

Aubrée Romain

29/11/2025

Sotoca

Groupe 1

## **Atelier 10 TP 1**

<b>FICHE PRÉPARATOIRE : RÔLE ANIMATEUR</b>	<b>2</b>
<b>DÉROULEMENT DE LA RÉUNION</b>	<b>3</b>
<b>LIVRABLES (PACKAGE GSB)</b>	<b>3</b>
<b>CONCLUSION</b>	<b>4</b>

# **1. FICHE PRÉPARATOIRE : RÔLE ANIMATEUR**

Contexte et Mission : Suite à l'infection virale causée par une clé USB, je dois convaincre le Comité de Direction d'adopter des règles plus strictes. Mon défi est de faire accepter ces contraintes de sécurité à des directeurs (Recherche, Opérations) qui ont peur que cela ralentisse leur travail.

## **Arguments principaux :**

- L'enjeu économique : Si on se fait voler nos données R&D (brevets, molécules), c'est l'avenir de GSB qui est menacé par la concurrence.
- Les obligations légales : On n'a pas le choix vis-à-vis des normes FDA et EMA. Si on ne peut pas tracer qui a copié quoi, on risque de lourdes sanctions lors du prochain audit.
- La production : Un virus pourrait mettre à l'arrêt nos chaînes de production, ce qui coûterait très cher.

## **Anticipation des blocages :**

- Pour la Recherche : Je sais que le Directeur aura peur pour ses délais. Je prévois de lui proposer une alternative : passer par un Cloud sécurisé plutôt que par des clés USB.
- Pour les Opérations : Pour éviter de bloquer les techniciens externes, je proposerai l'installation de bornes de décontamination ("stations blanches") à l'entrée des zones sensibles.

## **2. DÉROULEMENT DE LA RÉUNION**

Synthèse des échanges : J'ai commencé la réunion en rappelant les faits récents, en veillant à ne braquer personne mais en insistant sur les risques.

La discussion a été animée, notamment avec le Directeur de la Recherche qui était fermement opposé au blocage des ports USB, craignant pour l'innovation. J'ai dû faire preuve de diplomatie et lui garantir que le transfert de fichiers via le Cloud serait mis en place pour son équipe. Le Directeur des Opérations a soulevé des problèmes pratiques sur le terrain. Nous nous sommes mis d'accord sur une période de transition pour former ses équipes. Heureusement, j'ai pu compter sur le soutien de la Responsable Qualité, pour qui la sécurité informatique est devenue incontournable pour valider nos certifications.

Conclusion : Le comité a validé le plan : fin des clés perso et passage aux clés chiffrées fournies par l'entreprise.

## **3. LIVRABLES (PACKAGE GSB)**

### **A. Note de service**

Objet : Sécurisation des échanges de données. Constat : L'utilisation de périphériques personnels représente aujourd'hui une faille critique pour l'entreprise (virus, fuite de données). Décisions actées :

Interdiction d'utiliser des clés USB personnelles sur le réseau GSB.

Mise à disposition de clés professionnelles sécurisées (chiffrées) pour les collaborateurs qui en ont l'utilité.

Alternative : L'usage du portail documentaire sécurisé doit devenir la norme pour les transferts de fichiers.

### **B. Email aux collaborateurs**

De : Service DSI À : L'ensemble du personnel Objet : Important : Évolution de la politique de sécurité (Clés USB)

Bonjour à toutes et à tous,

Pour protéger nos travaux de recherche et rester conformes à la réglementation, nous devons renforcer notre sécurité informatique. À partir du 15 décembre, les clés USB personnelles ne seront plus détectées par vos ordinateurs.

Pas d'inquiétude : si vous avez besoin d'échanger des fichiers pour votre travail, le support informatique peut vous fournir une clé sécurisée GSB sur simple demande. Merci de votre compréhension et de votre vigilance.

L'équipe DSI.

### **C. Mise à jour de la Charte Informatique**

Modification de l'Annexe 4 concernant les supports amovibles :

Article 4 (Révisé) :

4.1 : Il est strictement interdit de connecter des supports de stockage personnels (clés, disques durs) au matériel de l'entreprise.

4.2 : Seuls les périphériques fournis et inventoriés par la DSI sont autorisés.

4.3 : Tout support externe provenant d'un tiers doit obligatoirement être analysé sur une station blanche avant utilisation.

### **D. Planning de déploiement**

Semaine 1 : Communication interne et commande du matériel.

Semaine 2 : Phase pilote avec le service R&D (utilisateurs prioritaires).

Semaine 3 : Formation des managers et distribution des clés.

Semaine 4 : Blocage technique effectif des ports USB.

## **Conclusion**

Le TP m'a appris qu'au-delà de la technique, la communication est la clé pour concilier les intérêts divergents des directeurs. J'ai réussi à faire valider le projet en proposant des solutions alternatives plutôt que de simples interdictions. C'est une expérience très formatrice sur la posture professionnelle à adopter en entreprise.