framatome

Engagements Fournisseurs Framatome en matière de Sécurité informatique

1. Accès au système informatique de l'Acheteur

Pour tout accès au système informatique de l'Acheteur, le Fournisseur s'engage à respecter, tant pour lui-même que pour son personnel, toutes les conditions de sécurité propre à l'exécution de la Commande, telles que notamment les conditions d'accès en vigueur dans le Site concerné et au système informatique de l'Acheteur, dont il a eu communication par écrit et dont il a pris connaissance avant toute intervention.

Le Fournisseur n'est autorisé par l'Acheteur à accéder au système informatique de l'Acheteur que pour les besoins d'exécution de la Commande.

Le Fournisseur s'engage à n'utiliser d'autres logiciels que ceux qu'il aura communiqués à l'Acheteur et qui auront été autorisés par ce dernier. Le Fournisseur prendra toutes les précautions nécessaires pour éviter d'introduire un "virus" informatique dans les logiciels, mises à jour et nouvelles versions fournis à l'Acheteur, et adoptera les mesures adéquates s'il constate l'existence d'un tel virus.

2. Incident de Cybersécurité

2.1 S'entend par incident de cybersécurité tout évènement résultant d'une action volontaire ou involontaire, impactant ou pouvant impacter de façon dommageable le système d'information ou les données que le système traite, stocke ou transmet, et qui requiert une réponse afin d'en mitiger les conséquences (« **Incident de Cybersécurité** »).

2.2 Le Fournisseur s'engage à prendre toutes les précautions et mesures qu'il juge nécessaires et suffisantes pour ne pas générer, faciliter ou induire d'Incident de Cybersécurité dans les [Prestations] et/ou dans le système d'information de l'Acheteur auquel il a accès.

En outre, en cas d'accès et/ou d'utilisation illicite ou non-autorisé(e) du système d'information de l'Acheteur, en cas de suspicion d'un tel événement, et/ou en cas d'Incident de Cybersécurité, le Fournisseur a l'obligation d'en alerter le CERT Framatome (Computer Emergency Response Team- Email : it.security@framatome.com - Téléphone : (+33) 1 34 96 96 95) ainsi que l'acheteur dédié dont les coordonnées figurent sur la commande, dès qu'il en a connaissance et au plus tard un (1) jour calendaire suivant l'Incident de Cybersécurité.

Toute notification d'Incidents de Cybersécurité à l'Acheteur doit préciser :

- Les coordonnées de l'interlocuteur IT qualifié du Fournisseur
- la date de début d'incident
- le périmètre du service impacté,
- les données impactées
- les indicateurs de compromission (mail, exploitation d'une faille réseau ou autre, le vecteur de propagation)
- tout autre élément utile à la remédiation et à l'investigation de l'incident par le Fournisseur.

Jusqu'à la clôture de l'Incident de Cybersécurité, le Fournisseur a l'obligation de :

- Prendre sans délai toutes les mesures adaptées et nécessaires comme par exemple et sans que la liste qui suit soit exhaustive :
  - Prendre les mesures de confinement afin de limiter le périmètre et les conséquences de l'Incident ;
  - Prendre les mesures d'éradication de la menace des systèmes d'information par i) la suppression des codes malicieux, des comptes ou des accès inappropriés, du patching des vulnérabilités etc. qui sont à la source de la compromission, et /ou ii) la mise à jour de solutions de sécurité ou le renforcement des systèmes et infrastructures IT, pour empêcher l'utilisation de tactiques, techniques et procédures utilisées dans les cyberattaques ; et
- Tenir le CERT de l'Acheteur au courant par écrit et de manière régulière de la résolution de d'Incident de Cybersécurité et de toute information s'y rapportant.

l'Acheteur pourra apporter son support dans la mesure du possible et sur demande raisonnable du Fournisseur pour aider à la résolution de l'incident de Cybersécurité.

Le Fournisseur doit notamment établir et documenter un Retour d'Expérience de l'Incident de Cybersécurité permettant l'enregistrement des informations relatives à cet incident.

S'entend par « **Retour d'Expérience »** un rapport d'incident identifiant le vecteur de compromission de l'incident et la bonne application de mesures techniques/organisationnelles garantissant la remédiation.

Le Retour d'Expérience doit être communiqué par le Fournisseur au CERT Framatome à la clôture de l'Incident de Cybersécurité.

En cas d'incident dont l'introduction ou la transmission serait imputable au Fournisseur, ce dernier est responsable des conséquences de tous dommages causés à l'Acheteur dans les limites de l'article responsabilité des Conditions Générales d'Achat.

2.3 En cas d'accès et/ou d'utilisation illicite ou non-autorisé(e) du système d'information du Fournisseur, ou en cas de suspicion d'un tel événement, le Fournisseur s'engage à alerter l'Acheteur d'un tel événement par écrit et dès qu'il en a connaissance à compter de son constat et/ou de toute notification adressée à ou reçue d'une autorité dont il dépend directement ou indirectement.