Exigences minimales de cybersécurité applicables aux achats

Version du 21 juillet 2026

1. Objet

La confidentialité et la résilience face aux risques de cybersécurité revêtent une importance capitale pour ST. Les exigences et protocoles de sécurité énoncés dans les présentes Exigences Minimales de Cybersécurité ont pour objet de protéger les informations et d'assurer la continuité des activités de ST et de sa chaîne d'approvisionnement, y compris celle de ses partenaires.

2. Définitions

MCRs : les Exigences Minimales de Cybersécurité (Minimum Cybersecurity Requirements) énoncées dans le présent document.

Informations Protégées : les informations propriétaires (y compris les informations à caractère personnel) fournies par ST ou auxquelles ST a donné accès, sous quelque forme ou sur quelque support que ce soit, qu'elles soient électroniques (« Données »), physiques, orales ou autres.

Contrat : les contrats signés par ST et le Fournisseur, le cas échéant, ainsi que les bons de commande émis par ST, régissant collectivement les conditions de la réalisation de la Fourniture.

Fourniture : les matériaux, composants, produits, dispositifs, équipements, logiciels et autres produits et services, tangibles ou intangibles, fournis par le Fournisseur au titre du Contrat.

Fournisseur : tout Fournisseur, y compris ses filiales, sociétés affiliées et sous-traitants, participant à la réalisation de la Fourniture au profit de ST.

Personnel du Fournisseur : toutes les personnes travaillant pour le Fournisseur ou ses partenaires et participant à la réalisation de la Fourniture, y compris les salariés, prestataires, mandataires, consultants et le personnel de toute filiale, société affiliée ou sous-traitant du Fournisseur.

Systèmes : les actifs de technologies de l'information utilisés pour la collecte, la transmission, le stockage ou le traitement des données, ainsi que les actifs de technologies opérationnelles (OT) utilisés pour surveiller, contrôler ou gérer des environnements physiques, industriels ou de production.

Systèmes ST : les Systèmes appartenant à ST, pris à bail par ST, prêtés à ST ou concédés sous licence à ST.

Services Cloud : les applications ou services hébergés, qu'ils soient mono-locataire ou multi-locataires, y compris les logiciels en tant que service (SaaS), les plateformes en tant que service (PaaS), les infrastructures en tant que service (IaaS) et les offres similaires permettant la collecte, la transmission, le stockage ou le traitement d'Informations Protégées.

Incident de Sécurité : toute compromission de la Fourniture, toute perte de confidentialité, d'intégrité ou de disponibilité des Informations Protégées, ou toute compromission des Systèmes ST.

3. Champ d'application et principes directeurs

a) Sauf disposition contraire dans un accord écrit dûment signé par ST et le Fournisseur, les présentes MCRs s'appliquent à toute commande passée par ST auprès du Fournisseur impliquant l'un des éléments suivants :

- la livraison de tout Système ;
- l'exécution de tout service impliquant la collecte, la transmission, le stockage ou le traitement d'Informations Protégées ;
- l'exécution de tout service impliquant l'accès aux Systèmes ST.

b) Le Personnel du Fournisseur participant à la réalisation de la Fourniture doit être tenu à des obligations de confidentialité et de sécurité substantiellement similaires à celles énoncées dans le Contrat et les présentes MCRs.

c) En complément des présentes MCRs, si la réalisation de la Fourniture nécessite des mesures de sécurité spécifiques ou supplémentaires, ST et le Fournisseur devront conclure un addendum distinct reflétant le niveau de cybersécurité requis, tel que déterminé par ST, lequel fera partie intégrante du Contrat.

d) En cas de conflit entre les présentes MCRs et le Contrat, les exigences les plus strictes prévalent.

e) L'utilisation de la marque, du nom ou du logo de ST à toute fin autre que la réalisation de la Fourniture est interdite, sauf autorisation écrite expresse de ST.

4. Continuité des activités et mesures de cybersécurité

a) Le Fournisseur doit maintenir des plans de continuité d'activité adéquats afin d'assurer la continuité de la réalisation de la Fourniture, en tenant compte des risques de cybersécurité, en adéquation avec les pratiques de son secteur d'activité et les normes de continuité des activités internationalement reconnues, telles que la norme ISO/IEC 22301.

b) Le Fournisseur doit mettre en œuvre des mesures administratives, techniques et organisationnelles appropriées afin de protéger la Fourniture, les Informations Protégées et les Systèmes ST contre les risques de cybersécurité, en adéquation avec les pratiques de son secteur d'activité et les normes de sécurité internationalement reconnues, telles que la norme ISO/IEC 27001 et, dans la mesure où elle est applicable à la Fourniture, la norme IEC 62443.

5. Protection des Informations Protégées

Le Fournisseur doit :

a) accéder aux Informations Protégées, les collecter, les transmettre, les stocker ou les traiter uniquement aux fins de la réalisation de la Fourniture et au seul bénéfice de ST, sauf autorisation écrite expresse de ST ;

b) lorsqu'une technologie d'intelligence artificielle ou d'apprentissage automatique est utilisée pour la Fourniture, s'assurer que le modèle sous-jacent n'est pas entraîné à l'aide d'Informations Protégées et n'utilise pas d'Informations Protégées, sauf autorisation écrite expresse de ST ;

c) gérer les droits d'accès aux Informations Protégées selon le principe du besoin d'en connaître, avec un réexamen régulier de ces droits d'accès. Cela inclut le retrait des droits d'accès dès qu'ils ne sont plus nécessaires, par exemple lorsqu'une personne change de fonction ou quitte son emploi ;

d) veiller à ce que le Personnel du Fournisseur fasse preuve de la diligence requise pour protéger les Informations Protégées et respecte les accords de confidentialité applicables ;

e) détruire les Informations Protégées comme suit (les « **Exigences de Suppression Sécurisée** ») : (i) les documents papier doivent être détruits selon la norme ISO 21964, au niveau de sécurité 4

au minimum ; et (ii) les supports et données électroniques doivent être effacés de manière sécurisée, écrasés ou rendus irrécupérables selon la norme ISO/IEC 27040 ou une norme équivalente.

6. Fourniture de Services Cloud

Dans la mesure où le Fournisseur fournit des Services Cloud :

a) Le Fournisseur doit isoler les Informations Protégées des données de ses autres clients et veiller à ce que les Services Cloud soient protégés, en adéquation avec les pratiques du secteur et les normes de sécurité internationalement reconnues, telles que la norme ISO/IEC 27017.

b) Le Fournisseur doit permettre à ST de restreindre l'accès aux Informations Protégées aux seules personnes autorisées, ainsi que de journaliser et surveiller ces accès, y compris l'accès par le Personnel du Fournisseur.

c) Le Fournisseur doit apporter à ST une assistance raisonnable afin de l'aider à répondre aux demandes de production de preuves électroniques (e-discovery) et à mener des investigations forensiques liées à l'utilisation des Services Cloud.

d) À la résiliation ou à l'expiration du présent Contrat, le Fournisseur doit apporter une assistance raisonnable afin de faciliter la migration des Services Cloud et le transfert des Informations Protégées à ST ou à un tiers désigné. Cette transition doit avoir lieu au cours d'une Période de Transition convenue d'un commun accord.

e) Le Fournisseur ne doit conserver les Informations Protégées que pour la durée spécifiée dans le présent Contrat ou telle que requise par la loi. À l'issue de la Période de Transition, le Fournisseur doit, conformément à ce qui est convenu avec ST, soit supprimer de manière sécurisée les Informations Protégées conformément aux Exigences de Suppression Sécurisée, soit restituer l'ensemble des Informations Protégées à ST.

7. Livraison de Systèmes à ST

Dans la mesure où le Fournisseur livre des Systèmes à ST :

a) Les Systèmes doivent être exempts de tout logiciel malveillant et de toute faille de sécurité connue et doivent pouvoir être configurés de manière sécurisée.

b) Le développement de tout logiciel, micrologiciel (firmware) ou jeu de composants (chipset) doit être réalisé en adéquation avec les pratiques de son secteur d'activité et les normes de sécurité internationalement reconnues, telles que la norme ISO/IEC 27001 et, dans la mesure où elle est applicable à la Fourniture, la norme IEC 62443.

8. Accès aux Systèmes ST

Dans la mesure où un accès du Personnel du Fournisseur aux Systèmes ST est requis (le **« Personnel Autorisé »**) :

a) Le Personnel Autorisé doit utiliser les Systèmes ST exclusivement aux fins de la réalisation de la Fourniture. Toute utilisation personnelle des Systèmes ST par le Personnel Autorisé est strictement interdite.

b) Le Fournisseur doit veiller à ce que le Personnel Autorisé reconnaisse expressément que son utilisation des Systèmes ST peut être journalisée et surveillée par ST, et qu'il est tenu de se conformer à toutes les instructions de sécurité fournies par ST applicables à ses accès et à ses missions.

c) Le Personnel Autorisé ne doit jamais utiliser, rechercher délibérément, explorer ou accéder à des Informations Protégées ou à des Systèmes ST qui ne sont pas nécessaires à la réalisation de la Fourniture, même si cela est techniquement possible.

d) Le Fournisseur doit informer ST dès qu'il a connaissance du fait qu'un membre du Personnel Autorisé n'a plus besoin d'accéder aux Systèmes ST pour quelque raison que ce soit, par exemple un changement de fonction ou un départ de l'entreprise.

e) Le Fournisseur doit restituer sans délai, ou à la première demande de ST, tout Système ST fourni par ST dès qu'il n'est plus nécessaire à la réalisation de la Fourniture.

9. Incidents de Sécurité

En cas de détection par le Fournisseur d'un Incident de Sécurité avéré ou raisonnablement suspecté :

a) Sans préjudice de toute obligation légale de notification, le Fournisseur doit :
   - notifier ST sans délai et suivre les instructions définies à l'adresse URL suivante : Security & Privacy - STMicroelectronics ;
   - s'abstenir d'informer toute autre entité ou personne de l'Incident de Sécurité, sauf autorisation expresse et écrite de ST.

b) Le Fournisseur est réputé responsable de tout Incident de Sécurité résultant de sa mise en œuvre inadéquate des dispositions du Contrat et des présentes MCRs.

10. Cessation de la Fourniture

Dans la mesure où la Fourniture implique la collecte, la transmission, le stockage ou le traitement d'Informations Protégées :

a) Le Fournisseur doit contacter ST sans délai à la cessation de la Fourniture afin d'obtenir des instructions concernant la restitution, la destruction ou toute autre mesure relative aux Informations Protégées.

b) La destruction doit être effectuée conformément aux Exigences de Suppression Sécurisée, et le Fournisseur doit notifier ST par écrit après la destruction.

11. Vérification de la conformité

a) À la demande de ST, le Fournisseur doit fournir toutes les informations nécessaires pour démontrer sa conformité au Contrat et aux présentes MCRs, ainsi qu'à l'ensemble des lois, réglementations et accords internationaux applicables.

b) Le Fournisseur doit notifier sans délai ST s'il n'est pas en mesure ou refuse de se conformer au Contrat ou aux présentes MCRs.

c) En cas de non-conformité avec le Contrat ou les présentes MCRs, ST peut, à sa discrétion : (i) suspendre la réalisation de la Fourniture ; (ii) exiger que le Fournisseur cesse de collecter, transmettre, stocker ou traiter les Informations Protégées ; (iii) exiger la restitution ou la destruction des Informations Protégées conformément aux Exigences de Suppression Sécurisée ; (iv) accorder une dérogation pendant laquelle le Fournisseur doit mettre en œuvre les mesures compensatoires convenues avec ST jusqu'à ce qu'il ait remédié à la non-conformité; ou (v) résilier immédiatement le Contrat.