**CHARTE DE BONNE CONDUITE CYBER**

La société %nom\_de\_la\_société% est titulaire du marché %nom\_de\_l’opération% pour le compte de l’SID Méditerranée. Certains documents ou informations étant sensibles, tous les intervenants s’engagent à respecter la présente charte de bonne conduite Cyber. Elle est communiquée individuellement à chaque utilisateur.

* Système d’information dédié à l’opération :

Le système d’information (SI) destiné à l’élaboration, au traitement et au stockage des informations pour l’opération citée en préambule doit être dédié et non raccordé à l’internet si le SI est défini diffusion restreinte.

Les données techniques sont conservées dans des conditions garantissant leur intégrité et leur confidentialité.

* Mention de protection « DIFFUSION RESTREINTE » :

La mention « DIFFUSION RESTREINTE » n’est pas un niveau de classification mais une mention de protection, dans certain cas elle est complétée par la mention complémentaire « Spécial France ».

Elle permet à un détenteur de l’information de le sensibiliser sur le besoin d’en connaître et de son devoir de discrétion. Si la mention complémentaire est utilisée, l’information ne devra pas être connue par un personnel étranger.

Dès que des documents contiennent des informations sensibles, il conviendra de faire porter la mention « DIFFUSION RESTREINTE » sur ces dits documents. A minima, l’ensemble des documents techniques doivent porter cette mention de protection.

* Conservation des documents papiers avec mention de protection :

Les documents portant une mention de protection ne doivent pas être en accès libre sur un réseau informatique ou sur un bureau. Ils seront conservés dans des meubles ou rangement les protégeant de la vue, sur un lecteur informatique ayant des droits d’accès particuliers, ou seront chiffrés.

S’ils sont sous format papier, ils seront détruits sous la responsabilité des détenteurs par lacération.

* Transmission des documents « DIFFUSION RESTREINTE » :

Le transfert de document ou d’information électronique protégé vers le SID Méditerranée, qu’il transite par internet ou non, doit être chiffré par le logiciel de chiffrement ACID V7 ou ZED ENTREPRISE. La communication du mot de passe (pour la solution ZED ENTREPRISE) se fera systématiquement par un moyen différent que celui utilisé lors de la transmission du fichier.

Dans le cas d’une transmission par courrier postal, les documents devront être envoyés sous double enveloppe. L’enveloppe intérieure portera la mention DIFFUSION RESTREINTE et la référence du document tandis que l’enveloppe extérieure ne comportera que les indications nécessaires à la transmission du courrier.

* Emploi de média amovibles :

Aucun support amovible personnel comme de l’entreprise ne pourra se connecter sur un ordinateur, réseau ou équipements du Ministère des Armées.

Si un transfert de données doit être réalisé, un personnel qualifié du ministère des armées fera l’échange des données sur un support amovible étatique via une station de décontamination dite station blanche.

Aucune donnée ne pourra être manipulée si la station blanche relate une détection virale.

* Emploi d’un ordinateur de maintenance :

L’utilisation de moyens professionnels extérieurs au ministère des armées est en principe interdite. Dans le cadre d’une exception, elle est soumise au respect de procédures de contrôle.

Par conséquent, si l’opération de maintenance exige l’emploi d’un ordinateur, l’utilisateur devra établir un certificat d’innocuité de moins de 24h (annexe 2). Ce certificat sera valable uniquement pour l’opération de maintenance citée et devra être remis au responsable de l’installation qui, aux vues des informations fournies, autorisera ou non son emploi.

* Incident de cybersécurité :

Tout incident de cybersécurité, quel que soit sa nature, doit être relaté immédiatement au point de contact Cyber du titulaire du marché ainsi qu’à l’accompagnant défense si l’incident se produit dans une enceinte militaire. Des mesures conservatoires doivent être prises afin de protéger le système d’information.

Je suis informé que l’usage de l’équipement informatique et les réseaux mis à ma disposition sont réservés à un usage professionnel

* Audits et contrôles SSI

Le représentant du pouvoir adjudicateur (RPA) doit pouvoir, à tout moment, procéder à des audits ou contrôles des systèmes industriel d’infrastructure mis en place.

Ils pourront être réalisés par le RPA directement, ou délégués à un tiers. Le RPA se réserve le droit de requérir l’expertise d’un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

L’audit ou contrôle sera notifié au titulaire 15 jours ouvrés à l’avance minimum, par email, sauf dans le cadre d’un incident de sécurité critique, pour lequel l’urgence nécessitera une intervention sans délai.

A charge du RPA de fournir les différents éléments de l’intervention à la société en charge du marché.

**Par cette signature, je reconnais avoir été informé des règles de cette charte de bonne conduite Cyber, avoir reçu une sensibilisation SSI de la part de mon entreprise et par conséquent, je m’engage à respecter ce document.**

**Nom : Prénom :**

**Société :**

**Lieu : Date :**

**Signature :**