



SECRETARIAT GENERAL

DEPARTEMENT DES SERVICES FINANCIERS (DSF)

Unité Billetterie – Frais de déplacement

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES SÉCURITÉ SYSTÈMES D'INFORMATION (SI)

Marché n°2026-09

« Fourniture de prestations d'agence de voyage destinées à l'organisation et à la gestion des déplacements professionnels des personnels, agents, élèves, stagiaires, intervenants et invités de l'Ecole nationale d'administration pénitentiaire (ENAP) »

Article 1. Objet du marché

Le présent marché a pour objet la fourniture de prestations d'agence de voyage destinées à l'organisation et à la gestion des déplacements professionnels des personnels, agents, élèves, stagiaires, intervenants et invités de l'Ecole nationale d'administration pénitentiaire (ENAP), dans le cadre de ses missions de formation initiale et continue.

Ces prestations ont pour objectif de permettre la préparation, la réservation et la gestion des déplacements nécessaires aux activités de formation, d'enseignement, d'intervention, d'encadrement ou d'expertise assurées par l'ENAP.

Les déplacements concernés peuvent avoir lieu en France métropolitaine, en outre-mer ou à l'étranger.

Dans ce cadre, le titulaire est notamment chargé :

- de la réservation et de l'émission de titres de transport ;
- la réservation de prestations d'hébergement et, le cas échéant, de services associés ;
- de la gestion de prestations annexes liées aux déplacements professionnels.

Les prestations sont exécutées conformément aux dispositions applicables aux frais de déplacements temporaires des personnels civils de l'Etat, notamment le décret n°2006-781 du 3 juillet 2006 modifié et les arrêtés pris pour son application, ainsi qu'aux textes spécifiques applicables au ministère de la Justice et à ses établissements publics.

Les conditions et modalités de prise en charge des frais de déplacement des agents, élèves, stagiaires et autres personnes relevant de l'ENAP sont déterminées par la réglementation en vigueur et par les décisions et délibérations des instances compétentes de l'Ecole.

Article 2. Contexte exigences techniques et environnementales

Une offre logicielle en mode hébergé (SaaS ou Acquisition de Licences) est demandée.

Le candidat tiendra compte des éléments de contexte et exigences ci-dessous.

Ces exigences sont portées par la réglementation positive et la sensibilité de la population traitée.

Les personnels, élèves de l'ENAP sont des personnels de l'Administration Pénitentiaire à ce titre ils font partie de la troisième force de sécurité intérieure, ils sont particulièrement exposés à des risques impactant de part la nature de leurs missions.

Article 3. Hébergement de la solution

L'hébergement de la solution devra être qualifié Secnumcloud 3.2 et à minima répondre à la norme ISO 27001, l'hébergeur de la solution devra être une société européenne pour répondre aux obligations de souveraineté des données.

Article 4. Obligations du Titulaire sur la sécurité de ses locaux informatiques

a. CCTP-Exigence SECU LOC 001

En cas de changement de localisation des données ou services, le Titulaire en informe préalablement l'ENAP.

b. CCTP-Exigence SECU LOC 002

Le Titulaire identifie tous les Titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours du marché ainsi que leur localisation. Il en informe l'ENAP au préalable avant toutes modifications.

c. CCTP-Exigence SECU LOC 003

Les bâtiments du Titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en

question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du Titulaire.

Le Titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du Titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès. Le Titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du Titulaire.

d. CCTP-Exigence SECU LOC 004

Le Titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

Le Titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du Titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès. Le Titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'ENAP et équipements de sûreté.

e. CCTP-Exigence SECU LOC 005

Les locaux du Titulaire et de ses sous-traitants qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, ...) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction. En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

f. CCTP-Exigence SECU LOC 006

Le Titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, ...) sont accompagnées par une personne habilitée.

g. CCTP-Exigence SECU LOC 007

Le Titulaire assure la protection de la documentation de l'ENAP sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

Article 5. Obligations du titulaire sur la sécurité des réseaux et de l'exploitation

a. CCTP-Exigence SECU SRE 001

Le Titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

b. CCTP-Exigence SECU SRE 002

Le Titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration permettant l'accès aux environnements de l'ENAP depuis le site du Titulaire doivent respecter les exigences suivantes (en suivant, à défaut d'une précision de l'ENAP, les recommandations de l'ANSSI) :

- Les correctifs de sécurité et les mises à jour antivirus doivent se faire quotidiennement ;

- Les postes ne doivent pas avoir accès à internet ni à un système d'information bureautique (messagerie, intranet, ...);
- Les postes d'administration utilisés doivent être réservés exclusivement à cet usage. Tout accès au poste doit se faire de manière sécurisée que ce soit pour l'ouverture d'une session ou l'accès physique;
- Les postes d'administration doivent être mis sur un VLAN dédié.

Si un tel dispositif s'avère impossible à réaliser pour le Titulaire, il devra préciser les mesures de sécurité des postes d'administration.

c. CCTP-Exigence SECU SRE 003

L'installation, l'exploitation et l'administration des produits mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'ENAP. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'ENAP. A ce titre, les mots de passe hérités des paramétrages d'usine des produits doivent systématiquement être modifiés lors de leur configuration pour les besoins de l'ENAP.

d. CCTP-Exigence SECU SRE 004

Le Titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation. La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement validée par l'ENAP.

e. CCTP-Exigence SECU SRE 005

Le Titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirus, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'ENAP.

f. CCTP-Exigence SECU SRE 006

Le Titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation dispose d'un compte individuel qui peut être :

- Soit un compte nominatif qui lui est personnel et qui sera utilisé uniquement par cette personne tout au cours de la vie du compte ;
- Soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

g. CCTP-Exigence SECU SRE 007

Le Titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. Il précise dans le PAS, la procédure de revue de ces comptes. Le cas échéant, il automatise le processus de blocage ou de suppression.

h. CCTP-Exigence SECU SRE 008

Le Titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

i. CCTP-Exigence SECU SRE 009

Le Titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'ENAP existants ainsi que des rôles et privilèges qui y sont associés. Il fournit cette liste à l'ENAP sur demande.

j. CCTP-Exigence SECU SRE 010

Le Titulaire s'assure que tous les comptes (accès système d'exploitation et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège. Le Titulaire s'assure que tous les comptes sont protégés (moyens d'authentification sur ses serveurs, applications et postes de travail) contre les attaques en essai et erreurs sur secrets d'authentification.

k. CCTP-Exigence SECU SRE 011

Le Titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves. Le Titulaire collecte et stocke à minima les informations suivantes :

- Connexion et déconnexion aux équipements et applications ;
- Consultations d'informations relatives à la vie privée ;
- Informations d'usage de l'Internet (accès aux sites Web) ;
- Accès en lecture et/ou en écriture à des fichiers et dossiers identifiés comme sensibles ;
- Informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du Titulaire.

Les traces enregistrées par le Titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

L'ENAP doit être sûr que les journaux concernant ses ressources hébergées ne sont pas divulgués à d'autres organismes co-hébergés (garantie de confidentialité) ;

L'ENAP doit pouvoir avoir accès aux journaux d'événements (réduits éventuellement à un extrait) à sa demande et dans un délai de 8 heures

l. CCTP-Exigence SECU SRE 012

Le Titulaire respecte la politique de définition des mots de passe (délibération n°2022-100 du 21 juillet 2022 de la CNIL) sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du Titulaire.

m. CCTP-Exigence SECU SRE 013

Le Titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation.

n. CCTP-Exigence SECU SRE 014

Le Titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'ENAP dans le cadre de la prestation.

o. CCTP-Exigence SECU SRE 015

Le Titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et aux traitements des incidents, pour la tenue de ses engagements contractuels.

p. CCTP-Exigence SECU SRE 016

Le Titulaire est capable de fournir à l'ENAP, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI de l'ENAP en astreinte dans un délai maximal d'un mois.

q. CCTP-Exigence SECU SRE 017

Le Titulaire est responsable de l'analyse des traces systèmes, applicatives et réseaux en vue de détecter toute attaque ou tentative d'attaque et, le cas échéant, ajuster les configurations et paramètres de sécurité.

Toute attaque fait l'objet d'une fiche d'alerte au DSI de l'ENAP précisant à minima :

- Un résumé de l'attaque (en précisant son vecteur) et ses impacts potentiels ;
- L'adresse IP de l'attaquant ;
- Les impacts de l'attaque sur l'écosystème du système d'information cible (avec une note CVSS) ;
- Les actions à mettre en œuvre (contournement ou correctif) ;
- La date de correction envisagée.

Les délais de correction sont assujettis à la note CVSS de la fiche d'alerte et doivent respecter les mêmes contraintes temporelles que celles indiquées dans le cadre du Maintien en Condition de Sécurité (MCS).

Article 6. Sauvegarde et restauration :

Les sauvegardes doivent être quotidiennes et conservées sur 15 jours minimum.

Le Titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l'application.

Un rapport de sauvegarde doit être envoyé à l'ENAP après chaque sauvegarde s'il en fait la demande, le rapport sera transmis sous 4 heures.

Le Titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :

- Confidentialité des flux lors des opérations de sauvegardes ;
- Stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du Titulaire et de l'ENAP. Aucune externalisation en dehors de l'Union Européenne ne sera admise.

Le Titulaire effectue au moins annuellement des tests de restauration des sauvegardes effectuées sur les données des systèmes d'information de l'ENAP qu'il héberge et/ou exploite selon les prestations du marché. Les tests de restauration devront être validés par l'ENAP.

Article 7. Obligations du Titulaire dans le processus d'homologation des SI

Tout système d'information traitant des informations ou supports à protéger doit faire l'objet d'une homologation, consistant en la déclaration par une autorité dite d'homologation, que le système d'information considéré est apte à traiter des informations ou supports protégés conformément aux objectifs de sécurité visés, et qu'elle accepte les risques de sécurité résiduels induits.

La démarche d'homologation de sécurité suit le cycle de vie de la cible. C'est pourquoi tout au long du marché les éléments constitutifs du dossier de sécurité seront amenés à évoluer dans la limite de ce qui est prévu par la réglementation et les directives associées.

Le Titulaire établit pour chaque projet, un dossier d'homologation présentant les données et leurs traitements, les mesures générales et particulières de sécurité, les moyens de protection associés ainsi que les moyens et techniques concourant au fonctionnement du système d'information. Il recense les vulnérabilités résiduelles.

a. CCTP-Exigence SECU HOM 001

Dans ses travaux d'ingénierie, le Titulaire doit proposer des solutions techniques qui ne constituent pas un obstacle au prononcé de l'homologation du système d'information.

b. CCTP-Exigence SECU HOM 002

Le Titulaire fournira les éléments nécessaires à l'établissement et au maintien à jour des documents du dossier en vue du maintien de l'homologation des systèmes de l'ENAP.

c. CCTP-Exigence SECU HOM 003

Le Titulaire réalise et met à jour les dossiers d'architecture de l'ensemble des systèmes d'information de l'ENAP. Ces documents doivent être marqués « Diffusion Restreinte » et traitent systématiquement des sujets suivants :

Détail de l'architecture fonctionnelle : description des échanges métiers permettant au système de remplir sa mission ;

- Détail de l'architecture applicative: description des différentes briques applicatives du système, des échanges entre ces dernières et des fonctionnalités métiers associées, la matrice des flux ;
- Détail de l'architecture technique : description du socle technique sur lequel s'appuie le projet et les flux techniques associés (serveurs, stockage, réseau, sauvegarde, liste géographique des data(s) center(s) actif(s)/passif(s), réplication de la liste des règles pare-feu, WAF, SIEM, SOC, protection DDOS, matrice des flux) ;
- Détail de la résilience du système: capacité à continuer de rendre le service en cas de défaillance d'un composant technique ;
- Gestion des journaux d'événements ;
- Description des mesures de sécurité permettant de garantir la confidentialité, l'intégrité et la disponibilité du système (durcissement des serveurs, identification/authentification, haute disponibilité, ...).
- Baseline du système et du middleware

La Baseline devra être envoyée après chaque mise à jour du système et du middleware au DSI de l'ENAP ou ouvrir un accès ssh, snmp v3 pour l'IP de ENAP pour supervision CENTREON.

d. CCTP-Exigence SECU HOM 004

Le Titulaire doit justifier dans le document d'architecture technique les mécanismes de sécurité mis en place dans la solution en vue de répondre aux objectifs de sécurité :

- PRA 72h00
- Risque de violation des données à caractère personnel,
- Intégrité de la BDD.

Ces objectifs peuvent être satisfaits par un logiciel personnalisé, un logiciel tiers ou l'environnement technique de la solution.

e. CCTP-Exigence SECU HOM 005

Le Titulaire réalise le Plan d'Exploitation de Sécurité (PES) regroupant à minima les points suivants :

- Organisation de la sécurité ;
- Sécurité physique ;
- Sécurité des personnes ;
- Sécurité des documents ;
- Sécurité du système d'information ;
- Résilience du système d'information.

f. CCTP-Exigence SECU HOM 006

Le Titulaire doit faire réaliser des audits de sécurité (test d'intrusion, architecture, configuration et audit de code) a minima tous les trois ans. Le rapport d'audit complet doit obligatoirement être communiqué à l'ENAP qui est systématiquement invitée à la réunion de lancement et de restitution.

L'ENAP pourra également à sa charge faire réaliser des audits de sécurité, il devra prévenir le Titulaire. L'ENAP fournira le compte rendu de l'audit au Titulaire.

En cas d'incident lors d'un audit, qu'il ait été demandé par le Titulaire ou par l'ENAP, aucune facturation supplémentaire ne sera demandée à l'ENAP pour la remise en état du SI lié à la prestation.

En cas de faille de sécurité critique le Titulaire devra se mettre en conformité dans un délai de 1 semaine.

Le Titulaire doit lancer les premiers audits dans un délai de 1 an suivant la notification du marché. Le délai de trois ans court à partir de la livraison du premier rapport d'audit.

g. CCTP-Exigence SECU HOM 007

Le Titulaire tient à jour les analyses de risque afin de prendre en compte les vulnérabilités résiduelles et conceptuelles. Il élabore des scénarios d'attaques puis en chiffre les impacts sur le système d'information de l'ENAP.

Le Titulaire justifie dans ce document, le cas échéant, qu'une vulnérabilité identifiée ne peut pas être exploitée dans l'environnement prévu pour le produit.

h. CCTP-Exigence SECU HOM 008

Lorsqu'une vulnérabilité affectant l'un des systèmes d'information de l'ENAP, ne peut pas être corrigée ou contournée, le Titulaire met à jour l'analyse de risques du système et la transmet au plus tôt au Département des Systèmes d'Information (DSI) de l'ENAP.

i. CCTP-Exigence SECU HOM 009

Tout document du dossier d'homologation doit être expressément validé par le DSI de l'ENAP afin d'être considéré comme finalisé. La validation est considérée comme tacite au-delà d'une période de soixante (60) jours à partir de la date de livraison.

Article 8. Obligations du Titulaire sur le Maintien en Condition Opérationnelle (MCO)

Le Titulaire devra corriger les bugs applicatifs

Article 9. Maintenance préventive

Le Titulaire devra informer dans un délai de quinze jours l'ENAP sur les opérations de maintenances planifiées et indiquer le(s) risque(s), l'objet et les délais de mise en œuvre.

Une information aux utilisateurs devra être diffusée sur le portail de l'application au moins 24h avant l'opération via la mise en place d'une page web spécifique.

Article 10. Obligations du Titulaire sur le Maintien en Condition de Sécurité (MCS)

Au titre du MCS, le Titulaire s'assure en permanence que le système reste apte à remplir sa mission de protection de l'information, à compter de l'installation sur site des premiers composants et tout au long de la vie du système.

a. CCTP-Exigence SECU MCS 001

Le Titulaire fournit les solutions de lutte contre les codes malveillants utilisés sur les systèmes des différents projets de l'ENAP ainsi que les mises à jour de sécurité de l'ensemble des constituants des systèmes selon une fréquence et des procédures qui sont définies et acceptées par l'ENAP.

b. CCTP-Exigence SECU MCS 002

En cas de mise en évidence d'une vulnérabilité affectant un système de l'ENAP relevant du marché, le Titulaire collabore avec l'ENAP pour déterminer l'origine de la vulnérabilité et les actions à engager pour sa résolution. Cette activité consiste à :

Maintenir une veille sur les produits et collecter, agréger et synthétiser les informations traitant des évolutions de la menace et des vulnérabilités ;

Collecter les alertes (bulletins) de sécurité observées en production ;

Analyser la criticité d'une alerte ou d'un incident sur le système concerné ;
Proposer des solutions de contournement en cas d'urgence (impossibilité de déployer rapidement un correctif) ;
Recevoir/Récupérer un correctif ;
Qualifier le correctif ;
Déployer le correctif ;
Entretien la documentation système.

c. CCTP-Exigence SECU MCS 004

L'évaluation de la criticité doit utiliser la méthode CVSS (Common Vulnerability Scoring System).

Le système CVSS propose le calcul de trois notes comprises entre 0 (risque nul) et 10 (risque très élevé) :

Note de base : impact maximum théorique ;

Note temporelle : note de base pondérée par les correctifs existants ou a contrario les « exploits » ;

Note environnementale : note temporelle affinée selon les déploiements des systèmes et leur contexte opérationnel. Cette note doit être soumise par le Titulaire au responsable sécurité de l'ENAP (ou un représentant habilité par l'ENAP) pour validation ou modification.

d. CCTP-Exigence SECU MCS 004

Les vulnérabilités découvertes au titre du MCS sont traduites sous forme de fiches de faits techniques de sécurité (FTS) permettant d'en assurer le suivi. Leur traitement (contournement ou correction) est réalisé dans un délai correspondant à un niveau de risque (criticité).

e. CCTP-Exigence SECU MCS 005

Pour les vulnérabilités de criticité « Nul » ou « Faible » découvertes au titre du MCS, le Titulaire applique un correctif suite à sa découverte d'une faille :

Dans les douze (12) mois pour les failles dont la note CVSS est égale à 0.

Dans les six (6) mois pour les failles dont la note CVSS est comprise entre 0 et 3,9.

Les délais sont comptés à partir de la validation par l'ENAP de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

Si les délais ne sont pas respectés, des pénalités de retard seront appliquées.

f. CCTP-Exigence SECU MCS 006

Pour les vulnérabilités de criticité « Moyen » découvertes au titre du MCS, le Titulaire :

Applique, si cela est techniquement possible, une mesure de contournement dans le mois ;

Trouve et applique un correctif dans les trois (3) mois pour les failles dont la note CVSS est comprise entre 4 et 6,9.

Les délais sont comptés à partir de la validation par l'ENAP de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

g. CCTP-Exigence SECU MCS 007

Pour les vulnérabilités de criticité « Elevé » découvertes au titre du MCS, le Titulaire :

Applique une mesure de contournement dans les sept (7) jours ;

Trouve un correctif dans le mois pour les failles dont la note CVSS est comprise entre 7 et 8,9.

En fonction des contraintes techniques, l'application du correctif peut être décalée en commun accord avec l'ENAP et sur justification dûment motivée par le Titulaire.

Les délais sont comptés à partir de la validation par l'ENAP de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

h. CCTP-Exigence SECU MCS 008

Pour les vulnérabilités de criticité « Critique » découvertes au titre du MCS, le Titulaire :
Applique, si cela est techniquement possible, une mesure de contournement dans les quarante-huit (48) heures ;

Trouve et applique un correctif dans les sept (7) jours pour les failles dont la note CVSS est supérieure ou égale à 9. En fonction des contraintes techniques, l'application du correctif peut être décalée en commun accord avec l'ENAP et sur justification dûment motivée par le Titulaire. Les délais sont comptés à partir de la validation par l'ENAP de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

Article 11. Pénalités appliquées dans le cadre de la maintenance

Si le titulaire ne respecte pas les Temps de mise en œuvre des MCS, des pénalités de retard seront appliquées.

Descriptions	Pénalités
Criticité « Critique »	200€ par jour de retard
Criticité « Elevé »	100€ par jour de retard
Criticité « Moyen »	50€ par jour de retard
Criticité « Nul » ou « Faible »	50€ par jour de retard

a. CCTP-Exigence SECU MCS 009

Le Titulaire assure le MCS dès la conception et pendant les évolutions des différents systèmes de l'ENAP définis dans le marché.

b. CCTP-Exigence SECU MCS 010

Le Titulaire analyse pour toute modification d'un des systèmes de l'ENAP réalisée au titre du MCS, les impacts sur la sécurité du système. Cette analyse doit être détaillée dans le document d'analyse de risques du projet, en précisant notamment :

- La description détaillée des modifications ;
- Les éventuelles vulnérabilités engendrées par les modifications ;
- L'impact de ces vulnérabilités sur le système ;
- Les solutions mises en place pour diminuer le risque associé aux modifications (action sur les vulnérabilités ou sur les impacts) ;
- Une estimation du risque résiduel après mise en place des solutions de diminution du risque.

c. CCTP-Exigence SECU MCS 011

Le Titulaire fournit et réalise des tests de non régression relatifs à la sécurité.

d. CCTP-Exigence SECU MCS 012

Le Titulaire garantit que le canal d'approvisionnement des correctifs de sécurité est de confiance. Le Titulaire garantit l'origine, assure un contrôle d'intégrité et en garde une trace pouvant être un élément de preuve en cas d'audit (par exemple : Procès-Verbal de livraison signé).

e. CCTP-Exigence SECU MCS 013

Le Titulaire offre les moyens d'appliquer les correctifs de sécurité sur chaque composant (système ou applicatif) des systèmes de l'ENAP. Cette mise à jour du système est la plus automatisée possible et est tracée dans les journaux.

f. CCTP-Exigence SECU MCS 014

Le Titulaire effectue la mise à jour des documents du dossier de sécurité impactés par les mises à jour du système. Le Titulaire informe le DSI de l'Enap par message en cas d'impossibilité de correction d'une vulnérabilité identifiée dans les plus brefs délais.

g. CCTP-Exigence SECU MCS 015

Le Titulaire identifie, au titre du MCS, les versions de logiciels obsolètes ou qui vont le devenir. Un logiciel qui n'est plus soutenu au niveau sécurité est déclaré obsolète. Cette déclaration est anticipée par le Titulaire en contactant les éditeurs pour obtenir leur calendrier de soutien (calendriers publiés pour les systèmes d'exploitation grand public par exemple).

h. CCTP-Exigence SECU MCS 016

Le Titulaire met en place une gestion de configuration permettant d'assurer l'intégrité et l'authenticité des composants ou correctifs livrés et leur déploiement sur les plates-formes.

i. CCTP-Exigence SECU MCS 017

Le Titulaire garantit que toute évolution majeure des systèmes de l'ENAP s'appuie sur des versions de logiciels à jour en termes de correctifs et annoncées maintenues pendant au moins la durée de Maintien en Condition Opérationnelle (MCO) contractualisée.

Article 12. Obligations du Titulaire à se conformer à l'Etat de l'art

CCTP-Exigence SECU EDA 001

Le Titulaire conçoit, met en œuvre et exploite les systèmes d'information sous sa responsabilité conformément à l'état de l'art en matière de sécurité numérique. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière.

En outre, le Titulaire doit respecter les exigences suivantes pour les services Web et de messagerie qu'il serait amené à fournir :

- **Systèmes :**
 - Installation antivirus à jour
 - Pare-feu system activé et configuration des flux entrants et sortants
 - Flux sortant des serveurs impérativement sur une liste blanche
 - Mises à jour de sécurité installées quotidiennement.
- **Services Web :**
 - Les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, ...) ou une technologie en particulier ;
 - Les mécanismes cryptographiques doivent être conformes aux annexes B du référentiel général de sécurité (RGS)¹ de l'ANSSI.
 - Les mécanismes cryptographiques TLS (HTTPS) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications. L'utilisation de la technologie HSTS est fortement recommandée ;
 - Les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
 - Une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;

¹ <https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/referentiel-general-de-securite/documents-referentiel-general-de-securite/>

- Les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés.
- Services de messagerie :
 - Les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, ...);
 - La mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (norme SPF), signature numérique (norme DKIM), politique de sécurité liant le tout (norme DMARC)).

Dans le cas où l'une des exigences ne peut être appliquée, le Titulaire le fait savoir au plus tôt à l'ENAP. Le Titulaire veille à exercer son devoir de conseil en proposant des mesures permettant de garantir, si cela est possible, un niveau de sécurité identique aux exigences supra dont seul l'ENAP peut valider ou non l'application.

Article 13. Obligations du titulaire en matière de reprise d'activité

Le Titulaire devra restaurer le service en 72h00 quel que soit l'incident ou accident. Il devra rédiger un Plan de Reprise d'Activité (PRA) à destination de l'ENAP.

Article 14. Pénalités d'indisponibilité

Les outils doivent être disponible 24/24 sur et 7j/7 avec une possibilité d'interruption de 8h ouvrées, avec un maximum de 6 fois par an.

Les pénalités seront calculées sur une période d'un an.

Pénalités des heures d'indisponibilité calculées sur une période d'un an		
Disponibilité	Seuils d'indisponibilité	Pénalité par heure d'indisponibilité
Entre 99.99% et 99.95%	Comprise entre 52,56mns et 4h38mns	100€ par heure
Entre 99.95% et 99.9%	Comprise entre 4h38mns et 8h45mns	150€ par heure
< 99.9%	Supérieure à 8h45mns	300€ par heure

Une indisponibilité correspond à arrêt de service de la solution sans que celui-ci ne soit demandé par l'ENAP.

Article 15. Obligations du titulaire en matière de continuité d'activité

a. CCTP-Exigence SECU PCA 001

Le Titulaire devra mettre en œuvre un dispositif technique de PCA en cas de rupture de service. Le Titulaire devra rédiger un PCA à destination de l'ENAP.

b. CCTP-Exigence SECU PCA 002

Le Titulaire précise dans le PES, toutes les dispositions prises (matériels de secours, contrats de service, ...) pour remplacer rapidement tout matériel sous sa responsabilité, endommagé ou perdu (poste de travail, serveur, équipement réseau), qui est utilisé dans le cadre des prestations du marché.

Article 16. Obligations du titulaire sur le traitement des incidents de sécurité

a. CCTP-Exigence SECU INC 001

Le service de supervision du Titulaire met en place un système de remontée d'alerte à l'ENAP, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau, surcharge système de plus 1 minute, indisponibilité de plus de 3 minutes...).

Le Titulaire fournit des précisions pour la mise en place de ce système, en particulier la liste des éléments à superviser pour garantir le bon fonctionnement de l'outil.

L'ENAP sera autorisée à mettre en place son propre système de supervision pour s'assurer du niveau de service délivré via snmpv3 et SSH avec CENTREON et filtrage IP ENAP.

b. CCTP-Exigence SECU INC 002

Le Titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

c. CCTP-Exigence SECU INC 003

Le Titulaire contacte le DSI de l'ENAP pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'ENAP :

- Si cet incident a lieu sur le SI lié à la prestation, le Titulaire autorisera l'ENAP ou un tiers désigné à participer au traitement de l'incident (si l'ENAP le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'ENAP (traitement des causes profondes).

d. CCTP-Exigence SECU INC 004

Le Titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit à l'ENAP sur demande.

e. CCTP-Exigence SECU INC 005

Le Titulaire prévoit dans sa procédure de gestion des incidents un chapitre sur la conservation et la consultation des traces utiles pour mener une analyse forensique suite à une suspicion d'attaque ou une analyse post incident.

Article 17. APPLICATIFS : Obligations du Titulaire sur les prestations d'Etude

a. CCTP-Exigence SECU CPE 001

Le Titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de préproduction.

Article 18. Obligations du titulaire sur la gestion des droits d'accès (serveurs et exploitation)

a. CCTP-Exigence SECU ACCES 001

Le Titulaire doit mettre en place sur l'ensemble de l'infrastructure hébergeant la solution utilisée par l'ENAP, des comptes d'accès nominatifs. Les droits des personnels d'exploitation doivent être limités au strict nécessaire pour la bonne réalisation de leurs missions. Les différents profils et les droits associés sont détaillés dans le PES.

b. CCTP-Exigence SECU ACCES 002

Le Titulaire doit veiller à limiter les droits des accès d'une application aux seuls fichiers légitimes.

Le Titulaire décrit dans le PES les règles de durcissement mises en œuvre pour s'assurer du respect de cette exigence, dès la phase de conception d'une application ou lors de son intégration sur les serveurs de l'ENAP.

c. CCTP-Exigence SECU ACCES 003

Le Titulaire doit garantir que l'accès d'une application à une base de données se fait avec un compte spécifique bénéficiant des privilèges nécessaires et strictement suffisants.

Article 19. Obligations du Titulaire dans la gestion des personnels

a. CCTP-Exigence SECU PERS 001

Le Titulaire a la responsabilité de vérifier que tous les membres de l'équipe de développement ont été formés aux techniques sécurisées de programmation et à la cybersécurité. A ce titre, le Titulaire précise dans le PAS la manière dont il veille à employer des personnels qualifiés dans le cadre des prestations rendues à l'ENAP.

b. CCTP-Exigence SECU PERS 002

Les opérations de maintenance sous la responsabilité du Titulaire sont exécutées par des personnels et sociétés habilités, sous la surveillance des personnels autorisés.

Article 20. Connexion à la plate-forme authentification :

Le Titulaire s'assure que tous les comptes utilisent une authentification multi facteur via mot de passe + otp mail

La stratégie de mots de passe mise en place par le Titulaire doit être conforme aux recommandations de la CNIL (délibération n°2022-100 du 21 juillet 2022).

Lors de la première identification l'utilisateur devra saisir une adresse mail renseignée dans le système et procéder à un renouvellement de mot de passe.

Article 21. Gestion des comptes voyageurs et import

- Les comptes voyageurs apprenants seront automatiquement supprimés de la base de données après sa période de formation à l'Enap majorée de trois mois.
- Les comptes voyageurs agents de l'Enap, seront supprimé automatiquement de la base de données au bout de trois ans sauf si acte positif de sa part (connexion au portail) auquel cas la date est majorée de trois ans après sa dernière connexion au portail (acte positif)
- Les comptes voyageurs extérieurs à l'Enap (chercheur, formateur occasionnel, personnel de l'A.P. ou du ministère non affecté à l'Enap, étudiant en Master 2, autre) seront automatiquement supprimés du système d'information un an après leur dernière connexion au portail.

L'import des voyageurs à partir d'une application interne qui gère les promotions (plus de 1000 élèves) est requis.

Les informations nécessaires pour les imports sont les suivantes: nom, prénom, adresse de messagerie, date de fin de scolarité, qualité et numéro d'identifiant.

Le Titulaire décrira sa procédure d'import des abonnés API REST ou SOAP, csv et ses prérequis techniques et la sécurité

Le Titulaire dressera la liste des contraintes de mise en œuvre nombre de caractères, caractères autorisés par champ.

Les auto inscriptions sont interdites.

Les gestionnaires métiers de la plateforme (services financiers) seront inscrits manuellement.

Article 22. Communication chiffrée

Un certificat numérique est obligatoire. La norme TLS 1.2 ou supérieure doit être respectée pour sécuriser l'accès au site.

Le Titulaire s'emploie à respecter les exigences du référentiel général de sécurité version 2 (RGS)

Article 23. Clause de réversibilité

En cas de résiliation ou d'expiration de tout ou partie des prestations, le Titulaire remet, à ses frais, le système dans l'état dans lequel il l'a trouvé à son arrivée. Le prestataire remettra les données (et les procédures associées) permettant la reprise de l'existant par le prestataire suivant.

L'ENAP est propriétaires de leurs données et de toutes les procédures qui ont été définies ou mises en place avec sa participation.

Avec cette prestation de ce service de réversibilité, l'ENAP remet au prestataire la liste des éléments à fournir ; cette demande pourra être globale ou détaillée. Le format et le mode de transfert seront précisés à cette occasion.

Le prestataire devra au titre de ce service :

- Produire un plan de réversibilité, indiquant notamment la façon dont les périodes de recouvrement sont assurées en fin de marché et le nombre d'ateliers de transfert de compétence proposé,
- Effectuer la livraison des existants (spécifications et données au format XML).

La réversibilité s'effectuera au maximum un mois après la commande.

Article 24. Compatibilité et Portabilité

L'ensemble du portail devra être accessible sur différents supports (Téléphone intelligent, tablette numérique, ordinateur portable ...) et sur les différents OS (Android, IOS, Windows et Mac OS) et différents navigateurs (Edge, Firefox, Safari, Chrome, Opéra, Brave ...) et être développé en Responsive Design

Article 25. Respect des normes et standards

Les solutions proposées doivent respecter les normes et standards suivants :

- Le RGI (Référentiel Général d'Interopérabilité) qui a pour objectif de guider les autorités administratives dans l'adoption de normes, standards et bonnes pratiques, afin de favoriser l'interopérabilité de leurs systèmes d'information.
- Le RGAA (Référentiel Général d'Accessibilité pour les Administrations) qui a pour objectif de favoriser l'accessibilité des contenus diffusés sous forme numérique à travers les canaux Web, Téléphonie, Télévisuel.

Le prestataire ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de L'ENAP.

L'ENAP se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par le titulaire.

Fin du CCTP - SI

(Date, cachet et signature)
Précédés de la mention « *Lu et approuvé* »