Échelle de sensibilité

Protection des informations[1]

Travail commun Inria / CNRS / INRA

1 OBJECTIF DU DOCUMENT 2

2 PERIMETRE D'APPLICATION 2

3 IMPACTS 2

4 CLASSIFICATION DE L'INFORMATION 4

4.1 NIVEAUX DE CLASSIFICATION 4

4.2 RESPONSABILITES DES ACTEURS 5

4.2.1 OBLIGATION DE DISCRETION 5

4.2.2 BESOIN D'EN CONNAITRE 5

4.2.3 RESPONSABILITE DU PRODUCTEUR DE L'INFORMATION 5

4.2.4 RESPONSABILITE DU DESTINATAIRE DE L'INFORMATION 6

4.3 PROCESSUS DE CLASSIFICATION 6

4.3.1 DUREE DE CLASSIFICATION 6

4.3.2 PROCÉDURE DE DÉCLASSIFICATION 7

5 GESTION DE L'INFORMATION 7

5.1 MARQUAGE 7

5.2 CREATION/STOCKAGE/SAUVEGARDE 7

5.3 IMPRESSION/REPRODUCTION 8

5.4 ACHEMINEMENT 8

5.5 ECHANGES numériques ET PÉRIMÈTRE DE CONFIANCE 9

5.5.1 Confiance dans l'opérateur de l'infrastucture 9

5.5.2 Confiance dans une solution d'échange numérique 10

5.5.3 Usages autorisés d'une solution d'échange numérique en fonction du niveau de classification 10

5.6 AFFICHAGE ET CONSULTATION EN LOCAL 11

5.7 RÉAFFECTATION INTERNE DE MATÉRIEL 11

5.8 FIN DE VIE AU SEIN DE L'ORGANISME 11

ANNEXE A EXEMPLES TYPES D'INFORMATIONS PAR NIVEAU DE CLASSIFICATION 12

ANNEXE B USAGE DES SOLUTIONS D'ÉCHANGES NUMÉRIQUES – EXEMPLES 13

[1] Ce document s'inspire de la « Directive pour la protection des informations non classifiées de défense » du CNES

1 OBJECTIF DU DOCUMENT

Il existe au sein de l'organisme des informations qui ne relèvent pas de la défense nationale et de la sécurité de l'État au titre de l'IGI 1300[2], mais qui doivent être protégées en raison de leur importance pour l'organisme, pour les partenaires, pour les industriels français et européens.

Ce document s'appuie sur l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation et sur l'II 901[3] qui concerne les établissements ou organismes placés sous l'autorité ou la tutelle d'un ministre. En effet, les risques qu'implique l'utilisation des systèmes d'information peuvent mettre en cause l'action de l'État. C'est pourquoi, protéger l'information et sécuriser les systèmes d'information sont des obligations nationales majeures.

Il définit les niveaux de classification des informations en fonction de l'impact potentiel de la divulgation non autorisée de ces informations, que la cause en soit volontaire ou involontaire. Par ailleurs, il informe les utilisateurs des règles, à la fois techniques et organisationnelles, qu'ils doivent respecter pour protéger de manière adéquate les informations qu'ils sont amenés à créer, visualiser, présenter, stocker, échanger, sauvegarder ou encore détruire.

Nota : Les niveaux de classification n'interfèrent pas avec le droit de la propriété intellectuelle ou le droit d'auteur.

2 PERIMETRE D'APPLICATION

La présente directive concerne tous les types d'information traités au sein de l'organisme, y compris dans des versions intermédiaires et quelle que soit leur forme : orale, visuelle, papier, numérique, physique, chimique ou biologique, que ces informations soient créées par les salariés de l'organisme ou du personnel non permanent (stagiaires, intérimaires, …), créées pour l'organisme par des prestataires ou encore transmises à l'organisme par des industriels, des partenaires institutionnels et des laboratoires scientifiques.

Ce document ne s'applique pas aux informations classifiées de défense ou aux informations tombant sous le coup de règlementations imposant des règles particulières[4].

3 IMPACTS

Le tableau ci-dessous permet d'évaluer l'impact lié à la divulgation d'une information selon ses conséquences :

- pour l'organisme, en termes juridiques, financiers, d'image, de patrimoine scientifique et technologique
- pour les personnes concernées
- pour la Nation

L'évaluation de cet impact va conditionner le niveau de classification à attribuer à l'information.

[2] Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale du 30/11/2011
[3] Instruction interministérielle relative à la protection des systèmes d'informations sensibles n°901/SGDSN/ANSSI du 28/01/2015
[4] Par exemple, la réponse des candidats aux marchés publics

Impact	Établissement				Personnes	Nation
	Conséquences juridiques	**Image**	**Conséquences financières**	**Patrimoine scientifique et technologique**	**Conséquences sur les personnes**	**Souveraineté, sécurité, intérêts économiques de la France**
Nul	Aucune	Aucun	Aucune	Aucune	Aucun	Aucun
Modéré	Pénalités contractuelles	Faible	Faible	Pas significatif	Les personnes concernées ne seront pas impactées ou pourraient connaitre quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).	Aucun
Important	Contentieux ou peut entrainer des condamnations civiles ou pénales (règlementation I&L[5])	Peut nuire à l'image ou induire le discrédit de l'organisme ou des partenaires	Significative à importante	Peut favoriser l'émergence de la concurrence ou lui donner un avantage décisif	Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...) ou de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...)	Faible
Catastrophique	Peut entrainer des condamnations pénales au titre de la règlementation sur la protection du secret de la défense nationale (IGI 1300)	Peut remettre en cause le fonctionnement de l'organisme ou des partenaires	Perte financière grave	*(Voir conséquences pour la souveraineté, la sécurité et les intérêts économiques de la nation)*	Les personnes concernées pourraient connaitre des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès...)	Peut porter atteinte à la souveraineté, la sécurité ou aux intérêts économiques essentiels de la France au titre de la loi n°68-678[6]

Tableau 1. Impacts liés à la divulgation d'une information

[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et Règlement Général sur la protection des données (Règlement UE 2016/679)

[6] Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères

4 CLASSIFICATION DE L'INFORMATION

La suite du présent document s'applique principalement aux besoins de confidentialité et d'intégrité.

4.1 NIVEAUX DE CLASSIFICATION

Le niveau de classification est lié aux impacts d'une éventuelle divulgation non autorisée des informations tels que définis précédemment et à la cible de la diffusion. Il détermine les précautions à prendre pour leur manipulation.

C'est l'impact potentiel le plus élevé du fait d'une divulgation non autorisée qui détermine le niveau de classification.

Le niveau de classification s'applique quelle que soit la forme que prend l'information ; ce sont les règles de gestion associées qui peuvent varier en fonction du support de l'information.

Les différents niveaux de classification ainsi définis sont les suivants :

- PUBLIC pour une information dont la cible de diffusion n'est pas contrôlée. Cette publication de l'information présente un impact nul pour l'organisme ;
- DIFFUSION LIMITÉE + Mention pour une information dont la cible n'est pas nominative mais dont la mention précise les structures ou entités destinataires de l'information ou des personnes es-qualité. La mention spécifique associée au niveau de classification peut être suffisante pour définir la liste de diffusion. Une divulgation non autorisée de l'information aurait un impact modéré ;
- CONFIDENTIEL + Mention pour une information dont la cible n'est pas nominative mais précise les structures ou entités destinataires de l'information, des personnes es-qualité et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact important ;
- DIFFUSION RESTREINTE conformément à l'II 901 pour une information dont la cible est nominative ou précise les structures ou entités destinataires de l'information, des personnes es-qualité ayant besoin d'en connaître et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact catastrophique

Des exemples types d'informations qui correspondent aux niveaux de classification DIFFUSION LIMITÉE et CONFIDENTIEL sont fournis en ANNEXE A.

Le tableau ci-dessous résume le niveau de classification à utiliser en fonction de l'impact. La diffusion découle de l'impact.

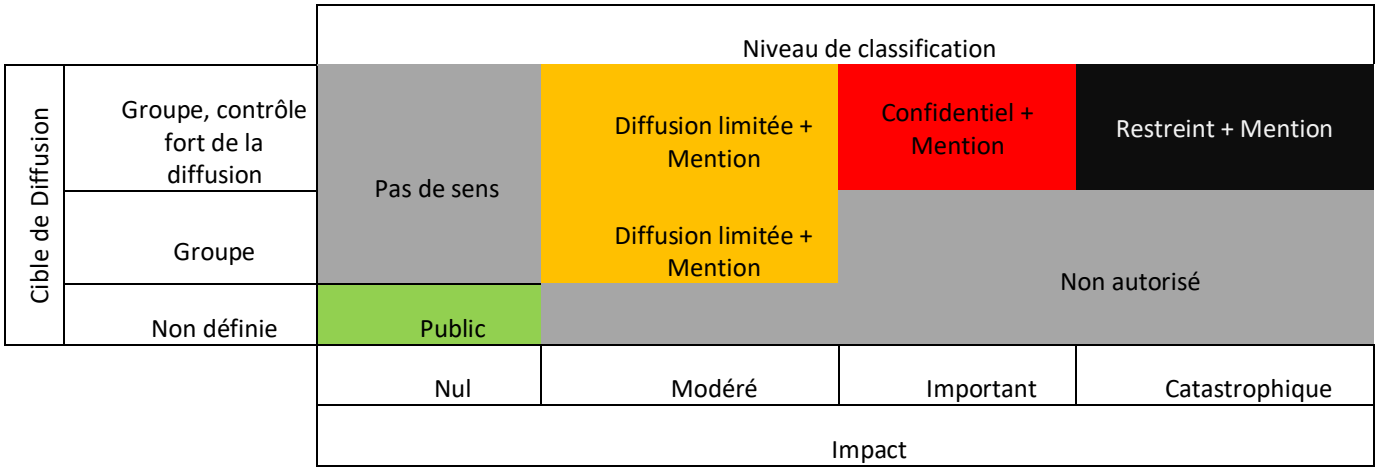

Tableau 2. Niveau de classification en fonction de l'impact

À partir du niveau DIFFUSION LIMITÉE, le niveau de classification doit être assorti d'une mention qui définit la cible de diffusion.

- <ORGANISME> si l'information n'est applicable qu'à l'organisme et ne doit pas être diffusée en dehors ;
- <STRUCTURE> si l'information ne doit être échangée qu'au sein de la structure (laboratoire, institut, délégation régionale, …)
- <GROUPE> si l'information ne doit être échangée qu'au sein d'une communauté définie (Comex, CPSI, managers, réseau métier, …).

- <PROJET> si l'information est liée à un projet donné et qu'elle ne doit être échangée qu'avec les partenaires du projet ; une convention commune à l'ensemble des partenaires du projet pourra être établie au démarrage pour s'assurer que les informations bénéficient des mêmes protections quel que soit le partenaire qui les manipule ;

La mention caractérise le périmètre de diffusion en réservant l'accès à l'information aux seules personnes ayant besoin de les connaître pour l'accomplissement de leur fonction ou de leur mission. Il n'est pas défini de mention par défaut.

Dans tous les cas, c'est le niveau de classification qui détermine les règles à respecter pour protéger une information. La mention accolée au niveau de classification précise ou renforce le cas échéant les règles applicables.

Les données en Open Data, par définition, ne peuvent concerner que des données publiques.

4.2 RÔLE ET RESPONSABILITÉS DES ACTEURS

4.2.1 OBLIGATION DE DISCRETION

Cette obligation de discrétion est rappelée dans le règlement intérieur de chaque établissement, qui s'applique à toute personne qui travaille au sein de l'établissement (salariés, stagiaires, intérimaires et intervenants d'entreprises extérieures). Il stipule que tout agent est tenu à une discrétion professionnelle absolue pour tout ce qui concerne les faits ou informations dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions. Cette obligation subsiste même lorsque l'agent a quitté l'organisme.

Dans tous les autres cas, pour lesquels le règlement intérieur ne s'applique pas, (un prestataire, un sous-traitant, une convention partenariale, etc.) le document juridique régissant la relation[7] doit faire l'objet d'une clause de confidentialité qui mentionne l'obligation de discrétion.

4.2.2 BESOIN D'EN CONNAITRE

L'accès à une information doit respecter le principe du « besoin d'en connaître », quels que soient le niveau de classification et la mention.

La gestion du besoin d'en connaître est une mission d'ordre fonctionnel[8], elle ne peut pas être déléguée à des personnels opérationnels.

Chacun ne doit détenir que les informations nécessaires à son activité. En cas de changement d'affectation ou de départ de l'organisme, l'utilisateur, prendra soin de procéder à l'effacement (conformément aux règles définies dans les chapitres 5.7 et 5.8) ou à la destruction de toute copie des informations qu'il détient et qu'il n'a plus le besoin de connaître.

4.2.1 MISE EN PLACE D'UN REFERENTIEL D'ETABLISSEMENT

Il est de la responsabilité du chef d'établissement de mettre en place un référentiel partagé, indiquant pour chaque type de document le niveau de classification initiale adéquat.

Ce référentiel est tenu à jour par le FSD de l'établissement, qui s'assure qu'il connaît une publicité adéquate afin d'être porté à la connaissance de tous[9]. Le FSD de l'établissement se coordonne avec les FSD des établissements partenaires afin d'harmoniser autant que possible les niveaux de classification de documents identiques par nature.

Le référentiel est mis à jour au fil du temps avec les informations remontées des différents services et unités, par exemple lorsqu'un document d'un nouveau type, ne figurant pas dans le référentiel est inventorié.

Le référentiel alimente les propriétés de sensibilité des objets métiers dans les cadres nationaux de cohérences recherche et enseignement pour une applicabilité globale.

Le FSD est responsable de la mise en place d'un processus opérationnel de mise à jour du référentiel. Ce processus est publié avec le référentiel afin d'être connu de tous.

4.2.2 RESPONSABILITÉ DU DIRECTEUR DE L'UNITÉ

Le directeur de l'unité de recherche est responsable de la bonne mise en œuvre du présent document dans son unité. Il est également responsable de l'application du référentiel d'établissement par les personnes travaillant au sein de son unité. Il est le garant du choix du niveau de classification proposé par le producteur.

[7] Contrat de droit privé ou public, convention, contrat de travail, MoU, etc

[8] Exemples : Responsable fonctionnel de l'application support concernée, responsable métier, responsable hiérarchique, producteur de l'information

[9] Par exemple, le référentiel est publié dans l'Intranet de l'établissement

Il doit mettre en place un processus de classification permettant de valider le choix d'un niveau de classification ou de déroger au référentiel d'établissement. Le processus de dérogation est mis en œuvre après validation par le FSD.

Lorsqu'une information produite ne figure pas dans le référentiel, le processus mis en place prévoit une classification par défaut et d'en informer le FSD de l'établissement afin qu'il détermine le bon niveau final de classification.

4.2.3 ROLE DU PRODUCTEUR DE L'INFORMATION

Le producteur d'une information s'appuie sur le référentiel en place pour proposer le niveau de classification de cette information. Dans le cas où il estime que le niveau indiqué dans le référentiel ne s'applique pas à l'information qu'il vient de produire, il peut y déroger suivant le processus existant dans l'unité.

Si le producteur rencontre une difficulté pour identifier le niveau de classification d'une information, il peut faire appel à sa ligne managériale ou se faire conseiller par son correspondant de sécurité du SI.

Le producteur d'une information est le responsable du suivi de la classification de cette information. Si l'information est produite dans le cadre d'un projet, les producteurs de l'information et le responsable du projet sont co-responsables du suivi de la classification de l'information. Dans la mesure du possible, la durée de classification de l'information doit être indiquée.

Le responsable du suivi de la classification d'une information est en charge de suivre et faire évoluer la classification de cette information tout au long de son cycle de vie en conformité avec le processus de son unité.

Dans le cas où le responsable du suivi de la classification d'une information change de fonction, quitte son service ou l'établissement il appartient à sa hiérarchie de désigner un nouveau responsable pour cette information.

Si le service venait à disparaître, c'est le responsable de l'unité ou de la direction à laquelle il appartenait qui devient le nouveau responsable de l'information.

4.2.4 ROLE DU DESTINATAIRE DE L'INFORMATION

Le destinataire d'une information doit être informé des règles qu'il doit respecter pour garantir la protection de l'information qui lui a été confiée. En particulier, les échanges d'information avec des tiers dans le cadre d'une relation contractuelle ou partenariale doivent faire l'objet de clauses de sécurité pour définir les exigences qu'ils doivent respecter en fonction du niveau de classification des informations reçues ; ces clauses sont garantes d'une protection adéquate des informations par son destinataire.

Le destinataire d'une information peut décider, si le besoin est motivé et justifié, de retransmettre une information reçue, dans le respect des engagements auxquels il est soumis, en appliquant le principe du « besoin d'en connaître » et à condition qu'il respecte les mesures de protection applicables du fait de la classification de cette information et de la mention spécifique éventuellement associée.

Pour une information de niveau DIFFUSION LIMITÉE, destinée à une population nominativement identifiée le destinataire doit informer l'émetteur de l'information en cas de diffusion au-delà du périmètre indiqué par la mention.

Pour une information de niveau CONFIDENTIEL, destinée à une population nominativement identifiée le destinataire doit préalablement obtenir l'accord de l'émetteur de l'information en cas de diffusion au-delà du périmètre indiqué par la mention.

Le fait que l'émetteur d'une information n'ait pas fait mention de son caractère sensible ne signifie pas que le destinataire, qui est soumis à l'obligation de discrétion et qui doit respecter le principe du « besoin d'en connaître », puisse la diffuser largement. Il peut par ailleurs interroger l'émetteur de l'information pour connaître les éventuelles précautions qu'il doit respecter concernant l'information que ce dernier lui a transmise. En particulier, la diffusion publique d'une information doit être le résultat d'une démarche volontaire et maîtrisée.

4.3 PROCESSUS DE CLASSIFICATION

Le processus de classification de l'information s'applique sur toutes les versions d'un document y compris les versions de travail.

4.3.1 DUREE DE CLASSIFICATION

La sensibilité d'un document évolue au cours du temps, très généralement dans le sens de la diminution des besoins en confidentialité. Par exemple une fois brevetée, une invention n'a plus à être confidentielle. Tout document est destiné à terme à être une archive publique ou disparaitre. Lorsque c'est possible, la date ou l'événement à partir duquel[10] le niveau de classification peut être revu doit être indiqué dans le document.

[10] Par exemple, publication d'un article, obtention d'un brevet, etc.

La législation, la réglementation ou les dispositions contractuelles peuvent imposer une durée de classification. Elle s'impose alors à toute autre disposition du présent document.

4.3.2 PROCÉDURE DE DÉCLASSIFICATION

Le niveau de classification d'une information ou la mention de diffusion peuvent être revus à tout moment par le responsable de cette information.

Le marquage initial de la classification doit indiquer explicitement la durée de classification. À l'issue de cette durée, le responsable de l'information doit décider s'il prolonge la durée de classification au même niveau ou s'il modifie le niveau de classification en conformité avec le processus de son unité.

À défaut d'indication de la durée de classification, le niveau de classification est modifié à la baisse tous les 5 ans.

5 GESTION DE L'INFORMATION

5.1 MARQUAGE

Pour faciliter la gestion de l'information, le niveau de classification, la mention spécifique et la durée de classification doivent être apposés ou doivent accompagner sa diffusion :

- Le niveau de classification doit être mentionné dans le nom du fichier, par exemple : NOMFICHIER-DL-MENTION, NOMFICHIER-CO-MENTION
- Pour un document, le marquage doit être apposé en haut de chaque page en caractères gras et en capitales ;
- Pour une information transmise oralement ou visuellement, l'interlocuteur doit être averti le cas échéant du niveau de classification et de la mention spécifique de l'information qui lui est transmise.

Tout au long de sa vie, une information doit changer de niveau de classification, l'émetteur prendra soin d'apposer un marquage en cohérence avec le nouveau niveau de classification.

Il est obligatoire de faire apparaître sur les supports de stockage informatiques amovibles (DVD, clé USB, disque externe, …) le niveau maximum de classification des informations contenues dans ce support et le cas échéant, la mention spécifique correspondante. L'usage de supports de stockage informatiques amovibles différentiés (e.g. clé USB dont le format est prévu pour permettre un tel marquage) peut faciliter la mise en œuvre de cette obligation.

5.2 CREATION/STOCKAGE/SAUVEGARDE

Les informations doivent être créées, stockées et sauvegardées sur des systèmes d'information dont le niveau de sensibilité est cohérent avec le niveau de classification. Des outils de sécurisation spécifiques (e.g. moyen de chiffrement) peuvent être mis à disposition des utilisateurs pour répondre à des besoins en confidentialité qui vont au-delà du niveau de sécurité offert par ces systèmes d'information.

Les informations professionnelles ne doivent pas être traitées (ni créées, ni stockées, ni sauvegardées) sur des moyens informatiques qui sont hors du périmètre de confiance de l'organisme (les moyens personnels, les moyens accessibles au public, les moyens mis à disposition par un tiers hors des clauses de sécurité établies entre l'organisme et ce tiers, voir le § 5.5). En particulier, l'usage à des fins professionnelles d'une messagerie électronique personnelle est interdit.

Tout support de stockage informatique amovible (DVD, clé USB, disque externe, …) ou document papier marqué CONFIDENTIEL ou plus doit être stocké dans une armoire fermant à clé ou dans un local protégé (bureau fermé à clé en l'absence de surveillance, zone à accès contrôlé, …).

En cas de déplacement, les documents marqués CONFIDENTIEL doivent être stockés dans un format chiffré ou sur un support numérique chiffré. En effet, lors des déplacements (transports, hôtels, …), un utilisateur s'expose au risque de vol de son poste de travail ou des supports de stockage qu'il détient.

Par ailleurs, lorsqu'un utilisateur prévoit de se déplacer à l'étranger, il doit :

- Préalablement vérifier que les démarches ont bien été réalisées pour lui permettre d'exporter et d'utiliser les outils mis à sa disposition par l'organisme (notamment les outils de chiffrement),
- Limiter le transport d'informations sensibles, y compris chiffrées, notamment à destination des pays qui imposent aux visiteurs, avant d'entrer sur le territoire ou d'en sortir, de mettre à disposition en clair et à des fins de contrôle le contenu de leur poste de travail ou de leurs supports de stockage informatiques amovibles (DVD, clé USB, disque externe, …).

Le correspondant à la sécurité du système d'information de l'unité, le RSSI ou le FSD de l'organisme est à sa disposition pour l'assister dans ses démarches.

5.3 IMPRESSION/REPRODUCTION

Les moyens d'impression et de reproduction constituent un système d'information particulier du domaine de fonctionnement de l'entreprise et chaque moyen est différent (photocopieurs en réseau, imprimantes individuelles, …).

Les imprimantes utilisées pour l'impression des documents CONFIDENTIELS ou plus doivent être sécurisées conformément aux préconisations de la Politique de Sécurité du SI de l'État[11]. Notamment les règles PDT-MUL-DURCISS, PDT-MUL-AUTH et PDT-MUL-SECNUM.

5.4 ACHEMINEMENT

Il peut être nécessaire de transmettre des informations sous forme physique (document papier, support de stockage informatique amovible, …). Dans ce cas, les règles suivantes doivent être respectées :

- Les informations de niveau DIFFUSION LIMITÉE peuvent être transmises sous simple enveloppe, par le courrier interne de l'organisme ou par voie postale et adressées à une personne physique ;
- Les informations de niveau CONFIDENTIEL doivent être transmises sous simple enveloppe portant la mention « Personnel à l'attention de… » ;
- Les informations de niveau DIFFUSION RESTREINTE doivent être transmises sous double enveloppe (l'enveloppe extérieure ne faisant pas apparaître de mention de confidentialité et l'enveloppe intérieure portant la mention « DIFFUSION RESTREINTE » et les références du document).

[11] Circulaire du Premier ministre du 17 juillet 2014 portant sur la politique des systèmes d'information de l'Etat

5.5 ÉCHANGES NUMERIQUES ET PÉRIMÈTRE DE CONFIANCE

Les échanges numériques regroupent notamment les usages suivants, sans que cette liste soit exhaustive :

- La messagerie électronique
- La messagerie instantanée
- La visioconférence ou l'audioconférence avec utilisation d'un pont de visioconférence
- La visioconférence ou l'audioconférence sur le poste de travail
- Le partage d'écran sur le poste de travail
- Les plateformes de synchronisation de fichiers entre postes de travail
- Les plateformes collaboratives
- Les plateformes d'édition en ligne

Ces applications permettent donc de façon générale l'échange d'information de façon synchrone ou asynchrone entre plusieurs personnes ou équipements.

5.5.1 CONFIANCE DANS L'OPÉRATEUR DE L'INFRASTUCTURE

La confiance dans l'entité qui opère ces services est un facteur important permettant d'évaluer leur adaptation à la transmission d'informations classifiées selon l'échelle de sensibilité, que ce soit au sein de l'organisme ou entre organismes.

Le tableau suivant précise comment évaluer le niveau de confiance à accorder à l'opérateur des infrastructures d'échanges numériques selon 4 niveaux.

Confiance dans l'opérateur de l'infrastructure d'échange		
Niveau	**Éléments d'appréciation**	**Exemples**
1	L'organisme n'a aucune information sur la façon dont est opérée l'infrastructure, sur le niveau réel de confidentialité des échanges, sur la gestion et l'exploitation des métadonnées. Le modèle économique de la plateforme est inconnu. Il y a des doutes raisonnables sur la possibilité qu'un État étranger puisse disposer d'un accès aux informations. La réglementation européenne n'est pas aisément applicable, l'opérateur n'est pas basé sur le territoire national. L'opérateur est soumis à une réglementation nationale qui le contraint à donner accès aux informations, y compris stockées sur le territoire européen.	Les opérateurs des solutions : • de visioconférence sur le poste de travail « gratuites » (Skype, Google Hangout, appear.in, WhatsApp, etc), • de stockage gratuites (Dropbox, Google Drive, Amazon, etc), • de messagerie instantanée gratuites (Skype, Google Hangout), etc
2	L'organisme n'a aucune information sur la façon dont est opérée l'infrastructure, sur le niveau réel de confidentialité des échanges, sur la gestion et l'exploitation des métadonnées. Le modèle économique de la plateforme est inconnu. La plateforme est hébergée sur le territoire national ou européen. Il n'y a pas un actionnaire majoritaire implanté hors du territoire européen. Il n'y a pas de relations contractuelles entre l'organisme et l'opérateur de l'infrastructure.	Les solutions opérées par des sociétés françaises ou européennes et dont l'infrastructure est basée sur le territoire européen.
3	L'organisme a des informations sur la façon dont l'infrastructure est opérée et sur le niveau de confidentialité des échanges ou la gestion et l'exploitation des métadonnées. Aucun État étranger n'a la possibilité de disposer d'un accès aux informations. La réglementation européenne est applicable. Il y a des relations contractuelles entre l'organisme et l'opérateur de l'infrastructure.	Toutes les solutions mises en œuvre et opérées par RENATER ou un organisme partenaire.
4	L'organisme opère l'infrastructure ou la fait opérer pour son compte par un prestataire dont l'infrastructure est basée sur le territoire national. La sous-traitance éventuelle du prestataire répond aux mêmes exigences. L'opérateur bénéficie du label SecNumCloud ou ESCloud.	Toutes les solutions proposées par l'organisme à ses personnels et partenaires (messagerie, plateforme collaborative, plateforme d'échange de fichier, visioconférence, etc)

Tableau 3. Niveaux de confiance dans un opérateur d'infrastructure

5.5.2 CONFIANCE DANS UNE SOLUTION D'ECHANGE NUMERIQUE

La confiance accordée à une solution d'échange numérique ne se résume pas au niveau de confiance qu'on accorde à l'opérateur de cette solution.

Elle dépend d'autres facteurs, tels que :

- L'exposition de la solution à Internet : une solution exposée à Internet subit plus d'attaques et expose les données hébergées de façon plus importante qu'une solution qui n'est accessible qu'en interne.
- L'utilisation du chiffrement de bout en bout :
    - Si le service d'échange numérique propose un chiffrement de bout en bout (possibilité pour plusieurs personnes d'échanger des informations de façon chiffrées sans que les administrateurs du service chez l'opérateur n'aient la possibilité d'accéder aux données) ceci augmente considérablement le niveau de confiance qu'on peut accorder à la solution.
    - S'il est possible d'utiliser une solution de chiffrement tierce permettant d'utiliser le service d'échange numérique comme infrastructure d'échange sans que l'opérateur n'ait le moyen d'accéder aux données en clair.

Les solutions de chiffrement utilisées doivent être validées par le RSSI de l'organisme.

Le tableau suivant indique donc pour une solution d'échange numérique, en fonction du niveau de confiance dans l'opérateur de l'infrastructure, de l'exposition de la solution à Internet et de l'utilisation d'un chiffrement de bout en bout, le niveau de confiance qu'on peut accorder à la solution.

Confiance dans l'opérateur de l'infrastructure	Exposition à l'Internet	Utilisation du chiffrement de bout en bout	Confiance dans le niveau de sécurité de la solution d'échange numérique
1	Oui	Non	Faible
1	Oui	Oui	Moyen
2	Oui	Non	Faible
2	Oui	Oui	Important
3	Non	Non	Moyen
3	Non	Oui	Très important
3	Oui	Non	Moyen
3	Oui	Oui	Très Important
4	Non	Non	Important
4	Non	Oui	Très important
4	Oui	Non	Moyen
4	Oui	Oui	Très important

Tableau 4. Niveaux de confiance d'une solution

La confiance dans le niveau de sécurité d'une solution d'échange numérique peut-être revu à la hausse ou à la baisse par le RSSI de l'organisme en fonction des informations dont il a connaissance[12].

5.5.3 USAGES AUTORISÉS D'UNE SOLUTION D'ÉCHANGE NUMÉRIQUE EN FONCTION DU NIVEAU DE CLASSIFICATION

Le tableau suivant indique pour un niveau de classification d'une information quelles sont les solutions d'échange numérique autorisées en fonction du niveau de confiance accordé à ces solutions.

Si plusieurs solutions d'échanges numériques sont simultanément disponibles et si le choix est possible, alors la solution offrant le niveau de confiance le plus élevé doit systématiquement être choisie. Le choix d'une solution offrant un niveau de confiance minimum ne doit pas être un choix par défaut mais le résultat d'une impossibilité technique, de l'absence de la possibilité de choisir ou d'une solution imposée par un partenaire.

Toute utilisation d'une solution inadéquate vis-à-vis du niveau de classification doit faire l'objet d'un signalement au directeur de l'unité et d'une déclaration d'incident de sécurité.

[12] exemple : informations envoyées par l'ANSSI, la DGSI, le service du HFDS du ministère en charge de la recherche, information sur les règles d'administration d'une solution, etc

Niveau de classification	Niveaux autorisés de confiance dans la solution d'échanges numérique	Chiffrement de bout en bout obligatoire (sauf si le niveau de confiance ne peut être atteint qu'avec le chiffrement voir § 5.5.2)	Mention
PUBLIC	Faible et plus	Non	Non
DIFFUSION LIMITÉE	Moyen et plus	Non	Dans le corps d'un message, 1ère ligne. Marquage d'un document ou d'une présentation en pied de page (chaque page). Mention orale au début d'une audio ou visioconférence. Destinataires ou participants cohérents avec la cible de diffusion.
CONFIDENTIEL	Important et plus	Non	
RESTREINT	Très important	Chiffré avec logiciel qualifié par l'ANSSI.	

Tableau 5. Mention à appliquer

5.6 AFFICHAGE ET CONSULTATION EN LOCAL

On traite ici de l'utilisation de l'information (écran ordinateur, écran projeté, tablette, smartphone, etc.), ou encore dans le cas d'un support papier, de la consultation du document.

Niveau de classification	Environnement public	Environnement Interne ou contrôlé (partenaire)
Public	Aucune recommandation particulière	Aucune recommandation particulière
Diffusion Limitée	L'utilisateur doit s'assurer avant d'afficher le document que son environnement permet l'affichage en toute discrétion	Pas de contraintes ou de restriction pour la consultation
Confidentiel	Utilisation d'un filtre recommandée mais non obligatoire Consultation déconseillée du document papier L'utilisateur doit s'assurer avant d'afficher le document que son environnement permet l'affichage en toute discrétion	L'utilisateur doit s'assurer avant de consulter le document que son environnement permet la consultation en toute discrétion quel que soit le support En cas de projection locale, s'assurer que l'ensemble des participants a besoin d'en connaître
Diffusion restreinte	• Utilisation d'un filtre de confidentialité obligatoire. L'utilisateur doit s'assurer avant d'afficher le document que son environnement permet l'affichage en toute discrétion • Pas de consultation du document papier dans un lieu public	• L'utilisateur doit s'assurer avant de consulter le document que son environnement permet la consultation en toute discrétion quel que soit le support • En cas de projection locale, s'assurer que l'ensemble des participants a besoin d'en connaître

Tableau 6. Affichage en fonction du niveau de classification et de l'environnement

5.7 RÉAFFECTATION INTERNE DE MATÉRIEL

Si le support est chiffré, il doit être reformaté et chiffré de nouveau avant d'être mis à la disposition d'un nouvel utilisateur.

Si le support n'est pas chiffré et qu'il contient des informations classifiées DIFFUSION LIMITÉE ou plus, il doit être effacé avec une procédure d'effacement sécurisée validée par le RSSI de l'établissement avant d'être mis à la disposition d'un nouvel utilisateur.

5.8 FIN DE VIE AU SEIN DE L'ORGANISME

Chiffrement de surface du support	Niveau de classification de certaines informations stockées sur le support	Fin de vie
Oui	Tous niveaux	Effacement sécurisé selon une procédure validée par le RSSI de l'établissement, puis traitement habituel de fin de vie sans autre précautions.
Non	DIFFUSION LIMITÉE	
	CONFIDENTIEL ou plus	Destruction physique selon une procédure validée par le RSSI de l'établissement.

Tableau 7. Traitement à appliquer en fin de vie d'un support

ANNEXE A EXEMPLES TYPES D'INFORMATIONS PAR NIVEAU DE CLASSIFICATION

Le tableau ci-dessous présente des exemples types d'informations pour les niveaux de classification DIFFUSION LIMITÉE et CONFIDENTIEL. L'objectif est d'aider l'émetteur de l'information à déterminer son niveau de classification. Il reste de sa responsabilité de décider de la pertinence et de l'applicabilité de l'exemple à l'information dont il doit définir le niveau de classification.

DIFFUSION LIMITÉE	CONFIDENTIEL
Bilan d'affaire, de projet ou de coopération	Dossier de dépôt de brevet
Retour d'expérience	Code source, code de calcul, outils de simulations hors logiciel libre
Rapport de revue et compte-rendu de comité de direction	Rapport de commission d'enquête suite à crise
Dossier justificatif et données sensibles associées (validation d'un dossier de programme, d'un CCTP, d'une spécification, d'une analyse de risques)	Dossier justificatif et données associées liés à une négociation ou à un choix
Veille stratégique, concurrentielle ou technologique	Rapport d'audit interne ou externe (identification de faiblesses techniques, sécuritaires ou organisationnelles, description des vulnérabilités)
Dossier d'avant-projet et études internes	Documents faisant l'objet d'un accord de confidentialité (NDA[13]) avec un autre établissement
Dossier de coopération (MOU, négociations, budget, calendrier)	
Rapport d'anomalie (technique ou non)	
Données RH « classiques » (dossier de carrière, avis managérial, prime, ...)	

Tableau 8. Exemples de classification de documents

[13] Non Disclosure Agreement

ANNEXE B USAGE DES SOLUTIONS D'ÉCHANGES NUMÉRIQUES – EXEMPLES

Solutions d'échanges numériques	Confiance dans l'opérateur de l'infrastructure	Exposition à l'Internet	Utilisation du chiffrement de bout en bout	Confiance dans le niveau de sécurité de la solution d'échange numérique	Niveau de classification maximum autorisé et format
Google Drive en clair	1	Oui	Non	Faible	Public
Google Drive avec logiciel de chiffrement	1	Oui	Oui	Moyen	Diffusion Limitée
Service FileSender RENATER	3	Oui	Non	Moyen	Diffusion Limitée
Service FileSender RENATER avec du chiffrement	3	Oui	Oui	Très Important	Diffusion Restreinte
Service Framatalk	2	Oui	Non	Faible	Public
Messagerie instantanée (iMessage, WeChat, Slack, Facebook Messenger, etc.)	1	Oui	Non[14]	Faible	Public[15]
Messagerie instantanée « sécurisée » (Telegram, WhatsApp, Signal, etc.)	1	Oui	Oui[16]	Moyen	Diffusion limitée
Skype (version gratuite)	1	Oui	Non	Faible	Public
Trello	1	Oui	Non	Faible	Public

Tableau 9. Exemples de solutions d'échange

[14] Le chiffrement est inexistant, optionnel (trop de risques d'erreur) ou n'est pas de bout en bout.
[15] Est-ce que cela a un vrai sens de parler de public pour des échanges entre deux individus ? On est dans une situation comparable au téléphone.
[16] La cryptographie de Signal, WhatsApp semble plutôt robuste, un peu moins pour Telegram. Par contre il y a un gros problème pour les métadonnées avec parfois un numéro de téléphone utilisé comme identifiant. Les risques sont le suivi du graphe des relations et des usurpations d'identités (il est assez facile de se faire passer pour quelqu'un d'autre). Cf. numéro (90 (mars/avril 2017) de MISC.