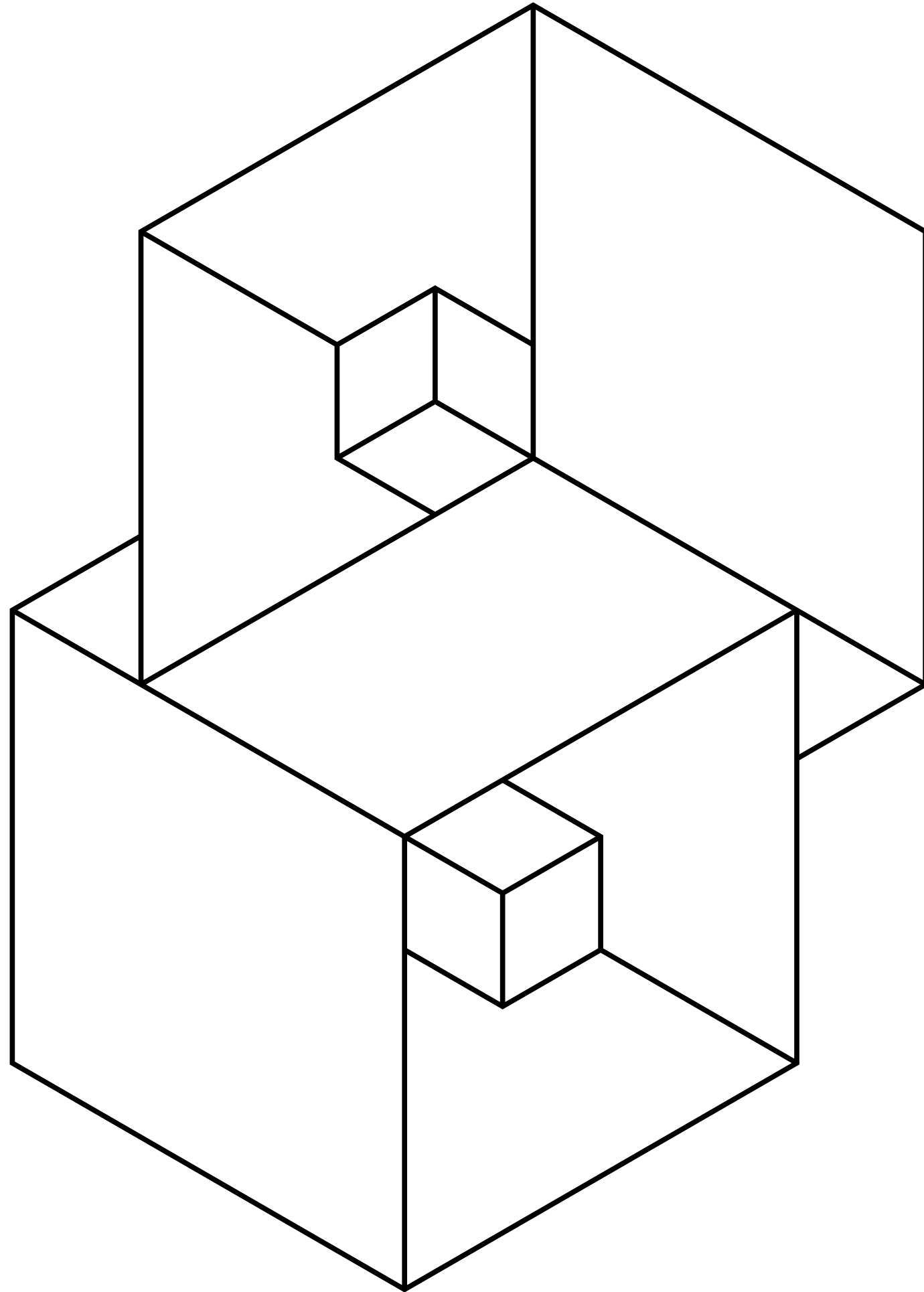




# **TP2- Mise en place des bonnes pratiques BYOD**

**FERRAND Tobias  
DRIEUX Valentin**





1)Établissez une liste d'outils potentiellement utilisables afin de sécuriserleur poste informatique.

1) Antivirus et Antimalware :

Norton, McAfee, Bitdefender, Malwarebytes

2) Pare-feu :

Windows Defender Firewall, ZoneAlarm, pfSense

3) Gestionnaires de mots de passe :

LastPass, 1Password, Bitwarden

4) Cryptage des données :

VeraCrypt, BitLocker (pour Windows), FileVault (pour macOS)

5) Logiciels de sauvegarde :

Acronis True Image, Backblaze, EaseUS Todo Backup

6) Outils de mise à jour automatique :

Ninite, Patch My PC

7) VPN (réseau privé virtuel) :

NordVPN, ExpressVPN, CyberGhost

# Liste d'outils et de logiciels qui ne peuvent être présents sur leur poste informatique.

## 1. Logiciels de piratage et d'intrusion

- Metasploit
- Aircrack-ng
- Cain & Abel

## 2. Applications de torrent

- uTorrent
- BitTorrent

## 3. Logiciels de gestion des mots de passe non sécurisé

- Gestionnaires de mots de passe sans chiffrement solide.

#### 4. Applications de communication non sécurisées ou non professionnelles

- Discord (pour usage personnel)
- Skype (si non configuré de manière sécurisée)

WhatsApp (non adapté pour des communications professionnelles)

#### 5. Logiciels non officiels ou cracks

#### 6. Jeux et logiciels de divertissement

- Jeux vidéo divers (ex. Steam, Epic Games).





# **Quels outils de communication allez-vous utiliser sur les postes informatiques ? Détaillez et précisez**

**Nous avons choisi talkspirits  
comme outils de communication**

---

Talkspirit protège les données et la pour l'entreprise. accessible sur divers ce qui facilite le centralisation des outils de communication favorise une meilleure organisation dans les échanges

# Politique de Sécurité des Mots de Passe



- 1 Longueur Minimale du Mot de Passe  
(entre 8 et 12 caractère minimum)
- 2 Complexité des Mots de Passe:
  - Majuscules (A-Z)
  - Minuscules (a-z)
  - Chiffres (0-9)
  - Caractères spéciaux (par exemple, ! @#\$%^&\*)
- 3 Changement Régulier des Mots de Passe
- 4 Authentification à Deux Facteurs (2FA)



Comment allez-vous sensibiliser vos utilisateurs à l'usage du BYOD ?

Il faut sensibiliser les utilisateurs sur la sécurité de leurs données, mettre des mots de passe de minimum 12 caractères sur leur poste de travail. Expliquer les règles d'utilisation, les applications autorisées et les procédures à suivre s'il y a un vol ou une perte de l'ordinateur. Effectuer les mises à jour du poste ou des logiciels. Ne pas mettre ensemble les données personnel et professionnel.



Quelles ressources allez-vous distribuer ?

Les ressources que nous allons utiliser sont le webinaire et des ateliers pour répondre aux questions et agrandir leurs cultures en informatique aux différents utilisateurs.

# bonne pratique personnel et professionnel



## Personnel

## professionnel

### Usage exclusif professionnel

Ne pas utiliser les applications ou équipements professionnels pour des activités personnelles comme les réseaux sociaux, les achats en ligne, etc.

### Stockage de données

Il est important de ne pas stocker les fichiers personnels et professionnels sur un même support pour éviter les risques de perte, d'attaques ou de fuites de données sensibles. La séparation facilite aussi la gestion des fichiers et garantit la conformité avec les normes de sécurité. Cela assure une meilleure protection des informations et optimise l'organisation.

### réseaux sociaux

Utiliser les réseaux sociaux sur un PC personnel permet de rester connecté avec des amis et la famille, de partager des moments de vie et d'accéder à du contenu varié et divertissant.

### réseaux sociaux

Dans un environnement professionnel, les réseaux sociaux servent à renforcer la visibilité de l'entreprise, à interagir avec les clients et à développer des relations professionnelles, tout en favorisant le marketing et la communication.

### fond d'écran

Changer de fond d'écran au travail peut être interdit pour maintenir un environnement professionnel et éviter les distractions. Cela préserve également l'image de l'entreprise.

### Navigation responsable

Éviter de visiter des sites non sécurisés ou douteux qui pourraient compromettre la sécurité de l'appareil personnel utilisé aussi pour le travail.