Guide Vitrolife sur la sécurité et la confidentialité

Pratiques recommandées en matière de cybersécurité

Table des matières

CohortView, CulturePro, EmbryoScope, EmbryoSlide, EmbryoViewer, Guided Annotation, iDAScore et KIDScore sont des marques commerciales ou déposées qui appartiennent au groupe Vitrolife.

©2024 Vitrolife A/S. Tous droits réservés.

1 Introduction

Ce guide explique comment utiliser les produits Vitrolife de la meilleure façon possible en matière de cybersécurité et de confidentialité. Il s'agit donc d'un guide de bonnes pratiques destiné aux utilisateurs du système. L'objectif ? Minimiser les risques liés aux menaces de cybersécurité et protéger les informations personnelles lors de l'utilisation des produits Vitrolife.

Dans ce guide, toutes les références aux incubateurs s'appliquent aux incubateurs EmbryoScope D, CulturePro, EmbryoScope+, EmbryoScope Flex et EmbryoScope 8. Les références aux clients s'appliquent à EmbryoViewer et Vitrolife Technology Hub.

2 Consignes de sécurité générales

Les utilisateurs sont invités à bien lire et comprendre les consignes générales suivantes avant d'utiliser les produits Vitrolife :

- Ne reliez jamais les produits Vitrolife à Internet sans avoir instauré des mesures de sécurité appropriées. Une exposition non autorisée à Internet peut entraîner des cybermenaces et compromettre des données sensibles.
- Protection par pare-feu : Les produits Vitrolife doivent être installés sur un réseau local derrière un pare-feu afin de les protéger contre les menaces extérieures.
- Responsabilité du service informatique de la clinique : Il incombe au service informatique de la clinique de garantir la mise en œuvre de mesures suffisantes en matière de cybersécurité. Les cliniques sont invitées à solliciter des experts locaux en sécurité pour les aider à mettre en place une infrastructure sécurisée.
- Réponse aux incidents : En cas d'incident de cybersécurité, les cliniques doivent rapidement contacter des experts en cybersécurité à des fins d'assistance et de résolution.

3 Pratiques recommandées en matière de cybersécurité

Lors de la configuration ou de l'utilisation des produits Vitrolife, veuillez respecter les pratiques recommandées qui sont énumérées dans cette rubrique. L'objectif ? Minimiser tout risque potentiel pour la sécurité ainsi que garantir la sécurité optimale des données, y compris les informations personnelles, dans la mesure du possible.

3.1 Recommandations générales en matière de cybersécurité

Les utilisateurs sont invités à prendre et devraient prendre les mesures suivantes en vue de réduire les risques de cybersécurité et de garantir que les produits fonctionneront comme prévu dans l'environnement utilisateur prévu :

- S'assurer que le personnel est correctement formé en matière de sensibilisation à la cybersécurité ;
- Empêcher tout utilisateur non autorisé à accéder physiquement aux équipements ;
- Consulter ce guide des pratiques recommandées en vue de réduire les risques liés à la cybersécurité.

Les utilisateurs doivent avertir Vitrolife A/S sans retard indu après avoir pris connaissance d'un incident relatif à une faille de cybersécurité ou de tout événement suspect en matière de sécurité.

3.2 Sensibilisation des utilisateurs à la cybersécurité

Dans l'optique de minimiser les risques de problèmes de sécurité qui sont susceptibles de compromettre le système, les appareils ou les données, y compris les informations personnelles, veuillez respecter les directives suivantes :

- Ne laissez aucune personne non autorisée observer vos actions à l'écran.
- Protégez le caractère personnel de votre compte utilisateur et ne laissez personne voir vos données d'identification.
- Lorsque vous quittez un incubateur ou un poste de travail client, activez la fonction écran de veille et/ou verrouillez l'interface utilisateur.

Les cliniques devraient désigner un collaborateur chargé des questions de sécurité au sein de l'organisation. Cet interlocuteur pourra être sollicité par les utilisateurs s'ils ont des questions ou s'ils constatent un comportement suspect.

3.3 Utilisation des supports portables

Il est recommandé de limiter l'utilisation des supports portables comme les clés USB, les disques durs externes et les cartes mémoire, entre autres. Si vous utilisez des supports portables pour transférer des données, vous devez prendre les mesures de précaution suivantes :

- Vérifiez que les supports portables ne contiennent pas de logiciels malveillants ou de virus avant de les insérer dans un quelconque produit Vitrolife ou un ordinateur exécutant le logiciel Vitrolife.
- Cryptez les données sur les supports portables pour éviter de compromettre les informations personnelles en cas de perte des supports.

- Ne stockez les données sensibles que dans des endroits sûrs.
- Supprimez le contenu des données du support portable après le transfert des données.
- N'utilisez jamais de supports portables d'origine inconnue.

3.4 Ordinateurs reliés à Internet

Les produits Vitrolife peuvent être connectés à un réseau avec accès à Internet, mais il faut prendre des mesures de précaution afin d'éviter toute exposition à des cybermenaces provenant de sites distants. Dans l'optique de minimiser le risque d'intrusion non autorisée dans le système et ses données :

- Configurez la connexion Internet avec les dernières fonctionnalités de sécurité logicielles disponibles, par exemple un pare-feu, des systèmes de surveillance du réseau et de détection des intrusions, entre autres, conformément aux recommandations du service informatique de la clinique.
- Assurez-vous qu'un logiciel antivirus et antimalware fiable a été installé à des fins de protection contre les logiciels malveillants.
- Respectez systématiquement les recommandations de Vitrolife concernant la mise à jour régulière du système d'exploitation avec les derniers correctifs de sécurité.
- Instaurez un accès restreint à Internet.
- Évitez tout accès inutile à des sites Internet qui ne sont pas strictement liés au travail.

3.5 Administration des utilisateurs et mots de passe

Veuillez respecter les directives suivantes afin de garantir que seule l'utilisation autorisée du système et des ressources est permise :

- Ne configurez que le nombre requis d'utilisateurs (comptes utilisateur) dans le système.
- Si un compte utilisateur est amené à ne plus être utilisé, supprimez-le totalement du système.
- N'utilisez pas de comptes utilisateurs partagés. Chaque compte doit être individuel et rattaché à une seule personne.
- Limitez le niveau d'accès d'un compte utilisateur à ce dont l'utilisateur a besoin pour effectuer son travail.
- Assurez-vous que le mot de passe d'un compte utilisateur est strictement confidentiel et unique à chaque utilisateur.
- Appliquez une politique imposant un changement régulier du mot de passe.
- Activez la protection par mot de passe dans la configuration du BIOS intégré de l'ordinateur, surtout si l'ordinateur est accessible à d'autres utilisateurs.
- Utilisez des mots de passe forts (au moins huit caractères comprenant des lettres en majuscule et en minuscule, des chiffres et au moins un caractère spécial).

- Utilisez des mots de passe faciles à retenir pour les utilisateurs.
- Ne consignez jamais les mots de passe à l'écrit.

3.6 Versions logicielles et maintenance logicielle

Maintenez tous les logiciels à jour :

- Maintenez le logiciel du système d'exploitation Windows à jour conformément aux recommandations de Vitrolife pour chaque PC installé dans la clinique.
- Assurez-vous que Windows Update est activé sur tous les PC opérant sous Windows.
- Respectez les recommandations de Vitrolife consistant à effectuer des mises à jour régulières des logiciels dans le cadre de l'entretien et de la maintenance.
- N'installez aucun logiciel sur les PC sans avoir obtenu l'autorisation de Vitrolife.

3.7 Interfaces utilisateur

Prenez les mesures de précaution suivantes afin de protéger les informations sensibles :

- Configurez l'interface utilisateur de sorte qu'elle se verrouille automatiquement (ex. : activation de l'écran de veille).
- Déconnectez-vous du logiciel lorsque vous ne l'utilisez pas activement.
- Activez la déconnexion automatique de Windows après une certaine période d'inactivité.

3.8 Sécurité physique et configuration de l'appareil

Les directives suivantes s'appliquent à la sécurité physique et à la configuration des appareils :

- Les ordinateurs clients sont connectés au serveur ES server via un réseau LAN. Reliez tous les incubateurs en utilisant un réseau local sans connexion à Internet.
- Évitez tout accès aux dispositifs de réseau dans des lieux publics où des personnes non autorisées (hostiles) sont susceptibles de trouver un moyen d'entrer dans le système via leur connexion réseau.
- Assurez-vous que seul le personnel autorisé accède physiquement à la zone du laboratoire, si possible. Toute personne non autorisée doit être surveillée.
- Pour tous les dispositifs dotés de la connectivité Bluetooth, activez cette fonction uniquement si elle est nécessaire au fonctionnement du dispositif.
- Désactivez toute forme de chargement ou d'exécution automatique de quelque forme que ce soit sur tous les dispositifs en cas d'insertion ou d'ajout de supports portables.
- Ne laissez aucun dispositif dans un état non sécurisé en l'absence d'une quelconque surveillance.

4 Coordonnées

Besoin d'aide en urgence ? Contactez notre service d'assistance téléphonique :

+45 7023 0500

(disponible 24 heures/24, 7 jours/7)

E-mail de l'assistance technique : support.embryoscope@vitrolife.com

(réponse en 2 jours ouvrables)

Vitrolife A/S
Jens Juuls Vej 16
DK-8260 Viby J
Danemark

Téléphone : +45 7221 7900

Site Web : www.vitrolife.com

VITROLIFE A/S, DANEMARK