Cluster protection Niger

Protocole de partage des informations sur la protection des données entre les membres et partenaires du cluster protection Niger

RAISONNEMENT

Assurer la confidentialité et la protection des données et des informations entre les partenaires concernés intervenant dans le domaine de la protection et le cluster protection.

OBJECT

Ce protocole de partage des informations a pour but d'établir les principes directeurs et de présenter les procédures à suivre pour partager et recevoir les informations du cluster protection.

PRINCIPE DE BASE ET ENGAGEMENT

- Les informations et les données ne doivent être partagées que dans le respect des principes de la responsabilité des données dans le domaine de la protection contenus dans les directives du Cluster protection sur la responsabilité des données ;
- Les informations ne doivent être partagées que conformément aux directives du IASC sur la gestion, le partage et la confidentialité des informations ;
- Les membres du cluster protection/ et ses partenaires doivent s'assurer que les données et les informations partagées par le cluster protection se sont communiquées qu'au personnel qui sont autorisés à le recevoir conformément à la conduite de leurs fonctions officielles sur la base du besoin du savoir ;
- Les membres du cluster protection et ses partenaires utiliseront / partageront toujours les informations de manière à reconnaître la sensibilité associée à la protection et à respecter le besoin de confidentialité et d'anonymat ;
- Lors du partage d'informations sensibles, la partie expéditrice est responsable de la classification des informations partagées. Elle doit à ce titre indiquer si celles-ci peuvent être à nouveau partagées et avec qui (sur la base de la classification de la sensibilité des données) afin de garantir que le ou les destinataires (s) adoptent les mesures appropriées et éviter toute compromission de la sensibilité ou divulgation inappropriée ;
- Les destinataires d'informations sensibles ou de données classées selon la classification de sensibilité sont chargés de stocker ces informations ou données en extrayant et en protégeant les informations qui ne peuvent pas être partagées avant leur partage.

SECURITE ET PROTECTION DES DONNEES

Pour assurer la confidentialité et la protection des données, cette partie décrit les diverses mesures de sécurité des données et informations partagées par le cluster protection :

- Les membres du cluster protection/ et ses partenaires doivent s'assurer que les données et informations sont protégées en tout temps et gardées en sécurité. Cela peut être assuré en installant un logiciel anti-virus à jour pour éviter la corruption et la perte d'informations. La sauvegarde de la ou les bases de données pertinentes et des

informations importantes devrait être effectuée sur une base régulière sans échec et une copie de sauvegarde doit être stocker à distance

- Les membres du cluster protection/ et ses partenaires doivent s'assurer que le (s) personnel (s) n'enregistrent pas les données sur les ordinateurs personnels et que les données ne peuvent être partagées que par courrier électronique officiel
- Les membres du cluster protection/ et ses partenaires doivent s'assurer que les ordinateurs doivent se verrouiller automatiquement si l'utilisateur est éloigné de la machine. S'assurer que les ordinateurs doivent avoir une protection par mot de passe forte. En outre s'assurer que le mot de passe doit être changé à intervalles réguliers
- Les membres du cluster protection/ et ses partenaires doivent s'assurer que les lecteurs réseaux partagés par défaut doivent toujours être désactivés
- Les membres du cluster protection/ et ses partenaires doivent s'assurer que les fichiers de cas électroniques, y compris les feuilles Excel avec des informations d'identification et des fichiers exportés à partir d'une base de données, doivent être protégés par un mot de passe à l'aide des mots de passe fournis par l'expéditeur (à partager confidentiellement dans un courrier électronique séparé) et stockés dans un endroit sécurisé
- Afin d'assurer et de respecter la confidentialité, les données doivent toujours être transférées uniquement par l'utilisation de moyens de communication protégés (avec un mot de passe, après un scanning anti-virus etc.)
- Les informations propres des bénéficiaires/survivantes et pouvant permettre de les identifier ne seront pas communiquées (ex : nom, initiales, date de naissance, etc.).

Les membres du clusters protection.et ses partenaires s'engagent à ne pas modifier le fichier reçu d'un autre membre sans l'autorisation explicite de ce membre en forme écrite et sans l'autorisation de la personne concerné.

VIOLATIONS DU PROTOCOLE ET RESOLUTION DES LITIGES

En cas de violation du présent protocole par l'un des membres participants, une réunion extraordinaire sera convoquée pour tous les membres dans un délai de dix jours afin de discuter de la violation et d'élaborer une résolution. Si une réunion complète n'est pas possible dans les dix jours ou si aucune résolution ne peut être trouvée, le responsable du cluster protection tiendra une réunion pour déterminer la marche à suivre. Si nécessaire, un interlocuteur externe peut être contacté pour faciliter la discussion et la résolution. Le cluster protection peut cesser de partager des données si le protocole est enfreint et informeront par avance les membres du cluster protection des raisons pour lesquelles ils ont interrompu le flux de données. La résolution d'une violation ou d'une violation présumée doit être approuvée par tous les membres du cluster.