|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |
| --- | --- |
| **2020_logo_signature_mail_directions_DGRH** |  |

**CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES**

**Annexe I de sécurité**

Expertise indépendante de la solution de vote électronique  
mise en œuvre pour les élections professionnelles en 2026 et en 2027  
au ministère de l’éducation nationale et de l’enseignement supérieur et de la recherche et du ministère des sports, de la jeunesse et de la vie associative

Sommaire

[1. Mesures de sécurité relatives à l’accès aux locaux de l’administration 2](#_Toc191820044)

[2. Protection des informations sensibles 3](#_Toc191820045)

[2.1. Principes 3](#_Toc191820046)

[2.2. Protection des informations sensibles sur support papier 4](#_Toc191820047)

[2.3. Protection des informations sensibles sur support électronique 4](#_Toc191820048)

[2.4. Sécurisation des locaux du titulaire 5](#_Toc191820049)

[2.5. Modalités d’exécution 5](#_Toc191820050)

[3. Acronymes 6](#_Toc191820051)

[4. Identification et signature 6](#_Toc191820052)

# Mesures de sécurité relatives à l’accès aux locaux de l’administration

Le secrétariat général des ministères de l’éducation nationale et de l’enseignement supérieur et de la recherche d’une part, et des sports, de la jeunesse et de la vie associative d’autre part, est désigné dans le présent document sous l’appellation « ministère » ou « ministères » ou encore « administration ».

Tout agent du titulaire, que celui-ci soit l'un de ses salariés ou salarié d'un des sous-traitants du titulaire, devant avoir accès aux locaux de l'Administration doit être préalablement nommément agréé selon la procédure en vigueur aux ministères. Cet agent du titulaire demeure soumis pendant son séjour dans les locaux de l’administration aux mêmes règles intérieures que les agents de l’administration, notamment les politiques et procédures de sécurité des systèmes d’information, ainsi que les chartes administrateurs et utilisateurs. L’administration peut retirer son agrément à tout moment sans avoir à énoncer ses motifs, le titulaire doit alors proposer immédiatement un remplaçant de niveau équivalent.

L'intervention dans les locaux de l'administration est conditionnée à l'obtention d'une autorisation d'accès délivrée à l'agent du titulaire après enquête diligentée par le service de sécurité compétent pour l'autorité contractante au profit de laquelle est exécuté l'accord-cadre désigné par le « marché ». Il est fait obligation au titulaire de fournir à l'administration :

* Le patronyme et les prénoms de son agent ;
* Une photocopie lisible et recto-verso d’un titre d'identité dont la nature varie selon la situation individuelle de l'agent visé :
  + Carte nationale d’identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires ;
  + Titre de séjour en cours de validité avec une autorisation de travail valable ou carte de résident pour les étrangers extracommunautaires ;
* Adresse actuelle de l'agent si celle-ci diffère de celle portée sur le titre d'identité fourni.

Au surplus, dès signature du marché le liant à l'administration et avant tout commencement d'exécution, le titulaire a obligation de communiquer à l'administration la liste de ses agents, que ceux-ci soient un de ses salariés ou salariés d'un de ses sous-traitants, susceptibles d'intervenir dans l'exécution du marché (ci-après désignée par la "Liste"). Tout changement dans la composition de cette Liste doit être porté à la connaissance de l'administration sans délai.

Le titulaire s'engage à prendre toutes les mesures nécessaires et conformes à l’état de l’art en matière de sécurité des systèmes d’information pour assurer, lors de l'exécution du marché, la protection effective et efficace des informations ou supports qui peuvent être détenus dans le service, au profit duquel le marché est exécuté, ou dans tout lieu où ce marché est exécuté.

Le titulaire reconnaît avoir pris connaissance des dispositions de l'arrêté du 9 août 2021 portant approbation de l’instruction générale interministérielle n°1300 (IGI 1300) sur la protection du secret de la défense nationale.

Le titulaire reconnaît avoir fait signer par tous les agents, appelés sous sa responsabilité à un titre quelconque à intervenir pour le compte du titulaire dans le cadre de l'exécution du marché, une déclaration individuelle d’engagement et de reconnaissance de responsabilité (ci‑après désignée par « ERR ») par lequel les dits agents attestent d’une part, avoir pris connaissance des dispositions de l’IGI 1300 et des articles 413-9 à 413-12 du code pénal, et d’autre part, qu'ils n'ont pas, sous peine de poursuite pénale, à connaître ou détenir des informations sensibles de l’administration ou des informations couvertes par le secret de la défense nationale.

Le titulaire s'engage à ce que seules les personnes physiques ayant préalablement souscrit l’ERR précité interviennent de quelque manière que ce soit dans l'exécution du marché. Le titulaire s’engage à remettre à au ministère les ERR avant tout commencement d'exécution du marché.

**Modalités de transmission de la Liste et des ERR :**

Dans les trois (3) jours ouvrés suivant la notification du marché et avant tout commencement d’exécution des prestations, le titulaire doit dresser la Liste des agents susceptibles d’intervenir à quelque titre que ce soit dans le cadre du marché. Chaque agent de la Liste doit obligatoirement compléter et signer un ERR.

La Liste et les ERR doivent être transmis avant commencement d’exécution à la direction projet de l’administration, ainsi qu’aux agents SSI de l’autorité contractante dont les coordonnées auront été communiquées par l’administration au titulaire.

Aucune dérogation aux présentes mesures de sécurité ne pourra être acceptée de l'autorité contractante ou exigée d'elle, y compris en vue de pourvoir au remplacement inopiné, fortuit ou même urgent d'un agent du titulaire.

Le non-respect ou l’inobservation par le titulaire de ces mesures de sécurité, même dans les cas où ils résultent d'une imprudence ou d'une négligence, peuvent entraîner le prononcé de sanctions contractuelles, sans préjudice des sanctions pénales.

# Protection des informations sensibles

## Principes

Par défaut, toutes les informations de l’administration doivent être considérées comme "sensibles" et notamment soumises aux dispositions de l’instruction interministérielle n° 901 (II 901). Des informations sensibles peuvent se voir attribuer une protection par un marquage « Diffusion Restreinte » selon les règles notamment posées par l'IGI 1300. Les informations « Diffusion Restreinte » sont déterminées en fonction de la nature de la prestation et du type de données à protéger dans le marché. Sont notamment systématiquement considérés comme « Diffusion Restreinte » :

* Les plans d'adressage IP de l’Administration (ou une partie de ces plages si cela permet de cartographier un sous-ensemble du système d’information) ;
* Les mots de passe ;
* Les fichiers de configuration ;
* Les codes sources des applications ;
* Les fiches d'expression rationnelle des objectifs de sécurité (FEROS) et dossiers d'analyse de risques ;
* Les dossiers de sécurité des systèmes d'information de l’Administration, que ces systèmes soient en mode projet ou en mode opérationnel ;
* Les dossiers d'architecture et d'installation ;
* Les données de production ;
* Toute donnée à caractère personnel.

Les informations sensibles classifiées "diffusion restreinte" sont marquées avec la mention "Diffusion Restreinte" conformément au modèle ci-dessous :

**DIFFUSION RESTREINTE**

Pour les documents papier, cette mention « Diffusion Restreinte » est portée en haut de toutes les pages du document.

Les informations techniques au format électronique, ne pouvant donc faire l’objet d’un marquage réglementaire comme indiqué ci-dessus (comme par exemple les journaux d’évènements, les fichiers de configuration, les codes sources), sont de facto considérées comme « Diffusion Retreinte » et le titulaire a l'obligation d'appliquer les dispositions réglementaires qui s’imposent pour la gestion de ces données.

Toute information sensible dont le titulaire a connaissance à l'occasion de l'exécution du marché ne peut en aucun cas être communiquée à un tiers (autre que les agents du titulaire préalablement déclarés et autorisés par l'administration dans la Liste) sans accord préalable exprès et écrit de l’administration.

La réalisation d'une copie sans autorisation préalable est considérée par l’administration comme une violation des dispositions relatives au respect du secret dans l'exécution du marché.

La Politique de Sécurité des Systèmes d'Information de l’administration, comme la PSSI pertinente pour le service au profit duquel le marché est exécuté, sont réputées connues du titulaire comme de ses agents de la Liste qu'il aura déclarée à l'administration préalablement à tout commencement d'exécution du marché. Le titulaire s’engage à respecter, et faire respecter par ses agents, l'ensemble des obligations de ces PSSI.

Dans les locaux du prestataire, les informations sensibles font l'objet d'une gestion spécifique. Le titulaire s'engage à ce que les informations sensibles, pendant tout leur cycle de vie, ne puissent être portées, même fortuitement, à la connaissance de personnes n'ayant pas le besoin d'en connaître.

## Protection des informations sensibles sur support papier

Le titulaire a l'obligation de mettre en place un système de gestion permettant d'identifier tous les documents comportant des informations sensibles, quel que soit leur marquage, et pour chacun de ces documents ainsi identifié :

* De connaître la liste des personnes physiques comme morales en ayant eu connaissance ou communication ;
* D'en connaître soit la date de restitution à l'administration soit la date de destruction, ainsi que le nom et la qualité de la personne ayant réalisé l'opération. En cas de destruction des documents, celle-ci doit être réalisée par broyage ou incinération. En cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui est remis le document. Au surplus, le bordereau doit stipuler que le titulaire certifie n'avoir ni établi ni conservé de copie du document.

La diffusion des documents papier se fait sous double enveloppe. L'enveloppe extérieure ne porte aucune mention particulière hormis le nom et l'adresse du destinataire. L'enveloppe interne porte le nom du destinataire et la mention pertinente, à savoir "Sensible" ou "Diffusion Restreinte". Les agents du titulaire qui gèrent les arrivées courrier doivent être sensibilisés à l'usage de ces mentions, ne pas ouvrir l'enveloppe et la distribuer au destinataire.

## Protection des informations sensibles sur support électronique

Il est fait obligation au titulaire que le traitement des informations sensibles sur support électronique ne soit pas réalisé sur des moyens informatiques connectés à un réseau non maîtrisé. L'administration considère qu'un réseau d'entreprise connecté à Internet ne permet pas de garantir ce niveau adéquat de protection des informations sensibles.

Le cas échéant, le titulaire peut s'efforcer de démontrer à l'administration son aptitude à protéger les informations sensibles qu'il serait amené à traiter en dehors des systèmes d'information de l’administration. Pour ce faire :

* Soit l'isolation des moyens de traitement des informations s'effectue de manière physique ;
* Soit cette isolation s'effectue par une interface logique de sécurité présentant des garanties suffisantes afin d'empêcher l'accès aux moyens de traitement des informations sensibles par des tiers.

Le titulaire doit alors soumettre à l'administration une documentation relative aux règles de gestion et aux règles techniques de sécurité de ces moyens de traitement des informations sensibles. Ces règles de gestion et règles techniques de fonctionnement concourant à la sécurité des informations sensibles doivent faire l'objet d'une validation formelle par l'administration. Cette dernière se réserve le droit de procéder à leur contrôle préalablement à toute validation comme après validation pendant l'exécution de l’accord-cadre.

Il est fait obligation au titulaire de respecter le besoin d'en connaître : seuls les agents de la Liste ont accès aux informations nécessaires pour l'exécution de l’accord-cadre. Le respect de cette obligation par le titulaire doit être garanti par la mise en place et l'utilisation de mécanismes de sécurité telle que notamment l’authentification individuelle, la gestion des droits et la traçabilité des accès.

La confidentialité des informations sensibles, quel que soit leur marquage, sur support électronique est réalisée au moyen d'un mécanisme de chiffrement reposant sur un logiciel "qualifié" par l'Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI). Ces logiciels sont fournis par l’administration et un document relatif à l’utilisation de ces logiciels est remis au titulaire dès signature de l’acte d’engagement de l’accord-cadre, il doit faire l'objet d'une diffusion auprès des agents de la Liste.

Au terme de la durée de validité de l’accord-cadre, le titulaire procède soit à la restitution, soit à la destruction de l’ensemble des informations sensibles sur support électronique et des documents associés incluant les courriels :

* En cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui sont remis les informations sensibles sur support électronique, en déclare la liste et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles ;
* En cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie les supports électroniques détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les moyens de destruction utilisés. Ce bordereau est transmis à l'administration sans délai et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles.

## Sécurisation des locaux du titulaire

Dans le cas où des informations sensibles, quel que soit leur marquage et quelle que soit la forme de leur support, sont appelées à être conservées dans les locaux du titulaire, leur support papier ou électronique doit être disposé en dehors de son utilisation dans des armoires fermant à clé et dont la clé est conservée par la seule personne responsable de son utilisation.

Préalablement à toute exécution de l’accord-cadre, le titulaire doit désigner un responsable sécurité qui devient l'interlocuteur privilégié de l'administration pour tous les sujets de sécurité pendant l'exécution de l’accord-cadre.

L'administration se réserve le droit de vérifier le niveau de compétences en SSI de ce responsable et de le récuser si elle juge ce niveau insuffisant, le titulaire ayant alors l'obligation de proposer sans délai à l'administration un nouveau responsable sécurité. Il appartient à ce responsable sécurité de sensibiliser les agents de la Liste pour un strict respect des obligations du titulaire en matière de SSI et d'en présenter un bilan sur simple demande formulée par l'administration.

## Modalités d’exécution

A tout moment pendant l'exécution de l’accord-cadre, l’administration se réserve le droit de réaliser tout contrôle, après un préavis de vingt-quatre (24) heures, dans les locaux du titulaire pour vérifier que sont effectivement respectées les préconisations validées par l'administration s'agissant des règles de gestion et des mesures techniques de sécurisation des moyens de traitement des informations sensibles de l’administration.

En cas de défaillance constatée dans la mise en œuvre de mesures de sécurité en adéquation avec le niveau de sensibilité des données traitées, il pourra être fait obligation au titulaire de réaliser à ses frais tous travaux de mise en conformité de ses locaux. En cas de refus, des pénalités pour violation des obligations de sécurité ou de confidentialité seront appliquées et l’accord-cadre pourra être résilié aux torts du titulaire.

Le titulaire a le devoir d’informer sans délai l’administration de toute difficulté dans l’application de ces mesures, de fuite ou de suspicion de fuite d’informations sensibles qu’il rencontre ou constate.

# Acronymes

|  |  |
| --- | --- |
| CNI | Carte Nationale d'Identité |
| DR | Diffusion Restreinte |
| DGRH | Direction Générale des Ressources Humaines |
| II | Instruction Interministérielle |
| IGI | Instruction Générale Interministérielle |
| IP | Internet Protocol |
| PSSI | Politique de Sécurité des Systèmes d'Information |
| RSSI | Responsable de la Sécurité des Systèmes d’Information |
| SSI | Sécurité des Systèmes d'Information |

# Identification et signature

|  |  |
| --- | --- |
| **Nom et prénom de la personne physique signataire** |  |
| **Qualité du signataire** Cette information doit permettre d'établir que la personne physique titulaire de l'annexe a bien autorité pour engager la responsabilité de la personne morale du prestataire |  |
| **Identification du titulaire pour le compte duquel le signataire intervient** |  |

|  |  |
| --- | --- |
| Cartouche destiné à recevoir la signature de la personne physique engageant la responsabilité de la personne morale du titulaire.  Cette signature doit être précédée par les mentions :   * "Fait à :" suivie de l'identification du lieu où a été apposée la signature ; * "Le : " suivie de la date de la signature.   En application des dispositions de l'article 1367 du code civil, cette signature manifeste le consentement du titulaire aux obligations qui découlent de cette annexe de sécurité. | **Fait à                                   Le** |