

CAHIER DES CLAUSES SIMPLIFIÉES DE CYBERSÉCURITÉ

Date de diffusion	Rédacteur	Vérificateur	Approbateur	Modifications
2025/11/05	P.PIERROT	Chefs de Groupes Informatiques	Directeur Division Stratégie des Systèmes d'Information	Ajout de l'annexe concernant les prestations de développement logiciel
Destinataires	Chefs de Groupes amenés à acheter des équipements ou prestations ayant une composante informatique			

PUBLIC

La version électronique fait foi.



CAHIER DES CLAUSES SIMPLIFIEES DE CYBERSECURITE

TABLE DES MATIERES

ARTICLE 1ER : <i>CHAMP D'APPLICATION</i>	3
ARTICLE 2 : <i>POLITIQUES DE SECURITE</i>	3
ARTICLE 3 : <i>CONTROLES ET AUDITS</i>	3
ARTICLE 4 : <i>DOCUMENTATIONS</i>	4
ARTICLE 5 : <i>MAINTIEN EN CONDITION DE SECURITE</i>	4
ARTICLE 6 : <i>SIGNALEMENTS DE SECURITE</i>	5
ARTICLE 7 : <i>HEBERGEMENT DE DONNEES</i>	6
ARTICLE 8 : <i>SOUS-TRAITANCES</i>	6
ARTICLE 9 : <i>LABELS ET CERTIFICATS</i>	6
ARTICLE 10 : <i>DEFAUTS ET REGLEMENT DES DIFFERENDS</i>	6
ARTICLE 11 : <i>ETATS DE L'ART</i>	7
ANNEXES	9
1.1. ANNEXE 1 : SECURITE DES DEVELOPPEMENTS INFORMATIQUES ET TESTS DAST/SAST	9

ARTICLE 1ER : CHAMP D'APPLICATION

1.1. Ce cahier de clauses simplifiées de cybersécurité (CCSC) n'est applicable qu'aux marchés qui s'y réfèrent.

1.2. Les clauses ont pour vocation d'assurer un premier cadre de sécurisation des systèmes d'information et des données associées via tout type de marché, aussi bien un marché à objet principal directement associé aux technologies de l'information et de la communication (ordinateurs, logiciels, développements ou hébergement d'application via le web) que des fournitures et services annexes (extranet de commande et service clients), ou même les simples échanges d'information par messageries électroniques.

1.3. Pour les marchés ayant un objet principal numérique comme l'externalisation d'une brique de système d'information, les présentes clauses simplifiées peuvent être complétées dans le cahier de clauses particulières du marché auquel fait écho la production par les candidats puis la contractualisation avec le titulaire d'un plan d'assurance sécurité (PAS).

1.4. Les annexes complètent et précisent le clausier pour des domaines particuliers. En cas de conflit entre un article du clausier simplifié et une annexe, c'est cette dernière qui prévaut.

ARTICLE 2 : POLITIQUES DE SECURITE

2.1. Les candidats et titulaires sont tenus de respecter les prescriptions de la politique de sécurité des systèmes d'information (PSSI) de SOLEIL.

2.2. Il en est de même pour les annexes techniques de la PSSI dès lors qu'elles sont disponibles à première demande motivée.

ARTICLE 3 : CONTROLES ET AUDITS

3.1. Durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants.

3.2. Dans tous les cas, des audits légitimés par la sélection ou le suivi de titulaires de marchés peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier (par exemple, User-Agent référençant une URL d'explication, reverse-DNS permettant de donner une origine claire à une adresse IP, etc).

ARTICLE 4 : DOCUMENTATIONS

4.1. Les politiques de sécurité prévoient généralement une revue formelle de sécurité appelée homologation, auquel les titulaires doivent apporter leur concours en matière de documentations et de réponses aux questions, permettant d'analyser les risques résiduels en matière de confidentialité, authentification, traçabilité, intégrité, disponibilité et résilience.

4.2. Par ailleurs, les réglementations applicables par exemple à la protection des données à caractère personnel (RGPD) prévoient la tenue de registres des traitements et la documentation des mesures de protection. Le candidat ou titulaire et leurs sous-traitants identifient proactivement les traitements de données personnelles ou sensibles et aident à la réalisation d'analyses d'impact relative à la protection des données et à la consultation préalable des autorités de contrôle.

4.3. Dans tous les cas, un titulaire de marché est tenu de fournir à première demande la documentation nécessaire à la sécurisation de leurs fournitures dans les systèmes d'information, la protection des données de SOLEIL et aux démonstrations du respect de leurs obligations par SOLEIL.

4.4. En particulier, la documentation explicite tous les flux échangés (entrants et sortants, applicatif mais aussi de maintenance, de statistiques, de mise à jour, d'administration distante, etc), et les dispositifs de contrôle d'accès et de maintien en condition de sécurité.

4.5. Si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part de SOLEIL, elles doivent être clairement identifiées dans un chapitre Sécurité du mode d'emploi (par exemple, la procédure de changement des mots de passe par défaut ou des interfaces exposées, de mise à jour de composants logiciels...).

ARTICLE 5 : MAINTIEN EN CONDITION DE SECURITE

5.1. La politique de sécurité exige la mise à jour des composants logiciels vers des versions supportées par l'éditeur ou la communauté Open Source qui les produisent. Dans ces conditions, une vérification d'aptitude au bon fonctionnement ou au service régulier (VABF et VSR) est refusée si des composants ne sont pas à jours des correctifs de failles de sécurité.

5.2. La responsabilité du maintien en condition de sécurité d'un titulaire comprend les composants et services développés en propre mais aussi ses composants et dépendances amont (librairies, cadriciels, environnement d'exploitation, API tierces) ou sous-traités.

5.3. Un candidat ou titulaire ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations qu'il fournit à l'emploi de composants dans une version non supportée, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens

de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi.

5.4. Dans tous les cas, les unités d'œuvre portant le maintien en condition opérationnelle (labellisée MCO mais aussi tierce maintenance applicative (TMA) ou simplement hébergement) incluent le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité.

ARTICLE 6 : SIGNALEMENTS DE SECURITE

6.1. Pour les prestations, produits et services qu'ils fournissent dans le cadre du marché, les titulaires mettent à disposition des fils publics par abonnement (flux RSS, liste de diffusion par courriel) ou autre dispositif d'information dédié à la sécurité informatique. Ces fils, identifiés dans le chapitre Sécurité des modes d'emploi, permettent aux bénéficiaires d'être tenu informés en continu des événements et changements impactant la sécurité, par exemple annonce de correctif, attaque en cours, nouvelle configuration à appliquer, violation de données à caractère personnel...

6.2. Afin de garder leur pouvoir d'alerte, ces canaux de diffusion ne sont pas mélangés avec des flux commerciaux et marketing. Les fils peuvent être multiples dans le cas de fournitures en plusieurs composants mais sans laisser de vide d'information.

6.3. Réciproquement, les outils numériques mis à disposition permettent à SOLEIL et à ses experts en cybersécurité de signaler directement aux équipes appropriées du titulaire de possibles failles ou détournements de dispositifs de sécurité.

6.4. Afin que ces signalements soient effectifs et efficaces, les conventions d'usage en cybersécurité sont respectées (security.txt, abuse@). Dans tous les cas, il faut moins d'une minute pour trouver le point d'entrée approprié du signalement.

6.5. Après analyse partagée et vérification, le titulaire a obligation d'enregistrer les failles auprès des autorités compétentes (CERT nationaux pour les éditeurs, registres RGPD et CNIL ou équivalent pour la divulgation de données personnelles, ANSSI pour les opérateurs d'importance vitale ou de services essentiels, etc.) en suivant les réglementations établies. L'emploi d'un système de cotation connu (par exemple CVSS) permet de hiérarchiser l'urgence pour tous les acteurs en aval. A défaut d'action sous 3 mois, l'acheteur a la possibilité de se substituer aux titulaires dans les actions précédentes ou de pratiquer une divulgation responsable (annonce de la faille avec embargo pendant au moins 90 jours sur les détails techniques)

ARTICLE 7 : *HEBERGEMENT DE DONNEES*

7.1. A première demande, le candidat ou titulaire identifie tous les prestataires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

Peuvent être exclus de cette déclaration les prestataires qui seraient dépositaires de copies chiffrées à condition que l'algorithme soit sans faille connue et que les prestataires ne soient pas en possession des clés cryptographiques.

ARTICLE 8 : *SOUS-TRAITANCES*

8.1. Les clauses de ce cahier s'appliquent aux marchés publics en incluant tous les sous-traitants. Comme les titulaires sont responsables de leurs sous-traitants, les contrôles et les éventuelles actions de remédiation en cas de défaut, y compris jusqu'au remplacement, sont donc à la charge des titulaires.

ARTICLE 9 : *LABELS ET CERTIFICATS*

9.1. Afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché, candidats et titulaires sont invités à présenter des labels et certificats qui permettent à SOLEIL d'avoir un premier niveau d'assurance au cours de l'évaluation d'offres.

9.2. Ces qualifications peuvent parfois être globales (ISO27000), partielles (référentiel en « Tier » 1 à 4 pour l'hébergement), ou très ponctuelles (rapports de test de l'état de l'art sur des interfaces spécifiques, cf. clause ci-dessous).

ARTICLE 10 : *DEFAUTS ET REGLEMENT DES DIFFERENDS*

10.1. Tout au long des processus d'attribution et d'exécution d'un marché, SOLEIL peut constater ou découvrir des non-conformités à la politique de sécurité de l'entité et des défauts de sécurisation.

10.2. SOLEIL apprécie l'enjeu du défaut eu égard à la sensibilité des données manipulées, de leurs volumes, et des conséquences prévisibles si le défaut persiste.

10.3. En fonction de cette analyse, ces défauts peuvent avoir comme conséquence le rejet d'une candidature, d'une offre, la non-validation d'aptitude au service régulier, pénalités de retard, l'ajournement, la suspension ou la résiliation des bons de commandes ou du marché.

10.4. Comme les différends peuvent être techniques et nécessiter un traitement confidentiel, le règlement des éventuelles contestations sur les décisions précitées passera systématiquement par un comité consultatif de règlement amiable.

10.5. Un comité consultatif est composé de membres qualifiés et habilités pour cette fonction, désignés au préalable ou choisis conjointement.

ARTICLE 11 : ETATS DE L'ART

11.1. La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient à chaque titulaire de marché de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition. Pour les interfaces web, les services de courriels, les appareils connectés, les sauvegardes de données et l'administration de systèmes d'information, les référentiels à retenir sont résumés ci-après et détaillés dans les textes techniques publiés par l'ANSSI. Les respects de référentiels sont aussi vérifiés par les agences de notation en cybersécurité.

11.2. A première demande, le candidat ou titulaire fournit la conformité à ces référentiels pour les services et objets numériques qu'il inclut dans son offre de fournitures. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration).

11.3. Interfaces web

- Interfaces utilisables par des navigateurs à l'état de l'art (part de marché cumulée supérieure à 50%), sans générer d'alerte de sécurité.
 - sans module d'extension.
 - dans leur mode Grand public le plus protecteur (souvent appelé navigation privée).
- et en exploitant les techniques de protections associées.
 - connexion TLS (https) pour authentifier la source et chiffrer les communications.
 - marquage approprié des cookies ou jetons de session pour se protéger des vols ou exploitation de sessions déjà ouvertes.
 - politique de sécurité des contenus pour se protéger contre les injections de contenus actifs malicieux.
 - activation des protections des navigateurs par l'emploi d'entêtes de sécurité.
- Publication d'un point de contact via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des bonnes équipes techniques.

11.4. Services de courriels

- Authenticité des émetteurs garantie par l'émission de messages depuis des serveurs associés publiquement aux domaines, signature numérique par domaine et une politique publique liant le tout.
- Identification claire du statut des comptes émetteurs de courriels, par exemple en ajoutant un suffixe à ceux fournis aux personnels qui ne sont pas salariés directs.
- Intégrité des messages par leur signature numérique.
- Confidentialité des échanges de machines en machines, confidentialité compatible avec les obligations d'interceptions légales.
- Analyse des rapports d'anomalies via DMARC ou abuse@.

11.5. Appareils connectés

- Dispositif de lutte contre les logiciels malveillants (anti-virus, ou système de vérification et détection à base de signatures ou condensats des logiciels autorisés).
- Dispositif de mise à jour sécurisé.
- Limitation de l'exposition via les réseaux en réduisant les ports acceptant des connexions entrantes et en authentifiant les accès distants, sans faille connue (ceci exclut les connexions non chiffrés TELNET, HTTP/SMTP sans TLS, et l'emploi de mots de passe génériques ou faciles à découvrir, par exemple du fait d'un hachage insuffisant).

11.6. Sauvegardes des données stockées

- Sauvegardes 3-2-1 (3 copies, 2 technologies, 1 exemplaire hors site principal, donc avec chiffrement) pour se protéger des rançongiciels, des erreurs de manipulations ou des défaillances de matériels.

11.7. Administration des systèmes d'information

- Consoles dédiées à l'exploitation et l'administration, et au minimum isolées des réseaux bureautiques et d'Internet, web et courriel notamment.
- Connexions aux machines administrées par des protocoles chiffrés, authentifiants et sans faille connue et bien configurés (VPN IPsec, TLS, ssh, RDP avec NLA).

ANNEXES

ANNEXE 1 : SECURITE DES DEVELOPPEMENTS INFORMATIQUES ET TESTS DAST/SAST

La sécurité, l'intégrité et la disponibilité des systèmes d'information, des données scientifiques et des systèmes de contrôle sont d'une importance capitale pour la réussite des missions du Synchrotron SOLEIL. L'intégration de la sécurité avec une approche DevSecOps est attendue dans le Cycle de Vie des Développements.

Cette annexe vise à garantir que les développements informatiques réalisés pour le Synchrotron SOLEIL respectent un haut niveau de sécurité, protégeant ainsi ses actifs informationnels et opérationnels critiques.

1.1.1. PRINCIPE GENERAL

Le Prestataire s'engage à intégrer les meilleures pratiques de sécurité tout au long du cycle de vie de développement des logiciels, applications, modules ou scripts (ci-après dénommés "les Développements") réalisés pour le compte du Synchrotron SOLEIL. Cette approche vise à identifier et à corriger les vulnérabilités de sécurité le plus tôt possible afin de minimiser les risques et les coûts associés.

1.1.2. OBLIGATION D'UTILISATION DES TESTS DE SECURITE AUTOMATISES DAST ET SAST VIA GITLAB

Pour tous les Développements hébergés et gérés au sein de l'infrastructure GitLab fournie ou désignée par le Synchrotron SOLEIL, le Prestataire a l'obligation d'intégrer et d'exécuter systématiquement les outils de tests de sécurité automatisés suivants, disponibles dans ladite plateforme GitLab :

- SAST (Static Application Security Testing) : Des analyses statiques du code source devront être configurées et exécutées régulièrement, a minima avant chaque demande de fusion (merge request) vers les branches principales (main/master, develop) et lors de chaque pipeline CI/CD. Ces tests visent à identifier les failles de sécurité potentielles directement dans le code source, telles que les injections SQL, XSS, failles de configuration, utilisation de bibliothèques obsolètes ou vulnérables, etc.
- DAST (Dynamic Application Security Testing) : Des analyses dynamiques des applications en cours d'exécution (dans des environnements de test ou de pré-production) devront être configurées et exécutées à des étapes clés du cycle de développement et avant chaque mise en production majeure. Ces tests simulent des attaques externes sur les applications en fonctionnement pour identifier des vulnérabilités liées à l'exécution, à la configuration du serveur, à la gestion des sessions, etc.

Le Synchrotron SOLEIL mettra à disposition du Prestataire l'accès à son instance GitLab et aux fonctionnalités de sécurité (SAST/DAST) intégrées. Le Prestataire devra s'assurer que

ses équipes sont compétentes pour configurer et interpréter les résultats de ces outils.

1.1.3. GESTION ET CORRECTION DES VULNERABILITES

1.1.3.1. RAPPORTS ET IDENTIFICATION

Les résultats des tests SAST et DAST seront accessibles via la plateforme GitLab. Chaque vulnérabilité identifiée sera documentée avec un niveau de sévérité (par exemple, Critique, Haute, Moyenne, Basse) basé sur les classifications standards (e.g., CVSS) et celles fournies par les outils GitLab.

1.1.3.2. OBLIGATION DE CORRECTION

Le Prestataire a l'obligation de corriger les failles de sécurité révélées par les tests SAST et DAST selon les modalités suivantes :

- **Vulnérabilités Critiques et Hautes** : Toutes les vulnérabilités classées comme Critiques ou Hautes devront être corrigées par le Prestataire avant toute mise en production du Développement concerné ou, pour les systèmes existants, dans un délai défini en accord avec le Synchrotron SOLEIL après leur découverte. Ce délai ne pourra excéder [par exemple, 5 jours ouvrés pour les critiques, 15 jours ouvrés pour les hautes] sans accord explicite du Responsable Sécurité des Systèmes d'Information (RSSI) du Synchrotron SOLEIL. Une nouvelle passe des tests SAST/DAST sera requise pour valider la correction.
- **Vulnérabilités Moyennes** : Les vulnérabilités classées comme Moyennes devront être évaluées conjointement par le Prestataire et le Synchrotron SOLEIL (représenté par son équipe technique et/ou son RSSI). Sur la base d'une analyse de risque (probabilité d'exploitation, impact potentiel sur les opérations du synchrotron, les données scientifiques, ou la sécurité des utilisateurs), une décision sera prise quant à :
 - La correction immédiate.
 - La planification de la correction dans un cycle de développement ultérieur.
 - L'acceptation du risque, documentée et validée formellement par le RSSI du Synchrotron SOLEIL si la correction s'avère techniquement complexe, trop coûteuse par rapport au risque, ou si des mesures compensatoires sont mises en place.
- **Vulnérabilités Basses** : Les vulnérabilités classées comme Basses seront revues et pourront être corrigées lors des cycles de maintenance réguliers ou acceptées après documentation, selon l'évaluation du Synchrotron SOLEIL.

1.1.3.3. CAS DE NON-CORRECTION ET DEROGATION

Toute non-correction d'une vulnérabilité identifiée, quelle que soit sa sévérité, devra faire l'objet d'une demande de dérogation écrite et argumentée de la part du Prestataire. Cette demande sera examinée par le RSSI et les responsables techniques du Synchrotron SOLEIL, qui pourront l'accepter ou la refuser. L'acceptation d'un risque sera formalisée.

1.1.3.4. PLAN DE REMEDIATION

Pour les ensembles de vulnérabilités importantes ou complexes, le Prestataire devra soumettre un plan de remédiation détaillé, incluant un calendrier de correction, pour approbation par le Synchrotron SOLEIL.

1.1.3.5. *PREUVE DE CONFORMITE ET REPORTING*

Le Prestataire devra être en mesure de fournir, sur demande du Synchrotron SOLEIL :

- La preuve de la configuration et de l'exécution des scans SAST et DAST (*sous réserve qu'il ait son code sur Gitlab*).
- Les rapports de vulnérabilités générés par GitLab.
- La documentation des actions de correction entreprises et des validations effectuées.
- Les demandes et acceptations formelles de dérogation pour les vulnérabilités non corrigées.

Un bilan régulier de la posture de sécurité des développements, incluant les statistiques sur les vulnérabilités détectées et corrigées, pourra être exigé par le Synchrotron SOLEIL.

1.1.4. *RESPONSABILITE*

Le Prestataire demeure responsable de la sécurité des Développements qu'il fournit, y compris après la validation des corrections. L'utilisation des outils SAST/DAST et les processus de correction décrits ne sauraient être interprétés comme un transfert de responsabilité vers le Synchrotron SOLEIL ou vers les outils eux-mêmes. Le Prestataire s'engage à une veille active sur les nouvelles vulnérabilités susceptibles d'affecter les technologies utilisées dans ses Développements.

1.1.5. *FORMATION ET SENSIBILISATION*

Il est attendu du Prestataire que ses équipes de développement soient formées et sensibilisées aux bonnes pratiques de développement sécurisé (e.g., OWASP Top 10, SANS CWE Top 25) et à l'utilisation des outils de sécurité intégrés à GitLab.