécessaire : les données peuvent être indisponibles sans conséquences. La violation de la disponibilité n'a pas de dommage en conséquence.
- Nécessaire : l'information ou le service peut être indisponible accidentellement, le processus autorise une indisponibilité accidentelle. La continuité devra reprendre après un délai raisonnable. La violation de cette classification peut engendrer un quelconque dommage (in)direct.
- Important : l'information ou le service ne peut quasi jamais être indisponible accidentellement, le processus n'autorise quasi pas d'indisponibilité accidentelle. La continuité devra reprendre rapidement. La violation de cette classification peut engendrer un sérieux dommage (in)direct.
- Essentiel : l'information ou le service peut être indisponible très exceptionnellement, par exemple à la suite d'une catastrophe. Le processus n'autorise à vrai dire pas d'indisponibilité. La continuité devra reprendre très rapidement. La violation de cette intégrité peut engendrer un dommage (in)direct très élevé.

Pas nécessaire : applications : 99,5 % de disponibilité les jours ouvrables entre 07h et 19h Intranet: 99,5 % de disponibilité les jours ouvrables entre 07h et 19h

Nécessaire	
Temps de travail	De 8h à 17h du lundi au vendredi excepté les jours fériés généralement reconnus.
Disponible pendant les heures de travail	99,6 %
Disponible en dehors des heures de travail	96,1 %
Nombre de perturbations	
3 minutes ou moins	4 par mois
Plus de 3 minutes	1 par mois

Important	
Temps de travail	De 7h à 21h du lundi au vendredi excepté les jours fériés généralement reconnus.
Disponible pendant les heures de travail	99,6 %
Disponible en dehors des heures de travail	96,1 %
Nombre de perturbations	
3 minutes ou moins	2 par mois
Plus de 3 minutes	1 par tranche de 2 mois

Essentiel	
Temps de travail	24 heures sur 24 et 7 jours sur 7, sauf en cas de maintenance planifiée
Disponible	99,9 %
Nombre de perturbations	
3 minutes ou moins	1 par mois
Plus de 3 minutes	1 par tranche de 6 mois

Annexe E : Lien avec la norme ISO 27002:2013

Nous renvoyons ici à la (aux) clause(s) principale(s) de la norme ISO 27002:2013 relative à l'objet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	**Oui**
Personnel sûr	
Gestion des moyens d'exploitation	
Sécurisation des accès	
Cryptographie	
Sécurité physique et de l'environnement	
Sécurisation des processus	
Sécurité de la communication	
Achats, maintenance et développement de systèmes d'information	
Relations fournisseurs	
Gestion des incidents de sécurité	
Aspects de sécurité de l'information de la gestion de la continuité	
Respect	

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