**ATTESTATION SUR L’HONNEUR**

Je soussigné : prénom + nom de la personne responsable de l’entreprise (autorité d’homologation)

Qualité : compléter

Société : compléter

***Marché :*** compléter

***Certifier*** *que, dans le cadre du marché indiqué ci-dessus, les dispositions de protection des données sensibles et plus particulièrement des supports ou informations portant la mention « diffusion restreinte » (DR) ont été appliquées au niveau de notre système d’Information (SI) en tenant compte des textes suivants :*

* *Instruction interministérielle relative à la protection des systèmes d’information sensibles n° 901/SGDSN/ANSSI ;*
* *Recommandations pour les architectures des systèmes d’information sensibles ou diffusion restreinte.*

***Avoir vérifié*** *que :*

* *Les supports ou informations à caractère sensible portant notamment la mention diffusion restreinte (DR) sont préservés de tout risque de vol, divulgation ou perte ;*
* *Les collaborateurs devant avoir accès aux SI sensibles ont pris connaissance de l’instruction interministérielle 901 et les recommandations de l’ANSSI ;*
* *Les éventuelles prestataires extérieurs ayant à intervenir sur le ou les postes de travail sensibles (informaticien, administrateur système, etc.) connaissent et maîtrisent l’instruction interministérielle 901 et les recommandations de l’ANSSI. A ce titre et dans le cadre de maintenance ou mise à jour de logiciel, je m’engage à fournir à l’administration la méthodologie d’intervention du prestataire, respectant l’intégrité des données sensibles de niveau DR.*

***Avoir identifié*** *et accepté les risques résiduels ne pouvant pas être couverts par la mesure de protection de mes systèmes d’information sensibles (art. 8 de l’II 901),*

***M’engager*** *à rendre compte au plus vite à l’administration de tout événement anormal survenu avec un support ou information DR en ma possession (perte, vol, tentative d’hacking, etc.).*

*La présente attestation est valable du 00/00/0000 au 00/00/0000 (Durée du contrat ou 5 ans).*

*Fait pour servir et valoir ce que de droit.*

*Fait à ………..……, le : Signature et qualité de l’autorité d’homologation*

*de l’entreprise :*

Pièce jointe :

* *Méthodologie de protection des données sensibles de l’entreprise*

**Méthodologie de protection des données sensibles**

**de l’entreprise**

(A joindre à l’attestation)

Le présent document permet à l’entreprise de décrire de manière exhaustive à l’administration sa méthodologie de protection des données sensibles pendant la durée d’exécution du marché (personnes, traitement et matériel).

Le but étant de permettre à l’officier de sécurité des systèmes d’information (OSSI) de l’ESID de Brest de comprendre l’architecture informatique de votre entreprise et établir la décision d’homologation.

Objectif et contexte

*Le Poste dédié au stockage et l’exploitation des informations sensibles est constitué indiquer le nombre de postes de travail et s’il s’agit d’ordinateurs fixes ou portables. Il ou ils sont exclusivement dédiés au traitement d’informations « diffusion restreinte » par les personnels, dûment habilités et formés, de la société nom.*

Procédure de traitement des données DR

*Les données sensibles doivent faire l’objet d’une attention particulière.*

*Le schéma suivant décrit la procédure de traitement des fichiers à mention DR depuis internet jusqu’au poste SI sensible de l’entreprise :*

**Fichier DR transmis par l’administration avec cryptage ACID**

Envoi par email ou sur la plateforme d’échange MERLIN CRYPTOBOX

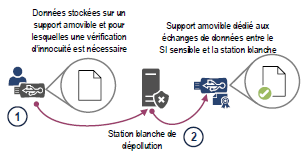
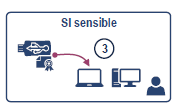
**Transit du fichier DR sur MERLIN CRYPTOBOX dans un répertoire dédié au projet**

(accès limité aux seuls membres)

Fichier récupéré par l’entreprise mais laissé en archive ACID

**SI usuel**

(poste de travail connecté à internet)



Fichier DR exploitable (après extraction ACID) sur le poste informatique DR isolé de tous réseaux.

**Précaution d’emploi en cas de d’ordinateur portable (nomade) :**

Chiffrage de l’équipement.

**Disque dur externe**

(nomade)

***Chiffrement au choix :***

*P1 Chiffrement complet du disque dur*

*P2 Chiffrement des fichiers uniquement*

Procédure de vérification de l’archive ACID au moyen de 2 clé USB distinctes et 1 sas antivirus

(« station blanche » isolée de tous réseaux)

Architecture

*Le poste de travail est composé des équipements suivants :*

* *Décrire la station blanche, passerelle de vérification antivirus (isolée de toute connexion réseau ou internet).*
* *Décrire le ou les postes de travail DR (isolée de toute connexion réseau ou internet) ;*
* *Décrire les autres équipements tels que disque dur de stockage de données (isolés de toute connexion réseau ou internet) ;*
* *Préciser que 2 clés USB clairement reconnaissables seront associées au transfert des données (code couleur par exemple) :*
  + *1 exclusivement dédiée à transférer les documents cryptés par ACID depuis le poste de travail équipé d’internet vers la station blanche ;*
  + *1 exclusivement dédiée à transférer les documents cryptés par ACID depuis la station blanche vers le poste de travail DR.*

Utilisation normale

*Dans les phases d’utilisation normale du poste de travail dédié DR (préciser le nombre de postes), celui-ci n’est connecté à aucun réseau filaire ou sans-fil.*

Contre-mesures

*L’ordinateur sera utilisé sans connexion réseau. Ainsi, la probabilité d’une attaque provenant d’Internet ou d’un réseau tiers est fortement abaissée.*

*Afin de limiter la perte de confidentialité des informations stockées sur l’ordinateur, l’ordinateur sera durci selon les bonnes pratiques de sécurité informatique de l’Instruction interministérielle n° 901 et des recommandations de l’ANSSI.*

*Deux niveaux de chiffrement seront mis en place :*

* *Chiffrement de l’ordinateur et du disque dur amovible (en cas de stockage externe) par le logiciel CRYHOD, afin de protéger l’ensemble des données contenues ;*
* *Chiffrement des fichiers par logiciel et clé ACID CRYPTOFILER, afin de protéger les données de niveau DR lors de transferts ou d’envoi internet.*

Maintenance et audit technique (si prévu dans l’entreprise)

* *Identifier ici au choix :*
  + *L’informaticien de votre entreprise (à déclarer à l’administration si inconnu) ;*
  + *Le prestataire extérieur (à déclarer à l’administration si inconnu).*
* *Préciser (ou via le prestataire) la méthode de maintenance de l’ordinateur ou de mise à jour des logiciels du poste de travail sensible.*
* *A confirmer avec votre informaticien : aucune connexion ne sera faite via internet. Les mises à jour (sous forme de fichiers EXE) seront transférées depuis le SI usuel selon la méthode décrite dans le schéma*

En cas de doute de votre entreprise ou du prestataire sur la méthode à appliquer, vous pouvez contacter l’ESDI de Brest qui sollicitera son réseau d’experts cyber et SSI.

*Logiciel de chiffrement et antivirus*

*Afin de garantir la sécurité des données et des équipements de travail, l’entreprise installera les logiciels suivants :*

* ***Station blanche :***
  + *Antivirus : SOPHOS (fourni par l’administration) ;*
* ***Poste de travail DR :***
  + *Chiffrement de l’ordinateur : CRYHOD ;*
  + *Chiffrement des données : ACID CRYPTOFILER (fourni par l’administration) ;*
  + *Antivirus : TREND MICRO APEX ONE (fourni par l’administration).*
* ***Support de stockage nomade :***
  + *Chiffrement du disque dur : CRYHOD ;*
  + *Chiffrement des données : ACID CRYPTOFILER.*

*Risque résiduel ne pouvant pas être couverts par la mesure de protection des systèmes d’information sensibles (art. 8 de l’instruction interministérielle 901),*

*A compléter si nécessaire (sera étudié par l’OSSI).*

*Précision complémentaire*

*Vous pouvez ici ajouter tout autre point qui vous semble indispensable ou important à déclarer.*