Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral du sport OFSPO
Politique du sport et ressources internes

Paolo Dünner, 19.10.2020 **public**

Système central de gestion de la sécurité des informations de l'OFSPO (SGSI)

Annonce des incidents ayant trait à la sécurité

Contrôle du document	
Valable du / au	19.10.2020
Version	2.0
Statut	Autorisé
Type de doc.	Notice
Diffusion	
Propriétaire du document	Häusler Roland OFSPO
Champ d'application	OFSPO
Lieu d'archivage	GRCS

Contrôle

Nom	Rôle	Date/Version
Cyril Stauffer	DISO	08.10.2018
Fritz Amsler	DISO	05.10.2020

Autorisation

Nom	Rôle	Date/Version
Roland Häusler	C IT OFSPO	09.10.2018
Roland Häusler	C IT OFSPO	19.10.2020

Table des matières

1 Introduction

1.1 But et objet

Le présent document vise à informer les collaborateurs, leurs supérieurs hiérarchiques, le Service Desk et d'autres personnes des événements qu'il convient de considérer comme des incidents ayant trait à la sécurité et qu'il faut annoncer.
Les incidents relatifs à la sécurité peuvent être accidentels ou intentionnels. Ils peuvent concerner des personnes, des bâtiments, des systèmes ou des informations. Même les «quasi-incidents», c'est-à-dire les événements qui auraient pu induire un incident ayant trait à la sécurité, doivent être annoncés.

2 Incidents à annoncer

Tout incident ayant trait à la sécurité doit être signalé au supérieur hiérarchique ou, en cas d'urgence, au DISO ou au C Sécurité (et au supérieur hiérarchique ensuite). L'annonce doit être faite

- par téléphone (DISO; C Sécurité; supérieur hiérarchique; selon «Sécurité à l'OFSPO» dans l'Intranet) ou
- par courriel (sicherheit@baspo.admin.ch).

Vous trouverez ci-dessous des exemples d'incidents ayant trait à la sécurité et de vulnérabilités (liste non exhaustive). Tous doivent être signalés immédiatement.

1. **Equipement ou appareils informatiques** endommagés intentionnellement ou volés.
2. Infection au moyen de logiciels malveillants (p. ex. **virus**, vers informatiques, chevaux de Troie).
3. **Informations** confidentielles ou **données personnelles** dignes de protection perdues, volées ou détruites sans autorisation.
4. Sauvegarde sur des **plateformes publiques** (p. ex. dropbox.com) d'informations confidentielles ou de données personnelles dignes de protection.
5. Publication par inadvertance de **données médicales** concernant des athlètes.
6. **Elimination** de supports de données ayant permis à des tiers d'accéder à des données personnelles particulièrement dignes de protection.
7. **Violation de la protection des données** rendue publique, avec probabilité de publications dans la presse.
8. **Menaces** orales ou écrites à l'encontre de clients ou de collaborateurs.
9. Présence de personnes non identifiées ou **non autorisées** dans des espaces sécurisés (p. ex. zone de sécurité).
10. Des personnes non autorisées interrogent des collaborateurs de façon ciblée pour obtenir des informations confidentielles telles que des mots de passe ou des renseignements sur l'infrastructure technique (**ingénierie sociale**).
11. Usage illicite ou blocage de ressources système ou de **systèmes informatiques.**
12. Blocage inexplicable de **données d'accès**.
13. **Contrôles de sécurité** manquants ou **inefficaces** (p. ex. login sans mot de passe).
14. **Violation** de directives, d'instructions ou de prescriptions de sécurité.
15. **Portes ou fenêtres** fracturées.
16. **Dysfonctionnements** graves de logiciels ou de matériel.
17. Découverte d'informations confidentielles ou de données personnelles dignes de protection lors de l'utilisation de **moteurs de recherche** (p. ex. Google).
18. Défiguration de **sites Internet** (p. ex. modification suspecte de l'apparence d'un site Internet connu, ou mauvaise traduction de son contenu).