

# PROTOCOLE DE GESTION DES ACCES A L'APPLICATION INTERMINISTERIELLE « CHORUS »

## **I – OBJET - DEFINITIONS**

### **1.1 – Objet**

Le présent protocole définit les règles applicables aux aspects suivants de l'application interministérielle « Chorus »<sup>1</sup> :

- les conditions d'obtention des habilitations d'accès,
- la conformité du profil «Chorus» aux fonctions exercées par le titulaire et la cohérence au sein des rôles «Chorus» du profil,
- les demandes d'habilitation, de modifications d'habilitation, de retraits d'habilitation (modalités, justification),
- la gestion et le suivi des certificats informatiques permettant à une personne de s'authentifier à «Chorus», dénommés «certificats» dans le protocole, ainsi que de leurs supports physiques, dénommés «tokens»,
- la sécurité et la traçabilité des opérations,
- les opérations de contrôle interne à mener (nature des contrôles, périodicité, reporting).

### **1.2 – Périmètre**

Le protocole est applicable à tous les services de l'académie, y compris les directions des services départementaux de l'éducation nationale, le cas échéant.

### **1.3 – Acteurs**

Sont concernés par le protocole :

- l'entité administrative de rattachement (bureau, département ...) de l'agent titulaire d'une habilitation « Chorus », dénommée « l'entité » dans le protocole,
- l'agent titulaire d'une habilitation, dénommé « le titulaire »,
- le responsable de l'entité de rattachement du titulaire, dénommé « le responsable »,
- le correspondant sécurité de la direction du système d'information du rectorat, dénommé « le CSSI »,
- le service chargé de la gestion des ressources humaines, dénommé le «SRH»,
- la plate-forme Chorus, dénommée «la plate-forme»,
- le responsable de la plate-forme Chorus,
- le responsable du contrôle interne comptable (CIC), dénommé «RCIC».
- le correspondant Chorus habilitations, agent désigné par l'académie en charge du paramétrage des habilitations Chorus, dénommé CCH.
- le correspondant Chorus habilitations suppléant, dénommé CCH suppléant,
- le correspondant Chorus formulaires.

---

<sup>1</sup> Sauf mention contraire, ces régies ne concernent pas « Chorus formulaire », le composant du système d'information comptable et financier de l'Etat « Chorus » qui permet de créer des pièces de gestion à distance.

## **II – LES CONDITIONS D'OBTENTION DES HABILITATIONS D'ACCES A « CHORUS »<sup>2</sup>**

2.1 – Sont éligibles à l'obtention d'une habilitation d'accès à «Chorus» les agents effectivement affectés à l'entité à la date de la demande d'habilitation, dont les fonctions justifient d'un besoin d'accès régulier à «Chorus» pour la gestion financière et budgétaire<sup>3</sup>.

2.1.1 - Les vacataires ou contractuels de courte durée sont considérés comme agents affectés.

2.2 – Par exception, il est admis que la procédure d'habilitation des personnes en cours d'affectation puisse être engagée par anticipation :

2.2.1 - Dans cette situation, l'entité s'engage à demander le retrait de l'habilitation si l'agent n'est pas effectivement affecté.

2.3 – Ne sont pas considérés comme «agents affectés» les stagiaires étudiants, les consultants et les prestataires externes.

2.3.1 - Dans l'hypothèse où les personnes citées au § 2.3 ci-dessus accomplissent une mission de longue durée (supérieure à trois mois) dont le bon accomplissement nécessite une habilitation «Chorus», l'entité peut demander une dérogation et s'engage à effectuer les contrôles internes précisés au § 7.3.

2.4 – Pour bénéficier d'une habilitation, le nombre minimal d'opérations préconisé (consultation ou transaction) effectuées dans «Chorus» est de 5 (cinq) opérations par semestre et par titulaire.

2.5 – Les habilitations à CHORUS formulaires ne sont pas conditionnées par un volume minimal de transactions. La nécessité fonctionnelle d'un accès à cet outil doit cependant être justifiée par le responsable de l'entité.

## **III – LA CONFORMITE DU PROFIL «CHORUS» AUX FONCTIONS EXERCEES PAR LE TITULAIRE ET LA COHERENCE AU SEIN DES ROLES «CHORUS» DU PROFIL**

Chaque titulaire d'une habilitation dispose d'une licence d'accès à «Chorus». Un profil, composé de différents rôles et adapté aux fonctions métier du titulaire est associé à son habilitation afin de lui permettre d'effectuer des opérations dans «Chorus» via des «transactions<sup>4</sup>».

### **3.1 – La conformité du profil aux fonctions**

3.1.1 - Le profil d'un titulaire doit correspondre aux fonctions exercées par ce dernier. Les profils proposés par l'application «Chorus» sont décrits en annexe 1 «Fiche de demande d'habilitations et sa notice d'utilisation», dans la partie notice d'utilisation.

3.1.2 - La cohérence entre le profil «Chorus» demandé pour l'octroi d'une habilitation et les fonctions exercées est matérialisée par la fiche de poste des titulaires.

<sup>2</sup> Les règles de cette section s'appliquent également aux habilitations d'accès à « Chorus formulaire ».

<sup>3</sup> Y compris pour la fonction de support et d'assistance (correspondants techniques ou de sécurité...).

<sup>4</sup> Terme technique désignant une séquence d'opérations effectuées dans Chorus.

- 3.1.3 - Il appartient au supérieur hiérarchique validant la demande d'habilitation de s'assurer que les rôles demandés pour le titulaire sont conformes à la délégation de signature dont il bénéficie. La validation de la demande implique la vérification de la conformité du rôle dans «Chorus» à la délégation de signature du titulaire. Cette vérification est matérialisée par l'application des termes suivants sur la «fiche de demande d'habilitations» (cf. annexe 1 «Fiche de demande d'habilitations et sa notice d'utilisation») :

« Vu conforme à la délégation de signature (référence) ..... du .....(date), signature, nom, fonctions ».

### **3.2 – La cohérence des rôles «Chorus»**

- 3.2.1 - Un agent ne peut se voir attribuer des rôles non compris dans la matrice jointe en annexe 2.
- 3.2.2 - En cas de mise en œuvre d'une combinaison de rôles identifiée comme «à surveiller» ou «fortement déconseillée» par la matrice précitée, le responsable de l'entité doit s'engager à mettre en place le dispositif de contrôle interne visé au § 7.3.

### **3.3 – Règles d'organisation et de gestion concernant la séparation des tâches métier**

- 3.3.1 - Un agent de la plate-forme CHORUS, ayant à la fois les rôles de responsable de paiement (RDP) et de responsable d'engagement juridique (REJ), ne doit pas saisir une demande de paiement en lien avec un engagement juridique qu'il a saisi.
- Toutefois, cette possibilité est admise en fonction des contraintes de gestion, dans le domaine des immobilisations, ainsi qu'en période de fin de gestion. Dans ces circonstances, un contrôle a posteriori est effectué par un agent de la plate-forme CHORUS autre que celui qui a saisi les demandes de paiement en lien avec l'engagement juridique.

## **IV – LES PROCEDURES DE DEMANDE D'ATTRIBUTION, DE MODIFICATION ET DE RETRAIT D'HABILITATION**

### **4.1 – Attribution d'habilitations**

- 4.1.1 - Lorsqu'un agent (futur titulaire) remplit les conditions d'obtention, son entité de rattachement remplit la fiche de demande d'habilitation «Chorus» (annexe 1).
- 4.1.2 - La notice jointe à l'annexe 1 décrit la manière de renseigner la fiche de demande d'habilitation, notamment :
- 4.1.2.1 - L'adresse courriel, élément obligatoire pour toute demande d'habilitation, doit être l'adresse personnelle (et non une adresse fonctionnelle) du titulaire<sup>5</sup> ;
- 4.1.2.2 - Cette adresse doit obligatoirement être institutionnelle ([xxx.vvv@ac-caen.fr](mailto:xxx.vvv@ac-caen.fr)).
- 4.1.3 - Le responsable de l'entité signe la fiche après avoir effectué les contrôles nécessaires (cf. point 3.1.3) et attesté de l'effectivité de ceux-ci.

---

<sup>5</sup> Dispositions également applicables pour l'attribution des habilitations d'accès à «Chorus formulaire».

- 4.1.4 - La signature du responsable engage sa responsabilité quant au respect de la conformité du profil Chorus aux fonctions exercées (cf. procédure détaillée au § 3).
- 4.1.5 - Toute demande de dérogation au principe de conformité énoncé au point 4.1.4 précédent doit être motivée ; la procédure de contrôle interne mentionnée au § 7.3. est alors mise en œuvre.
- 4.1.6 - L'entité adresse la fiche signée à la plate-forme Chorus de l'académie.
- 4.1.7 - La plate-forme vérifie la demande, traduit les besoins métier en rôles Chorus (cf. notice de l'annexe 1), complète la fiche de demande si besoin. La fiche, signée par le responsable de la plate-forme, est attribuée au CCH ou au CCH suppléant.
- 4.1.8 - Le CCH traite la demande et informe la plate-forme du résultat du traitement de la demande et toutes les informations la concernant. Il transmet également ces informations à l'entité et au titulaire.
- 4.1.9 - Le titulaire et l'entité informent la plate-forme du résultat de la première connexion à Chorus en lui adressant une copie d'écran portant la liste des rôles CHORUS accessibles.
- 4.1.10 - Les demandes d'habilitation à CHORUS formulaires sont à présenter, par courriel à la plate-forme CHORUS ([cspchorus@ac-caen.fr](mailto:cspchorus@ac-caen.fr)). Un formulaire spécifique comportant les informations utiles à l'habilitation de l'agent sera adressé au responsable de l'entité. La confirmation de l'habilitation sera communiquée par écrit à l'agent et au responsable de l'entité. Les obligations afférentes à l'adresse courriel (voir les § 4.1.2.1. et 4.1.2.2. ci-dessus) sont applicables aux demandes d'habilitations à CHORUS formulaires.

## 4.2 – Modification d'habilitation

- 4.2.1 - A chaque changement de fonctions d'un titulaire, au sein de la même entité, l'entité veille à la conformité des habilitations et demande, le cas échéant, la mise à jour de son profil «Chorus».
- 4.2.2 - La procédure suit (en cas de modification d'habilitation) celle décrite aux points 4.1.1 à 4.1.10.

## 4.3 – Retrait d'habilitation

- 4.3.1 - Lorsque le titulaire<sup>6</sup>
- quitte son entité de rattachement,
  - ou à l'issue d'un changement de fonctions, au sein de la même entité, ne répond plus aux conditions d'obtention des habilitations «Chorus» (cf. §II), son entité doit demander le retrait de son habilitation.
- 4.3.2 - Avant son départ de l'entité ou son changement de fonctions, l'agent procède à la remise de son «token» au CSSI. Il appartient au responsable de l'entité de s'assurer de la remise du «token» avant le départ effectif du titulaire et d'en tracer la restitution en archivant une copie du bordereau de restitution du «token» (annexe 4).

---

<sup>6</sup> Les règles de cette section s'appliquent également aux habilitations d'accès à «Chorus formulaires».

- 4.3.3 - L'entité adresse la demande de retrait d'habilitation (annexe 1 pour habilitation CHORUS et demande sur papier libre pour habilitation Chorus formulaires) au CCH, au CCH suppléant ou au Correspondant Chorus formulaires selon la nature de l'habilitation.

#### **4.4 – Réactivation d'une habilitation**

- 4.4.1 - Il est possible de demander la réactivation d'une habilitation retirée.
- 4.4.2 - La procédure de réactivation est identique à celle de la demande d'attribution (cf. § 4.1).

### **V – LA GESTION, L'UTILISATION ET LE SUIVI DES «TOKENS»**

- 5.1 – Un «token» est nécessaire pour tout accès à l'application «Chorus».
- 5.2 – Lors de la demande de création d'habilitation, une copie de la demande est transmise par le CCH ou le CCH suppléant au CSSI afin que celui-ci puisse effectuer le suivi des «tokens» distribués.
- 5.3 – A la validation de chaque demande de création d'habilitation «Chorus», le CCH ou le CCH suppléant communique les informations nécessaires au CSSI afin de procéder à la délivrance d'un «token» au titulaire.
- 5.4 – Le CSSI remet le «token» au titulaire, en face à face, contre la signature par ce dernier de la «Charte Porteur de certificat AC - Personnes Authentification» (annexe 3). Lorsque le titulaire exerce ses fonctions dans une direction des services départementaux de l'éducation nationale de l'académie, le CSSI mandate le responsable informatique de ladite direction pour assurer cette remise de «token» contre signature de la charte précitée.
- 5.5 – Cette signature engage le titulaire à respecter et à appliquer les consignes de sécurité décrites dans la charte, notamment :
- 5.5.1 - A garder le code d'accès associé au «token» confidentiel ;
- 5.5.2 - A ne partager son «token» ni le code d'accès associé avec personne, y compris pendant ses absences ou congés.
- 5.5.3 - A ne pas quitter son poste de travail en laissant actif son support de certificat.
- 5.6 – A la réception du «token», l'entité demande au service informatique d'installer sur le poste de travail informatique l'accès à «Chorus» et d'assister, si besoin, le titulaire pour sa première connexion à Chorus (après avoir reçu toutes les informations nécessaires à cette connexion).
- 5.7 – A chaque accès «Chorus», le titulaire doit insérer son «token» sur son poste de travail. Une fois connecté à «Chorus», il doit déconnecter son «token» afin d'éviter de le laisser accessible à des tiers.
- 5.8 – A chaque retrait d'habilitation, le CCH ou le CCH suppléant informe le CSSI afin que ce dernier récupère le «token» du titulaire.

**5.9** – Le «token» a une validité limitée. 90 jours avant la fin de cette validité, à chaque connexion à «Chorus», le système avertit le titulaire du nombre de jours restants avant l'expiration du «token».

5.9.1 - Le CSSI gère la liste des «tokens» arrivant en fin de validité et procède spontanément à leur renouvellement en temps approprié. Ce renouvellement consiste à la récupération du «token» (cf. point 5.8) et la remise d'un nouveau «token» (point 5.4), ou à l'extension informatique de la validité du «token».

5.9.2 - Par mesure de précaution, le titulaire peut avertir le CSSI, 30 jours avant la fin de validité de son «token».

**5.10** – Le CSSI tient une comptabilité matière des «tokens» distribués.

5.10.1 - Cette comptabilité matière comprend le nombre des «tokens» distribués, le nombre des «tokens» récupérés ainsi que celui des «tokens» actifs - ce dernier nombre doit correspondre au nombre de titulaires d'une habilitation «Chorus» au sein de l'académie.

5.10.2 - Le CSSI assure par ailleurs un suivi centralisé des «tokens» distribués par entité.

**5.11** – En cas de perte ou de vol du «token», le titulaire alerte immédiatement :

- le CSSI afin que ce dernier révoque le certificat informatique perdu ou volé et distribue un nouveau «token» au titulaire ;
- Le CCH ou le CCH suppléant afin qu'il procède à un nouvel enregistrement du titulaire dans Chorus.

**5.12** – A l'issue de chaque opération affectant l'identité et le nombre des détenteurs de «tokens» de l'académie, le CSSI adresse au CCH ou au CCH suppléant la liste des certificats actifs avec mention de leur date de fin de validité. En l'absence de mouvements dans l'année, cette liste est établie, à minima, chaque 1<sup>er</sup> janvier de l'année N+1.

## **VI – LA SECURITE ET LA TRAÇABILITE DES OPERATIONS**

**6.1** – Les fiches de demande d'habilitation «Chorus» (annexe 1), signées par les entités et par la plate-forme, tracent les demandes et les suites (rejet ou validation et traitement) données à ces dernières.

**6.2** – Le CSSI assure la sécurité de la transmission des «tokens» jusqu'à la remise aux titulaires.

**6.3** – Le CSSI consigne dans un document la distribution et la restitution des «tokens».

**6.4** – Ces documents sont conservés par les acteurs concernés pendant deux ans et doivent être produits en cas d'audit.

## **VII – LES OPERATIONS DE CONTROLE INTERNE**

Les opérations de contrôle interne sur les habilitations «Chorus» sont pilotées et coordonnées par le RCIC du processus Fonctions transverses/CHORUS : Fonctions support

### **7.1 – Les révisions d'habilitation**

- 7.1.1 - Dans le cadre de campagnes périodiques, le CCH ou le CCH suppléant révisé les habilitations. Ces révisions sont basées sur la durée d'inactivité telle que celle-ci est constatée par l'AIFE (Agence pour l'informatique financière de l'Etat, maîtrise d'œuvre de Chorus).
- 7.1.2 - Le RCIC pilote des révisions périodiques (annuelles) en s'appuyant sur la liste des titulaires mutés fournie par le SRH.
- 7.1.3 - Le CCH ou le CCH suppléant procède au retrait des accès (inactifs ou mutation). Il transmet cette information au CSSI aux fins de récupération des «tokens» correspondants.
- 7.1.4 - Au cas où les titulaires mutés hors de leur entité ont besoin d'accès «Chorus» dans leurs nouvelles fonctions, leur nouvelle entité de rattachement en fait la demande en suivant la procédure du § IV.
- 7.1.5 – Au cas où le CCH ou le RCIC constate qu'une entité n'a pas adressé de demande de retrait d'habilitation d'un titulaire<sup>7</sup> (conformément au point 4.3.3) ayant quitté son entité de rattachement ou ne répondant plus aux conditions d'obtention d'une habilitation, le CCH ou le CCH suppléant procède immédiatement au retrait des accès, dans une logique de contrôle interne de maîtrise des risques et transmet cette information au CSSI.

### **7.2 – L'adéquation du profil aux habilitations**

- 7.2.1 - A l'occasion de la campagne périodique de révision des habilitations, le responsable de l'entité doit contrôler l'adéquation des fonctions des titulaires aux habilitations octroyées.
- 7.2.2 - Le résultat de ce contrôle est consigné de manière formelle et archivé de manière traçable.
- 7.2.3 - Le cas échéant, ce résultat est complété des corrections nécessaires demandées par l'entité conformément au § III (retrait d'habilitation ou modification du profil) ou apportées par l'entité à la fiche de poste du titulaire. Celle-ci est alors archivée.
- 7.2.4 - Les résultats du contrôle, ainsi que les éléments de traçabilité, doivent être disponibles en cas de contrôle interne de deuxième niveau ou d'audit.

### **7.3 – Maîtrises des risques en cas de combinaisons de rôles classées «à surveiller» ou «fortement déconseillées», ou liées au non respect des règles d'organisation et de gestion définies en § 3.3**

---

<sup>7</sup> cette règle s'applique également aux habilitations d'accès à «Chorus formulaires».

7.3.1 - Le responsable d'entité doit procéder à une vérification sur un échantillon représentatif des transactions effectuées par le titulaire portant notamment sur :

7.3.1.1 - La conformité des transactions réalisées à la délégation de signature octroyée au titulaire ;

7.3.1.2 - La réalité des faits motivant les transactions ;

7.3.1.3 - La conservation des pièces justificatives des transactions.

7.3.2 - Le résultat de ces opérations de contrôle, ainsi que les pièces justificatives de l'appréciation apportée, doivent être matérialisés et archivés.

#### **7.4 – Contrôle de la comptabilité matière des «tokens»**

7.4.1 - A l'issue de campagnes de révision des habilitations, le CSSI et le responsable de la plate-forme rapprochent les documents de comptabilité matière des «tokens», tenus par le CSSI, des documents de suivi des habilitations tenus par la plate-forme, et du bilan de la campagne de révision.

### **VIII – DOCUMENTS DE REFERENCE (annexés au présent protocole)**

Annexe 1. Une fiche de demande d'habilitation pour l'accès à «Chorus» ;

Annexe 2. Une matrice de vigilance concernant les combinaisons de fonctions métier ;

Annexe 2 bis. Le lexique de la matrice ;

Annexe 3. Une charte d'utilisation d'un «token» ;

Annexe 4. Bordereau de restitution du «token».

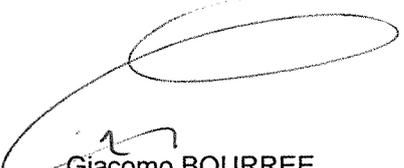
A CAEN, le 13/12/2016

Pour la Direction des Services Départementaux de l'Education Nationale du Calvados,  
La secrétaire générale de la DSDEN,



Françoise LAY

Pour la Direction des Services Départementaux de l'Education Nationale de la Manche,  
Le secrétaire général de la DSDEN,



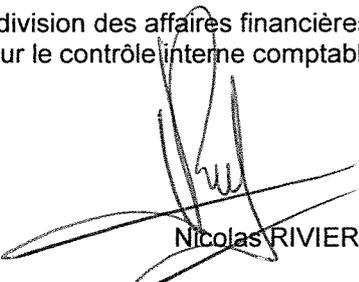
Giacomo BOURREE

Pour la Direction des Services Départementaux de l'Education Nationale de l'Orne,  
La secrétaire générale de la DSDEN,



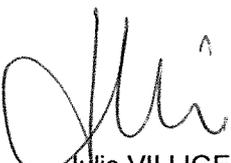
Isabelle FORET-SIMON

Pour la division des affaires financières,  
Le chef de division, référent technique académique pour le contrôle interne comptable



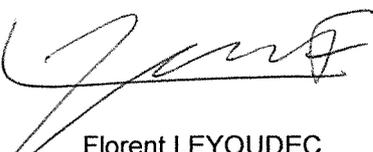
Nicolas RIVIERE

Pour la division de la prospective, de la performance et des moyens,  
La chef de division,



Julie VILLIGER

Pour la division de l'achat et des affaires générales,  
Le chef de division,



Florent LEYOUDEC

Pour la division de l'encadrement des personnels de l'administration et des prestations,

La chef de division,



Delphine MAUROUARD

Pour la division des examens et concours,

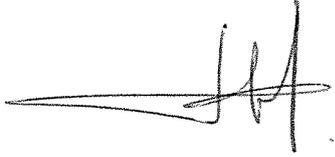
La chef de division,



Marya KHALES

Pour la division de la formation,

La chef de division,



Nadine DAGORN

Pour la direction des systèmes d'information,

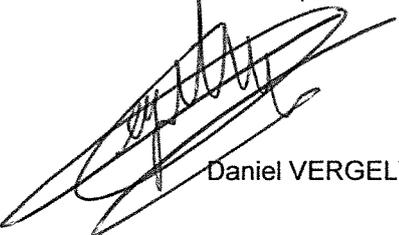
Le directeur,



Jean-Marc LEHOUX

Pour le service des affaires juridiques et de la modernisation,

Le responsable,



Daniel VERGELY

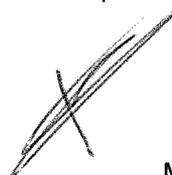
Pour le service construction et patrimoine,

L'ingénieur régional,



Karine BERARD

La responsable de la plate-forme CHORUS,



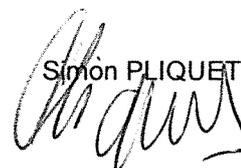
Marlène GOMES

L'adjoint à la responsable de la plate-forme CHORUS, CCH,



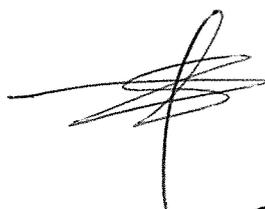
Pascal FOUGERES

L'adjoint à la responsable de la plate-forme CHORUS, CCH suppléant et correspondant  
CHORUS formulaires,



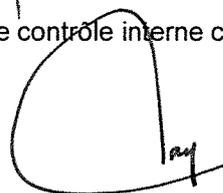
Simon PLIQUET

Le correspondant sécurité du système d'information,



Aziz HARRAK

Le référent promoteur académique pour le contrôle interne comptable,



Jérôme FEILLEL



## FICHE DE DEMANDE D'HABILITATIONS POUR L'ACCÈS A CHORUS

### 1. NATURE DE LA DEMANDE (cocher une seule case)

Création d'habilitation    
  Mise à jour d'habilitation    
  Retrait d'habilitation    
  Réactivation d'habilitation

### 2. INFORMATIONS SUR L'UTILISATEUR

NOM\* :

PRENOM\* :

CIVILITE : MR MME

EMAIL\* :

TELEPHONE\* :

FONCTION\* :

SERVICE\* (préciser l'académie si applicable) :

FONCTIONS EXERCEES (joindre la fiche de poste si celle-ci existe) :

IDENTIFIANT CHORUS<sup>1</sup> (obligatoire si modification ou suppression) :

\* Information obligatoire

### 3. DETAILS DE LA DEMANDE

Création d'habilitation	Identifiant Chorus de l'habilitation <b>à copier</b> (le cas échéant) :
Mise à jour d'habilitation	Identifiant Chorus de l'habilitation <b>à copier</b> (le cas échéant) :

### 4. COMMENTAIRES / INFORMATIONS COMPLEMENTAIRES

<input type="checkbox"/> Rôle responsable nécessitant délégation de signature  Vu conforme à la délégation de signature (référence) <sup>1</sup> ..... du .....  Date, signature, nom, fonctions	<input type="checkbox"/> Demande de dérogation à la matrice d'incompatibilité et de sensibilités des rôles Chorus  La demande de dérogation engage le demandeur à mettre en place de dispositif de contrôle interne supplémentaire.	<input type="checkbox"/> Complément d'informations (le cas échéant)
---	---	---

### 5. VALIDATION

Responsable du service du demandeur	Responsable de la plateforme Chorus	CCH
Nom :	Nom :	Traitée par :
Date :	Date :	Le :
Signature :	Signature :	Commentaires :

<sup>1</sup> A renseigner obligatoirement en cas de demande de rôle de responsable, y compris en cas de copie d'un profil existant ayant un rôle de responsable.

## Annexe : notice d'utilisation de la fiche de demande d'habilitation «Chorus»

La fiche est à remplir pour chaque demande (de création d'une nouvelle habilitation «Chorus», de modification d'une habilitation existante ou de retrait d'habilitation).

Une demande de réactivation d'une habilitation désactivée est assimilée à une demande de création. Dans ce cas, cocher la case « Réactivation d'habilitation ».

Une habilitation réactivée comporte les mêmes rôles qu'avant la désactivation.

Une fiche doit être remplie pour chaque agent.

Les champs indiqués par un '\*' sont obligatoires : les fiches incomplètes seront retournées aux demandeurs.

La case « rôle responsable nécessitant délégation de signature » est à cocher obligatoirement quand un rôle de ce type de responsabilité, par exemple « certificateur de service fait », « responsable d'EJ » ou de DP ou de RNF..., est demandé – **y compris en cas de création ou de modification par copie d'un profil existant qui comporte ces rôles**. La référence de la délégation de signature doit alors être fournie.

L'adresse courriel, élément obligatoire de toute demande de création d'habilitation, doit obligatoirement être :

- nominative et propre à l'agent demandeur,
- institutionnelle (type xxx@ac-yyy.zz).

En cas demande de combinaison de rôles classée « à surveiller » ou « fortement déconseillés » par la matrice d'incompatibilité des rôles «Chorus», cocher la case « demande de dérogation », joindre un document séparé justifiant la demande. La demande doit être signée par le responsable – qui s'engage, par cette signature, à mettre en place les dispositifs de contrôle interne appropriés (qui seront formalisés dans les protocoles de gestion d'habilitations «Chorus»).

La fiche de demande remplie et signée doit être envoyée à la plateforme Chorus, accompagnée de la demande de dérogation signée, le cas échéant.

Afin de minimiser le risque d'erreur de saisie, pour les demandes de création d'accès, il est demandé de fournir les coordonnées du titulaire d'accès à créer (nom, prénom, adresse courriel, fonction, numéro de téléphone), en mode dématérialisé (non manuscrites permettant l'opération « copier/coller » lors du traitement).

Dans la mesure du possible, il est conseillé d'indiquer un profil existant de «Chorus» à partir duquel peut être dupliquées les habilitations :

- indiquer, dans la zone « Identifiant Chorus de l'habilitation à copier (le cas échéant) : », l'identifiant «Chorus» du profil existant (et non du profil à créer ou à modifier) dans la fiche afin de permettre l'opération de duplication. Cet identifiant peut être fourni par son titulaire.

De même, il est nécessaire de fournir cet identifiant pour toute demande de retrait d'habilitation.

- indiquer en complément les modifications à apporter après la copie.

Dans l'hypothèse où il n'existe pas de profil préexistant, il est nécessaire de joindre à la demande une grille dûment remplie de « paramétrage utilisateur ».

# Protocole de gestion des accès à « Chorus » pour l'académie de CAEN

Annexe 1bis

## Notice d'utilisation de la fiche de demande d'habilitation « Chorus »

(Cette notice ne concerne pas les demandes d'habilitation à CHORUS formulaires)

La fiche est à remplir pour chaque demande (de création d'une nouvelle habilitation «Chorus», de modification d'une habilitation existante ou de retrait d'habilitation).

Une fiche doit être remplie pour chaque agent.

Les champs indiqués par un '\*\*' sont obligatoires : les fiches incomplètes seront retournées aux responsables des services demandeurs.

L'adresse courriel, élément obligatoire de toute demande d'habilitation, doit obligatoirement être :

- nominative et propre à l'agent demandeur (les adresses fonctionnelles impersonnelles ne sont pas acceptées),
- institutionnelle (par exemple xxx@ac-caen)

Les informations demandées dans la zone 3 du formulaire seront portées par le correspondant paramétrage de l'académie.

En cas de demande de rôle de responsabilité nécessitant une délégation de signature, cocher la case correspondante et renseigner les références de la délégation de signature.

En cas demande de combinaison de rôles classée «à surveiller» ou «fortement déconseillée» par la matrice d'incompatibilité et d'incohérence des rôles «Chorus», cocher la case «demande de dérogation», joindre un document séparé justifiant la demande. La demande doit être signée par le responsable – qui s'engage, par cette signature, à mettre en place les dispositifs de contrôle interne appropriés (qui seront formalisés dans les protocoles de gestion d'habilitations «Chorus»).

La fiche de demande d'habilitation CHORUS, dûment signée par le responsable de l'entité (zones 5 et 4 si nécessaire) doit être envoyée sous format papier au correspondant paramétrage académique (Monsieur FOUGERES Pascal, adjoint à la responsable de la plate-forme CHORUS).





MINISTÈRE DE  
L'ÉDUCATION NATIONALE

MINISTÈRE DE  
ENSEIGNEMENT SUPÉRIEUR  
ET DE LA RECHERCHE



# Bordereau de restitution de la clé CHORUS

Je,  
 Soussigné(e) .....  
 Fonction : .....  
 déclare avoir restitué la clé de sécurité CHORUS ayant le numéro de série : .....  
 .....  
 délivrée par la Direction des Systèmes d'information.

L'ISR de l'Académie de Caen

L'utilisateur de la clé Chorus

Nom :  
Prénom :

Le :  
A :

Le :  
A :

Signature

Signature



**L'utilisateur d'un certificat « Personnes Authentification » s'engage, par la signature de la présente charte, à appliquer ces consignes de sécurité dans leur intégralité.**

*Le non-respect de ces prescriptions pourra entraîner une révocation du certificat pour cet utilisateur.*

Le Porteur de Certificat  
de l'Académie de CAEN

L'ISR  
de l'Académie de CAEN

Nom :

Nom : HARRAK

Prénom :

Prénom : Aziz

Fonction :

Le :

Le :

A :

A :

Signature

Signature



## Charte Porteur de certificat AC « Personnes Authentification » :

### Académie de CAEN

#### Chaîne de responsabilités :

- Ingénieur de sécurité Racine (ISR), responsable dans l'Académie de l'ensemble des infrastructures Racine :

Identité : Aziz HARRAK

Téléphone : 02 31 30 16 03

Adresse électronique : aziz.harrak@ac-caen.fr

- Opérateur de Sécurité Racine (OSR), assiste l'ISR dans ses fonctions.

Identité : Jimmy MOURIER

Téléphone : 02 31 30 08 65

Adresse électronique : jimmy.mourier@ac-caen.fr

- Utilisateur d'un certificat « Personnes Authentification »,

Identité : .....

Téléphone : .....

Adresse électronique : .....

signataire de la présente charte, garant de l'application des consignes de sécurité pour l'utilisation du certificat sur son poste de travail ainsi que du Support de Certificat.....qui lui sont confiés

#### Attributions de l'utilisateur d'un certificat Personnes Authentification :

L'utilisateur d'un certificat, est **responsable** de son poste de travail ainsi que du Support de Certificat mis à sa disposition :

En application du référentiel documentaire du site <http://www.igc.education.fr> , il est le garant pour les matériels qui lui ont été confiés, des mesures de sécurité ainsi que des consignes d'emplois propres au support de certificat. Il exerce cette responsabilité en lien direct avec l'ISR ou les OSR responsables de la sécurité du réseau au niveau de l'Académie.

## Mesures Organisationnelles :

L'utilisateur d'un certificat « Personnes Authentification » s'engage à :

- permettre et faciliter tout audit de conformité de son poste de travail et du Support de Certificat qui lui sont confiés, dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.
- tenir à disposition de l'ISR ces matériels à des fins de mises à jours ou d'évolutions rendues nécessaires pour garantir la sécurité des dispositifs;
- déclarer à l'ISR, avec un délai d'anticipation d'un mois, tout changement d'affectation ou de fonction afin d'organiser les opérations liées à la restitution du Support de Certificat .

## Mesures de protection physique :

L'utilisateur d'un certificat « personnes Authentification » s'engage à respecter les mesures de protection définies dans le référentiel de sécurité, et notamment déclare à l'ISR :

- tout vol, tentative de vol ou perte du Support de Certificat, dans les plus brefs délais;
- tout vol ou tentative de vol de son poste de travail, dans les plus brefs délais;
- toute utilisation (ou tentative d'utilisation) abusive du Poste ou du Support de Certificat Racine et, de façon générale, toute anomalie qu'il peut constater ;
- toute intervention de maintenance sur le Poste avant sa réalisation
- toute installation logicielle sur le Poste avant sa réalisation.

## Mesures de protection logique :

Le code d'accès du Support de Certificat est choisi par L'utilisateur, il doivent comporter un minimum de 6 caractères et un maximum de 8.

L'utilisateur d'un support de certificat s'engage à :

- ce que le code d'accès demeure strictement personnel et ne soit pas communiqué à des tiers ;
- ne pas quitter son poste de travail laissant actif son Support de Certificat, sans se déconnecter des ressources ou services ;
- ce que les mesures de protections logiques du Poste de travail et validées par l'ISR (antivirus, firewall personnel, ...) soient, en permanence, actives.
- déclarer à l'ISR :
  - toute compromission de ce code ;
  - toute attaque visant à dénaturer l'intégrité du Poste de travail (virus, cheval de Troie...).