Au cours de l’implémentation du projet ESP, notre équipe s’est engagée à respecter certains standards de cybersécurité. La mise en place de ces mesures aura vocation à protéger l’entreprise ainsi que les utilisateurs de vols de données ou de denis de services (DOS).

A noter que ce document ne traitera que le sujet de la prévention de cyber-attaques et non celui de la cyber-résilience (Ce sujet sera traité dans la disaster recovery plan).

**Définition de la confidentialité :**

Chaque fichier ou production écrite produits par les membres de l’équipe de l’ESP devra se voir assigné un niveau de confidentialité. La liste ci-dessous décris les conditions d’attribution d’un niveau de confidentialité à une information.

Publique :

* Le partage de ce genre d’information a un impact très faible ou nul sur l’entreprise (Ex : publicité, communication à la communauté). Ces informations peuvent être partagés avec n’importe qui

Interne :

* Le partage de ce genre d’information a un impact faible ou modéré sur l’entreprise (Ex : évènements de team building…). Ces informations peuvent être partagés avec n’importe quel employé de l’entreprise

Confidentielle :

* Le partage de ce genre d’information a un impact fort sur l’entreprise (Ex : rapports de réunion, études de marchés…etc). Ces informations ne doivent être partagé qu’avec les membres de votre équipe

Secret:

* Le partage de ce genre d’information a un impact très fort sur l’entreprise (Ex : rapport de tests d’intrusion, stratégie non divulguée). Le principe du privilège amoindri s’applique sur ce genre d’informations.

**Politique de mots de passe**

Afin de rendre plus difficile le travail d’un attaquant qui essaierais de compromettre le compte d’un utilisateur, nous avons défini la politique de mot de passe suivante :

* Les mots de passe devraient contenir au moins 12 charactères (15 pour un administrateur) contenant (au moins) une majuscule, une minuscule, un nombre et un symbole.
* Les mots de passe ne devraient pas contenir de mots contenus dans le champ lexical de l’entreprise.
* Les mots de passe ne devraient pas contenir de suite de charactères facilement visible sur le clavier.
* Les mots de passe devront être hashés avant d’être stocké dans la base de données

**Cryptographie**

Toute information classé confidentielle ou secret devra être chiffré en utilisant un algorithme de cryptographie robuste avant d’être stocké.

Toute communication se faisant sur le réseau devra être chiffrée.

**Audits de sécurité**

Chaque année, l’entreprise se doit d’auditer la sécurité d’un capital donné si celui-ci est exposé sur internet ou qu’il à été jugé comme étant critique pour le bon fonctionnement de la société.

Cela dit, un capital doit être audité suite à une mise à jour majeure