AVENANT N°1

A LA CONVENTION DE PARTENARIAT ENTRE LES AUTORITES ACADEMIQUES DU GRAND EST ET LES COLLECTIVITES ADHERENTES AU GROUPEMENT DE COMMANDES POUR UNE SOLUTION D'ESPACE NUMERIQUE DE TRAVAIL DANS LES ETABLISSEMENTS SCOLAIRES DU GRAND EST

ENTRE

- L'Etat, représenté par Monsieur Pierre-François Mourier, recteur de région académique recteur de l'académie de Nancy-Metz, Monsieur Vincent Stanek, recteur de l'académie de Reims, Monsieur Olivier Klein, recteur de l'académie de Strasbourg, et Monsieur Pierre Bessin directeur régional de l'alimentation de l'agriculture et de la forêt ;
- La Région Grand Est, représentée par Monsieur Franck Leroy, Président du Conseil Régional du Grand Est ;
- Le Département des Ardennes, représenté par Monsieur Noël Bourgeois, Président du Conseil Départemental des Ardennes ;
- Le Département de l'Aube, représenté par Monsieur Philippe Pichery, Président du Conseil Départemental de l'Aube ;
- Le Département de la Marne, représenté par Monsieur Jean-Marc Roze, Président du Conseil Départemental de la Marne ;
- Le Département de la Haute Marne, représenté par Monsieur Nicolas Lacroix, Président du Conseil Départemental de la Haute-Marne ;
- Le Département de la Meurthe et Moselle, représenté par Madame Chaynesse Khirouni, Présidente du Conseil Départemental de la Meurthe et Moselle ;
- Le Département de la Meuse, représenté par Monsieur Jérôme Dumont, Président du Conseil Départemental de la Meuse ;
- Le Département de la Moselle, représenté par Monsieur Patrick Weiten, Président du Conseil Départemental de la Moselle ;
- La Collectivité européenne d'Alsace, représentée par Monsieur Frédéric Bierry, Président de la Collectivité européenne d'Alsace ;
- Le Département des Vosges, représenté par Monsieur François Vannson, Président du Conseil Départemental des Vosges.

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement général sur la protection des données personnelles », et notamment le Chapitre IV. Responsable du traitement, Responsables conjoints du traitement et sous-traitant ;

Vu le Code de l'Education, article L 214-6, établissant la compétence de la Région à l'égard des lycées, y compris pour les matériels informatiques et les logiciels prévus pour leur mise en service, nécessaires à l'enseignement et aux échanges entre les membres de la communauté éducative ;

Vu le Code de l'Education, article L213-2, établissant la compétence des Départements à l'égard des collèges, y compris pour les matériels informatiques et les logiciels prévus pour leur mise en service, nécessaires à l'enseignement et aux échanges entre les membres de la communauté éducative ;

Vu le Code de l'Education, article L211-1, établissant la compétence de l'état à l'égard du contrôle et l'évaluation des politiques éducatives, en vue d'assurer la cohérence d'ensemble du système éducatif ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Régional Grand Est en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental des Ardennes en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental de l'Aube en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental de la Marne en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la commission permanente du Conseil Départemental de la Haute Marne en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental de la Meurthe et Moselle en date du XXX

approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental de la Meuse en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental de la Moselle en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente de la Collectivité européenne d'Alsace en date du 17 novembre 2025 approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est ;

Vu la délibération n°XXX de la Commission Permanente du Conseil Départemental des Vosges en date du XXX approuvant l'avenant n°1 à la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est.

Vu la convention de partenariat pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est conclue en date du 21 août 2019

Il EST CONVENU CE QUI SUIT :

ARTICLE 1 : OBJET DE L'AVENANT

Le présent avenant a pour objet d'ajouter à l'espace numérique de travail (ci-après l'ENT) des mécanismes pour la sécurité et la sûreté de la communauté éducative et de modifier les informations sur les traitements de données personnelles et les processus permettant la communication des collectivités via l'ENT en application de la convention de partenariat entre les Autorités académiques du Grand Est et les collectivités adhérentes au groupement de commandes pour une solution d'espace numérique de travail dans les établissements scolaires du Grand Est signée le ...

Il intègre par ailleurs l'évolution administrative du périmètre du groupement de commandes avec la création de la Collectivité européenne d'Alsace au 1er janvier 2021 issue de la fusion des départements du Haut Rhin et du Bas Rhin.

ARTICLE 2 : MODIFICATION DE L'ARTICLE 7 « PROTECTION DES DONNEES PERSONNELLES » DE LA CONVENTION

L'article 7 de la convention est modifié et rédigé comme suit :

Article 7 – Protection des données personnelles

Les parties à la présente convention s'engagent à respecter le règlement général sur la protection des données (RGPD) de l'UE du 27 avril 2016 ainsi que la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, plus particulièrement lorsque la transmission d'informations à caractère personnel est nécessaire pour la mise en œuvre de l'ENT.

7.1. Objet de l'article

L'article 7 a pour objet de sécuriser juridiquement les conditions de traitement de ces données à caractère personnel en clarifiant notamment les obligations et responsabilités respectives de chacune des parties.

D'emblée, il est acté de la qualification de responsable de traitement conjoint ou de sous-traitant de chacune des parties tel que précisé dans l'article 7.2.

Aussi, et conformément aux exigences légales issues des textes susvisés et notamment des articles 26 et 28 du RGPD, la présente convention détaillera successivement le champ de l'activité de traitement sur lequel elle porte, le statut, les obligations et les responsabilités de chacune des parties, le point de contact qu'elles ont entendu désigner ainsi que les droits et les conditions d'information des personnes concernées.

7.2. Activité de traitement relevant de la responsabilité conjointe ou de la sous-traitance

L'activité de traitement relevant de la responsabilité conjointe ou de la sous-traitance des parties porte sur le déploiement d'un ENT à destination des élèves scolarisés dans les établissements désignés dans la présente convention de partenariat, ainsi que des personnels de ces établissements.

- *Les traitements liés au portail ENT, tel que l'administration de la plateforme, sont mis en œuvre en responsabilité conjointe entre les Autorités académiques, l'établissement et la collectivité compétente ;*
- *Les traitements liés aux outils de communication externe et interne sont mis en œuvre par les responsables de traitement pour leurs propres comptes ;*
- *Les traitements liés aux services numériques pédagogiques, de vie scolaire ou d'organisation scolaire de l'établissement, sont mis en œuvre sous la responsabilité de l'établissement et sous-traités par la Région Grand Est en tant que chef de file du groupement de commandes ENT.*

Ces traitements sont nécessaires à l'exécution d'une mission d'intérêt public ou relèvent de l'autorité publique dont sont investis les responsables du traitement conformément au e) du 1 de l'article 6 du RGPD à l'exception des traitements de communication externe qui relèvent de l'intérêt légitime du responsable du traitement à communiquer à l'attention des Internautes conformément au f) du 1 de l'article 6 du RGPD.

La liste complète des traitements mis en œuvre dans le cadre de l'ENT est disponible dans les registres des activités de traitement des parties prenantes.

7.3. Rôle des parties

De façon générale, les parties s'engagent à prendre en considération la protection des données à caractère personnel dans toutes les orientations stratégiques de mise en œuvre de l'ENT, issues des différentes instances de pilotage du projet (dont la composition et les prérogatives sont fixées dans la convention de partenariat).

Ce faisant, les parties sont conjointement garantes de la licéité, la légitimité et la transparence des finalités des activités de traitements associées à la mise en œuvre de l'ENT.

S'agissant des moyens du traitement, chacune des parties détermine pour les modules qui lui sont propres les catégories de données pertinentes, les destinataires de ces données et les durées de conservation à respecter.

Les conditions de garantie des principes d'exactitude et de sécurité procèdent toutefois de décisions concertées entre les parties. En tout état de cause, à cet effet, les parties s'engagent à respecter les préconisations figurant dans le schéma directeur des espaces numériques de travail (ci-après le SDET) en vigueur et à les faire respecter par la société en charge du développement et de la maintenance de la solution ENT.

Au-delà de la détermination de ces finalités et moyens, les parties prennent respectivement les engagements définis à l'article suivant.

7.4. Obligations des parties

7.4.1 – Obligations du groupement de commandes :

- *Assurer le pilotage du projet, notamment sous ses aspects contractuels ;*
- *Vérifier que l'éditeur de la solution ENT retenue présente toutes les garanties requises à la sécurité des données à caractère personnel de ses utilisateurs ;*
- *Formaliser, au nom de tous les responsables conjoints du traitement, avec l'éditeur désigné de la solution, un marché public incluant les exigences de l'article 28 du RGPD ;*
- *Transmettre aux autres parties à la présente convention la documentation de conformité aux règles de sécurité élémentaires de l'éditeur retenu ;*
- *Signaler à la CNIL et le cas échéant notifier aux personnes concernées, toutes les violations de données rencontrées afférentes à cette activité de traitement lorsque la violation concerne l'ensemble de l'ENT ;*
- *Alerter les autres parties des incidents éventuels liés à l'ENT, qui lui seraient notifiés, dans les plus brefs délais et au plus tard dans un délai maximal de 48h ;*
- *Apporter son assistance, dans la mesure du possible, aux autres parties, dans le respect de leurs propres obligations « Informatique et Libertés » ;*
- *Transmettre aux autres parties le nom et les coordonnées de son délégué à la protection des données ;*
- *Inscrire au sein de son registre des activités de traitement, l'activité de traitement objet de la présente convention ;*
- *Le groupement de commandes s'assure de la sécurité des traitements opérés par les sous-traitants ultérieurs. Les traitements de la présente convention ont fait l'objet d'une homologation de sécurité conforme au Référentiel Général de Sécurité (RGS) ;*
- *En tant que sous-traitant, le groupement de commandes s'assure que ses sous-traitants ultérieurs ne recrutent pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale des responsables du traitement des autres parties prenantes ;*
- *En tant que sous-traitant, le groupement de commandes ne traite les données à caractère personnel que sur instruction documentée des responsables du traitement des autres parties prenantes, y compris en ce qui concerne les transferts de données vers un pays tiers ou une organisation internationale ;*
- *Le groupement de commandes veille à ce que le délégué à la protection des données de la Région Grand Est soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.*

7.4.2 – Obligations des Autorités académiques :

- *Fournir au prestataire de la solution d'ENT les données extraites de l'annuaire fédérateur (AAF) pour alimenter l'annuaire de l'ENT conformément au SDET en vigueur ;*
- *Mettre à jour l'annuaire fédérateur chaque début d'année scolaire ainsi que lors de la suppression ou modification de comptes utilisateurs qui lui seront notifiées ;*
- *Effectuer tout transfert de données personnelles relatif à l'annuaire fédérateur de manière sécurisée ;*
- *Contribuer à la sécurité des données traitées via la formation des personnels de l'éducation nationale à l'utilisation de la solution ENT, via la mise à disposition d'une assistance téléphonique à leur destination et plus généralement via un appui aux établissements à la conduite du changement ;*
- *Signaler à la CNIL et le cas échéant notifier aux personnes concernées, toutes les violations de données rencontrées afférentes à cette activité de traitement lorsque la violation concerne plusieurs établissements ;*
- *Alerter les autres parties des incidents éventuels liés à l'ENT, qui lui seraient notifiés, dans les plus brefs délais et des suites leur ayant été données ;*
- *Apporter son assistance, dans la mesure du possible, aux autres parties, dans le respect de ses obligations issues de la présente convention ;*
- *Transmettre aux autres parties le nom et les coordonnées de son délégué à la protection des données ;*
- *Inscrire au sein de son registre des activités de traitement, l'activité de traitement objet de la présente convention ;*
- *L'autorité académique veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.*

7.4.3 – Obligations de chaque établissement :

- *Organiser le déploiement de l'ENT de son établissement : assurer la gestion de l'annuaire et des droits des utilisateurs de l'ENT ;*
- *Choisir (et justifier de la régularité de la finalité associée) les services proposés par l'ENT ;*
- *Sensibiliser les utilisateurs des ENT aux mesures élémentaires de sécurité telles que la non-divulgation de leurs identifiants de connexion à leur compte ENT ;*
- *Mettre en place l'assistance de 1er niveau des utilisateurs avec le concours des services d'appui de l'Académie ;*
- *Alerter les autres parties des incidents éventuels liés à l'ENT, qui lui seraient notifiés, dans les plus brefs délais ;*
- *Signaler à la CNIL et notifier, le cas échéant, aux personnes concernées toutes les violations de données rencontrées afférentes à cette activité de traitement, lorsque la violation ne touche que les élèves et personnels de ce seul établissement ;*
- *Apporter son assistance, dans la mesure du possible, aux autres parties, dans le respect de leurs propres obligations « Informatique et Libertés » ;*
- *Transmettre aux autres parties le nom et les coordonnées de son délégué à la protection des données ;*
- *Inscrire au sein de son registre des activités de traitement, l'activité de traitement objet de la présente convention ;*
- *L'établissement veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.*

L'établissement doit veiller à la conformité des services tiers qu'il intègre dans l'ENT et qui ne relèvent pas de cette convention. Ces services et leurs éventuels connecteurs doivent faire l'objet d'une inscription au registre et d'une information spécifique.

7.5. Analyse d'impact sur la protection des données

Les parties s'engagent à mener une Analyse d'Impact sur la Protection des Données (AIPD) pour le traitement des données personnelles dans le cadre de l'Environnement Numérique de Travail (ENT).

Les parties déclarent qu'une AIPD a été réalisée conformément aux exigences du Règlement Général sur la Protection des Données (RGPD). Cette AIPD a évalué les risques pour les droits et libertés des personnes concernées et a déterminé les mesures nécessaires pour atténuer ces risques. Les Parties s'engagent à mettre en œuvre les actions correctives identifiées dans l'AIPD.

Les parties s'engagent à documenter l'AIPD et à la mettre à jour régulièrement, notamment en cas de mise en œuvre d'une nouvelle finalité, d'une modification substantielle d'un traitement ou de l'apparition d'un nouveau risque. Les parties s'engagent également à maintenir à jour le plan d'action mis en œuvre.

7.6. Obligations spécifiques des parties quant aux conditions d'information et de respect des droits des personnes concernées

Information des personnes concernées : Les personnes concernées par les opérations de traitement recevront les informations requises, au moment de la collecte de données lorsque des données à caractère personnel sont collectées auprès d'elles ou, dans les délais requis lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, conformément aux articles 12 à 14 du RGPD.

Plus précisément, les parties conviennent que ces informations seront fournies selon les modalités suivantes :

Rôle de l'autorité académique : elle propose les mentions d'information ainsi que toutes les modifications ultérieures de celles-ci.

Rôle de la collectivité : La collectivité veille auprès de l'éditeur de l'ENT, à ce que les mentions d'information obligatoires et validées par l'académie soient bien apposées en pied de page des écrans d'accueil et de connexion pour être visibles même si l'utilisateur n'est pas encore connecté. Elle rédige les mentions d'information pour les éventuels modules la concernant.

Rôle de l'établissement : L'établissement valide et diffuse les mentions d'information ainsi qu'une information sur ladite activité de traitement au moment de la diffusion aux personnes concernées de leurs identifiants leur permettant d'accéder à l'ENT.

Exercice des droits des personnes concernées : Les personnes dont les données à caractère personnel sont traitées peuvent exercer l'ensemble des droits que le RGPD leur confère (droits d'accès, de rectification, d'opposition, de limitation, ainsi que le droit de formuler des directives post mortem), à l'égard de et contre chacun des responsables de traitement.

Les parties conviennent de traiter les demandes de droits selon la répartition suivante :

- *La collectivité traite toute demande portant sur un module lui étant propre ;*
- *Le chef d'établissement traite toute demande émanant d'un élève ou d'un membre du personnel de son établissement ;*
- *L'autorité académique traite toute demande portant sur un module lui étant propre ou excédant le champ d'application du seul établissement.*

Toute partie qui serait destinataire d'une demande de droit ne relevant pas de sa compétence la réoriente au plus tard 8 jours après sa réception accompagnée de toutes les informations utiles à son traitement.

En tout état de cause, les parties s'engagent à respecter l'effectivité des droits des personnes concernées et à effectuer à cet effet toutes les diligences requises, y compris, en tant que de besoin, de façon concertée.

Mise à disposition des grandes lignes de cet accord de responsabilité de traitement conjointe : Les grandes lignes de cet accord seront mises à disposition des personnes concernées, a minima, sur le site web de l'établissement depuis la page contenant les mentions relatives à la protection des données de l'ENT.

Les parties conviennent de la possibilité de prévoir une modalité de diffusion complémentaire de ces grandes lignes, sous réserve d'en informer les autres parties.

7.7. Point de contact privilégié

Le délégué à la protection des données de l'établissement est désigné comme le point de contact pour les personnes dont les données font l'objet de l'activité de traitement précitée.

L'établissement est, à ce titre, l'interlocuteur privilégié des personnes dont les données font l'objet de l'activité de traitement précitée.

7.8. Organisation des délégués à la protection des données

Les délégués à la protection des données (ci- après DPD) de chacune des parties s'engagent à faciliter le travail de leurs homologues, notamment en relayant les demandes d'exercice de droit sur les données personnelles qui leur aurait été adressées par erreur dans un délai raisonnable pour en permettre le traitement. Ils s'engagent également à collaborer sur les éventuelles violations de données.

Lorsqu'une notification de violation de données est nécessaire, c'est le périmètre des personnes physiques concernées qui détermine le responsable de traitement qui notifie la violation à l'autorité de contrôle nationale avec l'aide des DPD concernés. A titre d'exemple, une faille qui concernerait l'ensemble des utilisateurs serait notifiée par la Région, une faille qui concernerait l'ensemble des utilisateurs d'une académie serait notifiée par son autorité académique, une faille qui concernerait l'ensemble des utilisateurs d'un département serait notifiée par la collectivité concernée et une faille qui concernerait seulement un ou quelques établissements serait notifiée par le ou chefs d'établissement concerné(s).

7.9. Groupe de travail Conformité ENT

Les délégués à la protection des données des Autorités académiques et de la Région Grand Est, cheffe de file du groupement de commandes ENT, se constituent en groupe de travail afin d'examiner les suites qu'il convient de donner à tout événement (demande d'exercice de droit, actualité ou incident) concernant l'ENT que le groupe considéra comme utile.

Les délégués à la protection des données du groupe de travail Conformité ENT collaborent dans la rédaction des différents documents de conformité nécessaires à l'ENT incluant notamment les fiches de traitement liées à la présente convention, l'analyse d'impact sur la protection des données ou les documents d'information à l'attention des personnes concernées.

Le groupe de travail Conformité ENT peut inviter tout délégué à la protection des données d'une autre partie aux travaux menés dans le cadre de cette convention.

ARTICLE 3 : MODIFICATION DE L'ARTICLE 9 « COMMUNICATION » DE LA CONVENTION

L'article 9 de la convention est modifié et rédigé comme suit :

Article 9 – Communication

La communication via l'ENT est multicanale et peut être mise en œuvre par différents acteurs : les établissements scolaires, les Autorités académiques et les collectivités. Les contenus et modalités d'activation de cette communication varient en fonction des acteurs concernés.

Les chefs d'établissements et les Autorités académiques peuvent réaliser ces communications directement sur l'ENT sans formalité particulières.

Les collectivités territoriales pourront utiliser l'ENT dans le cadre d'une charte de bon usage, jointe en annexe de la présente convention (mise à jour avec l'avenant n°1 à la convention de partenariat, afin de prendre en compte la création de la Collectivité européenne

d'Alsace, préciser les moyens et les modalités de communication dans Mon Bureau Numérique, ainsi que les dispositions relatives au droit de regard et d'opposition du chef d'établissement) construite avec les Autorités académiques, et dans le respect des textes réglementaires dont :

- *Le code de l'éducation, notamment ses articles L213-2 et L214-6 relatifs aux compétences des collectivités ainsi que l'article D111-5 relatif à l'accès des parents à l'ENT ;*
- *Le schéma directeur des espaces numériques de travail (SDET) dans sa version actualisée.*

L'information transmise par les collectivités concernera exclusivement des actualités pratiques et utiles pour le public ciblé, touchant à la vie de l'élève au sens large.

9.1. Canaux de communication sur l'ENT

La communication sur l'ENT mobilise différents canaux :

- *Communication ciblée permettant de pousser un contenu sur la page d'accueil de l'ENT de l'utilisateur visé ;*
- *Messagerie ;*
- *SMS.*

Le choix du canal se réalise lors de la conception de la communication.

Le SMS induit un cout spécifique à l'usage.

9.2. Les niveaux d'urgence

Les niveaux d'urgence de la communication ENT sont : classique, urgent ou de crise.

9.2.1 – Urgent :

Une urgence est un évènement, une tâche ou encore un dossier nécessitant une réaction rapide, voire immédiate. Elle doit être traitée généralement dans les délais les plus brefs. Si elle ne l'est pas, elle peut entraîner des conséquences nuisibles pour les usagers, le projet global ou encore pour les organisations parties prenantes au projet.

Dans le contexte ENT, une communication d'urgence peut par exemple concerner le transport scolaire qui peut être impacté par des intempéries (inondations ; neige…) ou autres (grèves...) impactant la mise en œuvre du service et nécessitant une information rapide des usagers pour qu'ils puissent prendre des dispositions alternatives.

9.2.2 – De crise :

Le terme "crise" désigne une période, un phénomène critique où il est nécessaire de faire un choix pour faire face à un changement majeur. Une crise est alors une situation de forte tension, inattendue et qui est une menace pour le fonctionnement "normal" de l'établissement et/ou de son écosystème applicatif. Elle peut intervenir dans n'importe quel cadre.

La communication en situation de crise mobilisera exclusivement la messagerie ENT pour assurer la communication aux différents membres de la communauté éducative sauf si cette crise est liée à une compromission de la messagerie de l'ENT ou des éléments d'authentification qui y sont associés.

La communication de crise pourra être réalisée par l'ensemble des autorités intervenant sur le projet : les chefs d'établissement, les Autorités académiques, et les collectivités.

9.3. Le processus de validation d'une communication portée par une collectivité territoriale

9.3.1 – En situation classique :

Pour une communication ciblée ou un mail :

Les collectivités proposeront une communication aux Autorités académiques concernées (cf. 9.4) en précisant les éléments suivants :

- *La cible visée – en termes de public cible (parent : élèves – enseignants – personnel de direction…) ;*
- *La période de diffusion : date de début et date de fin de diffusion (avec une date de début prévue à minimum 8 jours après la date de demande) – la périodicité de diffusion classique varie entre 15 jours et 30 jours ;*
- *Le titre de l'article ;*
- *Une description courte de l'article ;*
- *Une description longue de l'article ;*
- *Les pièces jointes éventuelles associées à la communication ;*
- *Le lien vers les sondages ou questionnaires éventuellement associés à la communication ;*
- *L'objectif général de cette communication.*

Pour une communication par SMS, il convient de préciser :

- *L'objectif de cette communication ;*
- *La cible du SMS ;*
- *La date d'envoi du SMS ;*
- *Le texte du SMS.*

Le processus de validation se réalisera en deux temps :

- ***Temps 1 :** validation / adaptation ou rejet de la communication par les Autorités académiques :*

Les Autorités académiques disposeront d'un délai de cinq jours ouvrés pour valider, proposer des adaptations ou rejeter la proposition de communication.

Les propositions d'adaptations devront être formalisées et justifiées formellement dans les formulaires ad hoc.

Les rejets devront être justifiés formellement dans les formulaires ad hoc.

Sans réponse des Autorités académiques dans le délai de cinq jours ouvrés prévu, les communications seront réputées approuvées et seront soumises aux chefs d'établissement (temps 2).

- ***Temps 2 :** Acceptation ou rejet de l'intégration de la communication sur le portail ENT des établissements :*

Dans le cadre de l'autonomie des établissements traduite sur l'ENT par la fonction de directeur de publication exercée par le chef d'établissement sur le portail ENT de son établissement, le chef d'établissement peut accepter ou rejeter les communications proposées par des tiers (collectivités territoriales ou Autorités académiques).

Les chefs d'établissements disposeront d'un délai de deux jours ouvrés pour valider ou rejeter l'intégration de la communication sur leur portail.

Les rejets devront être motivés explicitement.

Par défaut la communication sera réputée approuvée et sera intégrée sur le portail des établissements.

9.3.2 – En situation d'urgence :

La communication se réalise directement sans processus de validation par les Autorités académiques.

Sur l'application, ces communications seront marquées comme « urgente » et devront être associées d'un texte de justification formelle par la collectivité dans le formulaire de saisie de la communication sur l'ENT. La communication sera alors déployée directement sur les portails ENT visés quel que soit le canal choisi.

Les communications relevant de l'urgence seront analysées à postériori par les instances du projets (COSUI / CST) pour vérifier le respect du cadre. La Région Grand Est, en tant que pilote du groupement de commandes, compilera l'ensemble des communications portées par les collectivités.

9.3.3 – En situation de crise :

Dans ce cadre :

- *Les communications portées par le projet feront l'objet d'un processus simplifié se limitant à une validation unique : adaptation du message par les Autorités académiques dans un délai réduit à 48h ouvrées. Cette situation de crise sera justifiée explicitement par la collectivité dans le formulaire de saisie de la communication sur l'ENT ;*
- *Les communications portées par les Autorités académiques devront faire l'objet d'une validation par la Région Grand est en tant que pilote du projet MBN.*

9.4. Autorité en charge de la validation d'une communication portée par une collectivité :

Les communications proposées par les collectivités seront validées par des autorités distinctes pour en fonction des thématiques concernées :

Pour l'Education Nationale :

- Le Directeur de Région Académique à l'Information et à l'Orientation (DRAIO) *validera les communications relatives à l'information sur l'orientation, les métiers et l'offre de formation ;*
- Le Directeur des Systèmes d'Information Grand Est (DSIGE) *validera l'ensemble des communications relatives à la sécurité informatique ;*
- Le Directeur des Services Départementaux de l'Education Nationale (DSDEN) *du territoire concerné validera les communications à destination des collèges (à l'exclusion des thématiques précédentes) ;*
- Le Délégué Régionale Au Numérique Educatif (DRANE) *validera l'ensemble des communications relatives au numérique éducatif pour les lycées (à l'exclusion des thématiques précédentes) ;*
- Le Secrétaire Général de Région Académique (SGRA) *validera les communications transversales (à l'exclusion des thématiques précédentes).*

Pour l'agriculture :

- Le Délégué Régional aux Technologies de l'Information et de la Communication (DRTIC) *validera l'ensemble des communications qui lui seront soumises quel que soit le périmètre visé.*

9.5. Interopérabilité des données :

Les actualités présentes sur les portails ENT pourront alimenter les portails des collectivités.

Les actualités présentes sur les portails des collectivités pourront alimenter l'ENT en respectant les processus de validation requis (cf. article 9.3).

ARTICLE 4 : AJOUT DE L'ARTICLE 11 « SECURITE »

L'article 11 « Sécurité » est ajouté et rédigé comme suit :

Article 11 – Sécurité

L'ENT Mon Bureau Numérique, étant un des sites publics de référence en France et faisant l'objet d'une consultation massive, est la cible permanente d'attaques informatiques.

La question de la sécurité est donc positionnée au cœur de l'écosystème ENT et se traduit par la réalisation d'une homologation RGS réactualisée régulièrement.

Dans le cadre de cette homologation de sécurité, l'ENT a été approuvé dans le cadre de son périmètre applicatif mais aussi au niveau de ses articulations / relations avec d'autres produits et applicatifs articulés techniquement avec lui.

11.1. Articulations de l'ENT avec les autres produits et solutions mobilisées par les usagers :

Ce mode de fonctionnement s'inscrit dans le cadre de la doctrine technique mise en œuvre par la Ministère de l'Education Nationale et en décline les grands principes : APIsation, plateformisation et création de communs numériques.

Les applications rendues accessibles directement depuis l'ENT en permettant un maintien de l'authentification initiale par la mobilisation d'un mécanisme SSO (« single sign-on ») font l'objet d'une demande spécifique de la part du demandeur (Etablissement / Autorité Académique ou Collectivité) décrivant les objectifs pédagogiques ou de gestion de l'application, son positionnement en termes de sécurité (hébergement…) et de protection des données.

Ces demandes feront l'objet d'une instruction au sein d'une instance dédiée (Le Comité de Suivi Sécurité) puis d'une intégration par le prestataire en charge de la solution.

La procédure décrivant les modalités de dépôt, traitement et d'activation des liens externes à l'ENT mobilisant du SSO (« single sign-on ») est positionnée en annexe « procédure liste blanche » de la présente convention.

11.2. Procédure de gestion de crise :

Une procédure de Gestion de Crise a été formalisée pour définir et formaliser les actions à activer en cas de crise par les différents acteurs du projet, les instances à mobiliser et les modalités de prise de décision et d'activation opérationnelle de ces dernières.

Cette procédure est actualisée périodiquement et autant que de besoin dans le cadre notamment des commissions d'homologation RGS périodiques de la solution.

La procédure de Gestion de Crise est positionnée en annexe « gestion de crise » de la présente convention.

11.3. Communication en situation de crise :

Pour assurer la cohérence et la sécurité des opérations, la messagerie ENT sera mobilisée par les utilisateurs de l'ENT (Etablissements, Collectivités et Autorités académiques) comme unique vecteur de communication pour informer les familles en cas de gestion de crise.

Ce mode de fonctionnement ne s'applique pas en cas de situation de crise impliquant la messagerie de l'ENT en elle-même.

ARTICLE 5 : AJOUT DE L'ARTICLE 12 « SURETE »

L'article 12 « Sûreté » est ajouté et rédigé comme suit :

Article 12 – Sûreté

Les différents acteurs (Etablissements, Collectivités et Autorités académiques) mobiliseront les outils de communication de l'ENT (sms, messagerie, communication ciblée), ou tout système de communication tiers disposant d'une validation RGS attestée et vérifiée de moins d'un an, comme vecteur de communication pour informer les familles en cas de problématique de sûreté.

ARTICLE 6 : AUTRES DISPOSITIONS

Toutes les clauses et conditions générales de la convention initiale demeurent applicables tant qu'elles ne sont pas contraires aux nouvelles dispositions contenues dans le présent avenant, lesquelles prévalent en cas de contestations.

Fait en 14 exemplaires à Strasbourg, le ……

[SIGNATURES]

ANNEXE 1

Charte de bon usage dans le cadre de toute communication des collectivités vers les familles et élèves par le biais de l'ENT Mon Bureau Numérique

Préambule

Dix collectivités territoriales du Grand Est (les départements des Ardennes, de l'Aube, de la Marne, de la Haute-Marne, de la Meurthe et Moselle, de la Meuse, de la Moselle, des Vosges, la Collectivité européenne d'Alsace et la région Grand Est) ont décidé conjointement de mettre à disposition des établissements d'enseignement du second degré (lycées et collèges, publics, privés et agricoles) l'espace numérique de travail « Mon Bureau Numérique » (MBN). Cet ENT propose diverses fonctionnalités auxquelles accèdent les personnels des établissements, des collectivités concernées, les élèves et leurs représentants légaux, selon des règles définies dans un autre cadre.

MBN propose notamment des dispositifs de communication (communication ciblée, actualités, email, sms) que les collectivités souhaitent utiliser, pour diffuser des informations institutionnelles aux élèves et aux familles, dans le cadre de leurs compétences prévues par les dispositions des articles L231-2 et L213-4 du code de l'éducation. Ce dispositif a pour intérêt d'être disponible, de permettre une diffusion instantanée et d'éviter des coûts importants d'envoi par courrier.

La communication générale, à tous les individus, reste du domaine du propriétaire des droits d'usage de MBN (le groupement de commandes associant les dix collectivités du Grand Est précédemment décrites). Toutefois, ces collectivités souhaitent faire de la communication spécifique, en direction des seuls établissements de leur ressort, ce qui passe par les divers systèmes d'authentification, donc sous la responsabilité éditoriale des chefs d'établissement.

Du fait de leur responsabilité personnelle, en tant que directeurs de la publication pour leur établissement et en application des dispositions de l'article 93-2 de la Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, les chefs d'établissement souhaitent avoir un droit de regard et d'opposition sur les diffusions des collectivités, concernant des communications pour lesquelles ils auraient un doute.

Objectif

La présente charte a pour objectif de définir les conditions dans lesquelles les présidents de collectivité et les chefs d'établissement s'entendent pour que le dispositif de communication en ligne de MBN puisse être utilisé de façon souple, chacune des parties s'obligeant à respecter les droits et devoirs de chacun.

Elle définit les modalités de diffusion pour les collectivités et d'intervention pour les chefs d'établissement.

Utilisation des dispositifs de communication de MBN

Les collectivités territoriales, membres du groupement, ont la possibilité d'utiliser les dispositifs de communication de MBN, dans le but de transmettre toute information utile aux élèves et à leurs représentants légaux, d'une manière dématérialisée, en rapport avec la fréquentation de leur établissement, ou en vue de leur fréquentation d'un autre établissement. Les échanges entre les collectivités et les personnels administratifs, enseignants et d'éducation de l'Education nationale ne sont donc pas concernés par cette charte. Ces informations sont de nature organisationnelle, administrative et financière et visent à améliorer le fonctionnement général des conditions de scolarisation des élèves. Elles sont conformes aux lois et règlements et exemptes de toute forme d'incitation délictueuse ou de propagande.

Par ailleurs, les collectivités locales s'obligent à une stricte neutralité à l'égard de la communauté éducative.

La collectivité qui souhaite user des dispositifs de communication de MBN s'oblige à transmettre préalablement le contenu exhaustif aux autorités académiques concernées (cf. article 9.4 de la convention tel que modifié par l'avenant 1).

Le processus de validation se réalisera en deux temps :

- Temps 1 : validation, adaptation ou rejet par les Autorités académiques :

Les autorités académiques disposeront d'un délai de cinq jours ouvrés pour valider, proposer des adaptations ou rejeter la proposition de communication. Les propositions d'adaptations devront être formalisées et justifiées formellement dans les formulaires ad hoc. Les rejets devront être justifiées formellement dans les formulaires ad hoc.

Sans réponse des autorités académiques dans le délai de cinq jours ouvrés prévu, les communications seront réputées approuvées et seront soumises aux chefs d'établissement (temps 2).

- Temps 2 : Acceptation ou rejet de l'intégration sur le portail ENT des établissements :

Dans le cadre de l'autonomie des établissements traduite sur l'ENT par la fonction de directeur de publication exercée par le chef d'établissement sur le portail ENT de son établissement, le chef d'établissement peut accepter ou rejeter les communications proposées par des tiers (collectivités territoriales ou autorités académiques).

Les chefs d'établissements disposeront d'un délai de 2 jours ouvrés pour valider ou rejeter l'intégration de la communication sur leur portail.

Les rejets devront être motivés explicitement.

Par défaut la communication sera réputée approuvée et sera intégrée sur le portail des établissements.

La communication réalisée par les collectivités pourra être « multicanale ».

En situation d'urgence (cf. article 9.2.1 de la convention tel que modifié par l'avenant 1) :

La communication se réalise directement sans processus de validation par les autorités académiques.

Sur l'application, ces communications seront marquées comme « urgente » et devront être associées d'un texte de justification formelle par la collectivité dans le formulaire de saisie de la communication sur l'ENT. La communication sera alors déployée directement sur les portails ENT visés quel que soit le canal choisi.

Les communications relevant de l'urgence seront analysées à postériori par les instances du projets (COSUI / CST) pour vérifier le respect du cadre.

En situation de crise (cf. article 9.2.2 de la convention tel que modifié par l'avenant 1) :

- Les communications portées par le projet feront l'objet d'un processus simplifié se limitant à une validation unique : adaptation du message par les autorités académiques dans un délai réduit à 48h ouvrées. Cette situation de crise sera justifiée explicitement par la collectivité dans le formulaire de saisie de la communication sur l'ENT ;
- Les communications portées par les Autorités Académiques devront faire l'objet d'une validation par la Région Grand est en tant que pilote du projet MBN.

Droit de regard et d'opposition des chefs d'établissement

Le chef d'établissement, à l'occasion de la réception préalable du contenu exhaustif d'une diffusion de la collectivité exerce pleinement sa responsabilité de directeur de la publication. Il s'oblige à faciliter la communication des collectivités concernées, avec les élèves et leurs représentants légaux, en dehors de toute considération de nature partisane ou intention de nuire.

En cas de doute sur le fond ou sur la forme de la communication, il saisit sans délai le président de la collectivité ou son représentant, en vue de faire rectifier le ou les éléments invoqués, avant diffusion. Il en informe les services académiques.

La collectivité transmet alors et préalablement le contenu exhaustif de sa diffusion rectifiée aux chefs des établissements concernés, dans un temps compatible avec le délai nécessaire à son examen.

Litige persistant

En cas de désaccord persistant entre le président de la collectivité et le chef d'établissement, le président de la collectivité saisit le recteur de l'académie ou le DRAAF, en vue d'obtenir son arbitrage.

Les refus de communication de la part des Chefs d'établissement devront être motivés.

En tout état de cause, chacune des parties conserve ses pleines prérogatives, notamment de saisir les juridictions concernées.

ANNEXE 2

Gestion de crise

1. PHASES DE LA PROCEDURE

Conformément à la norme ISO 27035 relative à la « Gestion des incidents de sécurité de l'information », la procédure de gestion des incidents de sécurité de Mon Bureau Numérique repose sur 5 phases que sont :

- La préparation et la planification ;
- La détection et le reporting ;
- L'analyse et la décision ;
- La réponse ou réaction ;
- Le retour d'expérience.

2. PHASE DE PREPARATION ET DE PLANIFICATION

Afin d'être en mesure de réagir de façon adaptée à un incident de sécurité il est nécessaire qu'une organisation soit définie, qu'elle soit sensibilisée et qu'elle dispose de l'outillage adéquat.

Dans le cadre du projet Mon Bureau Numérique, cette organisation se traduit de la façon suivante :

Nom Prénom	Fonction
PIAZZA Jeremie	RSSI RGE
CONQ Jean-Luc	RSSI Kosmos Responsable de l'équipe Kosmos de réponse aux incidents de sécurité
GUIMBRETIERE Gael	Responsable Kosmos Centre support et formation
MARTIN Hervé	Responsable Kosmos exploitation solutions SaaS

Annuellement une simulation d'incident de sécurité du projet Mon Bureau Numérique pourra être réalisée afin de vérifier que les différents acteurs dont les prestataires sont suffisamment sensibilisés et savent agir de concert et, le cas échéant, revoir la formation et/ou le corpus documentaire de gestion des incidents.

L'outil de workflow utilisé pour déclarer les incidents et suivre le traitement de ceux-ci est JIRA.

3. PHASE DE DETECTION ET DE REPORTING

La deuxième phase de gestion des incidents de sécurité consiste à s'assurer que la région Grand Est et plus précisément le projet Mon Bureau Numérique dispose des moyens permettant la détection d'un incident de sécurité.

La détection peut avoir pour origine :

- Toute personne qui a connaissance d'un fait ou d'une menace pour le projet MBN ;
- Un administrateur ou exploitant Kosmos, informé par un dispositif de supervision, ou lorsqu'il constate une anomalie lors des contrôles quotidiens ;
- Un acteur de la sécurité lorsqu'il est informé par un outil de surveillance ou lorsqu'il constate une anomalie lors de contrôles.

Cette détection dans le cadre du projet Mon Bureau Numérique s'appuie ainsi sur :

- Le centre de surveillance des événements de sécurité de la RGE ;
- La surveillance des évènements de sécurité réalisée par Kosmos ;
- La veille technologique assurée par Kosmos dans le cadre de sa prestation de MCS ;
- La veille des vulnérabilités effectuée par le RSSI RGE et Kosmos auprès des CERT ;

- Les remontées des utilisateurs via le service support du projet Mon Bureau Numérique.

Dans tous les cas de figure, la personne ou le service identifiant l'événement **doit ouvrir un ticket d'incident dans l'outil JIRA** et remplir les différents champs demandés. Il devra renseigner le ticket dans le **journal JIRA « Sécurité-Grand-Est » dédié à ce suivi.**

Il est à noter que le JIRA service Desk est accessible en 24/7.

Cette création de ticket aura pour conséquence d'envoyer automatiquement, pour information, un mail (incluant le titre du ticket et son contexte) au RSSI Kosmos, au RSSI de la Région Grand-Est ainsi qu'à l'équipe d'exploitation Kosmos et à l'adresse email d'escalade de Kosmos.

Toute modification d'état du ticket génèrera un envoi de mail.

L'enregistrement dans JIRA permet de garder une trace de chaque évènement et d'en effectuer un suivi dans toutes les phases ultérieures, d'analyse et de traitement, jusqu'à la fermeture de l'incident.

Il convient aussi dans cette phase de s'assurer que les éléments recueillis puissent, le cas échéant, faire office de preuves en cas de dépôt de plainte en garantissant leur rétention et leur intégrité.

Les éléments du journal JIRA sécurité-Grand-Est constituent également un outil d'analyse a posteriori dans le cadre d'analyses de risques avec les indicateurs associés qui serviront de point d'entrée au comité de sécurité (COSEC). Ils permettront d'évaluer l'efficacité des dispositifs en place et d'identifier les incidents récurrents pouvant être qualifiés de « problème ».

4. PHASE D'ANALYSE ET DE DECISION

A ce stade, un événement de sécurité a été identifié et remonté, il s'agit dans cette phase de catégoriser l'évènement et juger s'il doit ou non être traité comme un « incident de sécurité ».

Les différentes étapes de cette phase sont :

- Revenir le cas échéant vers l'émetteur de l'événement de sécurité si ce n'est pas un incident ou si le ticket n'est pas correctement rempli ;
- Evaluer les impacts et proposer la solution la plus adaptée au vu du périmètre impacté.

Cette phase est réalisée conjointement avec le RSSI RGE et la MOA/MOE du projet Mon Bureau Numérique.

Une première analyse, conduite par l'équipe de réponse aux incidents de sécurité, confirme ou infirme la catégorisation « incident de sécurité ».

Les incidents non confirmés « incident de sécurité » sont transmises aux équipes support pour traitement.

L'équipe de réponse aux incidents de sécurité procède si nécessaire à des investigations complémentaires pour qualifier l'évènement.

5. PHASE DE REPONSE OU DE REACTION

La quatrième phase de la procédure de gestion d'un incident de sécurité consiste à fournir la réponse à apporter à l'incident de sécurité en fonction des décisions prises lors de la phase précédente qui peut être :

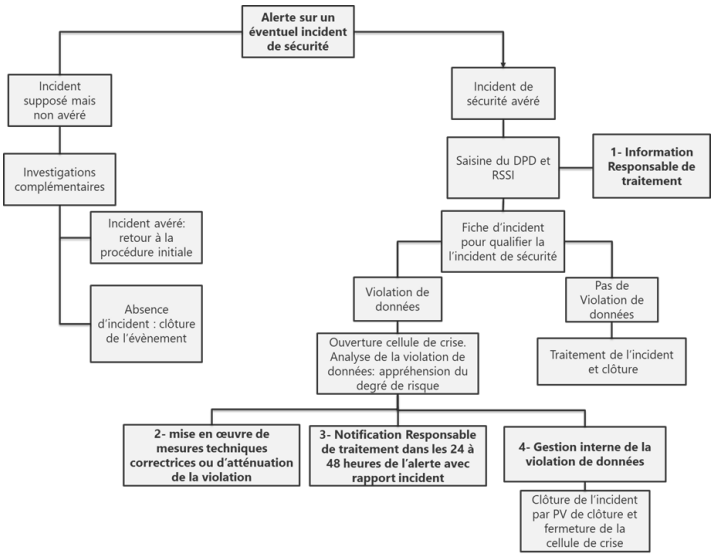
- Réponse immédiate avec solution à apporter ou avec mise en place d'une solution de contournement, action opérée par les équipes de support et d'exploitation Kosmos ;
- Escalade en cas d'incident de sécurité majeur avec mise en place d'une cellule de crise, action opérée, le cas échéant, par le cadre d'astreinte de la DN de la RGE épaulé par le RSSI RGE ;
- Possibilité de recours à des restrictions temporaires d'accès réseaux et/ou services applicatifs ;
- Recours à une étude post-mortem si nécessaire afin d'identifier la cause racine de l'incident et évaluer si d'autres périmètres sont impactés, recours opéré, le cas échéant, par le RSSI RGE ;
- Conservation des éléments de preuve, action opérée via l'outil de ticketing d'incident JIRA et le puit de logs Kosmos ;
- Communication interne voire externe, action réalisée sous le pilotage de la direction de la communication de la RGE par la MOA du projet Mon Bureau Numérique.

Situation de fuite de données personnelles

Dans l'hypothèse de survenance d'un incident de sécurité, Kosmos doit, au cas où son système d'information serait atteint par une violation de données, respecter les deux obligations suivantes :

- Prendre les mesures nécessaires afin de remédier à la violation de données et/ou en atténuer les éventuelles conséquences négatives du point de vue des données à caractère personnel ;
- Fournir toutes les informations qui s'imposent au responsable de traitement afin que ce dernier puisse respecter son obligation de notification à la CNIL et de communication aux personnes concernées lorsque celles-ci s'appliquent.

Dès lors, Kosmos présente ci-dessous le workflow applicable au sein du groupe ayant pour objet de formaliser le processus dès lors que l'environnement numérique de travail subirait un quelconque incident susceptible d'être qualifié de violation de données.



Associé à ce processus, Kosmos dispose d'une fiche d'incident type dont la table des matières est présentée ci-dessous :

1. Coordonnées de la personne effectuant la déclaration
2. Coordonnées de la personne à contacter pour obtenir des informations complémentaires relatives à l'incident
   a. Contact du Service Manager
3. Description de l'incident
   a. Dénomination du système d'information
   b. Brève description du système d'information
4. Incident constaté
5. Qualification de l'incident
6. Mesures prises et envisagées
7. Observations complémentaires

Faisant suite à l'incident, Kosmos alimente son registre de violation de sécurité.

6. PHASE DE RETOUR D'EXPERIENCE

L'analyse post-incident s'inscrit dans une démarche d'amélioration continue et de qualité (PDCA) permettant de prendre connaissance des éléments qui doivent évoluer sur le projet MBN.

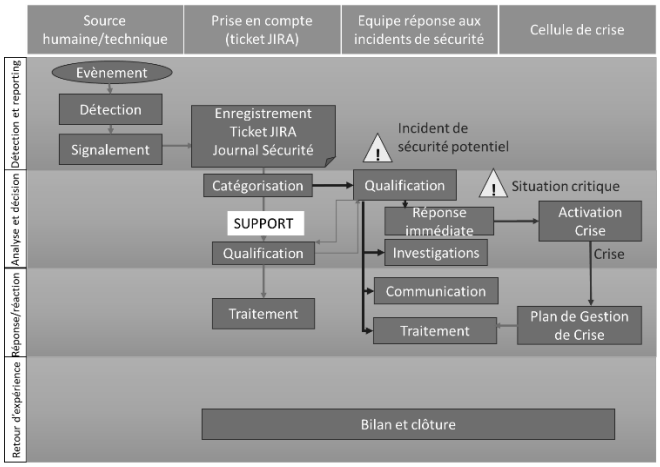
Cette dernière phase permet de tirer profit de l'incident passé via :

- Une revue des mesures de sécurité existantes organisationnelles et techniques ;
- Un enrichissement de la base d'incident de sécurité ;
- Une revue des coûts financiers de l'incident et des gains apportés par la réponse à incident.

7. WORKFLOW DE GESTION DES INCIDENTS DE SECURITE DU PROJET MBN

Le workflow de gestion des incidents de sécurité est représenté par le schéma ci-dessous.

La particularité du traitement des incidents de sécurité tient à l'intervention de l'équipe de réponse aux incidents de sécurité. Les autres volets du processus appartiennent soit au processus général de gestion des incidents (prise en compte de l'incident, qualification, traitement), soit au processus de gestion de crise (cf. document PGC).



Le signalement d'un évènement susceptible d'être qualifié d'incident de sécurité est réalisé soit par une personne (utilisateur, administrateur, exploitant,..) ou par des moyens techniques (outils de surveillance,..).

La prise en compte de l'évènement est réalisée via l'outil de traçabilité JIRA. C'est à ce stade de la prise en compte que l'évènement est catégorisé . Il peut être catégorisé « incident de sécurité » et être confié à des experts pour qualification.

Les incidents catégorisés « incidents de sécurité » sont immédiatement soumis à l'équipe de réponse aux incidents de sécurité. Les autres types d'incidents sont transmis aux équipes support pour leur traitement.

L'équipe de gestion des incidents de sécurité , après analyse, confirme ou infirme la catégorisation « incident de sécuritée (étape de qualification). Les incidents non confirmés « incident de sécurité » sont retransmis aux équipe support.

Les incidents qualifiés « de sécurité » font l'objet d'un traitement spécifique avec potentiellement des investigations complémentaires, un traitement de l'incident avec préservation des éléments de preuve et des actions adaptées de communication.

Dans le cas d'une fuite de données , des spécificités sont prises en compte dans le traitement de l'incident avec potentiellement une déclaration CNIL réalisée par le responsable de traitement sur la base d'un rapport d'incident circonstancié.

Lorque l'équipe de gestion des incidents de sécurité n'est plus à même de gérer la situation, ou lorsque les conséquences potentielles sont jugées de niveau trop important, la cellule de crise est alertée et juge de l'opportunité de passer ou non en mode « gestion de crise ».

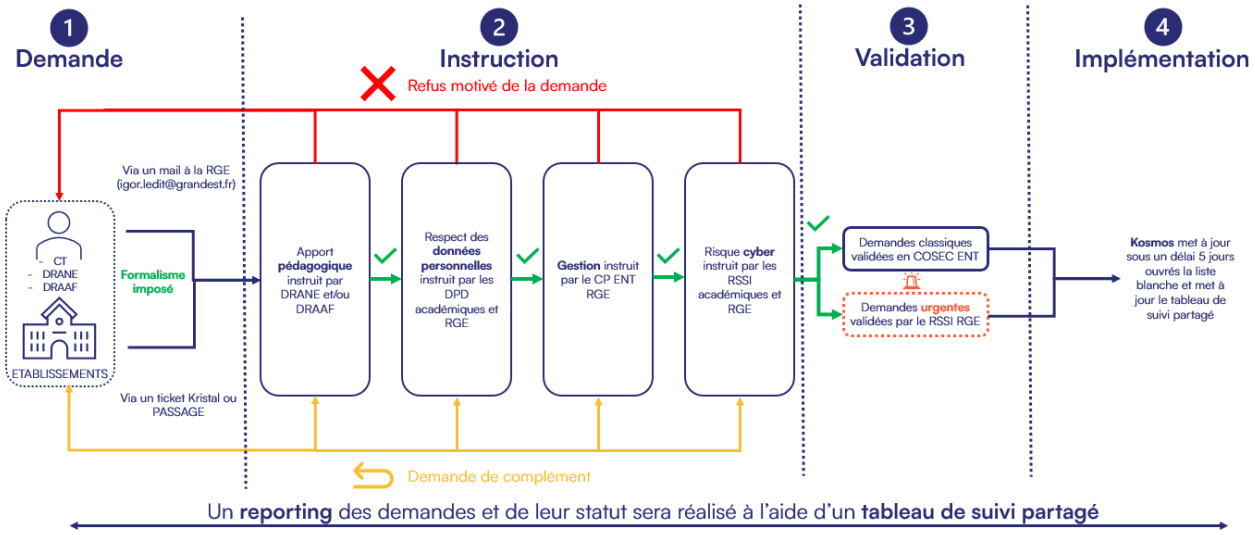
ANNEXE 3

Procédure liste blanche

1. PROCEDURE DE DEMANDE D'INTEGRATION D'UNE ADRESSE A LA LISTE BLANCHE

La procédure ci-dessous décrit comment émettre une demande d'ajout d'une adresse à la liste blanche de l'ENT MBN pour y accéder via SSO (single-sign-on/ authentification unique).

La liste blanche identifie les sites et applications autorisés pour la connexion en SSO depuis l'ENT.



2. PREREQUIS

Les demandes à instruire devront reprendre les éléments suivants :

Volet pédagogique ou de gestion :

- Qui est demandeur ?
- Légitimité de celui-ci ? (CE ou membre des AA)
- Préciser l'importance de l'outil, sites, ressources vis-à-vis des usages attendus ?
- Utilisateurs cibles ?

Volet protection des données :

- Type de données traitées ?
- Type de personne concernée ?
- Durées de conservation des données ?
- Catégories de destinataires ?
- Modalités d'information des personnes concernées ?
- Présence/absence de transferts hors UE ?
- Liste des cookies ou autres traceurs mis en œuvre dans le cadre du traitement ?
- Liste des sous-traitants ?

Volet sécurité :

- Mode de fonctionnement et sécurité des droits (s'adresser à l'éditeur le cas échéant) ?
- Modalités d'hébergement ?