Travail élaboré en collaboration avec :
Joseph Tengue (Directeur du Numérique), Guilhem Louis-François (Directeur adjoint du Numérique et RSSI), Alexandra Nahmiyace (Chargée de mission des Affaires Juridiques/DPO), Rebecca Lévy (Cheffe du service paie et carrière de la division des ressources humaines), Romain Greiner (Chef du service formation et recrutement), Fanjanirina Rajaobélina (Responsable du service intérieur)
Mise en place : octobre 2023/juillet 2024

N° Risque		Tâche	Acteurs concernés	Risques encourus	Probabilité	Impact	Criticité brute 2023	Niveau de maîtrise	Criticité nette 2024	Action de maîtrise du risque	Acteur de l'action	Calendrier	Observations
3	1	Mise à disposition du dossier agent pour sa prise en charge en paie	DRH/Service recrutement et formation/Service carrière et traitement	Le dossier agent a fait l'objet d'un partage puis d'un "copier-coller" du drive RH/SRF au serveur du SCT. La conservation du dossier agent sur le Drive ne respecte pas le RGPD dès lors que le SCT prend le dossier en charge en paie.	**5**	**5**	**25**	**5**	**125**				Il convient de mettre une règle en place afin que le SRF mette le dossier agent à disposition et que le SCT retire ce dossier en partage afin de le prendre en charge en paie en respect au RGPD.
48	1	RGPD	DPO/Direction du Numérique/Directions/Services	Les adresses mails génériques sont sources de risques dans le traitement de données personnelles. Au-delà de la qualité des membres qui composent cette adresse générique, de l'actualisation de ces membres, cet usage est en contradiction avec le principe de la minimisation de la collecte des données personnelles au sein d'un service et ne garantit pas la juste finalité de l'utilisation de ces données.	**5**	**5**	**25**	**5**	**125**				Utilisation a bon escient d'adresses mail génériques du Crous de Créteil de façon sécurisée et en conformité avec le RGPD (où seule la direction du numérique est la seule à intervenir en tant que propriétaire pour créer/modifier les membres et où les membres devront être des destinataires limités, définis et reconnus pour la finalité du traitement),
50	1	RGPD	DPO/Direction du Numérique/Directions/Services	La DPO ne réalise pas d'AIPD.	**5**	**5**	**25**	**5**	**125**				Il est nécessaire pour la DPO de réaliser un AIPD pour chaque traitement présentant au moins 2 critères de risque avec les acteurs concernés (à titre informatif prévoir des réunions d'échanges d'environ 2/3h).
49	1	RGPD	DPO/Direction du Numérique/Directions/Services	La DPO n'est pas informée de nouveau traitement.	**5**	**5**	**25**	**4**	**100**				Sensibilisation faite. Réflexes non acquis. Sensibilisation renforcée proposée avec élaboration d'un diaporama sur la présentation du RGPD (DPO et CI) et à renouveler à chaque rentée.
55	1	Positionnement	Direction du Numérique	Le RSSI est placé sous la responsabilité du directeur du numérique	5	4		5	100				Idéalement le RSSI devrait être indépendant de la direction du numérique ; Avoir sa propre cellule rattachée à la DG ; les priorités du RSSI et du DN peuvent être différentes (les priroités peuvent s'opposer : ex : d'une part optimiastion du fonctionnement de l'informatique et d'autre part la sécurité).
56	1	Quotité/ETPT	Direction du Numérique	Le RSSI n'est pas à temps plein	5	5		3	75				Idéalement le RSSI devrait assurer ses missions à CT à temps plein avec pour objectif de mutualiser les missions avec d'autres Crous d'IDF.
54	1	RGPD	DPO/Toutes les directions/Tous les services	Le principe de limitation de la durée de conservation des données à caractère personnel n'est pas respecté	**5**	**5**	**25**	**3**	**75**				Une sensibilisation a été par la DPO, accompagnée de la documentation relative à la durée de conservation selon la typologie des états. Pour autant la mise en pratique ne semble pas suivi dans touts les directions ou dans tous les services. Nouvelle sensibilisation renforcée à prévoir. Travail en lien avec les missions d'archivage.

45	1	Vidéosurveillance	DPO/Direction du Numérique	Les personnes habilitées visionnent les vidéos sans raison valable	**3**	**5**	**15**	**4**	**60**				Travail de réflexion sur un plan de contrôles. Revoir Alexandra/Guilhem
10	1	Ouverture/modifications des droits d'accès par les GA	GA	Les GA omettent d'ouvrir ou de modifier les droits. Ou accordent plus de droits que demandés ou **les GA ne sont pas informés des départs des agents et les droits d'accès ne sont pas désactivés : risques liés à la sécurité des droits d'accès SI notamment pour les applications liées à la monétique.**	**4**	**4**	**16**	**3**	**48**	1/ Il convient d'élaborer une/des procédure(s) pour formaliser le circuit de demande d'accès SI (en s'inspirant par exemple de la procédure de Karima Lakrib pour l'application monétique + des informations qu'il convient de préciser dans la demande pour y répondre efficacement), 2/ Travail de réflexion sur la manière de procéder pour informer des départs des agents en vue de désactiver les droits d'accès et d'avoir une liste actualisée des utilisateurs.			Risques abordés et estimés avec Karima Lakrib.
42	1	Vidéosurveillance	DPO/Direction du Numérique	La décision d'habilitations spécifiques n'est pas publiée sur le site internet	**4**	**4**	**16**	**3**	**48**				La décision est en cours de rédaction et la publication suivra
43	1	Vidéosurveillance	DPO/Direction du Numérique	La liste des personnes habilitées n'est pas actualisée + recensement des implantations des caméras	**4**	**4**	**16**	**3**	**48**				Travail en cours d'actualisation
46	1	Vidéosurveillance	DPO/Direction du Numérique	Les vidéos sont ou peuvent être visonnées au vu et au su de tous	**3**	**4**	**12**	**4**	**48**				Dans la pratique actuelle il n'y a aucune garantie que le visionnage soit fait selon les règles. Idéalement il conviendrait d'avoir une salle dédiée ou un bureau propice à l'isolement et sécurisé au niveau des services centraux et des UG.
12	1	Préparation d'un PC portable	Equipe de techniciens D°Numérique	Le pc n'est pas paramétré ou pas au bon profil utilisateur	**3**	**5**	**15**	**3**	**45**				Dans le cas où le pc n'est pas paramétré correctement : mise en place d'une Check liste des vérifications clés à réaliser et à moyen terme mise en place d'un contrôle automatique de supervision.

47	1	Vidéosurveillance	DPO/Direction du Numérique	Des droits sont accordés à des personnes non habilitées	**5**	**3**	**15**	**3**	**45**				Deux volets sont concernés : informatique et juridique. Les 3 coefficients ont été estimés approximativement car il n'y a pas de visibilité qui permette d'avoir une garantie si la situtation est en marge ou non. Certains agents ont accès à des caméras sur des sites dont ils n'ont pas la responsabilité. Ces droits élargis sont à revoir. Ces cas semblent pour autant rester en marge mais aucune vérification n'a permis de faire un état des lieux. Un contrôle de vérification sur l'ensemble des postes ayant l'applicatif "Jette un oeil" est prévu par la Direction du numérique. NB : les référents n'ont théoriquement pas de droits élargis. La non conformité dans le domaine juridique est forte si le risque est avéré.
53	1	Organisation du départ de l'agent par le responsable	RS	Aucune consigne n'a été formulée ou respectée pour assurer la continuité des missions après le départ d'un agent	**3**	**5**	**15**	**3**	**45**				Le responsable doit rappeler les consignes à l'agent avant son départ. A minima une réponse automatique par mail informant de son départ et précisant un contact pour prendre le relais, préciser l'emplacement des dossiers à suivre (physiques et/ou dématérialisés, ainsi que les éventuelles instances prioritaires.
19	1	Gestion des téléphones portables	FR	L'absence de gestion de suivi des téléphones portables ne permet pas d'avoir une vison globale de la tenue du matériel, de son stock (entrant/sortant). Il n'y a pas de traçabilité de ce qui est prêté/rendu.	**4**	**3**	**12**	**3**	**36**				Il n'y a pas de vision globale sur l'ensemble de la flotte des téléphones portables car le suivi mis en place est récent (fin 2023). Par ailleurs les UG n'ont pas toutes le réflexe de restituer les téléphones portables. Un travail de sensibilisation doit être réalisé ainsi qu'une étude sur l'analyse de la charte informatique pour la partie relevant de la téléphonie.
32	1	Revue annuelle des habilitations	Direction du Numérique/RSSI	Absence de garantie que tous les utilisateurs aient été recensés et actualisés	**3**	**4**	**12**	**3**	**36**				Travail à mettre en place avec le service carrière et traitement/RSSI/CIF
28	1	Récupération des badges Parking	DUG/Dug adjoint	Absence de garantie que l'agent/l'étudiant ait retiré (totalement ou partiellement) les moyens mis à sa disposition ou que les moyens aient été mis à sa disposition (totalement ou partiellement)	**3**	**3**	**9**	**3**	**27**	Travail de sensibilisation des bonnes pratiques quant à l'utilisation des cartes parking.			A l'UG de restauration de Créteil il y a une quarantaine de places de parking au Trident. Les badges sont paramétrés par un prestataire. Les badges sont pour partie utilisés en étant passés d'un agent à un autre et parfois non restitués. La gestion du suivi compte-tenu de ces pratiques devient problématique, énergivore et chronophage et l'utilisation des places n'est pas optimisée. La non restitution de cartes dont l'utilisation du parking est ponctuelle empêche d'autres agents de pouvoir accéder au parking.
30	1	Information du départ d'un agent	DRH/SCT	L'absence ou la carence d'information du départ d'un agent ne permet pas d'avoir la garantie que le matériel mis à disposition soit restitué et ne permet pas de désactivier des droits d'accès pour fiabiliser la sécurité.	**3**	**3**	**9**	**3**	**27**	Travail de coordination et d'information entre le SCT et le responsable (pour prise en compte de la date administrative de départ et de la date effective de départ de l'agent (congés déduits))			Proposition qu'un mail (similaire à celui envoyé dans le cadre de l'arrivée d'un agent) soit transposé au départ et envoyé au responsable SC et UG.
31	1	Revue annuelle des habilitations	Direction du Numérique/RSSI	Absence de garantie que tous les applicatifs aient été recensés et actualisés	**3**	**3**	**9**	**3**	**27**				Les plus importantes applications sont connues du Cnous. Travail de réflexion pour identifier et mesurer les applications qui ne seraient pas répertoriées.

38	1	Vidéosurveillance	DPO/Direction du Numérique	Il n'y a pas de personnes habilitées au sein de certaines UG et/ou services centraux	**3**	**3**	**9**	**3**	**27**				Au niveau des UG, désignation faite : Dug ou Adjoint ou Dug par intérim. Au niveau des SC : personne n'a été encore désigné.
40	1	Vidéosurveillance	DPO/Direction du Numérique	Il n'y a pas de charte de vidéosurveillance mise en place	**3**	**3**	**9**	**3**	**27**				Charte en cours de rédaction en intégrant l'engagement de confidentialité. NB : prévoir de la faire signer à tous les nouveaux arrivants et à tous ceux déjà en fonction.
41	1	Vidéosurveillance	DPO/Direction du Numérique	Il n'y a pas de décision d'habilitations spécifiques à visionner des images enregistrées de vidéosurveillance	**3**	**3**	**9**	**3**	**27**				En cours de rédaction.
22	1	Récupération du PC portable	Direction du Numérique	Absence de garantie que l'agent ait restitué (totalement ou partiellement) les moyens mis à sa disposition ou que les moyens aient été récupérés à sa disposition (totalement ou partiellement)	**3**	**2**	**6**	**4**	**24**				Travail de sensibilisation à réaliser au niveau des UG pour ne pas garder/stocker les PC des agents partis. Travail de réflexion sur la définition du circuit à formaliser (SC +UG). Attestation mise en place. 1 exemplaire est destiné à l'agent un autre exemplaire est conservé en version papier à la direction du numérique et classé par ordre alphabétique.
51	1	Vidéosurveillance ou RGPD	DPO	La DPO n'a pas de binôme ou de suppléance	**3**	**2**	**6**	**4**	**24**				Pas de suppléance/Fishing se développe/Obligation de notifier dans les 72H à la CNIL toute violation de données. Idéalement externalisation de la prestation + Référent DPO au sein de la structure.
36	1	Vidéosurveillance	DPO/Direction du Numérique	Il n'y a pas ou plus de référents et/ou ils ne sont pas connus	**2**	**3**	**6**	**3**	**18**				Une liste existe et nécessite d'être actualisée.
39	1	Vidéosurveillance	DPO/Direction du Numérique	Les personnes habilitées n'ont pas suivi de formation dans le cadre de la vidéosurveillance	**3**	**3**	**9**	**2**	**18**				Il est recommandé que les agents puissent suivre une formation dans toute la mesure du possible dans les 2 mois qui suivent leur nomination.
29	1	Téléphone portable	DMPC	Absence ou retard de l'étude et de la coordination entre service pour assurer la continuité de la prestation de téléphonie mobile sans rupture de contrat	**2**	**4**	**8**	**2**	**16**				
37	1	Vidéosurveillance	DPO/Direction du Numérique	Il n'y a pas de désignation de personnes habilitées à visionner les vidéos	**2**	**4**	**8**	**2**	**16**				Les fonctions impliquent une désignation d'office.
44	1	Vidéosurveillance	DPO/Direction du Numérique	Il n'y a pas de signalétique conforme aux recommandations de la CNIL pour informer le personnel et les étudiants de l'utilisation de caméras vidéosurveillance	**2**	**4**	**8**	**2**	**16**				
1	1	Communication de la date d'arrivée prévisionnelle d'un agent afin de l'accueillir au mieux et de lui mettre à disposition les moyens/ressources pour travailler au moment de sa prise de poste	DRH/Service recrutement et formation	La communication pour la date d'arrivée prévisionnelle d'un agent n'a pas été faite (absence de coordination et d'organisation pour l'arrivée de l'agent, qui in fine n'a pas les moyens de travailler) /obstacle pour le bon fonctionnement du service ; image de marque impactée	**2**	**3**	**6**	**2**	**12**				
7	1	Organisation de l'arrivée de l'agent par le responsable	RS	Le responsable reçoit le mail de la DRH informant de l'arrivée de l'agent ; le responsable omet partiellement ou totalement de s'organiser pour accueillir l'agent. L'agent ne dispose pas de tous les moyens pour travailler. Perte de temps, dysfonctionnement du service	**2**	**3**	**6**	**2**	**12**				
18	1	Préparation d'un téléphone portable	FR	Il n'y a pas de téléphone portable disponible.	**2**	**3**	**6**	**2**	**12**				La gestion est assurée par le service intérieur et sous réserve que le responsable de service respecte le délai entre la commande et la livraison.
27	1	Récupération des badges	Service carrière et traitement	Les badges ne sont pas rendus ou désactivés.	**2**	**2**	**4**	**3**	**12**	Proposition de transférer la tâche au service intérieur			Au niveau de services centraux les badges ne sont pas tous rendus. Pour autant les badges sont bornés dès que la date de départ de l'agent est connu. Au niveau des UG les badges sont récupérés et réutilisés pour un nouvel agent arrivant.

35	1	Vidéosurveillance	Division des Marchés Publics et Conventions/Direction du numérique	Absence ou retard de l'étude et de la coordination entre service pour assurer la continuité de la sécurité des biens et des personnes sans rupture de contrat	**2**	**3**	**6**	**2**	**12**				Risque de rupture de contrat possible. Risque technique : minime car la probabilité que le parc des caméras tout site confondu tombe en panne au même moment est très faible. Si une intervention est nécessaire il sera fait appel à un prestataire dans le cadre de la commande publique hors marché public. Risque financier : les interventions et dépenses hors marché public doivent être limitées dans le temps et ne pas dépasser le seuil correspondant aux principes fondamentaux de la commande publique (raison pour laquelle la cotation de l'impact a été estimée à 3).
52	1	Préparation téléphone portable et badges d'accès physiques	Service intérieur	La responsable du service intérieur n'a pas de binôme ou de suppléance	**2**	**2**	**4**	**3**	**12**				Officialiser la suppléance en cas d'absence. Le suivi Excel n'est tenu que par la responsable du service intérieur (NB : Base sur internet SFR disponible).
8	1	Traitement du Ticket Cesir pour ouvrir/modifier les droits d'accès SI	Cesir	La vérfication de la qualité du demandeur n'est pas faite et les droits d'accès sont accordés.	**1**	**5**	**5**	**2**	**10**				Le risque peut être lié à la confidentialité d'une information et/ou à un enjeu pour l'établissement : raisons pour lesquelles l'impact a été estimé à 5. Sensibilisation de l'équipe de techniciens. Procédure à formaliser en vue de vérifier la qualité du demandeur des droits d'accès et sécuriser le circuit de validation + relayer la demande auprès des gestionnaires d'applications le cas échéant.
17	1	Préparation des badges d'accès physiques	Métroscop	Les badges paramétrés ne sont pas remis à la personne chargée de les réceptionner	**1**	**5**	**5**	**2**	**10**				Le personnel de Métroscop a été formé pour vérifier les personnes habilitées.
4	1	Paramétrage du badge de pointage	DRH/Service carrière et traitement ou UG	L'absence de suppléance pour paramétrer le badge peut engendrer un retard sur la déclaration horaires de l'agent et sa régularisation. Perte de temps	**2**	**2**	**4**	**2**	**8**				Chaque responsable est en mesure de paramétrer le badge. Un pas à pas est disponible sur l'intranet.
5	1	Paramétrage du badge de pointage	DRH/Service carrière et traitement/UG	Omission de paramétrer un badge pour un agent devant pointer	**2**	**2**	**4**	**2**	**8**				Chaque responsable veille à ce que l'agent puisse badger dès sa prise de fonction.
6	1	Paramétrage du badge de pointage	DRH/Service carrière et traitement	Il n'y a plus de badge en stock. Retard pris sur la déclaration horaires de l'agent et sa régularisation. Perte de temps	**2**	**2**	**4**	**2**	**8**				La gestion du stock est tenue et l'anticipation de commandes est faite.
20	1	Badges physiques (ascenseur)	Métroscop	Métroscop n'a plus de badges d'accès et/ou l'outil métier de paramétrage dysfonctionne ou ne fonctionne plus et/ou il n'y a plus de personnel d'accueil	**1**	**4**	**4**	**2**	**8**				Risques extérieurs - A minima le personnel du Crous est solidaire pour pallier à ces possibles dysfonctionnements.
33	1	Revue annuelle des habilitations	Direction du Numérique/RSSI	Les gestionnaires d'applications en interne n'ont pas de suppléant	**1**	**4**	**4**	**2**	**8**				
34	1	Revue annuelle des habilitations	Direction du Numérique/RSSI	Les gestionnaires d'applications en externe n'ont pas de suppléant	**1**	**4**	**4**	**2**	**8**	Risque extérieur non maîtrisé			Risque extérieur maîtrisé par le Cnous qui pilote un réseau de 26 Crous.
2	1	Mise à disposition du dossier agent pour sa prise en charge en paie	DRH/Service recrutement et formation	Le dossier agent n'a pas été déposé sur le Drive RH en partage avec le service carrière et traitement. Il n'est pas identifié comme personnel appartenant au Crous et ne pourra pas a minima avoir des habilitations SI.	**2**	**3**	**6**	**1**	**6**				
9	1	Traitement du Ticket Cesir pour ouvrir/modifier les droits d'accès SI	Cesir	Omission de traiter la demande formulée	**1**	**3**	**3**	**2**	**6**				Suivi assuré dans l'outil indiquant le degré d'avancement de la demande et avec un délai de traitement de 48H de la demande. Des contrôles de supervision sont faits de façon ponctuelle par le RSSI.

11	1	Préparation d'un PC portable	Equipe de techniciens D°Numérique/Directeur du Numérique	Il n'y a plus de pc portable de disponible	**1**	**3**	**3**	**2**	**6**				La gestion est assurée avec un travail d'anticipation (le délai d'environ d'un mois entre la commande et la livraison est pris en considération pour répondre aux besoins) et un inventaire est suivi.
15	1	Préparation des badges d'accès physiques et clés électroniques	FR	Il n'y a plus de badge et de clé en stock. L'agent ne peut accéder à son lieu de travail	**1**	**3**	**3**	**2**	**6**				Stock toujours maintenu et si dysfonctionnement d'une clé la solidarité entre collègues y pallie. La mise en place d'un référentiel profils et des demandes par écrit pour les droits d'accès par des personnes habilitées par la DG sécuriseraient les accès.
16	1	Préparation des badges d'accès physiques (y compris les badges parking)	DUG/Dug adjoint	Il n'y a plus de badge en stock. L'agent/l'étudiant ne peut accéder à son lieu de travail	**1**	**3**	**3**	**2**	**6**				Stock au niveau de l'UG, du patrimoine et à défaut commande faite auprès du fournisseur. Pour le parking : stock et paramétrage assuré par le prestataire de service.
24	1	Récupération du téléphone portable, des badges, de la clé électronique	Service formation/Service intérieur	Absence de garantie que l'agent ait retiré (totalement ou partiellement) les moyens mis à sa disposition ou que les moyens aient été mis à sa disposition (totalement ou partiellement)	**1**	**3**	**3**	**2**	**6**				
25	1	Récupération des badges	DUG/Dug adjoint	Absence de garantie que l'agent/l'étudiant ait retiré (totalement ou partiellement) les moyens mis à sa disposition ou que les moyens aient été mis à sa disposition (totalement ou partiellement)	**1**	**3**	**3**	**2**	**6**				Les UG sont informées de l'arrivée d'un agent ou d'un étudiant et l'outil métier permet d'assurer une traçabilité des utilisateurs et de leurs droits.
14	1	Bonnes pratiques informatiques de l'utilisateur	Direction du Numérique	Il n'y a pas de charte informatique	**1**	**5**	**5**	**1**	**5**				Une charte informatique existe. Il convient de s'assurer qu'elle soit signée par l'ensemble du personnel, et conservée.
13	1	Préparation d'un PC portable	Equipe de techniciens D°Numérique	Absence de garantie que l'agent ait retiré (totalement ou partiellement) les moyens mis à sa disposition ou que les moyens aient été mis à sa disposition (totalement ou partiellement)	**1**	**2**	**2**	**2**	**4**				Dans un premier temps le responsable hiérarchique direct de l'agent fait une demande via un ticket sur Cesir pour mettre à disposition un PC portable. Un suivi est assuré dans l'outil indiquant le degré d'avancement de la demande et avec un délai de traitement de 48H de la demande. Des contrôles de supervision sont faits de façon ponctuelle par le RSSI. Un mail est envoyé au responsable de l'agent par l'équipe de techniciens informatiques pour informer que le pc portable est disponible. Lors de la remise du pc portable à l'agent, une attestation est établie et signée par les parties respectives. 1 exemplaire est destiné à l'agent un autre exemplaire est conservé en version papier à la direction du numérique et classé par ordre alphabétique.
21	1	Préparation du "Package logistique" (badges, téléphones)	Service intérieur	Absence de garantie que l'agent ait retiré (totalement ou partiellement) les moyens mis à sa disposition ou que les moyens aient été mis à sa disposition (totalement ou partiellement)	**1**	**2**	**2**	**2**	**4**				Attestation mise en place.
23	1	Récupération du PC portable	Direction du Numérique	Le PC rendu n'est pas vérifié (présence du disque dur, du non formatage du pc, de son état de fonctionnement…)	**1**	**2**	**2**	**2**	**4**				Suivi d'un inventaire avec état et ancienneté du PC pour mise au rebut quand cela est nécessaire.
26	1	Récupération du téléphone portable, de la clé électronique	Service intérieur	Le téléphone portable rendu n'est pas vérifié (état de fonctionnement…). Les clés ne sont pas désactivées.			**0**		**0**				Situation non encore rencontrée
	56												