Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

Département du TARN
Arrondissement de CASTRES

DECISION N° DC-260311-020
(Commande Publique)
Marché Sans Publicité ni mise en Concurrence (MSPC)
N°2026-TIC-01
« Prestation de sensibilisation et de formation à la cybersécurité par la simulation et l'apprentissage par l'action »

M. le Maire de Saint-Sulpice-la-Pointe,

- Vu l'article L 2122.22 du Code Général des Collectivités Territoriales ;
- Vu les dispositions du Code de la Commande Publique et notamment l'article R.2122-8 permettant à l'acheteur de passer un marché sans publicité ni mise en concurrence préalables lorsque le besoin est inférieur aux seuils réglementaires ;
- Vu la délibération du Conseil Municipal n° DL-240229-0032 du 29 février 2024 relative aux délégations d'attributions du Conseil au Maire ;
- Vu la demande de devis réalisée auprès de trois opérateurs économiques spécialisés dans le domaine d'activité conformément aux bonnes pratiques visant à assurer une utilisation optimale des deniers publics ;
- Vu les trois devis reçus et analysés ;
- Considérant que l'offre de la société **HUCENCY** répond le mieux aux attentes de la Commune au regard du prix et de l'offre de services ;
- Considérant que le montant de la dépense est inférieur au seuil permettant de recourir à un marché sans publicité ni mise en concurrence préalable ;

DÉCIDE,

Article 1. De signer le contrat n° 2026-TIC-01 avec la société **HUCENCY** *(129 rue Delamare Deboutteville 76160 St Martin du Vivier)* pour un montant total de 9 091,90 €HT réparti sur 3 ans soit 3 030,63 €HT / an.

Article 2. De transmettre une ampliation à Monsieur le Sous-Préfet de Castres (Tarn) et à Monsieur le Comptable Public de la Collectivité.

Article 3. De mentionner que la présente décision sera publiée conformément à la réglementation en vigueur puis portée à la connaissance du Conseil Municipal lors de sa prochaine séance.

Saint-Sulpice-la-Pointe, le 11 mars 2026
Le Maire,
Raphaël BERNARDIN

Délai et recours
La présente décision peut faire l'objet d'un recours contentieux devant le Tribunal Administratif de Toulouse dans un délai de deux mois à compter de sa publication.
Cette saisine pourra se faire, pour les particuliers et les personnes morales de droit privé non chargés de la gestion d'un service public, par la voie habituelle du courrier ou via l'application informatique Télérecours, accessible par le lien : http://www.telerecours.fr.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

MARCHÉ VALANT CAHIER DES CHARGES

CONTRAT N° 2026-TIC-01

NOTIFIE-LE

L'ESSENTIEL DU CONTRAT		
	Objet	**PRESTATION DE SENSIBILISATION ET DE FORMATION A LA CYBERSECURITE PAR LA SIMULATION ET L'APPRENTISSAGE PAR L'ACTION**
	Lieu d'exécution	81370 Saint-Sulpice-la-pointe
	Forme de contrat	Ordinaire
	CCAG applicable	CCAG TIC 2021
	Mode de passation	Procédure sans publicité ni mise en concurrence
	Durée / Délai	3 ans, à compter du 1er Mai 2026
	Prix	Prix unitaires / utilisateur

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

SOMMAIRE

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

1 - Parties contractantes

Le contrat est passé entre le pouvoir adjudicateur :
COMMUNE DE SAINT-SULPICE-LA-POINTE
Hôtel de Ville
Parc Georges Spénale
81370 SAINT SULPICE LA POINTE

Et

HUCENCY
129 RUE DELAMARE DEBOUTTEVILLE
76160 ST MARTIN DU VIVIER
SIRET : 83208005500037

Il est convenu ce qui suit :

2 - Objet du marché

L'objet du présent contrat soumis aux dispositions du Code de la commande publique. Il s'agit d'un marché ordinaire.

La Commune de Saint-Sulpice-la-Pointe souhaite renforcer la vigilance de ses agents face à la recrudescence des cyberattaques (phishing, ransomwares, fraude au président). L'objectif est de transformer le facteur humain de vulnérabilité en un levier de défense active.

Le présent contrat définit les prestations attendues dans le cadre de la mise en place d'un programme complet, automatisé et évolutif de sensibilisation à la cybersécurité, reposant sur :

- La simulation d'attaques (phishing, spear-phishing, smishing, quishing, vishing, USB dropping, QR code),
- La formation continue par scénarios,
- L'accès à une plateforme d'e-learning,
- Des outils de signalement et de pilotage,
- La surveillance du dark web et du nom de domaine,
- L'accompagnement par un expert cyber.

L'objectif global est de renforcer la cyber-résilience des agents de la Commune.

3 - Mode de passation

Le marché est passé sans publicité ni mise en concurrence.
Il est soumis aux dispositions des articles L. 2122-1 et R. 2122-8 du Code de la commande publique.

4 - Montant de l'offre

Les prestations seront rémunérées par application aux quantités réellement exécutées des prix unitaires du contrat.

L'évaluation de l'ensemble des prestations à exécuter est la suivante :

☑ **Sensibilisation de 213 utilisateurs (tranche 101-300).**

☑ **BUNDLE:**
- **Sensibilisation**
- **Outil de création**
- **E-learning**
- **Bouton d'Alerte Phishing**
- **ChatBot**
- **Interface Admin**

☑ **240 SMS / AN**

☑ **Co-création jusqu'à 6 scénarios personnalisés par an.**

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

BUNDLE	Phishing Pentest	✓
	Sensibilisation par mises en situation (Mail, USB, QR Code)	✓
	E-Learning	✓
	Bouton d'Alerte Phishing (BAP)	✓
	ChatBot	✓
	Outil de personnalisation de templates (bientôt disponible)	✓
	Administration plateforme	✓
OPTIONS	Surveillance des fuites de données (dark web)	✓
	Surveillance du nom de domaine	✓
	Supervision multi-organisations	
	Langues supplémentaires	
	Smishing	✓
	Smishing étranger	
	Vishing Pentest Offert	
	RTSA	
TARIFS	Paiement	ANNUEL
	Prix / utilisateur / an Prix / utilisateur / mois	14,23 € HT 1,19 € HT
	TOTAL / AN **TOTAL DU CONTRAT**	**3 030,63 € HT** **9 091,90 € HT**

5 - Durée / Délai d'exécution

La durée du marché est de 3 ans à compter du 1er mai 2026, non reconductible, soit une fin fixée au 30/04/2029.

6 - Modalités de règlement des comptes

Les demandes de paiement sont définies sur une fréquence annuelle.
Les modalités de règlement des comptes sont définies dans les conditions de l'article 11 du CCAG-TIC.
Délai global de paiement : 30 jours.

7 - Conditions d'exécution

Le présent contrat sera soumis aux dispositions du CCAG - Technique de l'Information et de la Communication.
Les conditions générales ou particulières de vente ou d'achat du titulaire, sauf lorsqu'elles résultent d'obligations légales impératives, ainsi que toute réserve portant sur les exigences du présent contrat, sont inopposables au pouvoir adjudicateur, quelle qu'en soit la forme.

7.1 CONTEXTE ET ENJEUX

Face à l'augmentation des attaques informatiques (phishing, ransomware, fraude au président), l'humain demeure le principal point d'entrée (entre 80 et 95 % des cyberattaques débutent par du phishing).
Afin de réduire l'exposition et d'améliorer les réflexes de vigilance, la Commune engage un programme proactif basé sur l'apprentissage par la mise en situation.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

Ce programme vise notamment à :

- Réduire significativement le taux de clic sur les attaques simulées,
- Augmenter les signalements via un bouton d'alerte,
- Développer une culture interne de cybersécurité,
- Disposer d'indicateurs mesurables pour l'équipe informatique et le DPO,
- Répondre aux exigences du RGPD en matière de mesures organisationnelles.

7.2 PÉRIMÈTRE ET VOLUMÉTRIE

La solution devra couvrir un effectif de 213 utilisateurs (nombre d'utilisateurs à date de rédaction du CCTP)

7.3 SPÉCIFICATIONS FONCTIONNELLES ET TECHNIQUES

7.3.1 Audit de Vulnérabilité Initiale

Le titulaire réalisera :

- Un audit initial « à blanc » par envoi d'un phishing de référence,
- Une analyse des comportements (ouverture, clic, fourniture d'identifiants),
- Une identification des services les plus vulnérables,
- Un rapport initial de maturité.

7.3.2 Simulations d'attaques (phishing et autres vecteurs)

Le programme devra inclure un large spectre d'attaques :

- Phishing massif,
- Spear-phishing ciblé,
- Quishing (QR code),
- Smishing (SMS),
- USB Dropping,
- QR Code malveillant,
- Attaques scénarisées personnalisables.

Les scénarios devront :

- Évoluer selon l'actualité cyber,
- Être adaptés automatiquement au niveau de chaque utilisateur via un algorithme de difficulté progressive.

7.3.3 Sensibilisation Immédiate :

En cas de clic, l'utilisateur devra être redirigé vers une page d'éducation courte incluant :

- Explication de l'erreur,
- Indices permettant de reconnaître l'attaque,
- Bonnes pratiques à retenir.

7.3.4 Plateforme e-learning :

La plateforme devra proposer à minima :

- Modules interactifs,
- Quiz,
- Fiches mémos,
- Vidéos courtes,
- Actualités cyber régulières,
- Suivi de la complétion par agent.

7.3.5 Services de Surveillance Avancée

Dark Web Monitoring : Surveillance des fuites de données liées aux agents.
Surveillance de domaine : Détection de l'usage malveillant du nom de domaine de la collectivité.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

7.3.6 Outils de Reporting et Pilotage

Bouton d'Alerte :

Installation d'un plug-in Outlook permettant :

- Signalement d'un email suspect en 1 clic,
- Transmission automatique au service informatique / SOC,
- Analyse centralisée.

Interface Admin :

L'interface devra permettre :

- Suivi en temps réel du taux de clic,
- Taux de signalement,
- Typologie des attaques réussies/évitées,
- Progression individuelle et collective,
- Export des rapports pour audits internes ou assurances cyber.

Chatbot d'assistance cyber :

Un chatbot intégré devra permettre aux agents :

- De proposer des scénarios déjà définis, des réponses à choix multiple,
- D'obtenir des réponses pédagogiques immédiates,
- D'améliorer leur autonomie.

Un chatbot intégré devra permettre aux administrateurs :

- De créer nos propres scénarios par le biais d'un éditeur mis à disposition,

7.3.7 Outil de création de scénarios personnalisés

Le marché inclut :

- Un outil de personnalisation de Template (sortie prévue avant fin 1er semestre 2026)
- Jusqu'à 6 scénarios cocréés par an avec un expert cyber.

7.3.9 Kit de Communication et Ressources

Mise à disposition de supports numériques (exemples : affiches avec QR codes, écrans de veille pédagogiques, stickers de rappels)

Accès à des modules de formation théoriques complémentaires en ligne.

7.4 CONTRAINTES TECHNIQUES

7.4.1 Mode de déploiement

- Solution Cloud SaaS hébergée en France (de préférence)
- Aucune installation lourde sur le SI municipal.

7.4.2 COMPATIBILITE

- Outlook (plugin BAP),
- Navigateurs web,
- Windows,
- Intégration collaboratifs (Teams, suite 365, …).

7.4.3 RGPD / Sécurité

Le fournisseur devra :

- Respecter strictement le RGPD,
- Stocker les données en France,
- Garantir la confidentialité des résultats individuels,
- Ne pas utiliser les données à des fins commerciales.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

7.4.4 Livrables et Accompagnement.

Livrables attendus

Livrable	Fréquence
Rapport initial de maturité	Une fois
Rapports trimestriels d'avancement	Trimestriel
Rapport annuel consolidé	Annuel
Statistiques détaillées par agent	En continu
Exports pour audit / assurance	À la demande
Scénarios personnalisés	Jusqu'à 6/an

Accompagnement

Le titulaire doit assurer :

- Un accompagnement par un chargé de compte dédié joignable par mail et/ou téléphone
- Conseil dans l'analyse des résultats,
- Aide au pilotage du plan de sensibilisation.

7.5 MODALITÉS D'EXÉCUTION

7.5.1 DEPLOIEMENT :

Mode SaaS (Cloud), hébergement et conception en France de préférence

7.5.2 Accompagnement :

Un Customer Success Manager dédié avec 3 points de suivi annuels.

7.5.3 Critères de conformité de la solution

La solution sera évaluée sur :

- Pertinence des scénarios et réalisme des attaques,
- Qualité de l'algorithme d'adaptation,
- Simplicité pour les agents,
- Diversité des vecteurs d'attaque (mail, SMS, téléphone, QR…),
- Qualité du tableau de bord,
- Capacité d'accompagnement.

7.5.4 Clauses de réversibilité

En fin de marché, le titulaire fournira :

- L'intégralité des statistiques,
- Les scénarios créés,
- Un export intégral du suivi agent,
- Suppression des données dans un délai de 60 jours.

7.5.5 Clause de confidentialité

Le titulaire s'engage à respecter une stricte confidentialité concernant l'ensemble des informations, données, documents ou éléments auxquels il pourrait avoir accès dans le cadre de l'exécution du présent marché.

7.6 NIVEAUX DE SERVICE ET PENALITES (SLA)

7.6.1 Objet du SLA

Le présent Accord de Niveau de Service (SLA) définit les engagements techniques, opérationnels et qualitatifs du Fournisseur concernant la disponibilité, la performance, la conformité fonctionnelle et la production des rapports liés à la plateforme SaaS de sensibilisation et de formation à la cybersécurité.
Les modalités de pénalités en cas de non-respect sont également décrites.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

7.6.2 Définitions

- **Plateforme** : solution SaaS de formation et simulation d'attaques (phishing simulé, modules interactifs, parcours d'apprentissage, reporting…).
- **Indisponibilité** : impossibilité totale pour les utilisateurs d'accéder à la plateforme ou exécution dégradée rendant l'usage impossible (erreurs 5xx, SSO inopérant, latence > 10 secs en continu, etc.).
- **Fenêtre de maintenance** : périodes programmées, communiquées au client avec un préavis de 7 jours, non comptabilisées dans l'indisponibilité.
- **Rapports** : documents ou exports prévus au contrat (rapports mensuels, bilans de campagne, indicateurs pédagogiques, statistiques de phishing, etc.).
- **Périmètre fonctionnel** : ensemble des fonctionnalités intégrées au contrat (modules, scénarios, reporting, intégrations techniques…).

7.6.3 Disponibilité du service

Engagement de disponibilité :

Le Fournisseur garantit une disponibilité annuelle **≥ 98 %** hors fenêtres de maintenance.

Calcul :

$$Disponibilité = 1 - \frac{\text{Durée d'indisponibilité}}{\text{Durée totale}}$$

Exclusions :

- Maintenances planifiées notifiées 7 jours ouvrés à l'avance
- Indisponibilité imputable au client (réseau interne, SSO interne, firewall…)
- Cas de force majeure (selon droit applicable)

7.6.4 Production des rapports

Types de rapports :

- **Rapport mensuel d'activité** (statistiques, taux de complétion, performances)
- **Rapport par campagne** (phishing simulé, modules spécifiques)
- **Rapport incident sécurité** (selon SLA interne, si applicable)

Délais de livraison :

- Rapport mensuel : **J + 5 ouvrés**
- Rapport de campagne : **J + 7 ouvrés**
- Rapport incident de sécurité : **J + 1 ouvré**

7.6.5 Respect du périmètre fonctionnel

Engagements :

Le Fournisseur s'engage à fournir l'ensemble des fonctionnalités prévues au contrat, notamment :

- Modules de formation (e-learning, micro-learning, vidéos, quiz)
- Scénarios de simulation (phishing, smishing, USB drop, etc.)
- Outils de reporting et dashboards
- Intégration SSO / LDAP / Azure AD (le cas échéant)
- Multilinguisme prévu
- Fonctionnalités de gestion des utilisateurs

Conformité :

Un écart est considéré comme :

- **Mineur** si l'usage est possible mais réduit
- **Modéré** si l'usage est dégradé mais les objectifs pédagogiques atteignables
- **Critique** si l'usage normal est impossible

Pénalités :

Les pénalités ci-dessous sont appliquées automatiquement sur la facture annuelle ou trimestrielle du Fournisseur. Elles sont **cumulables**, dans la limite d'un plafond de **30 % du montant annuel du contrat**.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

7.6.6 Pénalités – Indisponibilité de la plateforme

Applicable dès dépassement de **12 % d'indisponibilité annuelle**.

Indisponibilité annuelle constatée	Pénalité appliquée
> 12 % et ≤ 15 %	5 % du montant annuel du contrat
> 15 % et ≤ 20 %	10 % du montant annuel
> 20 %	15 % du montant annuel + faculté de résiliation pour faute

7.6.7 Pénalités – Retard ou absence de rapports

Pour chaque rapport non remis dans les délais contractuels :

Retard constaté	Pénalité
1 à 7 jours	1 % du montant annuel par rapport
8 à 15 jours	2 % du montant annuel par rapport
> 15 jours ou absence totale	3 % par rapport + mise en demeure

7.6.8 Pénalités – Non-respect du périmètre fonctionnel

Type d'écart	Exemples	Pénalité
Mineur	Option de filtre manquante	1 % / fonctionnalité
Modéré	Module incomplet, scénario partiel	3 % / fonctionnalité
Critique	Impossibilité d'utiliser un module clé, échec SSO	5 % / fonctionnalité
Écart non corrigé sous 30 jours	Manquement persistant	+5 % supplémentaires

7.7 PLAFOND ANNUEL DES PÉNALITÉS

Le cumul des pénalités financières ne peut dépasser **30 % du montant annuel du contrat**.
Au-delà ou en cas de manquement grave récurrent, le Client peut :

- Déclencher une **clause de remédiation**,
- Demander un **audit technique**,
- Engager une **résiliation anticipée pour faute**.

7.8 SUIVI ET GOUVERNANCE

- **Comité de pilotage trimestriel** : revue des indicateurs SLA, incidents, roadmap formation.
- **Comité opérationnel mensuel** : suivi des campagnes, taux de complétion, incidents techniques.
- **Responsables désignés** : un référent Client / un référent Fournisseur.

7.9 REVISION DU SLA

Le présent SLA peut être revu annuellement, notamment en fonction des exigences cybersécurité en vigueur, des retours utilisateurs, ou de l'évolution du périmètre.

7.10 ENTREE EN VIGUEUR

Le présent SLA entre en application à la date de signature du contrat et demeure valide pendant toute sa durée.

7.11 OBLIGATIONS GÉNÉRALES

Le titulaire, ainsi que l'ensemble de ses collaborateurs, sous-traitants, partenaires ou intervenants :

- S'engagent à ne divulguer aucune information relative à la Commune de Saint Sulpice la Pointe, à ses agents, à son infrastructure ou à son système d'information ;
- S'engagent à ne pas utiliser les informations obtenues dans le cadre du marché à d'autres fins que celles strictement nécessaires à son exécution ;
- S'engagent à protéger les données traitées, conformément aux exigences du RGPD et des politiques internes de sécurité de la collectivité ;
- S'engagent à restreindre l'accès aux seules personnes dûment habilitées à intervenir sur les prestations.

Envoyé en préfecture le 13/03/2026
Reçu en préfecture le 13/03/2026
Publié le 16/03/2026
ID : 081-218102713-20260311-DC260311020-AR

7.12 DUREE DE L'OBLIGATION

Cette obligation de confidentialité s'applique :

- Pendant toute la durée du marché,
- Et demeure en vigueur pendant cinq (5) ans après son expiration ou sa résiliation, quels qu'en soient le motif ou les circonstances.

7.13 DONNEES SENSIBLES ET RESULTATS INDIVIDUELS

Le titulaire reconnaît que :

- Les résultats individuels issus des tests de phishing, évaluations, scénarios ou modules ne peuvent en aucun cas être communiqués à des tiers ;
- Aucune donnée ne peut être utilisée à des fins statistiques, commerciales ou d'entraînement algorithmique en dehors du cadre contractuel, sauf accord express et écrit de la collectivité.

7.14 SOUS-TRAITANCE

Toute sous-traitance impliquant l'accès à des informations confidentielles doit :

- Être préalablement autorisée par la Commune,
- Faire l'objet d'une clause contractuelle de confidentialité au moins équivalente à la présente.

7.15 MESURES TECHNIQUES

Le titulaire mettra en œuvre :

- Des mesures de sécurité adaptées (chiffrement, cloisonnement, contrôle d'accès),
- Un hébergement préférentiellement en France
- Des procédures garantissant l'intégrité et la confidentialité des données collectées dans le cadre du programme (tests, clics, signalements, statistiques).

7.16 RESTITUTION ET DESTRUCTION DES DONNEES

À l'issue du marché, et en complément de la clause de réversibilité :

- Toutes les données devront être restituées à la Commune,
- Puis supprimées des systèmes du titulaire dans un délai maximum de 60 jours,
- Une attestation de destruction devra être fournie.

Signature du pouvoir adjudicateur
Le
À

Signature de l'entreprise
Le
À