MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Organisme	Chapitre	Sommaire	Commentaires	Modification MENJ
Collectivité territoriale	**1. PRÉAMBULE**	1.1. Contexte	Ce cadre de sécurité gagnerait en compréhension à ne rappeler que les règles applicables et leurs origines. On s'attend à un schéma global des responsabilités. Il est souvent fait mention d'une responsabilité conjointe mais sans savoir de quel service il s'agit le document est difficilement applicable. Les services du numérique éducatif sont en effet larges... Il faudrait peut-être simplement rappeler les règles applicables et leurs significations. Quid de la matrice d'hygiène et de sécurité élaborée par les collectivités, n'a-t-elle pas sa place dans ce document ?	Une matrice de de responsabilité RACI vient d'être finalisée et est diffusée aurpès des RSSI, DRANE et DRASI. Le chantier RACI va continuer pour s'articuler avec la doctrine technique. L'équipe prend note de l'existence d'une matrice d'hygiène et de sécurité élaborée par les collectivitéset va étudier la pertinence de la rapprocher de la doctrine technique.
Collectivité territoriale	**1. PRÉAMBULE**	1.1. Contexte	L'exclusion du périmètre de sécurité des éléments choisis par le CE n'est plus conforme à la stratégie nationale de souveraineté et de sécurité cyber (cf. « à l'exception des services numériques contractualisés directement par le chef d'établissement ») ; La Région Grand Est demande de l'intégrer dans le cadre réglementaire législatif –cf. la situation actuelle d'usurpation d'identité (alertes à la bombe et diffusion de vidéo de décapitation) où les chefs d'établissement ne ferment pas la messagerie Pronote contrairement à la consigne du MENJ Personne ne contrôle et/ou certifie le bon usage de l'AAF par les éditeurs d'ENT, qui se déclarent comme tel sans contraintes particulières (le SDET est imposé aux éditeurs d'ENT uniquement dans la doctrine technique via « les contrats de commande publique liant les exploitants à leurs donneurs d'ordre) – A contrario, la responsabilité incomberait aux collectivités alors qu'elles n'ont pas accès à l'AAF elles-mêmes ! ;La Région Grand Est demande d'intégrer dans le cadre réglementaire législatif une certification des éditeurs d'ENT + l'accès à l'AAF pour les collectivités territoriales(au même titre que des sociétés privées éditeurs d'ENT et en tant que partenaire public lié à la communauté éducative)	Le commentaire est pris en compte pour la mise en place d'ateliers de travail. Les modifications qui s'en suivont seront prises en compte dans une version ultérieure du document
Collectivité territoriale	**1. PRÉAMBULE**	1.2. Objectifs du document	il faudrait expliciter EIDAS	Une note d'explication est ajoutée dans le document.

Ministère	**1. PRÉAMBULE**	1.2. Objectifs du document	Page 4 : " La sécurité numérique a pour objectif …..des personnes" => inutile de réinventer une définition déjà donnée dans l'IGI 1337. Celle- ci est : "Sécurité numérique : ensemble d'activités organisationnelles, techniques ou juridiques visant à protéger et défendre les systèmes d'information et de communication, ainsi que les informations qu'ils manipulent, contre d'éventuels incidents de sécurité de nature accidentelle ou intentionnelle, et à assurer la résilience numérique des entités concernées." Page 4: "les responsabilités des différents acteurs, qui partagent juridiquement et techniquement les compétences liées à la sécurité, sont à conjuguer avec subsidiarité." => La notion de subsidiarité sous entends l'existence d'un lien d'autorité hiérarchique ou fonctionnel. Ceci n'est pas forcément le cas dans le cadre des acteurs concernés par cette pile documentaire. La notion de partage de responsabilité doit être porté par une notion d'identification claire des responsabilités et des moyens de gouvernances au vu des objectifs. Ceci à travers plusieurs type de relation à installer suivant les périmètres : - soit client / fournisseurs - soit projet d'interet commun. Page 4 : Ne pas laisser penser que la conformité règlementaire est optionnelle. Page 5 : " ... les aspects d'exploitations des différents systèmes d'information, relèvent de la responsabilité des collectivités territoriales" =< Ajouter à la suite : " CT qui expriment clairement les engagements de sécurité qu'elles maintiennent ainsi que leur limitation pour les services numériques qu'elles proposent aux acteurs de l'éducation" Page 5 :	Le point est pris et le contenu est remplacé par la définition donnée dans l'IGI 1337 (instruction générale interministerielle). Le point est noté et sera étudié dans la prochaine version du cadre général de sécurité. Une formulation plus précise est intégrée.
Académie	**1. PRÉAMBULE**	1.2. Objectifs du document	Quels objectifs pour le premier degré ? Sécurité informatique des écoles	
Collectivité territoriale	**2. LES RÈGLES DE SÉCURITÉ DU NUMÉRIQUE POUR L'ÉDUCATION COMPOSANT LA DOCTRINE TECHNIQUE**	2.1. Relativement aux homologations	Question : Donc le ministère est autorité d'homogation pour l'ensemble du SI de l'EN, quelle que soit la compétence ? YC sur les systèmes des éditeurs d'ENT par exemple ? Ministère au niveau concentré / déconcentré … ? Que se passe-t-il lorsque le service n'est pas homologué ? Quid des services achetés directement par les EPLE ?	Le ministère n'est pas autorité d'homologation pour l'ensemble du SI de l'EN mais il existe plusieurs AQSSI qui peuvent déléguer le rôle d'autorité d'homologation au sein du ministère et des collectivités. Pour les collectivités, le RGS impose de réaliser des homologations, il doit donc y avoir une autorité d'homologation au sein des collectivités. Le chef d'établissement est autorité d'homologation et il en répond au SSI académique.
Académie	**2. LES RÈGLES DE SÉCURITÉ DU NUMÉRIQUE POUR L'ÉDUCATION COMPOSANT LA DOCTRINE TECHNIQUE**	2.3. Relativement aux clauses de sécurité dans les marchés	p.6 formulation : "règles réglementaires"	Modification du paragraphe
Collectivité territoriale	**2. LES RÈGLES DE SÉCURITÉ DU NUMÉRIQUE POUR L'ÉDUCATION COMPOSANT LA DOCTRINE TECHNIQUE**	2.4. Relativement à la gestion d'incidents de sécurité numérique	Question : l'important n'est-il pas de conserver une chaîne d'alerte fiable et pérenne : qui est le contact pour les RSSI des collectivités (asso des RSSI) ? Y-a-t-il un référentiel de chaîne d'alerte commune à toutes les entités à respecter (comme par ex l'alerte des services de secours) ? Mais pe est-ce dans les textes référencés dans la partie 3 ?	Il existe une note complète sur les responsabilités et la chaine d'alerte qui a été diffusée à l'ensemble des acteurs concernés, académies, collectivités, filière industrielle. Elle sera diffusée à nouveau.
Académie	**2. LES RÈGLES DE SÉCURITÉ DU NUMÉRIQUE POUR L'ÉDUCATION COMPOSANT LA DOCTRINE TECHNIQUE**	2.4. Relativement à la gestion d'incidents de sécurité numérique	Il pourrait être pertinent d'expliciter la notion de chaine d'alerte, voire de proposer un scénario sur la base des derniers evenements	Les travaux sont en cours pour produire le film annuel sur les environnements numériques de travail. Dès finalisation, les éléments seront diffusés.
Académie	**2. LES RÈGLES DE SÉCURITÉ DU NUMÉRIQUE POUR L'ÉDUCATION COMPOSANT LA DOCTRINE TECHNIQUE**	2.4. Relativement à la gestion d'incidents de sécurité numérique	Quelle chaine d'alerte dans le premier degré ? Pas mentionné	Commentaire pris en compte pour la prochaine version

	Filière privée	**2. LES RÈGLES DE SÉCURITÉ DU NUMÉRIQUE POUR L'ÉDUCATION COMPOSANT LA DOCTRINE TECHNIQUE**	2.4. Relativement à la gestion d'incidents de sécurité numérique	Apple publie en temps réel l'état de ses systèmes d'information (en service / hors service / en cours de résolution) : https://www.apple.com/fr/support/systemstatus/	Ce commentaire n'appelle pas de réponse.
	Ministère	**3. MISE EN APPLICATION : LES TEXTES DE RÉFÉRENCE**	3. Mise en application : les textes de référence	La partie "Textes relatifs à la protection des données personnelles" apparait en double : une fois page 9 et une fois à la fin de la page 10.	Suppression d'un des deux paragaphes