Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la sécurité alimentaire et des affaires vétérinaires OSAV
Applications métier OSAV

Fiche d'information sur la sécurité informatique pour le Système d'information sur les antibiotiques en médecine vétérinaire (SI ABV)

Remarques générales :

- Les comptes et les accès à SI ABV doivent être protégés. Les tokens générés par SI ABV doivent être tenus secrets, c'est-à-dire qu'ils ne peuvent être consultés et utilisés qu'au sein du cabinet vétérinaire et, le cas échéant, par le fabricant du logiciel de cabinet.
- Les appareils avec lesquels on accède à SI ABV doivent être protégés en conséquence. Maintenez les logiciels et les antivirus à jour.
- Les données doivent être utilisées exclusivement pour l'exercice de sa/ses tâche(s) et être traitées de manière confidentielle, dans la mesure où elles ne sont pas librement accessibles au public.

Sécurité des données :
L'utilisateur est responsable de l'exactitude et de l'exhaustivité des données. Les données sont enregistrées localement sur les appareils du cabinet et ne sont envoyées au serveur que si l'utilisateur actionne "Envoyer". Du côté de l'OSAV, aucune modification ne peut être apportée aux données reçues sur les serveurs. Pour les données locales de SI ABV sur les systèmes de postes de travail, le cabinet est le seul propriétaire des données. L'utilisateur est responsable de la sécurité des données locales (sauvegarde, protection des données, etc., voir : Protection des données / Backup (admin.ch)).

Mises à jour régulières :
Pour garantir la sécurité des données et des systèmes, il faut procéder régulièrement à des mises à jour des systèmes d'exploitation et de la protection antivirus. Voir aussi à ce sujet : Protection des appareils (admin.ch). Les systèmes de SI ABV sont régulièrement mis à jour. Le fonctionnement sûr et correct n'est garanti que pour la version la plus récente.

Protection contre les virus :
Le dernier antivirus et le dernier correctif système doivent toujours être actifs sur les clients.
Par défaut, il est recommandé de désactiver la fonction « autorun » lors de la connexion de supports de données externes. Respectez les consignes pour une utilisation sûre des e-mails : (Gestion sûre du courrier électronique (admin.ch))

Sécurité physique :
Les sessions ouvertes doivent être protégées de l'accès en cas d'absence du poste de travail ; par exemple avec un mot de passe d'économiseur d'écran. L'utilisateur est responsable d'empêcher tout accès non autorisé.

Manipulation des supports de données :
Les données de l'application doivent être effacées lorsque le support de données (ou l'appareil avec support de données) est donné en réparation ou mis au rebut.

Obligation de déclaration :
En cas d'incident lié à la sécurité, le prestataire doit être informé immédiatement sur isabv@blv.admin.ch.

Documentation, formation et soutien
Le manuel de l'utilisateur avec des descriptions détaillées et des aides se trouve sur le site de l'OSAV : Informations sur l'application web SI ABV (admin.ch) *(sous "Informations complémentaires" - "Instructions")*