POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION (PSSI)

La PSSI, associée à la charte des utilisateurs, reflètent la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information. Elle est conforme aux dispositions législatives et réglementaires et cohérente avec les politiques et directives de niveau supérieur (ministérielles et interministérielles).

Cette PSSI s'applique au CRHEA. Elle se fonde, par ses aspects généraux sur les règles PSSI du CNRS du 02/10/2013 de F. Morris et L. Di Benedetto définies ici : https://extra.core-cloud.net/collaborations/RSSI-CNRS/Lists/PSSI%20rgles/AllItems.aspx et sur la PSSI d'état de l'ANSSI définie ici : https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/.

Le directeur d'unité :

Le DU est responsable de la sécurité des systèmes d'information (SSI) dans son unité et nomme une personne chargée de la SSI (CSSI) pour l'assister en la matière. Le DU est responsable du suivi du bon respect des règles en matière de protection des données à caractère personnel pour l'ensemble des traitements dont son unité est responsable. Le DU s'assure de la mise en œuvre de moyens de prévention visant à interdire la consultation et la diffusion de messages à caractère violent, pornographique ou de nature à porter atteinte à la dignité humaine.

Personnels :

- La sensibilisation à la SSI doit être réalisée à l'ensemble des personnels de l'unité.
- Toute dérogation aux règles de cette PSSI doit être validée par le DU avec avis motivé.
- Le personnel entrant dans l'unité doit être accueilli suivant une procédure d'accueil formalisée qui inclut la prise de connaissance de la charte SSI et des règles élémentaires de sécurité informatique avant l'ouverture des accès sur le SI. Le personnel sortant de l'unité doit être connu de l'équipe informatique qui applique une procédure de départ formalisée incluant la fermeture des droits sur le SI et la restitution des matériels appartenant à l'unité.
- Les personnes qui ne font pas partie du personnel doivent prendre connaissance des règles SSI de l'unité avant toute connexion au SI de l'unité

Utilisation des ressources :

- La gestion des traces de l'activité des systèmes informatiques suit les directives nationales et les traces générées par les systèmes informatiques sont centralisées et stockées sur 12 mois glissants.
- Les logiciels (OS, applications, etc.) utilisés par le personnel doivent faire partie de la liste des logiciels autorisés par le CSSI de l'unité.
- Seuls les comptes individuels (non partagés) sont autorisés pour l'identification préalable à l'accès aux ressources informatiques (postes de travail, systèmes d'information, etc.).

Description des ressources :

Le CRHEA met à disposition de ses utilisateurs un réseau informatique dont la grande majorité des postes et serveurs sont interconnectés dans un Domaine « CNRS-CRHEA ». Le CRHEA se charge de fournir à chacun de ses utilisateurs des postes raccordés à ce domaine.

Dès leur arrivée, les utilisateurs ayant une durée d'activité au laboratoire supérieure à 3 mois ont la possibilité de demander l'ouverture d'un compte de domaine et d'obtenir des adresses de courriel. Les utilisateurs s'engagent à ne pas perturber et entraver les mises à jour automatiques des systèmes d'exploitations et anti-virus des postes qui leur sont confiés.

Les entreprises hébergées de longue durée utilisent leurs ressources informatiques propres et ont accès à internet à travers des réseaux dédiés (selon acceptation du DU) ou le réseau wifi « Visiteur » du laboratoire.

Le CRHEA met à disposition des visiteurs ou stagiaires de moins de 1 mois un réseau wifi « Visiteur » sécurisé et indépendant des réseaux du laboratoire. Il donne accès à internet.

Les utilisateurs ayant un compte de domaine du CRHEA peuvent accéder à certaines ressources du laboratoire de l'extérieur moyennant des règles de sécurité obligatoires comme l'utilisation d'un poste de travail fourni par le laboratoire et équipé des règles en vigueur (Anti-virus, firewall, VPN installés et configurés par le service informatique du laboratoire). Les personnels du CRHEA souhaitant faire du télétravail sont soumis aux mêmes règles.

Suivant les directives imposées par le CNRS, les postes de travail doivent, sauf dérogations décidées par le DU, avoir des disques chiffrés avec le logiciel Veracrypt imposé par la position de ZRR du CRHEA. Les postes portables ont obligation d'être

chiffrés. Les utilisateurs du domaine souhaitant se rendre à l'étranger ont la possibilité de demander le déchiffrage de l'ordinateur pendant leurs séjours en acceptant de le vider de toutes données scientifiques et personnelles sensibles et relatives au laboratoire.
Le CRHEA fournit des adresses mails pour chaque personne ayant un compte de domaine. Les courriels sont accessibles via un logiciel fourni dans les postes ou par accès Webmail dont le lien est sur le site internet de l'unité. Le CRHEA met en place des outils de filtrage Exchange pour les courriels indésirables. Ces courriels sont automatiquement sauvegardés et consultables par les utilisateurs.

Protection des données personnelles :

Toutes les données personnelles conservées au CRHEA sont soumises aux lois RGPD (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679) décrites dans le formulaire disponible sur le site intranet du CRHEA. Il doit être lu et signé par chaque utilisateur. Ces données personnelles sont consultables et modifiables par leurs propriétaires à tout moment.

Fait au CRHEA (Valbonne) le 13/06/2019

Signature du directeur d'unité