MINISTÈRE
CHARGÉ
DES TRANSPORTS

Liberté
Égalité
Fraternité

dgac direction générale de l'Aviation civile
DSAC

GUIDE DE CONCEPTION DE SESSIONS DE SENSIBILISATION CYBERSECURITE

Direction de la sécurité de l'aviation civile
Direction de programme cybersécurité
Édition nº 1
Version nº 1 du 3 septembre 2021

Gestion documentaire

Historique des révisions

Edition et version	Date	Modifications
Ed1v1	3 sept. 2021	Création du document

Approbation du document

Nom	Responsabilité	Date	Visa
Pierre **ABDOULHADI** Adjoint à la directrice de programme cybersécurité – DSAC / DP-Cyber	Rédacteur	3 sept. 2021	Ok
Emmanuelle **PERILLAT** Adjointe au chef du pôle performance – DSAC / DT-SUR	Vérificateur*	3 sept. 2021	Ok
Anne **FRISCH** Directrice de programme cybersécurité – DSAC / DP-Cyber	Approbateur	3 sept. 2021	OK

*La vérification concerne la cohérence du contenu du document avec les dispositions actuelles et futures en matière de formation sûreté.

Pour tout commentaire ou suggestion à propos de ce cadre de conformité cyber France, veuillez contacter la direction de programme cybersécurité de la DSAC à une des adresses suivantes :

- anne.frisch@aviation-civile.gouv.fr ;
- pierre.abdoulhadi@aviation-civile.gouv.fr.

Sommaire

1. Objet du document

L'objet du présent document est de guider les opérateurs dans la conception de sessions de sensibilisation prévues par le règlement (UE) n° 2015/1998 [1].

Ce document définit :

- les objectifs principaux d'une sensibilisation ;
- les éléments à intégrer lors de la conception des sessions, pour pouvoir atteindre ces objectifs.

2. Objectifs de résultat

A l'issue de la sensibilisation, les personnes ont :

- la connaissance des enjeux cybersécurité ;
- la connaissance des objectifs et moyens mis en œuvre ;
- la connaissance des règles et bonnes pratiques à adopter.

3. Conception des sessions de sensibilisation

Lors de la conception d'une session de sensibilisation, l'opérateur en adapte le contenu en fonction :

- des menaces pesant sur les missions critiques[1] au regard de la sûreté qu'il réalise ;
- des populations visées, notamment :
  - leur fonction ;
  - leur rôle ;
  - leur responsabilité ;
  - leur besoin d'en connaître.

Concernant le format des sessions de sensibilisation, l'opérateur :

- les dispense :
  - en présentiel, ou ;
  - à distance, ou ;
  - en *e-learning* ;
- veille à ce que celles-ci durent au moins 30 minutes ;
- les dispense au moins 1 fois tous les 3 ans pour chaque personnel visé.

A l'issue des modules de sensibilisation, l'opérateur peut réaliser une évaluation des connaissances.

L'opérateur est en mesure de montrer sa démarche de sensibilisation et de démontrer son efficacité au regard des objectifs définis ci-dessus.

[1] Fonctions critiques à la sûreté du transport aérien [2]

4. Contenu de la sensibilisation : Lignes directrices

Afin d'accompagner l'opérateur dans la conception d'une session de sensibilisation, le présent guide identifie, pour chaque objectif, des lignes directrices qui constituent le socle minimal des sujets à aborder.

4.1. Objectif 1 : Connaissance des enjeux cybersécurité

Afin de mieux appréhender les enjeux liés à la cybersécurité, l'opérateur :

- introduit la cybersécurité en illustrant le sujet au travers d'exemples actualisés ;
- apporte un éclairage au sujet des différentes menaces [3] existantes et pouvant peser sur son organisation ;
- fait prendre conscience des enjeux de l'opérateur en matière de cybersécurité, en précisant notamment :
    - les exigences règlementaires auxquelles il est soumis, à savoir la protection des systèmes d'information critiques au regard de la sûreté, ainsi que la défense et le rétablissement de ces derniers en cas d'attaque ;
    - les conséquences d'une attaque sur son activité et celle des autres opérateurs avec lesquels il est interconnecté.

4.2. Objectif 2 : Connaissance des objectifs et moyens mis en œuvre

L'opérateur fait connaître :

- les objectifs de sécurité qu'il s'est fixés ;
- son organisation en matière de cybersécurité pour contribuer à atteindre ces objectifs ;
- les moyens mis en œuvre, participant à la sécurité des systèmes d'information.

4.3. Objectif 3 : Connaissance des règles et bonnes pratiques à adopter

L'opérateur fait :

- prendre conscience à tous les personnels du rôle qu'ils ont à jouer en tant qu'acteurs et responsables de la cybersécurité ;
- connaitre les règles et consignes de sécurité prévues pour se prémunir d'incidents cybersécurité ;
- connaitre et adopter les bonnes pratiques [4] en matière de cybersécurité, notamment :
    - Les mesures préventives ;
    - Les bons réflexes à avoir en cas de compromission.

Références

[1] *Règlement d'exécution (UE) 2019/1583 de la commission du 25 septembre 2019 modifiant le règlement d'exécution (UE) 2015/1998 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, en ce qui concerne les mesures de cybersécurité*, Union Européenne, Septembre 2019.

[2] *Fonctions critiques au regard de la sûreté du transport aérien,* DSAC, Version 1.0, Septembre 2021

[3] *Cybermenaces, https://www.cybermalveillance.gouv.fr/*

[4] *Bonnes pratiques, https://www.cybermalveillance.gouv.fr/*

Direction générale de l'Aviation civile
Direction de la Sécurité de l'Aviation civile
50, rue Henry Farman
75720 PARIS CEDEX 15
Tél. : +33 (0)1 58 09 43 21
www.ecologie.gouv.fr