Centre intégré
de santé
et de services sociaux
des Laurentides
Québec

Direction de la performance, de l'amélioration continue et de la qualité

POLITIQUE

TITRE : POLITIQUE DE SÉCURITÉ DE L'INFORMATION		
DIRECTION RESPONSABLE :	**DIRECTION DE LA PERFORMANCE, DE L'AMÉLIORATION CONTINUE ET DE LA QUALITÉ**	**N°**
En vigueur le : 30 novembre 2016 **Révisée en date :**		Préparation : DPACQ Approbation: Comité de direction le 7 octobre 2016 Adoption : Conseil d'administration le 30 novembre 2016
Manon Léonard, directrice de la performance, de l'amélioration continue et de la qualité		

N.B. : Nous vous prions de noter que seul le genre masculin a été utilisé afin de simplifier la lecture du texte

1. Préambule

Le ministère de la Santé et des Services sociaux (MSSS), sur approbation du secrétariat du Conseil du trésor, adoptait en août 2015 une nouvelle politique de sécurité de l'information et un nouveau cadre de gestion de la sécurité de l'information remplaçant et renouvelant le Cadre global de gestion des actifs informationnels – volet sécurité (CGGAI) existant.

Les organismes du Réseau de la santé et des services sociaux (RSSS), dont les centres intégrés de santé et services sociaux (CISSS), doivent respecter et mettre en œuvre ce nouveau cadre normatif en sécurité de l'information. La présente politique de sécurité de l'information s'inscrit dans la démarche visant la mise en œuvre du cadre de gestion de la sécurité de l'information du Réseau (voir annexe 3).

Pour se donner les conditions permettant de relever les défis relatifs aux besoins d'échanges d'information et de mobilité des intervenants et considérant l'apport grandissant des technologies de l'information à l'innovation et à la transformation de la pratique clinique, le président-directeur général du CISSS des Laurentides reconnaît la nécessité d'assurer la disponibilité, l'intégrité et la confidentialité de l'information.

Pour ce faire, il met en place une gouverne claire de la sécurité de l'information en conformité avec la politique provinciale de sécurité de l'information par la mise en place de la présente politique sur la sécurité de l'information.

Cette dernière permet aussi d'unifier les anciennes politiques de sécurité des actifs informationnels des organismes qui composent le CISSS des Laurentides et démontre l'importance que l'organisation accorde à la sécurité de l'information.

2. Domaine d'application

Cette politique s'applique à :

2.1 L'ensemble du personnel et des professionnels du CISSS, à tous les médecins, sages-femmes, aux stagiaires, aux chercheurs qui ont accès aux dossiers et informations détenues par le CISSS aux fins de leurs fonctions ainsi qu'aux intervenants externes, fournisseurs de services ou tiers qui exercent pour le CISSS. De plus, elle s'étend à toute personne physique ou morale qui utilise ou accède pour le compte du CISSS, ou non, à des informations confidentielles, ou non, quel que soit le support sur lequel elles sont conservées. Afin de simplifier la lecture du texte, le terme « utilisateur » remplace et inclut tout ce qui précède.

2.2 Tous les actifs informationnels tels les documents sous format papier ou électronique, les systèmes d'information, les banques d'information, les équipements informatiques et de télécommunications, les réseaux, etc. appartenant au CISSS ou sous sa responsabilité.

2.3 Tous les contrats ou les ententes de service avec tout intervenant externe. Les ententes doivent contenir les dispositions requises pour garantir le respect de la présente politique et les règles qui en découlent.

2.4 Toutes les informations que le CISSS traite ou détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

3. Objectifs

La politique de sécurité de l'information sert de fondation en matière de sécurité de l'information dans le CISSS des Laurentides et permet de définir un ensemble de principes, tirés directement de la politique provinciale, visant à :

3.1 Structurer la prise en charge de la sécurité de l'information au sein du Réseau.

3.2 Garantir la conformité avec les orientations, lois et règles gouvernementales notamment en matière de reddition de comptes.

3.3 Assurer la disponibilité, l'intégrité et la confidentialité de l'information, tout au long de son cycle de vie.

3.4 Protéger les informations des usagers du Réseau.

S'ajoute pour le CISSS

3.5 Protéger les informations du CISSS tout en bénéficiant des opportunités d'optimisation.

4. Fondements légaux

Se référer à l'annexe 1 – Cadre légal et administratif.

5. Énoncés et principes généraux

Le CISSS des Laurentides reconnaît que la gouvernance de la sécurité de l'information est basée sur une prise en charge engagée et imputable mettant en avant-plan l'amélioration continue, la proactivité et la reddition de comptes à tous les niveaux hiérarchiques, tout en favorisant une collaboration soutenue avec les différents intervenants, la sensibilisation, le partage et le renforcement des connaissances.

Tirés directement de la politique provinciale :

5.1 Responsabilité et imputabilité

5.1.1 Le plus haut dirigeant d'un organisme est l'ultime responsable de la sécurité de l'information relevant de son autorité. À ce titre, il prend les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité de l'information de son organisme.

5.1.2 Les organismes du Réseau sont responsables devant le ministre de la Santé et des Services sociaux et conservent leurs responsabilités dans toute forme d'impartition. À ce titre, ils précisent leurs exigences en matière de sécurité de l'information dans toute entente ou contrat signé avec un partenaire interne ou externe.

5.1.3 Toute personne autorisée à avoir accès aux actifs informationnels d'un organisme assume des responsabilités particulières en matière de sécurité de l'information, notamment en termes de protection de l'information et répond de ses actions auprès du plus haut dirigeant de cet organisme.

S'ajoute pour le CISSS

5.1.4 Les actifs informationnels sont mis à la disposition des utilisateurs à des fins professionnelles pour les tâches reliées à l'exercice de leurs fonctions.

5.2 Approche holistique de la sécurité de l'information

Tirés directement de la politique provinciale :

5.2.1 La gestion de la sécurité de l'information repose sur une compréhension commune et sur une approche globale qui tient compte des aspects humains, organisationnels, financiers, juridiques et technologiques.

5.2.2 La gestion de la sécurité demande la mise en place d'un ensemble de mesures coordonnées, adaptées à la nature des organismes, supportant ses besoins d'affaires, encadrées par des exigences de sécurité et des pratiques reconnues, tout en laissant le choix des moyens de mise en œuvre aux organismes.

S'ajoute pour le CISSS

5.2.3 Les mesures sont spécifiées dans divers documents d'encadrement de la sécurité de l'information qui s'additionnent, se complètent et précisent la présente politique.

5.3 Gestion intégrée des risques de sécurité de l'information

Tirés directement de la politique provinciale :

5.3.1 La gestion intégrée des risques de sécurité de l'information est une responsabilité organisationnelle qui requiert la mise en place d'un système basé sur un principe d'amélioration continue et qui permet l'identification, l'analyse et le traitement des risques de sécurité à tous les niveaux hiérarchiques de chaque organisme.

5.3.2 Les organismes du Réseau identifient et évaluent sur une base régulière et dans le cadre de projets d'informatisation, les risques d'atteinte à la disponibilité, l'intégrité et la confidentialité de l'information, pouvant affecter la réalisation de leurs missions et mettent en place des mesures permettant de réduire ces risques.

5.3.3 Les organismes du Réseau mettent en œuvre des processus de gestion de la sécurité de l'information qui assurent le respect des exigences de sécurité de l'information, ainsi que l'adoption de pratiques recommandées en sécurité de l'information.

5.3.4 Tout manquement à la sécurité de l'information fait l'objet d'une vérification afin de rendre compte de la situation au responsable de la sécurité de l'information de l'organisme.

5.4 Sensibilisation et formation

Tirés directement de la politique provinciale :

5.4.1 La sensibilisation et la formation du personnel en sécurité de l'information sont indispensables à l'implantation d'une culture de sécurité à l'échelle du Réseau.

5.4.2 Les principaux intervenants en sécurité de l'information et les gestionnaires reçoivent une formation et le soutien nécessaire pour s'assurer qu'ils maîtrisent les concepts de base en sécurité de l'information et prennent des décisions éclairées.

5.4.3 Les organismes du Réseau effectuent, sur une base régulière, des activités de sensibilisation et de formation de leurs utilisateurs à la sécurité de l'information, aux conséquences d'une atteinte à la sécurité de l'information, ainsi qu'à leurs rôles et leurs obligations en cette matière.

5.5 Droit de regard

Tirés directement de la politique provinciale :

5.5.1 Le ministre de la Santé et des Services sociaux exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels du Réseau.

5.5.2 Des mécanismes sont mis en place pour permettre aux organismes du Réseau de démontrer au ministre de la Santé et des Services sociaux, une prise en charge maîtrisée de la sécurité de l'information à leur niveau organisationnel, conformément à la directive sur la sécurité de l'information gouvernementale.

S'ajoutent pour le CISSS

5.5.3 Le CISSS exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels du CISSS.

5.5.4 D'autres mécanismes peuvent être mis en place par le CISSS dont des logiciels de sécurité qui peuvent enregistrer et archiver, pour des fins de gestion, le contenu des actifs informationnels ou les activités réalisées à partir des actifs informationnels du CISSS.

5.5.5 Le CISSS peut aussi soumettre de façon ponctuelle ses actifs informationnels à des audits ou vérifications informatiques.

6. Rôles et responsabilités

Le cadre de gestion de la sécurité de l'information du Ministère de la Santé et des Services sociaux (MSSS-CDG01) définit la structure fonctionnelle de la sécurité de l'information du Réseau de même que les rôles et responsabilités détaillés des instances des organismes du Réseau, notamment :

Pour le conseil d'administration

- L'adoption d'une politique de sécurité de l'information conforme à la politique provinciale de sécurité de l'information et au cadre de gestion de la sécurité de l'information.

Pour le dirigeant de l'organisme

- Nomme un employé de la classe d'emploi cadre à titre de Responsable de la sécurité de l'information (RSI) de son organisme et s'assure de lui octroyer les pouvoirs et ressources nécessaires à la réalisation de ses tâches et responsabilités. Le formulaire de nomination du RSI doit être retourné annuellement au 1er avril ou au besoin au ROSI lors d'un changement du RSI;

- S'assure de la mise en place d'un comité chargé de la sécurité de l'information au sein de son organisme et mandate le RSI pour présider ce comité.

Pour le responsable de la sécurité de l'information (RSI)

- Planifie les activités nécessaires à la mise en place de la sécurité de l'information au sein de son organisme, entre autres, l'élaboration et l'application d'une politique et d'un cadre de gestion adaptés en sécurité de l'information;

- Préside pour le compte du dirigeant de l'organisme, le comité de sécurité de l'information au sein de son organisme et lui soumet pour consultation, les orientations, les politiques, les directives, les cadres de gestion, les plans d'action, les bilans et les rapports sur les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisme, ainsi que toute proposition d'action ou état d'avancement des projets destinés au dirigeant de l'organisme.

7. Définitions

Se référer à l'annexe 2- Définitions des termes.

8. Sanctions

Lorsqu'un utilisateur contrevient ou déroge à la présente politique, ou aux documents en découlant, notamment et sans s'y limiter le cadre de gestion, les directives et règles de l'organisme, il s'expose selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste.

9. Dispositions finales

La présente politique de sécurité de l'information entre en vigueur à la date de son approbation.

Tous les utilisateurs doivent signer la déclaration de la personne quant à la connaissance et au respect de la Politique de sécurité de l'information du CISSS avant d'utiliser les actifs du CISSS (Annexe 4).

Cette politique est réévaluée minimalement aux trois ans afin d'intégrer les nouveaux besoins, les nouvelles pratiques, les nouvelles menaces et les nouveaux risques encourus.

Annexe 1- Cadre légal et administratif

Tirés directement de la politique provinciale.

La présente politique s'inscrit principalement dans un contexte régi par:

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q., c. G-1.03;
- La Loi concernant le cadre juridique des technologies et l'information, L.R.Q., c. C-1.1;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1;
- La Loi sur la protection des renseignements personnels dans le secteur privé;
- La Loi sur la protection des renseignements personnels et les documents électroniques;
- La Loi sur le droit d'auteur, L.R., 1985, c. C-42;
- La Loi sur les services de santé et les services sociaux, L.R.Q., c. S-4.2;
- La Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales;
- La Loi sur les services de santé et les services sociaux pour les autochtones cris, L.R.Q., c. S-5;
- La Loi sur les services préhospitaliers d'urgence, L.R.Q, c. S-6.2;
- La Loi sur la Régie de l'assurance maladie du Québec, L.R.Q., c.R-5;
- La Loi sur l'assurance maladie, L.R.Q., c. A-29, section VII;
- La Loi médicale, L.R.Q., c. M-9;
- La Loi sur la pharmacie, L.R.Q., c. P-10;
- La Loi sur la santé publique, L.R.Q., c. S-2.2;
- La Loi sur la protection de la jeunesse, L.R.Q., c. P-34.1;
- La Loi sur le curateur public, L.R.Q., c. C-81;
- La Loi sur la santé et la sécurité au travail, L.R.Q., c. S-2.1;
- La Loi sur les accidents de travail et les maladies professionnelles, L.R.Q., c. A-3.001;
- La Loi sur la recherche des causes et des circonstances de décès, L.R.Q., c. R-0.2;
- Le Code des professions, L.R.Q., c. C-26, articles 60.4 à 60.6 et 87;
- Les Codes de déontologie des différents ordres professionnels œuvrant dans le domaine de la santé et des services sociaux;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, c. A-2.1, r. 02;
- La Charte des droits et libertés de la personne, L.R.Q., c. C-12;
- Le Code civil du Québec, L.Q., 1991, c. 64;
- La Loi sur les archives, L.R.Q., c. A-21.1;
- La Loi sur l'administration publique, L.R.Q., c. A-6.01;
- La Loi sur la fonction publique, L.R.Q., c. F-3.1.1;
- La Loi canadienne sur les droits de la personne, L.R., 1985, c. H-6;
- Le Code criminel, L.R., 1985, c. C-46;
- La politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- La directive sur la sécurité de l'information gouvernementale, décret 7-2014;
- Loi sur le système de justice pénale pour les adolescents, L.C. 2002, ch. 1.

ANNEXE 2- Définition des termes

Pour la présente politique, son cadre de gestion et documents connexes, les termes et expressions suivantes signifient :

1˚ **Actif informationnel:** Actif informationnel au sens de la loi concernant le partage de certains renseignements de santé (LPCRS), soit, une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

2˚ **Confidentialité:** Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.

3˚ **Cycle de vie de l'information:** L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme.

4˚ **Disponibilité:** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

5˚ **Détenteur de l'information**[1]: Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

6˚ **Gestion intégrée des risques de sécurité:** Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques de sécurité à tous les niveaux hiérarchiques de l'organisation.

7˚ **Intégrité:** Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

8˚ **Réseau:** Ensemble des organismes qui relèvent du Dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).

9˚ **Risque de sécurité de l'information:** Probabilité que survienne un événement préjudiciable, plus ou moins prévisible, qui peut affecter la réalisation des objectifs de l'organisme ou du Réseau.

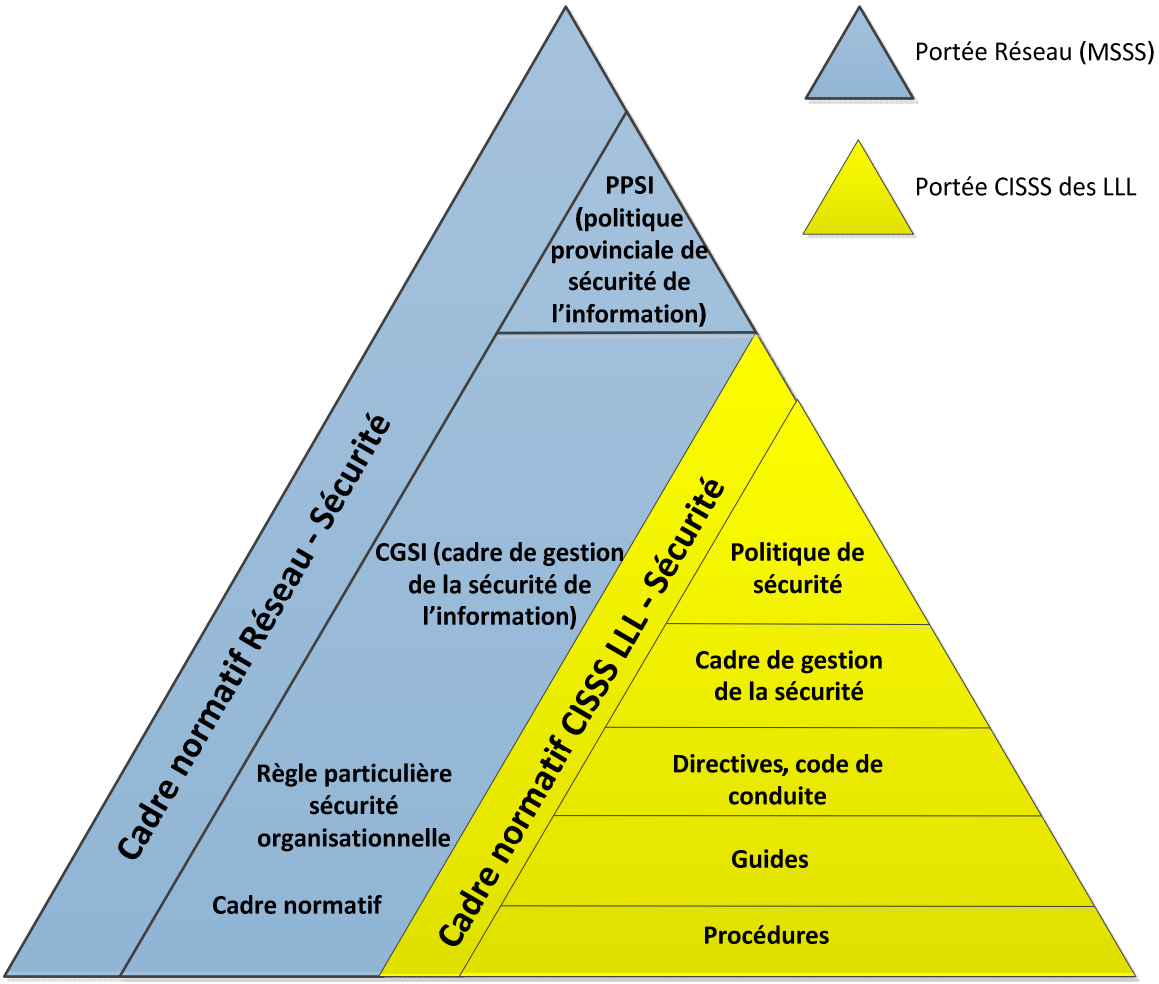
10˚ **Système d'information :** Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'un organisme.

11˚ **Utilisateur**[2]: Toute personne de l'organisme de quelque catégorie d'emploi, de statut d'employé, médecin, stagiaire, etc. ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel sous la responsabilité de l'organisme ou y a accès.

[1] SCT - Directive sur la sécurité de l'information gouvernementale
[2] Guide d'élaboration d'un cadre de gestion de la sécurité de l'information

ANNEXE 3 – Positionnement de la politique de sécurité de l'information

La politique de sécurité de l'information s'inscrit dans le cadre normatif du CISSS, tout en s'appuyant sur le cadre normatif du Réseau. Les CISSS de Lanaudière, Laurentides et Laval adoptent le même modèle tel qu'illustré ci-dessous :



Centre intégré de santé et de services sociaux des Laurentides
Québec

Annexe 4- Déclaration de la personne quant à la connaissance et au respect de la politique de sécurité de l'information du CISSS des Laurentides

Je soussigné(e), *(prénom)* _____ *(nom)* _____

(fonction ou titre d'emploi) _____

☐ Employé(e) du CISSS	☐ Médecin/professionnel(le) œuvrant au CISSS
☐ Consultant(e) de la compagnie	☐ Stagiaire de l'institution
☐ Bénévole	☐ Autre

Travaillant au Centre intégré de santé et de services sociaux (CISSS) des Laurentides situé au 290, rue De Montigny Saint-Jérôme, déclare avoir reçu l'information sur la Politique de sécurité de l'information du CISSS. Le texte intégral de cette politique est disponible sur demande en format papier, auprès de mon chef de service, sur l'intranet du CISSS sous la rubrique politique.

Je m'engage à prendre connaissance de cette politique, des mesures qui en découlent, ainsi que les codes de conduite applicables, à y adhérer et à les respecter. Je dois en tout temps prendre toutes les mesures mises à ma disposition afin d'appliquer cette politique dans l'exercice de mes fonctions et des tâches qui y sont associées.

J'ai le devoir d'informer immédiatement mon supérieur immédiat de tout incident ou toute situation portée à ma connaissance qui serait susceptible de compromettre la confidentialité des renseignements confidentiels et la sécurité concernant l'utilisation des actifs informationnels et de télécommunication.

Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la confidentialité des renseignements et des données sociosanitaires confidentiels auxquels j'ai accès, soit la sécurité des actifs informationnels et de télécommunication du CISSS.

Je suis pleinement conscient(e) que le CISSS utilise des logiciels de sécurité qui peuvent enregistrer, pour des fins de gestion, le contenu de mon courrier électronique, les adresses Internet des sites que je visite et conserver un dossier de toute activité réalisée sur ses réseaux d'information au cours de laquelle je transmets ou reçois quel que document que ce soit lorsque j'utilise les systèmes d'information et ressources du CISSS.

J'ai été informé(e) que le CISSS peut enregistrer et archiver pour des fins de gestion les messages que je reçois ou envoie et peut me soumettre, de manière ponctuelle, à un audit ou à une vérification informatique si requis par le responsable de la sécurité de l'information du CISSS. J'ai été informé(e) également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.

Signature de la personne *(prénom et nom)*	n° d'employé ou de licence *(si applicable)*	Date

Original à conserver au dossier de l'employé