Fiche informatique

❖ Sécurisation du poste de travail

- Ne consultez pas les données sur un ordinateur d'accès public.
- Évitez la consultation des données sur votre téléphone portable.
- Verrouillez votre ordinateur (ou votre session sur un ordinateur familial) par un solide mot de passe, strictement personnel. Limitez l'accès des personnes à votre ordinateur.
- Si vous devez vous absenter, ne laissez pas votre ordinateur accessible à tous (mettez-le en veille, éteignez-le…)

- Vérifiez que le pare-feu de votre ordinateur soit actif ; à défaut installez-en un.
- Assurez-vous d'avoir un anti-virus sur votre ordinateur et actualisez-le régulièrement.
- Attention à la consultation sur certains sites internet pouvant être malveillant, mettez en place un bloquer (Adblock, AntiSpam…)
- Ne téléchargez pas d'application ou programme non-issus d'un site officiel (Play store ; Apple store…).

❖ Transmission et suppression des données

❖

- Privilégiez votre mail étudiant et les supports externes (clé USB, DVD…).
- N'ouvrez pas les spams ou publicités douteuses.
- Évitez les envois de groupe ; ayez recours à la copie cachée lors des envois groupés.
- Privilégiez un espace d'échange sécurisé (Cloud notamment…).
- Pensez à vider votre corbeille après un acte de suppression.

❖ Conservation et archivage des données

- Privilégiez la conservation des données sur un réseau sécurisé (cloud notamment).
- Pensez à flouter vos vidéos et brouiller vos audios après analyse.
- Dans la mesure du possible, anonymisez vos données avant de les conserver ou archiver.
- Définissez des modalités d'accès spécifiques aux données archivées.
- Faites une copie des données déconnectée du support principal (par exemple sur une clé USB, un disque externe, un autre ordinateur…), verrouillée par un mot de passe.
- En cas d'utilisation d'un ordinateur familial, faites attention de bien enregistrer le ficher sur votre session personnelle.
- Verrouillez les fichiers sensibles par un mot de passe.
- Veilliez à avoir des mots de passe différents pour les types de verrouillage (session/fichier/copie).

En cas de vol, perte, fuite de données, vous devez prévenir le plus rapidement possible le délégué à la protection des données de l'UPJV.