

PREREQUIS TECHNIQUES ET SECURITE DES SYSTEMES D'INFORMATION

Afin de préserver l'intégrité du Système d'Information et garantir au maximum sa sécurité contre les attaques externes et internes, il est primordial d'appliquer les bonnes pratiques de sécurité informatique de l'entreprise.

L'ensemble des règles en vigueur en matière de sécurité informatique à l'Ineris est détaillé dans la PSSI¹ (Politique de Sécurité des Systèmes d'Information) et dans la charte informatique.

Tous les matériels, logiciels et processus associés fournis par le prestataire doivent donc respecter les principes définis et dont les principaux sont exposés ci-dessous.

- Les principaux prérequis à respecter pour accéder au réseau informatique de l'Ineris sont les suivants :
 - **Pas d'utilisation, sur une machine, de comptes avec droits d'administration** (en cas de besoin de déroger à cette règle, l'Ineris dispose d'une surcouche logicielle permettant la gestion de la granularité des droits sur des applicatifs définis) ;
 - **Dernière version disponible du système d'exploitation Windows 10 LTSC** (Long Term Service Channel – variant support long-terme de Windows 10 Enterprise. Une nouvelle version est mise sur le marché tous les 2 à 3 ans. Chaque nouvelle version LTSC peut bénéficier des mises à jour de sécurité Microsoft pendant 10 ans après sa sortie. Aucune mise à jour de fonctionnalités n'est implémentée afin de ne pas altérer la compatibilité avec les logiciels installés) ;
 - **Utilisation d'un antivirus à jour** (McAfee Endpoint Security) ;
 - **Intégration à l'annuaire Active Directory de l'Ineris** – application des paramètres de sécurité des postes de l'Ineris (GPO) ;
 - **Utilisation d'un certificat machine pour l'accès au réseau** (norme d'authentification 802.1x) ;
 - **Respect de la politique de mots de passe².**

- Il est également capital de porter une attention particulière sur les points suivants :
 - **Mise à jour des logiciels** (contrats de maintenance) ;
 - **Mise à jour de l'OS** (gestion de l'obsolescence du système d'exploitation – montées de version de Windows 10) ;
 - **Utilisation de comptes nommés** (pas de comptes génériques) ;
 - **Confidentialité des mots de passe ;**
 - **Limitation au strict nécessaire et contrôle de l'utilisation des supports de stockage amovible.**

Cas des ordinateurs destinés au pilotage d'instruments de laboratoires

Pour permettre aux utilisateurs de l'Ineris de disposer des accès réseaux nécessaires à leurs travaux, les machines de pilotage doivent respecter les contraintes de sécurité définies ci-dessus.

Pour garantir le bon fonctionnement des ordinateurs de pilotage dans une configuration compatible avec les systèmes d'information de l'Ineris, il est nécessaire de procéder à la vérification du bon fonctionnement des ordinateurs de pilotage et de traitement fournis au travers du marché dans une configuration validée par la DSI de l'Ineris.

Pour cela, l'Ineris propose 2 possibilités :

- Machine standard³ fournie par l'Ineris (recommandé) :
 - Le prestataire définit les caractéristiques techniques de la machine ;
 - L'Ineris approvisionne lui-même la machine ;
 - L'Ineris configure cette machine comme une machine Ineris standard ;
 - L'Ineris envoie cette machine au prestataire qui installe alors la solution logicielle destinée à piloter l'appareil ;
 - Lors de la mise en service dans les locaux de l'Ineris, le bon fonctionnement est vérifié sur cette machine, alors conforme et intégrée au Système d'Information de l'Ineris.
- Machine spécifique³ fournie par le prestataire :
 - Le prestataire envoie à l'Ineris l'ordinateur au moins 3 semaines avant la date d'installation prévue ;
 - L'Ineris configure cette machine pour la doter des logiciels de l'Ineris et l'intégrer à son réseau ;
 - Si besoin, l'Ineris renvoie la machine au fournisseur pour valider la configuration avec l'instrument ;
 - Lors de la mise en service dans les locaux de l'Ineris, le bon fonctionnement est vérifié sur cette machine, alors conforme et intégrée au Système d'Information de l'Ineris.

A l'issue des opérations d'installation, une validation formelle et conjointe Ineris / Fournisseur, du bon fonctionnement de l'ensemble et de sa compatibilité avec les exigences Ineris sera réalisée.

⇒ Cette validation formelle conditionnera le paiement de la prestation.

1 – PSSI : Politique de Sécurité des Systèmes d'Information ➔ VDOC (DI-1353)

2 – Politique de mots de passe ➔ VDOC (DI-1365)

3 – Machine standard / spécifique ➔ Une machine dite "standard" est caractérisée par des performances et une connectique comparables à celles d'un poste de travail bureautique habituellement fourni par la DSI. La connectique est considérée comme spécifique dès lors qu'il n'est pas possible de répondre au besoin par la simple entremise de convertisseurs USB, ou que le nombre de ports requis dépasse les capacités maximales d'une machine standard.