

Thème du groupe 5 :

# Répondre aux exigences en matière de sécurité et de confidentialité des données

- ✓ Identifier les risques potentiels et les garanties pour protéger les données aéronautiques sensibles
- ✓ se conformer aux lois sur la protection des données dans différents pays africains.

## Répondre aux exigences en matière de sécurité et de confidentialité des données

2

▀ Membres du Groupe 5 :

N°	NOMS	PAYS
1	DEANCE KAZADI ILUNGA	RD CONGO
2	PAULIN TABU KALUFANDO	RD CONGO
3	TOTO ASSI PASCAL	COTE D'IVOIRE
4	BANAKINAO WIYAO	TOGO
5	MOUHAMED EL HACEN AHMED DEDDE	MAURITANIA
6	JOSE DAVID FERNANDES	CABO VERDE
7	CHAKIR IHSSANE	MOROCCO
8	AMETH DIOUF	SENEGAL
9	NGUIE NIETCHE DISRAELY	CONGO

## ➡ SOMMAIRE

- Définition de la donnée
- Types de données
- Risques potentiels des données
- Moyens de protection de données

- Définition de la donnée

Les données sont un ensemble d'informations (de faits ou de valeurs) quantitatives ou qualitatives définies, recueilli auprès de différentes sources et qui est utilisé pour la prise de décision.

### ○ Types de données

#### Au nombre de 4

Types	Définition	Exemple
<b>Publiques (non protégées)</b>	Données ouvertes à tout public sans restriction.	Données de trafic (passagers, mouvement d'aéronefs et fret)
<b>A diffusion restreinte</b>	Données destinées à une liste d'entités ou de personnes préalablement établie.	Informations relatives à un vol non régulier, licence de personnel,...
<b>Confidentielles</b>	Données à accès restreint soumises à un code d'accès.	Données personnelles de passagers (nom et prénoms, itinéraire, adresse, passeport, numéro de téléphone...), l'identité de PNC sur un vol, données financières des exploitants...
<b>Top secret (secret défense)</b>	Données hautement confidentielles relevant de la sécurité de l'Etat.	Informations sur le vol d'Etat (présidentiel, militaire...), statistiques de transports des armes et équipements militaire, ...

## ○ Risques potentiels des données

### ❖ **Législation**

- absence d'une législation relative à la classification et à la gestion des données sensibles
- Absence de procédures de travail
- Absence de définition du niveau d'autorisation (droit d'accès, des lieux de sécurisation,...)
- Absence d'une entité en charge de la protection des données sensibles

### ❖ **Personnel**

- Absence ou Insuffisance du personnel qualifié en matière de protection de données
- Inadéquation de profil

### ❖ **Formation**

- Absence de programme et de plan de formation pour le maintien et le développement de compétences du personnel en matière de protection de données.
- Absence de modules de formation appropriés à la protection de données
- Absence de culture de protection de données sensibles

○Risques potentiels des données (suite)

❖ Equipements

- Absence d'infrastructures adéquates (bâtiments et locaux)
- Absence du matériel
- Absence de logiciels authentifiés
- Absence de réseaux informatiques sécurisés
- cyberattaques



## ○ Moyens de protection de données

### ❖ **Législatif et réglementaire**

- Elaborer des lois et règlements relatifs à la classification et à la gestion des données sensibles
- Elaborer des procédures de travail
- Définir les niveau d'autorisation (droit d'accès, des lieux de sécurisation,)
- Mettre en place une instance nationale en charge de la protection des données sensibles

### ❖ **Personnel**

- Doter l'institution en charge de la gestion de données du personnel qualifié.

### ❖ **Formation**

- Elaborer un programme et plan de formation pour le maintien et développement de compétences du personnel
- Concevoir les modules de formation appropriés à la protection de données
- Promouvoir une culture de protection de données sensibles



○ Moyens de protection de données (suite)

❖ Equipements

- Mettre en place des infrastructures adéquates (bâtiments et locaux)
- Doter l'institution des outils (logiciels et matériel) nécessaire à la protection de données
- Absence de authentifiés
- Mettre en place des réseaux informatiques sécurisés
- Mise en place de protocoles de chiffrement avancés.
- Authentification multi-facteurs pour l'accès aux systèmes.
- Surveillance continue et audits de sécurité réguliers.

### Actions recommandées

- Effectuer une **cartographie des risques** spécifiques aux données aéronautiques.
- Se conformer aux **normes internationales** comme le **RGPD** et les réglementations locales.
- Collaborer avec les **autorités de protection des données** pour garantir une mise en œuvre efficace.
- Mettre en place des **protocoles de gestion des incidents** pour réagir rapidement en cas de violation.

**MERCI DE VOTRE AIMABLE ATTENTION**