

	Procédure	
	PS03-PR0001 Procédure de gestion des données informatiques	I.E. :6

Détails du document		
Mat. Superviseur	Superviseur	Processus
000031	Lauriane Marie LE FLOUR	Gestion du Système d'Informations

Historique de l'évolution du document		
I.E.	Date	Justification de la MAJ
1	14/11/2017	Création
2	06/03/2019	Révision suite à révision du processus
3	29/10/2019	Révision suite à audit
4	09/11/2020	Révision annuelle
5	05/10/2021	Modification
6	07/05/2024	Modification

Liste des documents de renvoi		
Code	Désignation	Type

Liste des rédacteurs				
Nom\Prénom	Fonction	Signature	Date de Validation	Heure
Lauriane Marie LE FLOUR	Directrice des Opérations		18/04/2024	16:51:49

Liste des vérificateurs				
Nom\Prénom	Fonction	Signature	Date de Validation	Heure
Khadidiatou NAKOULIMA	Présidente		07/05/2024	09:10:58

Liste des approbateurs				
Nom\Prénom	Fonction	Signature	Date de Validation	Heure
Lauriane Marie LE FLOUR	Directrice des Opérations		07/05/2024	09:24:23

Objet de la procédure

Cette procédure a pour objet de décrire les dispositions de la gestion des données numériques. Elle vise à assurer que l'ensemble des connaissances sous forme numérique soit sécurisé, intègre et cohérent. Le SI doit également faciliter le partage de l'information tout en contrôlant les accès.

Domaine d'application

Les dispositions s'appliquent à tous les utilisateurs du SI de NEST.

Responsabilité

Le pilote doit s'assurer de l'application et du respect de cette procédure.

Référence

Norme ISO 9001 V 2015

Description du mode opératoire

Sécurité

Un antivirus est installé sur l'ensemble des postes et serveurs avec une mise à jour automatique via internet.

La mise à jour automatique du système d'exploitation est activée sur les postes de travail.

Les postes de travail pertinents et les serveurs sont secourus par des onduleurs et un groupe électrogène (ou batteries) qui relaient en cas de coupure d'électricité.

Stockage

Les applications CRM/BI, Eyone, Odoo, Icare et Qualipro ainsi que la messagerie électronique sont hébergées en Cloud sur des serveurs sécurisés.

Les autres fichiers de travail partagés (Excel, Word, Powerpoint, etc...) sont stockés sur Dropbox ou Drive.

Sauvegarde

La sauvegarde automatique des serveurs Cloud et des postes de travail pertinents est activée, sur le Cloud.

Gestion des accès

Tous les postes critiques sont protégés par un mot de passe et seuls les utilisateurs agréés en ont connaissance.

Pour les applications CRM/BI, Icare, Eyone et Odoo, ainsi que pour Dropbox ou Drive, seuls les utilisateurs agréés disposent d'un compte avec un identifiant et un mot de passe.

Les responsables d'activité, en accord avec la Direction, définissent les droits d'accès et les transmettent à la cellule informatique pour mise en œuvre. Les droits sont définis en fonction des profils et des responsabilités des utilisateurs.

Ainsi, les utilisateurs n'ont accès qu'aux informations pour lesquelles les droits leur ont été accordés par le pilote ou le super administrateur.

Maintenance

La maintenance des équipements sous garantie est assurée par le fournisseur.

Le technicien informatique est responsable de toute autre maintenance ainsi que du support utilisateur, en collaboration avec la chargée des opérations.

Incidents

Les incidents sont gérés au fur et à mesure qu'ils surviennent. En cas d'incident, une analyse de la situation est faite et les dispositions sont prises pour corriger les dysfonctionnements.

Pour les cas nécessitant une restauration, la dernière sauvegarde est utilisée après remplacement de l'équipement ou reconstitution de l'environnement de travail.