DISPOSITIONS RELATIVES À LA CLASSIFICATION, À L'HABILITATION ET À LA PROTECTION DU SECRET DE SÉCURITÉ NATIONALE

Annexe à l'Arrêté Ministériel n° 2016-723
du 9 décembre 2016

ANNEXE AU « JOURNAL DE MONACO » N° 8.308

DU 16 DECEMBRE 2016

SOMMAIRE

Table des matières

INTRODUCTION

Certaines informations présentent, en cas de divulgation, un risque tel d'atteinte à la sécurité nationale que seules certaines personnes sont autorisées à y accéder. Considérer qu'une information présente ce risque conduit le Gouvernement Princier à la classifier, c'est-à-dire à lui conférer le caractère de secret de sécurité nationale et à la faire bénéficier d'une protection juridique et matérielle stricte.

La présente annexe décrit l'organisation générale de la protection du secret de sécurité nationale. En s'efforçant de clarifier les obligations juridiques et matérielles inhérentes à cette protection, elle précise les conditions dans lesquelles le Ministre d'Etat et chaque Conseiller de Gouvernement-Ministre, pour chaque direction et service dépendant de son autorité, met en œuvre l'application de ces dispositions, en veillant à limiter le nombre et le niveau des habilitations et la production de documents classifiés à ce qui est strictement nécessaire, afin de garantir la plus grande efficacité du dispositif.

Elle définit également les procédures d'habilitation et de contrôle des personnes pouvant avoir accès au secret, les conditions d'émission, de traitement, d'échange, de conservation ou de transport des documents classifiés et veille aux modalités de leur protection que ce soit sur le support papier ou informatique.

La présente annexe détermine en outre les critères, les niveaux et les conditions de classification des informations et supports concernés ainsi que les règles d'accès aux lieux abritant de telles informations.

Elle prend également aussi en compte l'accroissement constaté des échanges d'informations classifiées, au niveau national ou au niveau international. Dès lors que tous les Etats protègent leurs informations classifiées, Monaco, au titre des accords de sécurité conclus, est tenue de garantir, à charge de réciprocité, la protection des informations classifiées qui lui sont transmises par les Etats parties.

Enfin, il appert que la protection du secret de sécurité nationale ne se limite pas aux documents classifiés sur support papier mais s'étend également aux moyens informatiques et électroniques servant à leur élaboration, leur traitement, leur stockage et leur transmission. La menace constante d'une attaque informatique multiforme et la possibilité, à tout moment, de compromission à l'insu même de l'utilisateur exigent, en réponse, des règles de sécurité des systèmes d'information adaptées à l'évolution rapide des techniques et une expertise fortement développée auprès de tous les acteurs publics ou privés.

Dans la suite du document, les termes *« Secret de Sécurité Nationale »*, avec majuscules, font référence au niveau de classification. Les termes « secret de sécurité nationale », avec minuscules, font référence à la notion de secret créée par l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée.

TITRE I^ER
PRINCIPES ET ORGANISATION DE LA PROTECTION

La protection du secret de sécurité nationale concerne tous les domaines d'activité relevant de la sécurité nationale. Sont classifiées les informations dont la divulgation est de nature à porter atteinte à ladite sécurité.

La Principauté de Monaco peut également protéger les informations échangées avec les organisations internationales et les Etats étrangers.

La protection du secret de sécurité nationale est assurée par une chaîne de responsabilité, qui s'applique aux domaines public et privé.

Le Ministre d'Etat est l'autorité nationale de sécurité (ANS).

CHAPITRE I^ER
PRINCIPES GÉNÉRAUX DE LA PROTECTION DU SECRET DE SÉCURITÉ NATIONALE.

Paragraphe 1

Fondements de la protection

Certaines informations intéressant la protection des intérêts fondamentaux de la Principauté nécessitent une protection particulière, permettant d'en maîtriser et d'en limiter la diffusion, dans des conditions définies dans la présente annexe.

L'atteinte pouvant être portée à la protection desdits intérêts fondamentaux par la divulgation de certaines informations ou de certains supports justifie leur classification. Les informations et support classifiés visés au premier alinéa de l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée, font l'objet d'une classification comprenant trois niveaux :

1° Très Secret de Sécurité Nationale ;

2° Secret de Sécurité Nationale ;

3° Confidentiel-Sécurité Nationale.

Peuvent faire l'objet de ces classifications les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation est de nature à nuire à la sécurité nationale ou pourrait conduire à la découverte d'un secret de sécurité nationale.

La politique de protection du secret de sécurité nationale vise à rendre responsable, pénalement et administrativement, toute personne ayant accès à des informations ou supports classifiés.

Une information classifiée est compromise lorsqu'elle est portée à la connaissance du public ou d'une personne non habilitée ou n'ayant pas le besoin d'en connaître. L'évaluation des risques de compromission des informations ou supports classifiés et des vulnérabilités des personnes ou des systèmes les traitant, au regard de la protection des intérêts fondamentaux de la Principauté, est essentielle afin de garantir la protection du secret de sécurité nationale. La stricte application des mesures de sécurité définies dans la présente annexe, complétée par la diffusion de règles et la sensibilisation des personnels, contribue à l'efficacité du dispositif et permet de lutter contre des actions malveillantes, souvent facilitées par l'ignorance, l'imprudence, l'inattention ou la négligence.

La protection du secret de sécurité nationale, qu'il s'agisse d'une information ou d'un support, doit être assurée par les personnes, physiques ou morales, de droit public ou de droit privé, y accédant. En cas de manquement, même involontaire, ces personnes se rendent coupables de compromission et encourent les sanctions prévues à l'article 19 de la loi n° 1.430 du 13 juillet 2016, précitée.

Paragraphe 2
Définitions

Comme indiqué à l'article 2 de l'arrêté auquel est rattachée cette annexe :

Le niveau *« Très Secret de Sécurité Nationale »* est réservé aux informations et supports qui concernent les priorités gouvernementales en matière de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la protection des intérêts fondamentaux de la Principauté ;

Le niveau *« Secret de Sécurité Nationale »* est réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la protection des intérêts fondamentaux de la Principauté ;

Le niveau « *Confidentiel-Sécurité Nationale »* est réservé aux informations et supports dont la divulgation est de nature à nuire à la protection des intérêts fondamentaux de la Principauté ou pourrait conduire à la découverte d'un secret classifié au niveau *« Très Secret de Sécurité Nationale »* ou *« Secret de Sécurité Nationale »*.

Au sens de la présente annexe, il faut entendre par :

- *« habilitation »* : décision explicite, prise et délivrée à l'issue d'une procédure spécifique définie dans la présente annexe, permettant à une personne, en fonction de son besoin d'en connaître, d'avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s) ;

- *« informations ou supports classifiés »* : procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de sécurité nationale ;

- *« systèmes d'information »* : ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire l'information.

Paragraphe 3
Champ d'application

Les dispositions de la présente annexe sont applicables à l'ensemble des services placés sous l'autorité directe du Ministre d'Etat et des Conseillers de Gouvernement-Ministres, aux entités placées sous leur tutelle ainsi que, de manière générale, aux autres entités, publiques ou privées, concernées par le secret de sécurité nationale, ainsi qu'à toute personne dépositaire, même à titre provisoire, d'un tel secret, y compris dans le cadre de la passation et de l'exécution d'un contrat.

Les informations ou supports classifiés confiés à la Principauté de Monaco, en application d'un accord de sécurité, bénéficient des mesures de protection du secret de sécurité nationale en fonction des concordances définies par ledit accord, dès lors qu'elles portent une mention de classification équivalente à l'un des trois niveaux définis.

Paragraphe 4
La classification

La décision de classifier au titre du secret de sécurité nationale une information ou un support a pour conséquence de le placer sous la protection de dispositions spécifiques de la loi. L'apposition du marquage de classification constitue le seul moyen de lui conférer cette protection particulière.

Une information, n'ayant pas fait l'objet d'une décision de classification à l'un des trois niveaux définis, n'est pas protégée pénalement au titre du secret de sécurité nationale. Aussi le fait d'omettre de procéder à la classification d'une information dont la divulgation est de nature à nuire au secret de sécurité nationale, caractérise une faute, qu'il revient à l'autorité hiérarchique d'apprécier et, le cas échéant, de sanctionner conformément au régime disciplinaire applicable.

Paragraphe 5
Mentions particulières de confidentialité

Certaines informations qu'il n'y a pas lieu de classifier peuvent cependant recevoir, de la part de leur émetteur, une marque de confidentialité destinée à restreindre leur diffusion à un domaine spécifique (précisé par une mention particulière[1]) ou à garantir leur protection (telle que Diffusion Restreinte).

Ces mentions, qui ne traduisent pas une classification, ne suffisent pas à conférer aux informations concernées la protection pénale propre au secret de sécurité nationale. Leur seul objectif est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

L'auteur de la divulgation, qu'il relève de la sphère publique ou de la sphère privée, s'expose à des sanctions disciplinaires et professionnelles[2], sans préjudice de l'application éventuelle des dispositions spécifiques aux traitements d'informations nominatives contenues dans la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée

Paragraphe 6
L'accès aux secrets de sécurité nationale

Seules des personnes habilitées peuvent accéder aux secrets de sécurité nationale.

Une personne habilitée, sous réserve du besoin d'en connaître, peut avoir accès aux informations ou supports classifiés au niveau précisé dans la décision d'habilitation ainsi qu'au(x) niveau(x) inférieur(s).

La décision d'habilitation est une autorisation explicite, délivrée à l'issue d'une procédure spécifique définie dans la présente annexe, permettant à une personne, sous réserve du besoin d'en connaître, d'avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s). La décision d'habilitation est assortie d'un engagement de respecter, après en avoir dûment pris connaissance, les obligations et les responsabilités liées à la protection des informations ou supports classifiés.

Paragraphe 7
Les lieux abritant des informations classifiées

Les lieux abritant des éléments couverts par le secret de sécurité nationale sont les locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau, par des personnes par ailleurs habilitées au niveau requis.

L'accès à ces lieux, pour motif de service, est encadré par les dispositions relatives au droit du travail, aux contrats de prestation de service, au droit pénal, ou issues de conventions internationales.

Paragraphe 8
Contrôles et inspections

Des contrôles et des inspections sont assurés périodiquement par l'officier de sécurité mentionné au paragraphe 12 de la présente annexe, pour vérifier l'application et le respect, par l'ensemble des services placés sous l'autorité directe du Ministre d'Etat et des Conseillers de Gouvernement-Ministres, par les entités placées sous leur tutelle ainsi que par toutes autres entités, publiques ou privées émettant, recevant, traitant ou conservant des informations classifiées, des règles et des directives relatives à la protection du secret de sécurité nationale.

En cas d'anomalies constatées, l'officier de sécurité établit un rapport de synthèse incluant les mesures préconisées pour rectifier les déficiences constatées et leur planification. Ce rapport est transmis, selon le cas, soit au Ministre d'Etat ou au Conseiller de Gouvernement-Ministre concerné, soit aux autorités responsables des autres entités publiques ou privées.

La Direction de la Sûreté Publique ou l'Agence Monégasque de Sécurité Numérique proposent toutes mesures propres à améliorer les conditions générales de sécurité.

CHAPITRE II
ORGANISATION DE LA PROTECTION

La protection du secret de sécurité nationale relève de différentes autorités qui, en s'appuyant sur une organisation précise, s'assurent de la bonne application des mesures définies dans la présente annexe.

---

[1] Par exemple : « *Confidentiel Personnel* », « *Confidentiel Médical* »,» « *Confidentiel Technologie* », « *Confidentiel Industrie* », « *Confidentiel Commercial* », « *Confidentiel Concours* », information non classifiée soumise à un contrôle, ou encore « *Spécial Monaco* » (voir article 63 de la présente annexe).

[2] Loi n° 975 du 12 juillet 1975 portant statut des fonctionnaires de l'Etat.

SECTION 1
AUTORITÉS COMPÉTENTES

Paragraphe 9
Le Ministre d'Etat

Le Ministre d'Etat détermine les critères et les modalités d'organisation de la protection des informations et supports classifiés au niveau *« Très Secret de Sécurité Nationale »*.

Pour les informations et supports classifiés au niveau *« Très Secret de Sécurité Nationale »*, le Ministre d'Etat définit les classifications spéciales dont ils font l'objet et qui correspondent aux différentes priorités gouvernementales.

La décision d'habilitation précise le niveau de classification des informations et supports classifiés dont le titulaire peut connaître ainsi que le ou les emplois qu'elle concerne. Elle intervient à la suite d'une procédure définie par le Ministre d'Etat.

Elle est prise par le Ministre d'Etat pour le niveau « *Très Secret de Sécurité Nationale »* et indique notamment la ou les catégories spéciales auxquelles la personne habilitée a accès.

Paragraphe 10
Le Ministre d'Etat et les Conseillers de Gouvernement-Ministres

Le Ministre d'Etat et chaque Conseiller de Gouvernement-Ministre s'assurent, dans les directions et services relevant de leur autorité, de la mise en œuvre des dispositions relatives à la sécurité des informations ou supports classifiés détenus par tout service ou toute entité publique ou privée relevant de ses attributions.

Dans les conditions fixées par le Ministre d'Etat, chaque Conseiller de Gouvernement-Ministre, pour le département ministériel dont il a la charge, détermine les informations et supports qu'il y a lieu de classifier au niveau *« Très Secret de Sécurité Nationale »*.

Pour les niveaux de classification *« Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »*, la décision d'habilitation est prise par chaque Conseiller de Gouvernement-Ministre (autorité d'habilitation) pour le département ministériel dont il a la charge.

Il détermine, dans les conditions fixées par le Ministre d'Etat, les informations ou supports qu'il y a lieu de classifier, et les modalités d'organisation de leur protection pour les niveaux « *Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »*.

Pour ce qui relève de ses attributions, chaque Conseiller de Gouvernement-Ministre définit, par une note particulière [3], les conditions d'emploi des niveaux de classification *« Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »* et les informations qui doivent être classifiées au niveau *« Très Secret de Sécurité Nationale »*.

En matière de sécurité des systèmes d'information, ses attributions sont définies au titre V de la présente annexe.

Au sein du département ministériel dont il a la charge, il veille à la bonne gestion des informations et des supports classifiés, vérifie l'exactitude des inventaires, procède aux contrôles et inspections nécessaires et propose toutes dispositions destinées à renforcer l'efficacité des mesures de protection mises en place.

Pour les départements ministériels utilisant des systèmes d'information nécessitant une protection, l'Agence Monégasque de Sécurité Numérique anime la politique de sécurité de ces systèmes et en contrôle l'application.

SECTION 2
ORGANISATION FONCTIONNELLE

Paragraphe 11
Le rôle des autorités hiérarchiques

Le Ministre d'Etat et les Conseillers de Gouvernement-Ministres définissent pour chaque direction et service dont ils ont la charge, et pour chaque niveau de classification, la liste des emplois ou fonctions nécessitant l'accès à des informations ou supports classifiés. Ces listes sont désignées *« catalogues des emplois »*.

C'est en référence aux catalogues des emplois que les demandes d'habilitation sont établies. Lorsqu'une demande d'habilitation lui parvient, l'autorité d'habilitation vérifie l'inscription de la fonction concernée dans le catalogue des emplois correspondant. Elle examine, à titre exceptionnel, le bien-fondé de la demande lorsque l'emploi ne figure pas au catalogue.

Dans les entreprises titulaires d'un contrat impliquant l'accès ou la détention d'informations ou de supports classifiés, un répertoire des personnes habilitées tient lieu de catalogue des emplois.

Les autorités hiérarchiques doivent veiller à l'habilitation des personnels placés sous leur responsabilité et initier la procédure d'habilitation au niveau requis par le catalogue des emplois.

---

[3] Les recommandations pour la rédaction de cette note sont détaillées dans l'appendice 2 de la présente annexe.

Paragraphe 12
L'officier de sécurité

L'officier de sécurité est désigné, pour l'ensemble des services placés sous l'autorité directe du Ministre d'Etat et des Conseillers de Gouvernement-Ministres, ainsi que pour les entités placées sous leur tutelle et traitant des informations ou supports classifiés, par le Ministre d'Etat.

En ce qui concerne les autres entités, publiques ou privées, dépositaires de secrets de sécurité nationale ou titulaires de marchés impliquant le traitement ou la détention d'informations ou de supports classifiés, l'officier de sécurité est désigné par les responsables desdites entités, en liaison avec l'Agence Monégasque de Sécurité Numérique et la Direction de la Sûreté Publique.

Il est le correspondant de l'Agence Monégasque de Sécurité Numérique et a pour mission, sous les ordres de son autorité d'emploi et en fonction des modalités propres à chaque structure, de fixer les règles et consignes de sécurité à mettre en œuvre concernant les personnes et les informations ou supports classifiés, et d'en contrôler l'application. Il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret. Il est chargé de la gestion des habilitations et, en liaison avec les services concernés, du contrôle des accès.

Paragraphe 13
Les réseaux de sécurité
Très Secret de Sécurité Nationale

Aucun service ni organisme ne peut élaborer, traiter, stocker, acheminer, des informations ou supports classifiés au niveau *« Très Secret de Sécurité Nationale »* sans y avoir été préalablement autorisé par le Ministre d'Etat. La circulation desdits informations ou supports par voie électronique est interdite. Le service ou l'organisme doit en outre disposer impérativement d'un enregistrement spécifique. Ces registres sont créés par décision du Ministre d'Etat sur proposition du Conseiller de Gouvernement-Ministre concerné.

Paragraphe 14
Les réseaux de sécurité Secret de Sécurité Nationale

Le Ministre d'Etat et les Conseillers de Gouvernement-Ministres veillent à l'élaboration, le traitement, le marquage, le stockage, l'expédition et le suivi de la destruction des informations ou supports classifiés au niveau Secret de Sécurité Nationale. Le Ministre d'Etat et les Conseillers de Gouvernement-Ministres dressent l'inventaire annuel des informations ou supports classifiés qu'il traite.

Les informations et supports classifiés au niveau *« Secret de Sécurité Nationale »*, sont traités exclusivement par des personnes habilitées au niveau *« Secret Sécurité Nationale »*, et dans une zone réservée, répondant aux normes de sécurité définies dans la présente annexe.

A ces fins, le Ministre d'Etat et les Conseillers de Gouvernement-Ministres doivent mettre en place un système assurant par voie informatique les fonctions suivantes :

- identification du support d'information (numéro d'enregistrement arrivé ou départ, auteur ou service émetteur, date de création, domaine, titre ou objet, pagination, niveau de classification, mode et date prévue de déclassification, nombre d'exemplaires) ;
- traçabilité des événements concernant les exemplaires du support d'information (arrivée, départ, reproduction, archivage, destruction, déclassification, numéro de référence de l'événement, date de l'événement, référence individuelle des exemplaires, nom et fonction du détenteur physique de chaque exemplaire) ;
- modification éventuelle des données précédentes ;
- recherche sur les supports d'information (des détenteurs successifs d'un exemplaire, de la date de création, du service émetteur...) ;
- inventaire des supports d'information ;
- fourniture d'états relatifs aux actions effectuées sur les supports d'information (historique, fiche d'enregistrement, fiche de suivi, bordereau d'envoi, procès-verbal de destruction, avis de déclassification, archivage, reproduction...).

TITRE II
MESURES DE SÉCURITÉ RELATIVES AUX PERSONNES

CHAPITRE I^ER
L'ACCÈS AU SECRET DE SÉCURITÉ NATIONALE

Paragraphe 15

Nul n'est qualifié pour connaître des informations et supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, selon l'appréciation de l'autorité d'emploi sous laquelle il est placé, au regard notamment du catalogue des emplois justifiant une habilitation établie par cette autorité, de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission.

Les décisions relatives aux habilitations sont notifiées aux intéressés selon les dispositions prévues par l'article 20.

Paragraphe 16

Nul n'est qualifié pour accéder à un système d'information ou à ses dispositifs, matériels ou logiciels, de protection, lorsque cet accès permet de connaître des informations classifiées qui y sont contenues ou de modifier les dispositifs de protection de ces informations, s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, selon l'appréciation de l'autorité responsable de l'emploi du système, d'y accéder pour l'exercice de sa fonction ou l'accomplissement de sa mission.

Les décisions relatives aux habilitations d'accès sont notifiées aux intéressés selon les dispositions prévues par l'article 20.

Paragraphe 17
Information des candidats à l'habilitation

Lors de leur demande d'habilitation, les candidats sont informés, par les mentions portées sur la notice individuelle qui leur est remise, des obligations induites par l'habilitation ainsi que des dispositions relatives à leur responsabilité pénale en cas de compromission[4].

La notification d'une décision d'habilitation favorable par l'officier de sécurité est complétée par une séance de sensibilisation aux risques de compromission puis, par la suite, par des rappels périodiques de la réglementation en vigueur.

Une sensibilisation aux menaces d'investigations ou d'approches par des individus ou des organisations étrangères est faite aux personnes devant se rendre hors du territoire national, que l'Etat de destination soit ou non lié à Monaco par un accord de sécurité. Avant leur départ, des règles de prudence élémentaire leur sont rappelées.

CHAPITRE II
L'HABILITATION

Paragraphe 18
Objet de l'habilitation

L'autorité hiérarchique doit veiller à l'habilitation du personnel placé sous sa responsabilité et, à ce titre, initier, par la constitution d'un dossier, la procédure d'habilitation au niveau requis par le catalogue des emplois.

La demande d'habilitation déclenche une procédure destinée à vérifier qu'une personne peut, sans risque pour la sécurité nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l'exercice de ses fonctions. La procédure comprend une enquête de sécurité permettant à l'autorité d'habilitation de prendre sa décision en toute connaissance de cause.

Toute personne visant ou occupant un poste pour lequel le besoin d'une habilitation est avéré et qui refuserait de se soumettre à la procédure d'habilitation devra être écartée du poste considéré.

Paragraphe 19
Procédure d'habilitation

Seuls les emplois figurant au catalogue des emplois doivent faire l'objet d'une habilitation. Aussi, lorsqu'un poste à pourvoir exige une habilitation au niveau *« Secret de Sécurité Nationale »* ou *« Confidentiel-Sécurité Nationale »*, la procédure n'est engagée qu'au seul profit de la personne effectivement nommée dans l'emploi, sauf cas particulier. Anticiper la prise de poste en engageant la procédure d'habilitation sans attendre la prise effective de fonction peut être une mesure de bonne gestion, qui permet à la personne nouvellement affectée de prendre connaissance des informations classifiées sans perdre de temps. Il convient toutefois d'éviter toute surcharge inutile des services chargés de cette mission en limitant autant que possible le nombre de demandes d'habilitation.

Lorsque l'habilitation requise est du niveau *« Très Secret de Sécurité Nationale »* ou *« Secret de Sécurité Nationale »*, il revient à l'autorité administrative d'emploi d'apprécier l'opportunité d'une enquête de sécurité portant sur chacun des candidats au poste concerné.

1. Constitution du dossier :

Le dossier d'habilitation a pour objet de réunir les éléments qui sont vérifiés lors de l'enquête de sécurité.

Le dossier d'habilitation constitué, en trois exemplaires, de la notice individuelle, de la demande d'habilitation du service employeur et de trois (3) photos d'identité, est adressé à l'autorité d'habilitation, qui vérifie qu'il est complet et le transmet pour instruction à la Direction de la Sûreté Publique.

2. Instruction du dossier :

L'enquête de sécurité menée dans le cadre de la procédure d'habilitation est une enquête administrative permettant de déceler chez le candidat d'éventuelles vulnérabilités.

[4] Article 19 de la loi n° 1.430 du 13 juillet 2016 relative à la préservation de la sécurité nationale.

Elle est diligentée par la Direction de la Sûreté Publique.

L'enquête administrative est fondée sur des critères objectifs permettant de déterminer si l'intéressé, par son comportement ou par son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour le secret, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'Etat.

3. Clôture de l'instruction et avis de sécurité :

L'enquête administrative menée par la Direction de la Sûreté Publique dans le cadre de l'habilitation s'achève par l'émission d'un avis de sécurité, par lequel le Directeur de la Sûreté Publique fait connaître ses conclusions techniques à l'autorité compétente pour prendre la décision d'habilitation.

Cet avis comporte une évaluation des vulnérabilités éventuellement détectées lors de l'enquête et formule une conclusion de nature à permettre à l'autorité d'habilitation d'apprécier l'opportunité de l'habilitation[5] de l'intéressé, au regard des éléments communiqués et des garanties qu'il présente pour le niveau d'habilitation requis.

Les conclusions de l'avis de sécurité sont de trois types :

- « avis sans objection », lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ni pour celle de l'intéressé ;
- « avis restrictif », lorsque l'intéressé présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels il aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;
- « avis défavorable », lorsque des informations précises font apparaître que l'intéressé présente des vulnérabilités faisant peser sur le secret des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.

Les avis restrictifs ou défavorables peuvent être classifiés selon l'appréciation du Directeur de la Sûreté Publique et sont assortis d'une fiche confidentielle ne pouvant être reproduite, indiquant les motifs de l'avis. Ladite fiche est retournée après communication, sans délai au service enquêteur qui l'a émise, aux fins de conservation.

[5] Titre I, Chapitre II, section 1, articles 9 et 10 de la présente annexe.

La durée de validité de l'avis de sécurité est fonction du niveau d'habilitation demandé. Elle ne peut excéder :

- cinq ans pour le niveau *« Très Secret de Sécurité Nationale »* ;
- sept ans pour le niveau *« Secret de Sécurité Nationale »* ;
- dix ans pour le niveau *« Confidentiel-Sécurité Nationale »*.

L'avis de sécurité ne constitue en soi ni une autorisation ni un refus et ne lie pas l'autorité d'habilitation, qui prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier.

Paragraphe 20
La décision

L'autorité d'habilitation[6] peut décider, lorsque l'enquête a mis en valeur des éléments de vulnérabilité, de n'accorder l'habilitation qu'après avoir pris des précautions particulières. Ainsi, afin de garantir le plus efficacement possible la protection des informations ou supports classifiés, l'attention de l'employeur, par une procédure de mise en garde, ou celle de l'intéressé lui-même, par une procédure de mise en éveil, est attirée sur les risques auxquels l'un ou l'autre se trouve exposé. Les procédures de mise en garde et de mise en éveil peuvent être cumulées.

1. La mise en garde :

Cette procédure permet à l'autorité d'habilitation de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si nécessaire avec le conseil du service enquêteur.

A l'issue de l'entretien de mise en garde, une attestation particulière est signée par l'officier de sécurité. La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'autorité d'habilitation.

Au niveau *« Très Secret de Sécurité Nationale »*, la procédure de mise en garde est menée par le Ministre d'Etat, qui conserve l'attestation.

2. La mise en éveil :

Lorsque l'autorité d'habilitation ou son représentant décide d'accorder l'habilitation sur la base d'un avis de sécurité restrictif ou en dépit d'un avis de sécurité défavorable, elle peut choisir de demander la mise en éveil de l'intéressé, qui consiste à sensibiliser ce dernier sur les éléments communicables de vulnérabilité révélés

[6] Titre I, Chapitre II, section 1, articles 9 et 10 de la présente annexe.

par l'enquête. La mise en éveil est menée par l'autorité d'habilitation ou son représentant, en présence de l'officier de sécurité concerné. L'autorité d'habilitation définit les modalités de la mise en éveil en liaison avec le Directeur de la Sûreté Publique et peut, au cas par cas, solliciter sa présence lors de l'entretien avec l'intéressé. Le cas échéant, l'officier de sécurité étudie avec la Direction de la Sûreté Publique les mesures de sécurité complémentaires à mettre en œuvre au regard de la situation.

A l'issue de l'entretien de mise en éveil, une attestation particulière est signée par l'autorité d'habilitation, ou son représentant, par l'officier de sécurité et par l'intéressé.

La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'autorité d'habilitation.

Au niveau *« Très Secret de Sécurité Nationale »*, la mise en éveil est menée par le Ministre d'Etat, qui conserve l'attestation.

3. Le refus d'habilitation :

L'intéressé est informé de la décision défavorable prise à son endroit. Un refus d'habilitation n'a pas à être motivé conformément aux dispositions de l'article 5 de la loi n° 1.312 du 29 juin 2016 relative à la motivation des actes administratifs.

4. Décision favorable et engagement de responsabilité :

La décision d'habilitation est notifiée par l'officier de sécurité compétent à l'intéressé, qui signe un engagement de responsabilité. Par cet acte, le candidat reconnaît avoir eu connaissance des obligations particulières imposées par l'accès à une information ou à un support classifié ainsi que des sanctions prévues par la loi en cas d'inobservation, délibérée ou non, de la réglementation protégeant le secret de sécurité nationale.

Il est également notifié à l'intéressé qu'il est tenu d'informer au plus vite, pendant toute la durée de son habilitation, l'officier de sécurité dont il relève de tout changement affectant sa vie personnelle (mariage, divorce, établissement ou rupture d'une vie commune...), professionnelle ou son lieu de résidence. Il lui est signifié qu'il devra l'informer de toute relation suivie et fréquente dépassant le strict cadre professionnel avec un ou plusieurs ressortissants étrangers. L'officier de sécurité devra alors lui faire remplir, afin de mettre à jour les informations, une notice individuelle et la transmettre à l'autorité d'habilitation (sous forme électronique lorsque la procédure est dématérialisée). Ce changement de situation pourra justifier un réexamen du dossier d'habilitation et, le cas échéant, la saisine de la Direction de la Sûreté Publique en vue de l'émission d'un nouvel avis.

Le second volet de cet engagement est signé par l'intéressé à la cessation de ses fonctions ou au retrait de l'habilitation, et précise que les obligations relatives à la protection des informations classifiées auxquelles il a pu être donné accès perdurent au-delà du terme mis à ses fonctions ou à son habilitation. Une fois signé, ce second volet est retourné à l'autorité d'habilitation.

Paragraphe 21
Habilitation et changement d'affectation

Lorsqu'une personne habilitée change d'affectation, son habilitation pour le poste initial prend fin et une autre décision peut être prise, si la nouvelle affectation l'exige, sur la base de l'avis de sécurité en cours.

Paragraphe 22
Conservation des décisions

Pendant leur durée de validité, les décisions d'habilitation sont conservées par l'officier de sécurité. Ces documents, qui portent une mention de protection, ne sont en aucun cas remis aux intéressés ni reproduits.

En cas de nécessité, il peut être remis aux intéressés, par l'autorité d'habilitation, un certificat de sécurité délivré pour une mission déterminée et une période limitée. La délivrance de ces certificats peut être déléguée à l'officier de sécurité. Il est de la responsabilité de l'intéressé de procéder ou de faire procéder à la destruction de ce certificat dès le retour de mission.

Les éléments relatifs à l'habilitation des personnels sont conservés pour une durée que chaque Conseiller de Gouvernement-Ministre définit pour le département ministériel dont il a la charge. Cette durée ne peut pas être inférieure à cinq ans à compter de leur date de péremption.

Paragraphe 23
Répertoire des habilitations

Dans chaque département ministériel, il est tenu, pour chacun des trois niveaux de classification, un répertoire :

- des dossiers d'habilitation en cours d'instruction ;

- des habilitations en cours de validité.

Le Ministre d'Etat tient à jour le répertoire central des habilitations au niveau *« Très Secret de Sécurité Nationale »*, y compris dans le domaine international.

CHAPITRE III
LES CAS PARTICULIERS

Paragraphe 24
La décision d'agrément

Lorsqu'une personne dont le poste n'est pas inscrit au catalogue des emplois est amenée, dans le cadre de ses fonctions ou d'une mission particulière, de façon ponctuelle, à avoir accès à des informations ou à des supports classifiés ou à en prendre connaissance, elle peut se voir délivrer une décision d'agrément. Il en est de même lorsque l'intéressé est habilité à un niveau et qu'il a besoin, de façon ponctuelle, d'accéder à des informations classifiées à un niveau supérieur.

L'agrément accordé après demande dûment motivée par l'autorité responsable et à l'issue d'une procédure d'enquête administrative ordinaire, autorise occasionnellement l'accès aux informations ou supports classifiés.

Paragraphe 25
La décision de sécurité pour convoyeur

Sans préjudice des dispositions prévues aux articles 44 et suivants de la présente annexe, un document ou support classifié au niveau *« Confidentiel-Sécurité Nationale »* ou *« Secret de Sécurité Nationale »* ne peut être transporté que par des personnes habilitées au niveau approprié ou par des personnels internes au service ou à l'organisme titulaires d'une décision de *« sécurité convoyeur »*. Cette décision est délivrée par l'autorité d'habilitation valant pour une mission particulière et un certificat de sécurité est délivré au convoyeur.

Avant le début du voyage, le convoyeur est informé des règlements de sécurité relatifs au convoiement d'envois classifiés et de ses obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.). Il lui sera également demandé de signer une déclaration attestant qu'il a lu et compris les obligations relatives à la sécurité et qu'il se conforma à celles-ci.

Cette décision n'autorise en aucun cas à prendre connaissance d'informations classifiées.

Paragraphe 26
Portée de la décision d'habilitation en matière internationale

Toute décision d'habilitation aux informations ou supports classifiés du domaine national peut en soi, à défaut d'une habilitation spécifique et sous réserve du besoin d'en connaître, donner accès aux informations ou supports classifiés du niveau correspondant et des niveaux inférieurs des domaines internationaux ou confiés à Monaco en application de l'accord de sécurité conclu entre Monaco et les Etats partenaires.

Une décision d'habilitation aux informations ou supports classifiés du domaine international ne donne pas accès aux informations ou supports classifiés du domaine national.

TITRE III
MESURES DE SÉCURITÉ RELATIVES AUX INFORMATIONS OU SUPPORTS CLASSIFIÉS

CHAPITRE I^ER
PRINCIPES GÉNÉRAUX DE LA CLASSIFICATION

Paragraphe 27
Critères de classification

La décision de classifier résulte de l'analyse de l'importance de l'information au regard de son contexte, des textes applicables et des notes du Conseiller de Gouvernement-Ministre compétent. L'autorité classificatrice veille à ce que le niveau de classification soit approprié à l'information ou au support concerné(e), c'est-à-dire à ce qu'il soit à la fois nécessaire et suffisant.

En cas d'évolution, dans le temps ou en fonction des circonstances, de la sensibilité des informations classifiées, l'autorité classificatrice peut décider de procéder à leur déclassification, dans le respect des dispositions de l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée, leur déclassement ou leur reclassement. Elle notifie sa décision de modification ou de suppression de classification aux destinataires de l'information ou du support.

Lorsqu'un document comprend diverses parties, les unes nécessitant une classification, les autres non, il convient de s'efforcer de les présenter de manière distincte afin de ne pas entraver la diffusion des informations non classifiées. La diffusion de la partie non classifiée du document est rendue possible en plaçant en annexe classifiée l'information couverte par le secret de sécurité nationale.

Tout ensemble de documents contenant des informations classifiées à des niveaux différents doit être classifié lui-même au moins au niveau le plus élevé de ces documents.

Un ensemble d'informations ou de supports, dit parfois *« agrégat »*, est classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ses éléments, pris isolément, n'est classifié.

Un extrait d'information classifiée conserve le niveau de classification de l'information elle-même, à moins que l'autorité classificatrice en décide autrement.

Paragraphe 28
Identification de la classification

Une information ou un support, quel qu'il soit, acquiert juridiquement le caractère de secret de sécurité nationale dès lors qu'il fait l'objet de mesures de classification destinées à restreindre sa diffusion, matérialisées par la mention de niveau de classification sur le support de l'information.

Les supports préparatoires ayant servi à l'élaboration de l'information classifiée (brouillons, impressions sur papier, matériels informatiques nomades, qui ne sont pas identifiés, sont placés sous la responsabilité de celui qui les a élaborés. Ils doivent être détruits ou effacés le plus rapidement possible dès qu'ils sont devenus sans objet et, en tout état de cause, au plus tard lorsque le document classifié est émis.

Paragraphe 29
Principe général du marquage

Le marquage, par ses trois éléments constitutifs que sont le timbre, l'identification et la pagination, permet de vérifier l'authenticité et l'intégrité du support. Chaque exemplaire d'un document classifié porte la mention du niveau de classification des informations qu'il contient.

Les paragraphes, alinéas, annexes, traitant d'informations classifiées à un niveau inférieur ou non classifiées, sont mis en évidence, s'il y a lieu, par la mention, dans la marge, de leur propre niveau de classification et par une mise en page qui les détache sans ambiguïté du contexte général du document.

Jusqu'au niveau Secret de Sécurité Nationale, les abréviations indiquant la classification peuvent être utilisées pour préciser le niveau de classification des paragraphes du texte. Les abréviations admises sont les suivantes :

- Confidentiel-Sécurité Nationale : C.S.N. ;

- Secret de Sécurité Nationale : S.S.N..

Ces abréviations ne remplacent pas la mention de classification inscrite en toutes lettres sur le document papier, réalisée par le timbrage.

S'il est matériellement impossible d'apposer le marquage sur le support classifié ou contenant une information classifiée, il convient de mettre en œuvre des mesures de protection destinées à lever toute ambiguïté qui pourrait naître de l'absence de mention visible de classification. A cette fin, chaque département ministériel édicte, après autorisation du Ministre d'Etat, des directives particulières afin d'adapter aux caractéristiques des supports la réglementation relative au marquage, et de permettre leur identification au niveau de classification requis.

L'absence de mise en œuvre de ces consignes rend inopérante la protection pénale accordée au secret de sécurité nationale. Le respect scrupuleux des consignes constitue par conséquent un enjeu majeur.

Paragraphe 30
Le marquage d'un support papier

Le marquage d'un support papier comprend à la fois le timbre, l'identification et la pagination :

- le timbre indique le niveau de classification et permet par sa position, sa taille et sa couleur d'attirer immédiatement l'attention sur le caractère secret de l'information ou du support ;

- l'identification est constituée par les références du support ;

- la pagination consiste en la numérotation de chaque page et la mention du nombre total de pages contenues dans le document.

1. Timbre :

Le timbre de la mention de classification est apposé, avec une encre de couleur rouge, ou, à titre exceptionnel, d'une couleur contrastant avec celle du support, au milieu du haut et du bas de chaque page.

Lorsque des documents sont élaborés sur un poste de travail informatique, le marquage doit être ajouté par voie électronique à l'en-tête et au pied de page.

Le timbre, dont la dimension peut être adaptée à celle du support, est définitif et toujours visible.

2. Identification :

Tout document classifié est identifié dès sa première page. En plus des références ordinaires de toute pièce administrative, des mesures particulières sont prises. Ainsi, sur la première page du document, figurent les références du service émetteur, de la date d'émission, du numéro d'enregistrement, le timbre du niveau de classification et celui indiquant l'échéance de la classification (c'est-à-dire la date à laquelle la classification du document est réévaluée ou le document déclassifié). Le cas échéant, la mention de déclassement ou de déclassification est apposée sur cette même page.

Pour les documents classifiés au niveau Secret de Sécurité Nationale ou plus, chaque exemplaire est individualisé et le nombre total d'exemplaires est porté sur le document.

3. Pagination :

Chaque page du document est numérotée. Au bas de la première page est mentionné le nombre total de pages, d'annexes ou de plans qui composent le document.

Les pages de chaque annexe sont numérotées indépendamment de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe.

Pour les documents classifiés au niveau Secret de Sécurité Nationale ou plus, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention *« PAS DE TEXTE »*.

Paragraphe 31
Le marquage d'un support non papier

Le marquage d'un support non papier d'information classifiée est adapté au type de support, définitif et toujours visible. Il consiste en un timbre et une identification.

1. Timbre :

Le timbre spécifiant le niveau de classification a une dimension adaptée à celle du support et comporte la mention de ce niveau en toutes lettres. En cas de difficultés pratiques, les abréviations précédemment évoquées peuvent y être substituées.

2. Identification :

L'identification des supports non papier d'informations classifiées est assurée par l'inscription des références et, le cas échéant, du volume de chacune des informations enregistrées. Lorsqu'il est impossible d'inscrire sur le support l'ensemble des références, l'identification est faite par le numéro d'enregistrement.

3. Pagination des documents électroniques :

Chaque page du document est numérotée. Au bas de la première page est mentionné le nombre total de pages, d'annexes ou de plans qui composent le document.

Les pages de chaque annexe sont numérotées indépendamment de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe.

Pour les documents classifiés au niveau Secret de Sécurité Nationale, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention *« PAS DE TEXTE »*.

4. Dispositions particulières :

En raison de la possibilité technique de faire réapparaître des informations en principe effacées, un support informatique d'informations classifiées conserve toujours le niveau de classification qui lui a été initialement attribué. Il ne peut être déclassé ou déclassifié qu'à la condition que les informations qu'il contient ou a contenues aient elles-mêmes préalablement fait l'objet d'une telle mesure.

Paragraphe 32
L'enregistrement des informations ou supports classifiés

Tout support contenant des informations classifiées est enregistré, par un système d'enregistrement manuel ou informatisé dédié, autre que la base de courrier et permettant l'identification des destinataires.

L'enregistrement établit sans ambiguïté l'attribution du support à un détenteur, personne physique, clairement identifiée. Ce détenteur assume alors la responsabilité de la protection du support. Cet enregistrement est la seule référence de cette attribution de responsabilité.

Paragraphe 33
La durée de vie des classifications

La sensibilité d'une information ou d'un support classifié pouvant évoluer en fonction du temps ou des circonstances, il revient à l'autorité émettrice d'en apprécier la durée utile de classification. L'autorité émettrice mentionne sur le document la date à partir de laquelle le document sera automatiquement déclassifié. Lorsque cette date ne peut être déterminée, l'autorité émettrice mentionne la date ou le délai au terme duquel le niveau de classification devra être réexaminé. La réévaluation peut avoir pour résultat le maintien du niveau de classification, le déclassement ou la déclassification du document. L'autorité émettrice peut également fixer comme terme non pas une date mais un événement défini (par exemple, début de production d'un matériel, retrait de service d'un matériel, fin d'un exercice...), à la suite duquel le document sera automatiquement déclassé au niveau qu'elle aura précisé ou sera déclassifié. Elle conserve la possibilité de prolonger à tout moment le délai qu'elle a fixé.

En tout état de cause, la révision du besoin et du niveau de classification des informations ou supports doit être effectuée rigoureusement selon une périodicité inférieure ou égale à dix ans, précisément définie par chaque Conseiller de Gouvernement-Ministre pour le département ministériel dont il a la charge.

Par défaut toute classification est valable 50 ans à compter de sa date d'émission. La question de la communicabilité du document et de sa déclassification avant cette date est soumise à la commission instituée par l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée.

Pour les informations ou supports classifiés étrangers, seule l'autorité étrangère émettrice peut procéder à une déclassification ou à un déclassement.

CHAPITRE II
GESTION DES INFORMATIONS OU SUPPORTS CLASSIFIÉS

SECTION 1
CONSERVATION DES INFORMATIONS OU SUPPORTS CLASSIFIÉS

Paragraphe 34
Conditions matérielles de conservation

En dehors des périodes d'utilisation, les informations ou supports classifiés sont conservés dans des coffres forts ou des armoires fortes conformes aux dispositions relatives aux meubles de sécurité énoncées dans la présente annexe. Aucune indication relative à la nature des informations n'est visible à l'extérieur du coffre ou de l'armoire.

La combinaison des coffres forts, suffisamment complexe pour être fiable, n'est connue que des seuls utilisateurs. Une copie de cette combinaison est conservée sous enveloppe opaque, fermée, dans le coffre-fort d'une autorité spécialement désignée, la clé du coffre-fort de cette autorité étant elle-même placée dans un coffre distinct.

Les combinaisons sont changées au moins tous les six mois, et à chaque fois qu'il y a mutation des utilisateurs, risque ou suspicion de compromission.

Les clés sont impérativement mises en sécurité, notamment hors des heures ouvrables, suivant une procédure clairement établie par chaque autorité responsable (dépôt dans un coffre mural, sans clé, à combinaisons et à commande unique ou avec ouverture par lecture de badge, garde permanente avec système d'alarme).

Il est formellement interdit d'emporter à l'extérieur des lieux de travail :

- des informations ou supports classifiés, sauf nécessités impérieuses de service ;
- les clés des coffres ou armoires où sont conservés de tels informations ou supports.

La responsabilité de la conservation des informations ou supports classifiés incombe à un détenteur responsable.

SECTION 2
REPRODUCTION

Paragraphe 35
Règles générales de la reproduction

La généralisation et la diversité des moyens de reproduction accroissent les risques de diffusion incontrôlée des informations ou supports classifiés.

Pour les niveaux *« Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »*, des consignes précises sont établies par chaque Conseiller de Gouvernement-Ministre pour le département ministériel dont il a la charge afin de fixer :

- les personnes habilitées à effectuer la reproduction ;
- les procédures de contrôle de la reproduction ;
- la nécessité de consigner sur un système d'enregistrement le nombre de pièces reproduites et leurs détenteurs.

Les matériels utilisés pour la reproduction d'informations classifiées (photocopieuses, télécopieurs, systèmes informatiques...) doivent être physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées. Les opérations de maintenance sur ces matériels sont effectuées dans des conditions permettant de garantir la sécurité des informations classifiées qui ont été reproduites, dans le respect des dispositions de la présente annexe. Il en est de même pour leur mise au rebut, qui doit garantir la destruction des mémoires de ces appareils.

Paragraphe 36
Reproduction totale

Au niveau Secret de Sécurité Nationale, la reproduction totale d'informations ou supports classifiés n'est possible qu'avec l'autorisation préalable de l'autorité émettrice. Le dépositaire de l'information ou du support qui souhaite en effectuer une reproduction doit adresser une demande motivée à cette autorité. Si celle-ci consent à la reproduction, elle spécifie les numéros à attribuer aux exemplaires supplémentaires et porte mention de cette reproduction sur l'exemplaire en sa possession.

En cas d'urgence et à titre exceptionnel, le dépositaire peut s'affranchir de cette procédure à la condition de prendre les dispositions suivantes :

1. Limiter au minimum indispensable le nombre des reproductions ;

2. Procéder au marquage réglementaire en attribuant à chaque exemplaire un numéro individuel composé de deux nombres fractionnaires :

- le premier ayant en numérateur le numéro d'ordre de la copie dans la série des reproductions et en dénominateur le nombre total de reproductions ;
- le second étant le numéro individuel de l'exemplaire attribué par l'autorité émettrice du document ;

3. Porter si nécessaire, sur l'exemplaire reproduit, la destination qui en est faite ou établir une liste séparée des destinataires ;

4. Rendre compte sans délai à l'autorité émettrice du nombre de reproductions, des numéros de reproductions et de la destination des exemplaires. L'autorité émettrice porte mention de cette reproduction sur l'exemplaire en sa possession.

Au niveau *« Confidentiel-Sécurité Nationale »*, la reproduction peut être effectuée par les autorités détentrices, sous leur responsabilité, à condition de conserver sur un système d'enregistrement la trace du nombre et des destinataires des exemplaires reproduits.

Paragraphe 37
Reproduction partielle

Les extraits de documents classifiés sont eux-mêmes classifiés au niveau approprié à leur contenu. Si un extrait de document classifié ne justifie pas lui-même une classification, son importance doit rester limitée de façon à ne pas compromettre, en cas de divulgation, l'information dont il a été extrait. La diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite.

Des extraits d'informations classifiées *« Confidentiel-Sécurité Nationale »* ou *« Secret de Sécurité Nationale »* peuvent être reproduits par leur dépositaire dans les conditions fixées par l'article 36 de la présente annexe.

Lorsque des extraits de documents contenant des informations classifiées sont transférés sur un autre support, si ces extraits sont eux-mêmes classifiés, la mention de classification est reportée sur le nouveau support conformément aux dispositions de la présente annexe.

SECTION 3
INVENTAIRE

Paragraphe 38
La procédure d'inventaire

Les documents classifiés font l'objet d'un suivi permanent afin d'assurer leur traçabilité et leur prise en compte par des détenteurs habilités.

A cet effet, chaque Conseiller de Gouvernement-Ministre préconise les modalités d'inventaire annuel et de suivi des documents classifiés *« Confidentiel-Sécurité Nationale »* et *« Secret de Sécurité Nationale »* détenus dans l'ensemble des services et organismes relevant de son département ministériel.

Un inventaire est effectué sous forme contradictoire à chaque mutation de personnel, l'ancien détenteur et le nouveau apposant tous deux leur signature sur le procès-verbal.

La période d'inventaire est mise à profit pour alléger la gestion des documents classifiés. Les dates d'expiration de validité sont vérifiées aux fins de déclassement ou de déclassification : la réévaluation du niveau de protection des documents classifiés et, le cas échéant, leur destruction doivent être réalisées.

Au niveau Secret de Sécurité Nationale, l'inventaire annuel, est transmis au Ministre d'Etat, au plus tard le 31 mars de chaque année.

Le procès-verbal d'inventaire annuel, est accompagné, le cas échéant, de l'une ou l'autre des pièces administratives suivantes :

- un récépissé du nouveau détenteur ;
- un procès-verbal de destruction ;
- un procès-verbal de versement à un dépôt d'archives.

SECTION 4
LA PROTECTION DES MATÉRIELS CLASSIFIÉS

Paragraphe 39
Dispositions générales et classifications

La protection des matériels classifiés implique la mise en œuvre de mesures de sécurité à tous les stades de la réalisation (programme, étude, plan, fabrication ou construction, essai, etc.) de même que pour l'utilisation, l'entretien, la réparation et le transport jusqu'à leur mise hors service et à leur destruction.

Un moyen efficace d'assurer la protection des matériels classifiés au niveau Secret de Sécurité Nationale consiste à les entreposer dans une zone répondant aux règles de protection définies par la présente annexe. Lorsque les matériels sont en service ou exposés à la vue en dehors de ces zones, les autorités responsables font prendre des mesures de protection adaptées pour les matériels classifiés et leurs éléments constitutifs.

Paragraphe 40
La protection des matériels classifiés en cours de transport en dehors du territoire monégasque

La circulation et le transport des matériels classifiés nécessitent des mesures particulières de sécurité : protection contre les vues dans la mesure du possible et garde permanente pendant la durée de l'acheminement.

L'autorité ayant prescrit le mouvement assume la responsabilité des tâches suivantes :

- conditionnement des matériels ;
- choix de l'itinéraire et des lieux d'étape, en accord avec les autorités intéressées ;
- organisation du convoyage ou de l'escorte et des dispositions techniques en cas de panne ou d'accident.

Le transport des matériels classifiés est effectué, sauf impossibilité absolue ou opération conjointe, par des moyens nationaux. A défaut, il doit être convoyé et toutes dispositions sont prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport.

CHAPITRE III
DIFFUSION ET ACHEMINEMENT DES INFORMATIONS OU SUPPORTS CLASSIFIÉS

SECTION 1
LA DIFFUSION ET L'EXPÉDITION DES INFORMATIONS OU SUPPORTS CLASSIFIÉS

Paragraphe 41
La diffusion

Lorsqu'elle diffuse des informations ou supports classifiés, l'autorité d'expédition établit la liste des destinataires et s'assure qu'ils sont habilités au niveau de classification requis.

Au niveau Secret de Sécurité Nationale et plus, le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par le service émetteur sont précisés dans la liste de diffusion (deux exemplaires au moins, dont un original destiné, à terme, aux archives).

La liste des destinataires, lorsqu'elle constitue en elle-même un secret, n'est pas jointe à l'envoi de chacun des exemplaires du support.

Paragraphe 42
La diffusion, l'expédition et la réception d'informations ou supports classifiés par voie électronique

La diffusion, l'expédition et la réception d'informations classifiées par voie électronique sont régies par les dispositions du titre V.

Paragraphe 43
L'expédition et la réception d'informations ou supports classifiés

L'expédition d'informations ou supports classifiés est soumise à une procédure particulière qui permet d'assurer le suivi et de garantir l'intégrité physique du document grâce à un conditionnement spécial.

L'autorité émettrice procède, après marquage et enregistrement de chaque support, aux opérations suivantes :

1. Pour l'expédition :

a. Conditionnement :

L'envoi de supports d'informations ou de supports classifiés se fait sous double enveloppe présentant des garanties de solidité de nature à assurer au maximum l'intégrité physique des supports :

- l'enveloppe extérieure, plastifiée, porte l'indication du service expéditeur, l'adresse du destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère classifié du contenu) et la mention du suivi. Elle ne porte en aucun cas la mention du niveau de classification de l'information ou support qu'elle contient. Au niveau Secret de Sécurité Nationale ou plus, chaque enveloppe est numérotée ;
- l'enveloppe intérieure de sécurité de bonne qualité, opaque, si possible du modèle toilé ou armé, doit interdire une ouverture ou une refermeture discrète. Elle porte le timbre du niveau de classification, la référence des supports transmis, le cachet de l'autorité expéditrice, le nom et la fonction du destinataire ainsi que l'indication du service ou de l'organisme dans lequel il est affecté.

b. Suivi de l'expédition :

Un bordereau d'envoi, sans timbre de classification ni indication de l'objet des informations envoyées, est placé dans l'enveloppe intérieure de sécurité dont il porte le numéro. Il comporte trois feuillets détachables A, B et B' signés par le responsable de l'autorité expéditrice ou une personne désignée par lui. Les feuillets A et B sont adressés au destinataire, qui conserve le premier à titre d'élément de preuve et renvoie le second à titre d'accusé de réception. Le feuillet B', de couleur, est conservé par l'expéditeur jusqu'à réception du feuillet B, qui lui est alors substitué.

2. Pour la réception :

Il convient :

- de vérifier l'intégrité de l'emballage afin de déceler une éventuelle compromission ;
- d'enregistrer ou de faire enregistrer l'information ou le support classifié conformément aux dispositions de l'article 32 ;
- de signer et de renvoyer le feuillet B du bordereau d'envoi à titre d'accusé de réception.

SECTION 2
ACHEMINEMENT

Paragraphe 44
L'acheminement d'informations ou supports classifiés sur le territoire national

Les procédures de transmission des supports classifiés doivent permettre de respecter des délais compatibles avec le degré d'urgence et d'assurer la meilleure protection des supports transmis.

L'acheminement de supports classifiés sur le territoire national se fait de la façon suivante :

1. A l'intérieur d'un même immeuble :

Afin d'éviter leur observation, les informations ou supports classifiés sont acheminés sur place, sous enveloppe, soit :

- par le détenteur lui-même ;
- par une autre personne habilitée ;
- par un convoyeur ou par une personne du service de courrier interne autorisé(e).

2. Avec changement d'immeuble ou de zone géographique :

Pour le niveau *« Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »*, l'acheminement peut s'opérer par convoyeur autorisé ou par toute personne habilitée au niveau requis. Les informations ou supports classifiés sont placés dans une sacoche ou une valise fermant à clef, dépourvue d'indication extérieure ; le porteur ne peut en aucun cas s'en dessaisir jusqu'à la remise au destinataire.

Paragraphe 45
L'acheminement d'informations ou supports classifiés vers l'étranger

Les informations ou supports classifiés envoyés à l'étranger ou transitant par des pays étrangers doivent être protégés en permanence pour interdire leur compromission pendant le transport, et notamment lors des escales.

Le seul moyen autorisé est la valise diplomatique.

La voie postale en recommandé avec accusé de réception, peut être autorisée, pour les supports de niveau *« Confidentiel-Sécurité Nationale »* à destination de la France, dans les conditions du paragraphe 43.

Pour les informations échangées dans le cadre d'un accord ou d'un programme international, il convient de se référer aux dispositions prévues par les réglementations applicables.

CHAPITRE IV
DESTRUCTION ET ARCHIVAGE DES INFORMATIONS OU SUPPORTS CLASSIFIÉS

SECTION 1
DESTRUCTION DES INFORMATIONS OU SUPPORTS CLASSIFIÉS

Paragraphe 46
La procédure ordinaire

Lorsque des informations ou supports classifiés sont périmés ou devenus inutiles, il peut être procédé à leur destruction sauf pour le document original qui est versé au service central des archives.

La destruction ne peut être réalisée que par des personnes habilitées. Les supports préparatoires devenus sans objet sont détruits sans formalité particulière.

La destruction de tels documents est effectuée de façon à rendre impossible toute reconstitution même partielle des informations contenues sur les supports. Les principales formes de destruction[7] sont le brûlage, l'incinération, le broyage, le déchiquetage. Lorsque des documents classifiés doivent être transportés afin d'être incinérés, ils doivent impérativement avoir été préalablement déchiquetés et mélangés.

Après l'opération, un procès-verbal de destruction est dressé. Les procès-verbaux de destruction portent la signature de l'autorité détentrice.

Au niveau Secret de Sécurité nationale, l'autorité détentrice du document informe par écrit l'autorité émettrice que, sauf avis contraire de sa part, elle va procéder à la destruction du support. Sans réponse dans un délai de deux mois, l'autorité détentrice procède à la destruction du support et en rend compte à l'autorité émettrice en lui adressant une copie du procès-verbal.

Paragraphe 47
Evacuation et destruction d'urgence

Pour faire face à des circonstances exceptionnelles et en cas de menace immédiate nécessitant l'évacuation des bâtiments par le personnel ou la destruction des informations ou supports classifiés, des plans d'évacuation et de destruction d'urgence sont établis par chaque service ou organisme détenteur d'informations ou supports classifiés. Ces plans prévoient notamment les procédures d'accès, en toute circonstance, aux locaux et aux informations ou supports classifiés.

Les modalités d'exécution pratique de ces plans figurent sur des fiches disponibles en permanence, pour les personnes concernées, dans chaque service ou organisme détenteur. Elles précisent :

- la liste et la localisation des informations ou supports classifiés à détruire ou à évacuer ;
- les mesures applicables aux systèmes d'information ;
- la liste et la localisation des moyens de destruction et d'évacuation à utiliser ;
- les autorités qualifiées pour donner l'ordre de destruction ou d'évacuation.

Le dispositif ainsi établi doit être contrôlé par une simulation, selon une périodicité définie par chaque département ministériel pour les niveaux *« Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »*, qui ne peut excéder trois ans.

[7] Le brûlage consiste à exposer l'ensemble du support ou la surface utile à une température de plus de 1 000 °C avec un chalumeau ; l'incinération est une combustion complète réduisant le support à l'état de cendres, destinée à empêcher toute dispersion de fragments ; le broyage consiste à réduire le support en pulpe afin que les morceaux résiduels n'excèdent pas 2 mm de diamètre ; le déchiquetage est une opération qui réduit le support en lambeaux de moins de 0,8 mm de large et 13 mm de long.

SECTION 2
ARCHIVAGE

Paragraphe 48
Les principes généraux de l'archivage d'informations ou de supports classifiés

Toute autorité détenant une information ou support classifié, produit ou reçu, a pour obligation de faire assurer sa conservation et sa protection conformément aux dispositions législatives ou réglementaires et aux règles de fonctionnement du service central des archives.

CHAPITRE V
LES MENTIONS ADDITIONNELLES DE LIMITATION DU CHAMP DE DIFFUSION

CHAPITRE VI
ATTEINTE AU SECRET DE SÉCURITÉ NATIONALE.

Les atteintes au secret de sécurité nationale sont réprimées selon les dispositions de l'article 19 de la loi n° 1.430 du 13 juillet 2016, précitée.

Paragraphe 49
Procédure à suivre en cas d'atteinte au secret de sécurité nationale

La rapidité et la discrétion de l'intervention revêtent une importance primordiale pour limiter les conséquences de la divulgation des informations ou supports classifiés compromis. Il est rendu compte immédiatement de toute découverte de compromission possible à l'autorité hiérarchique. Qu'il y ait une compromission avérée ou une simple suspicion, doit être directement et dans les plus brefs délais informés le département ministériel.

En matière informatique, les disparitions, vols, pertes accidentelles de supports matériels classifiés ou les agressions contre les systèmes d'information font l'objet d'un procès-verbal de perte ou d'agression informatique, adressé sans délai à l'Agence Monégasque de Sécurité Numérique.

Le fait de ne pas signaler de tels actes, favorisant la divulgation d'une information classifiée, fait encourir des sanctions administratives ou professionnelles.

Le Conseiller de Gouvernement-Ministre de l'Intérieur, outre l'information obligatoirement donnée au cas par cas, fournit au Ministre d'Etat un bilan annuel des cas constatés et de l'état d'avancement des procédures ou des suites réservées à chacune d'elles.

Lorsque la compromission porte sur des informations classifiées étrangères, le Ministre d'Etat informe dans les plus brefs délais l'autorité étrangère concernée.

TITRE IV
LA PROTECTION DES LIEUX

Les règles de sécurité applicables aux lieux sont mises en œuvre pour protéger les informations ou supports classifiés contre toute menace d'origine interne ou externe qui pourrait mettre en cause leur disponibilité, leur intégrité, leur confidentialité et afin d'empêcher qu'une personne non autorisée puisse y accéder.

Les mesures de protection physique appliquées à une information dépendent de son niveau de classification.

Tout système de protection physique doit s'appuyer sur une analyse des risques. Un dispositif de protection est satisfaisant lorsqu'il retarde suffisamment l'intrusion pour permettre la mise en œuvre des moyens d'intervention avant que les éléments couverts par le secret de sécurité nationale ne soient compromis.

CHAPITRE I^ER
PRINCIPES DE PROTECTION PHYSIQUE DES LIEUX

Paragraphe 50
Principes généraux

La protection physique est l'ensemble des mesures de sécurité destinées à garantir l'intégrité des bâtiments et des locaux spécifiquement dédiés aux informations ou supports classifiés, ainsi que la fiabilité des meubles dans lesquels ils sont conservés, afin d'éviter toute perte, dégradation ou compromission. Elle vise aussi à faciliter l'identification du ou des auteurs d'une éventuelle intrusion.

Le degré de sécurité physique à appliquer aux lieux pour assurer leur protection dépend du niveau de classification des documents ou supports qu'ils abritent, de leur volume et des menaces auxquelles ils sont exposés le dispositif global de protection et la solution technique retenue reposent sur les conclusions de l'évaluation des menaces et des contraintes inhérentes à l'environnement du site, ainsi que des méthodes de travail et de gestion des informations ou supports classifiés concernés (par exemple, en fonction de la circulation de ces informations ou supports dans le site et du nombre de personnes y ayant accès). Les vulnérabilités liées aux systèmes d'information doivent également être prises en compte.

Cet ensemble de mesures de protection se compose de quatre éléments combinés ou dissociés en fonction du niveau de classification :

- un ou plusieurs dispositifs de protection (les obstacles) ;
- un ou plusieurs dispositifs de détection et d'alarme ;
- des moyens d'intervention articulés sur des procédures et des consignes préétablies ;
- un ou plusieurs dispositifs de dissuasion (indications).

Ainsi, un dispositif de sécurité satisfaisant a pour objectif, en retardant l'intrusion (aucun obstacle n'étant infranchissable), de permettre la mise en œuvre des moyens d'intervention, alertés et guidés par les dispositifs de détection avant que les informations ou supports classifiés ne soient compromis.

Pour être efficace, un système de protection physique doit s'appuyer sur une analyse précise des risques et :

- être multiple, c'est-à-dire, dans une logique de sécurité en profondeur, comporter plusieurs dispositifs successifs, complémentaires, de nature différente, associés ou combinés à un ou plusieurs dispositifs de détection-alarme reposant eux-mêmes sur des principes différents ;
- être homogène, c'est-à-dire garantir la même efficacité en tous points, l'intrusion s'opérant toujours dans la zone de moindre résistance et la valeur d'un système équivalant à celle de son élément le plus faible ;
- être dissuasif, c'est-à-dire contribuer à réduire le risque d'une tentative d'intrusion ;
- être contrôlé, c'est-à-dire être testé fréquemment afin de vérifier qu'il est en état opérationnel ;
- être traçable, c'est-à-dire fournir tout moyen pouvant apporter un historique du fonctionnement des différents composants.

Afin d'éviter l'intrusion, à l'intérieur d'un site ou d'un local protégé par des dispositifs, d'une personne non autorisée qui représente toujours une menace pour les informations ou supports classifiés détenus, la protection physique comprend nécessairement un système de contrôle d'accès.

Le contrôle d'accès constitue un moyen matériel de s'assurer qu'une personne qui demande à pénétrer dans un lieu ou à accéder à une information a le droit de le faire. Il a donc pour objectif :

- de filtrer les flux de circulation, les individus et les véhicules qui souhaitent entrer ou sortir d'un site, d'un bâtiment ou d'un local ;

- de contrôler les individus et les véhicules dans les zones protégées ;

- d'empêcher ou de limiter les déplacements de personnes non autorisées.

Le contrôle d'accès comprend des mécanismes de différents niveaux :

- l'autorisation d'accès ;

- l'identification et/ou l'authentification de la personne ;

- la traçabilité, afin d'identifier a posteriori celui qui est entré ou sorti.

La sécurisation physique des accès d'énergie, des locaux techniques et des moyens de communication participe également à la protection physique des informations ou supports classifiés.

Paragraphe 51
Les modalités matérielles de protection

Les types de mesures de protection physique, leur articulation selon le type de barrière et les mesures spécifiques aux niveaux supérieurs de classification sont détaillés en appendices 4 à 6.

Le système de protection physique de toute information ou support classifié est constitué de plusieurs *« barrières »* cohérentes, inclusives et successives :

- l'emprise du bâtiment et/ou le bâtiment lui-même ;

- le local qui contient le meuble ;

- le meuble dans lequel est conservé l'information ou le support classifié.

Le degré de protection de l'ensemble du dispositif est fonction du niveau de protection assuré par les mesures appliquées à chacune de ces « barrières ».

Sur un territoire étranger et compte tenu de leur environnement particulier, les organismes détenteurs d'informations ou de supports classifiés doivent appliquer les mesures de protection décrites dans la présente annexe.

Paragraphe 52
Consultation de la Direction de la Sûreté Publique pour la protection physique des documents et supports secret de sécurité nationale

Le traitement et la conservation, dans des locaux, d'informations ou de supports classifiés de niveau Secret de Sécurité Nationale et plus ne peut intervenir, sauf en cas d'impossibilité majeure, qu'après avis de la Direction de la Sûreté Publique et de l'Agence Monégasque de Sécurité Numérique quant à l'aptitude de ces locaux à accueillir de tels documents ou supports.

Les services enquêteurs s'assurent notamment que l'analyse de risques et les mesures de protection physique, qu'elles soient réglementaires ou compensatoires, prennent en compte le délai réel écoulé entre la détection de l'intrusion, la résistance des moyens mécaniques et la possibilité d'une intervention.

CHAPITRE II
MESURES DE SÉCURITÉ POUR LES RÉUNIONS

Paragraphe 53
La préparation et l'organisation des réunions de travail et des conférences

L'autorité organisatrice doit veiller à la protection des informations ou supports classifiés échangés au cours d'une réunion de travail, d'une conférence, d'un exercice ou d'une présentation de matériel.

Le local prévu pour la séance au cours de laquelle sont traités des informations ou supports classifiés doit :

- être à l'abri des interceptions par écoute directe ou indirecte (insonorisation, absence de microphone) et des prises de vues non autorisées ;

- n'être accessible qu'aux personnes autorisées.

Le contrôle technique des lieux est effectué de manière régulière par le service chargé de la sécurité.

L'autorité organisatrice précise, lors des invitations ou convocations à une réunion de travail, à une conférence, à un exercice ou à une présentation de matériel, le niveau de classification des informations ou supports classifiés qui seront communiqués, pour permettre la désignation de personnes habilitées au niveau requis et ayant besoin d'en connaître. Les limites et le degré de précision à apporter à la communication, au cours de conférences ou de présentations de matériels, doivent être déterminés au préalable par le responsable.

L'autorité organisatrice s'assure de l'identité et du niveau d'habilitation de chacun des participants présents. Elle s'assure que personne ne détienne, lors de la réunion, d'appareil permettant la captation, la réémission et l'enregistrement d'informations tels que, par exemple, un téléphone mobile, un assistant personnel (PDA) ou un ordinateur portable ou tout objet connecté (montre, vêtements etc…).

Paragraphe 54
Les mesures de sécurité à l'issue d'une réunion de travail ou d'une conférence

En cas de communication d'informations du niveau « Très Secret de Sécurité Nationale » ou « Secret de Sécurité Nationale », l'organisateur consigne, dans un procès-verbal succinct à classifier éventuellement, les domaines d'information qui ont été exposés, les mesures prises pour en assurer la protection ainsi que la liste des participants avec mention de la justification de leur habilitation.

L'autorité organisatrice de la réunion fait procéder en fin de séance :

- à la récupération et à la mise en sécurité des informations ou supports classifiés éventuellement mis à la disposition des auditeurs (documents, graphiques, plans, films, bandes d'enregistrement, etc.) ;

- à la destruction des supports provisoires et préparatoires.

Les auditeurs et les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont à classifier au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

CHAPITRE V
ACCÈS DES PERSONNES NON HABILITÉES AUX LIEUX ABRITANT DES SECRETS DE SÉCURITÉ NATIONALE

Paragraphe 55

La nécessité d'exécuter une prestation de service, qu'il s'agisse d'un contrat ou de l'obligation d'intervenir en urgence, ou une mission de contrôle peut rendre indispensable l'accès de personnes non habilitées à des lieux abritant des éléments couverts par le secret de sécurité nationale.

Les personnes non habilitées ayant besoin de pénétrer dans une zone abritant des éléments couverts par le secret de sécurité nationale pour des raisons justifiées doivent y être autorisées par le responsable de la zone après vérification de leur identité et être en permanence accompagnée par une personne habilitée.

Les personnels d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence avérée, sont autorisés à procéder aux opérations requises par la situation sans être soumis aux formalités ordinaires. Si, dans des circonstances exceptionnelles, l'une de ces personnes accède fortuitement à un secret de sécurité nationale, elle s'expose, en cas de divulgation, aux peines prévues par la loi n° 1.430 du 13 juillet 2016.

TITRE V
MESURES DE SÉCURITÉ RELATIVES AUX SYSTÈMES D'INFORMATION

Pour les systèmes d'information traitant d'informations classifiées s'appliquent les règles de la présente annexe et des règles spécifiques d'application émises par l'Agence Monégasque de Sécurité Numérique.

La sécurité des systèmes d'information (S.S.I.) concerne tous les acteurs ayant une responsabilité dans la mise en œuvre de ces principes et mesures : les services informatiques pour la sécurité logique et les autres aspects de la sécurité informatique, les chefs de service pour les droits d'accès aux informations, et les responsables de la sécurité physique des locaux.

Le responsable de la sécurité des systèmes d'information (RSSI), est chargé de prescrire, d'appliquer pour ce qui la concerne, et de contrôler les mesures de sécurité nécessaires ; ce dernier s'assure de la disponibilité, la confidentialité et l'intégrité, en restant proportionnées aux enjeux des informations et des systèmes concernés.

L'homologation est l'acte formel par lequel l'autorité responsable certifie, après évaluation des risques, que la protection des informations et du système est assurée au niveau requis.

CHAPITRE I^ER

Paragraphe 56
Champ d'application

Le présent titre précise les mesures à appliquer pour protéger les informations classifiées dans les systèmes informatisés de traitement de l'information.

Ces mesures s'appliquent à tout système d'information ayant vocation à traiter des informations classifiées, qu'il soit placé sous la responsabilité d'un département ministériel, d'un organisme ou d'un établissement qui en relève, d'un organisme public ou privé qui traite de telles informations.

Des règles et des directives techniques complètent en tant que de besoin les mesures générales exposées dans la présente annexe.

CHAPITRE II
L'ORGANISATION DES RESPONSABILITÉS RELATIVES AUX SYSTÈMES D'INFORMATION

Paragraphe 57
Les instances chargées de la sécurité des systèmes d'information

Le Ministre d'Etat met en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information, notamment pour les systèmes traitant d'informations relevant du secret de sécurité nationale. Il s'assure que l'Etat dispose des moyens de communication électronique nécessaires en matière de secret de sécurité nationale. Il est à ce titre également chargé de garantir la sécurité de ces moyens de communication. Il dispose à cette fin d'un service à compétence nationale, l'Agence Monégasque de Sécurité Numérique (A.M.S.N.).

L'Agence Monégasque de Sécurité Numérique créée par l'ordonnance souveraine n° 5.664 du 23 décembre 2015 est placée sous l'autorité du Conseiller de Gouvernement-Ministre de l'Intérieur.

L'Agence Monégasque de Sécurité Numérique est l'autorité nationale en charge de la sécurité des systèmes d'information.

Paragraphe 58
Les départements ministériels

Le Ministre d'Etat et les Conseillers de Gouvernement-Ministres sont responsables, dans le département et les organismes dont ils ont la charge, de la sécurité des systèmes d'information. Ils sont assistés pour ces missions par un responsable de la sécurité des systèmes d'information.

En matière de sécurité des systèmes d'information, le Conseiller de Gouvernement-Ministre, anime la politique de sécurité des systèmes d'information et en contrôle l'application dans son département. En particulier, il veille au déploiement, dans son département ministériel, des moyens sécurisés gouvernementaux de communication électronique. Le responsable de la sécurité des systèmes d'information est plus particulièrement chargé de :

- diffuser les règles relatives à la sécurité des systèmes d'information à l'ensemble des personnels concernés et d'en préciser les modalités d'application ;
- élaborer les règles particulières pour son département, en définissant, pour chaque type de système d'information, les mesures de protection nécessaires ;
- contrôler l'application de ces règles et l'efficacité des mesures prescrites ;
- recenser les besoins de protection des systèmes d'information et de veiller à ce qu'ils soient satisfaits ;
- demander à l'Agence Monégasque de Sécurité Numérique les inspections et les contrôles nécessaires pour vérifier l'application effective des règles et des directives traitant de la sécurité des systèmes d'information ;
- organiser la sensibilisation et la formation des personnels ;
- assurer l'administration de la sécurité des systèmes non classifiés. L'administrateur de la sécurité doit dans la mesure du possible être distinct de l'administrateur du système.

Paragraphe 59
L'Agence Monégasque de Sécurité Numérique

Le Directeur de l'Agence Monégasque de Sécurité Numérique est responsable de l'administration de la sécurité des systèmes classifiés ; il peut déléguer cette fonction en s'assurant de l'habilitation des personnes concernées.

L'administration comprend :

- l'installation des logiciels correctifs de sécurité et des logiciels de protection ;
- la gestion des moyens d'accès et d'authentification du système ;
- la gestion des comptes et des droits d'accès des utilisateurs ;
- l'exploitation des alertes de sécurité et des journaux de sécurité.

L'Agence Monégasque de Sécurité Numérique prend les mesures organisationnelles et techniques afin de protéger l'information traitée et à garantir l'intégrité, la disponibilité et la confidentialité des informations sensibles pour les systèmes du secret de sécurité nationale.

Paragraphe 60
Qualification des dispositifs de sécurité

Les dispositifs de sécurité sont des moyens matériels ou logiciels destinés à protéger les informations traitées par le système ou à protéger le système lui-même. Ces dispositifs peuvent être développés pour un usage général ou spécifiquement pour un système particulier.

Ces dispositifs mettent en œuvre différents types de fonctions et de mécanismes de sécurité, notamment :

- des fonctions de cryptologie, chiffrant les informations stockées ou transmises sur des réseaux et assurant la signature, l'authentification ou la gestion de clés cryptographiques ;
- des fonctions de contrôle d'accès aux informations, comme l'authentification, le filtrage, le cloisonnement logique entre niveaux de sécurité ou le marquage des informations ;
- des fonctions ou des mécanismes destinés à protéger le dispositif lui-même, comme l'enregistrement et l'imputabilité des accès au dispositif, à empêcher ou à détecter les intrusions physiques ou logiques non autorisées, à garantir la protection, ou l'effacement le cas échéant, des données sensibles stockées, et plus généralement toute fonction ou tout mécanisme destiné à garantir l'intégrité et la disponibilité du dispositif ;
- des fonctions d'administration et de gestion sécurisée du dispositif ;
- des fonctions protégeant la transmission d'un signal radio, notamment contre le brouillage ;
- des fonctions ou des mécanismes limitant les émissions de signaux compromettants.

Un dispositif de sécurité mis en place dans un système d'information doit être qualifié par l'Agence Monégasque de Sécurité Numérique.

La qualification est demandée par l'autorité responsable de l'emploi du système.

L'Agence Monégasque de Sécurité Numérique peut procéder à une évaluation qui a pour objectif de vérifier la cohérence des objectifs de sécurité, identifiés dans la cible de sécurité, au regard des menaces, et d'évaluer l'efficacité des fonctions et des mécanismes de sécurité. En fonction des résultats de l'évaluation, l'Agence Monégasque de Sécurité Numérique peut prononcer une qualification qui atteste de l'aptitude du dispositif à protéger les informations classifiées à un niveau spécifié, dans des conditions d'emploi identifiées. A l'issue de sa période de validité, une qualification doit faire l'objet d'un renouvellement pouvant nécessiter de réévaluer le dispositif. En raison de l'évolution des menaces ou de la découverte de vulnérabilités, une qualification peut être retirée avant son échéance.

Paragraphe 61
L'homologation de sécurité

1. Démarche d'homologation

Il est nécessaire de mettre en œuvre une démarche dite « d'homologation » pour permettre d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré, compte tenu du besoin de protection requis. Cette démarche s'appuie sur une gestion globale des risques de sécurité concernant l'ensemble du système d'information tout au long de son cycle de vie.

L'homologation de sécurité d'un système est globale en ce qu'elle inclut dans son périmètre tout ce qui peut avoir un impact sur la sécurité du système, de nature technique, physique ou organisationnelle. En particulier, il devra être tenu le plus grand compte :

- des interconnexions avec d'autres systèmes ;
- des supports amovibles ;
- des accès à distance par des utilisateurs « nomades » ;
- des opérations de maintenance, d'exploitation ou de télégestion du système, notamment lorsqu'elles sont effectuées par des prestataires externes.

Tout système d'information traitant des informations classifiées ou non doit faire l'objet d'une homologation par une autorité dite autorité d'homologation. Cette autorité déclare que le système d'information considéré est apte à traiter des informations du niveau de classification retenu conformément aux objectifs de sécurité visés, et qu'elle accepte les risques résiduels de sécurité. Lorsque le système recourt à des dispositifs de sécurité qualifiés par l'Agence Monégasque de Sécurité Numérique, l'autorité d'homologation prend en compte les conditions attachées à ces qualifications.

2. Autorité et commission d'homologation

L'homologation est prononcée par une autorité désignée dans les conditions suivantes :

- dans le cas où le système d'information traite d'informations classifiées au niveau *« Très Secret de Sécurité Nationale »*, le Ministre d'Etat est l'autorité d'homologation ;

- dans le cas où le système d'information appartient à une administration, un service, un organisme ou un établissement relevant de la responsabilité d'un Conseiller de Gouvernement-Ministre, celui-ci désigne l'autorité d'homologation ;

- dans le cas où le système d'information relève de la responsabilité de plusieurs Conseillers de Gouvernement-Ministres, une autorité d'homologation unique est désignée conjointement par les Conseillers de Gouvernement-Ministres intéressés ;

- dans les autres cas, notamment lorsque le système d'information appartient à un organisme privé, la désignation de l'autorité d'homologation relève de la responsabilité du ou des organismes concernés par le système d'information.

L'autorité d'homologation doit être choisie au niveau hiérarchique suffisant pour assumer la responsabilité afférente à la décision d'homologation, et notamment pour accepter les risques résiduels. Elle est en principe l'autorité chargée de l'emploi du système.

L'autorité d'homologation met en place une commission d'homologation, pilotée par le responsable de la sécurité des systèmes d'information, chargée de l'assister et de préparer la décision d'homologation. Une telle commission comprend notamment le responsable de la sécurité des systèmes d'information, des représentants des utilisateurs du système, et des responsables de l'exploitation et de la sécurité du système et un représentant de l'Agence Monégasque de Sécurité Numérique.

3. Décision d'homologation

La décision d'homologation est prise après l'examen du dossier d'homologation. Celui-ci comporte notamment :

- une analyse de risques ;

- la politique de sécurité du système ;

- les procédures d'exploitation de la sécurité ;

- la gestion des risques résiduels ;

- les résultats des tests et des audits menés pour vérifier la conformité du système à la politique de sécurité et aux procédures d'exploitation ;

- le cas échéant, les agréments des dispositifs de sécurité.

La décision d'homologation doit intervenir avant la mise en service opérationnel du système. Cependant, de façon exceptionnelle, lorsque l'urgence opérationnelle le requiert, il peut être procédé à une mise en service provisoire, sans attendre l'homologation du système, en tenant compte de l'avancement de la procédure d'homologation et des risques résiduels de sécurité. Dans ce cas, la mise en service définitive interviendra ultérieurement, lorsque l'homologation de sécurité aura été prononcée.

La décision d'homologation est prononcée pour une durée maximale :

- de cinq ans pour un système d'information jusqu'au au niveau *« Confidentiel-Sécurité Nationale »* ;

- de deux ans pour un système d'information au niveau *« Secret de Sécurité Nationale »* ou *« Très Secret de Sécurité Nationale »*.

L'Agence Monégasque de Sécurité Numérique est destinataire de toute décision d'homologation portant sur les systèmes d'information.

4. Contrôle et renouvellement de l'homologation

L'autorité d'homologation fixe les conditions du maintien de l'homologation de sécurité au cours du cycle de vie du système d'information. Elle contrôle régulièrement que le système fonctionne effectivement selon les conditions qu'elle a approuvées, en particulier après des opérations de maintien en condition opérationnelle.

L'autorité d'homologation examine le besoin de renouvellement de l'homologation avant le terme prévu notamment lorsque :

- les conditions d'exploitation du système ont été modifiées ;

- des nouvelles fonctionnalités ou applications ont été installées ;

- le système a été interconnecté à de nouveaux systèmes ;

- des problèmes d'application des mesures de sécurité ou des conditions de maintien de l'homologation ont été révélés, par exemple lors d'un audit de sécurité ;

- les menaces sur le système ont évolué ;

- de nouvelles vulnérabilités ont été découvertes ;

- le système a fait l'objet d'un incident de sécurité.

PARAGRAPHE 62
Articles contrôlés de la sécurité des systèmes d'information (A.C.S.S.I.)

Certains moyens, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d'évaluation, etc.) peuvent nécessiter la mise en œuvre d'une gestion spécifique visant à assurer leur traçabilité tout au long de leur cycle de vie. Il s'agit des moyens et des informations, qu'ils soient eux-mêmes classifiés ou non, qu'il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée.

Ces moyens et informations sont appelés *« Articles Contrôlés de la Sécurité des Systèmes d'Information »* (A.C.S.S.I.). Ils portent un marquage spécifique les identifiant, en plus, le cas échéant, de leur mention de classification.

Les principes de gestion de ces articles ont pour objectif :

- de former, de sensibiliser et de responsabiliser les détenteurs de tels moyens et informations ;
- d'assurer la comptabilité de ces moyens et informations, et d'en établir l'inventaire au niveau de l'Agence Monégasque de Sécurité Numérique ;
- de contrôler périodiquement leur localisation et leur état ;
- d'informer toute compromission suspectée ou avérée à la suite d'événements tels que la perte, le vol ou la disparition, même temporaire ;
- de s'assurer de leur destruction.

PARAGRAPHE 63
Systèmes d'information particuliers

1. Traitement des informations « Spécial Monaco »

Les systèmes d'information susceptibles de traiter des informations portant la mention « Spécial Monaco » doivent faire l'objet de mesures de sécurité particulières pour garantir que les utilisateurs étrangers qui auraient un besoin d'accès légitime au système ne puissent accéder aux informations dont l'accès n'est autorisé qu'aux seuls utilisateurs monégasques.

2. Echanges internationaux

Lorsque des informations classifiées sont transmises dans des systèmes d'information relevant de la responsabilité d'Etats étrangers ou d'organisations internationales, des mesures de protection doivent être fixées par des accords ou des règlements de sécurité avec ces partenaires, qui assurent à ces informations un niveau de protection au moins équivalent à celui prévu dans la présente annexe.

La protection des systèmes d'information traitant d'informations classifiées confiées à Monaco par des Etats étrangers ou par des organisations internationales, est assurée conformément aux accords et aux règlements de sécurité établis avec ces partenaires. Ces accords et règlements font, le cas échéant, l'objet de règles complémentaires pour l'application de ces mesures. A défaut de tels accords ou règlements, les dispositions de la présente annexe s'appliquent à ces systèmes.

GLOSSAIRE

Accord de sécurité : accord intergouvernemental conclu entre au moins deux Etats ou au sein d'une alliance multinationale et ayant pour objet la protection d'informations ou de supports classifiés. Ces accords comprennent l'identification et la reconnaissance mutuelle des autorités nationales de sécurité, la correspondance des niveaux de classification, la reconnaissance mutuelle des habilitations de personnes, les modalités de transmission et de protection des informations et supports classifiés.

Administrateur de sécurité : personne chargée de la mise en œuvre, du maintien, du contrôle et de l'évolution des mesures de sécurité à appliquer à tout système d'information contenant des informations ou supports classifiés aux niveaux « Secret de Sécurité Nationale » ou « Confidentiel-Sécurité Nationale ».

Administrateur système : personne chargée de la mise au point, de l'exploitation, de la maintenance, du contrôle et des évolutions du système informatique.

Archivage : opération consistant à verser à un service d'archives des supports d'information lorsqu'ils ne sont plus d'utilisation habituelle. Les supports faisant encore l'objet d'une classification ne peuvent être archivés que dans certaines conditions et dans des services habilités à les recevoir. Un support classifié au niveau « Très Secret de Sécurité Nationale » ne peut en aucun cas être archivé.

Authenticité : propriété d'une information ou d'un traitement qui garantit son identité, son origine et, éventuellement, sa destination.

Autorité d'habilitation : autorité compétente pour solliciter une enquête d'habilitation ou un contrôle élémentaire et émettre la décision.

Autorité Nationale de Sécurité (A.N.S.) : organisme gouvernemental chargé des relations avec les autres Etats et les structures internationales en matière d'habilitation de personnes et de protection des informations ou supports classifiés.

Avis de sécurité : conclusion émise par un service enquêteur à l'issue d'investigations se rapportant à une personne et visant à détecter et à évaluer les vulnérabilités de cette personne. L'avis de sécurité est une aide à la décision d'habilitation, mais il ne lie pas l'autorité responsable de la décision.

Besoin d'en connaître : nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée, pour la bonne exécution d'une mission précise.

Catalogue des emplois : dans un organisme, liste des emplois qui peuvent nécessiter l'accès aux informations ou supports classifiés. Le catalogue est dressé sur le seul critère du besoin d'en connaître.

Certificat de sécurité : document prouvant l'habilitation d'une personne au traitement d'informations ou supports classifiés à un niveau précisé.

Classification spéciale : catégorie d'informations ou supports classifiés au niveau « Très Secret de Sécurité Nationale » et répondant à la nécessité de cloisonnement. Les classifications spéciales sont organisées en réseaux de sécurité constitués d'antennes d'utilisation. Les habilitations au niveau « Très Secret de Sécurité Nationale » sont prononcées au titre d'une ou plusieurs classifications spéciales expressément désignées.

Convoyeur : personne titulaire d'une « décision de sécurité convoyeur » délivrée par une autorité d'habilitation pour convoyer un document, équipement ou composant classifié.

Compromission : prise de connaissance, certaine ou possible, d'une information ou d'un support classifié par une ou plusieurs personnes non qualifiées.

Confidentialité : caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés.

Décision d'habilitation (au secret de sécurité nationale) : acte administratif autorisant, au terme de la procédure d'habilitation, le titulaire, en fonction de son besoin d'en connaître, à accéder aux informations ou aux supports classifiés d'un niveau déterminé. L'intéressé est informé de la décision d'habilitation, qui ne lui est jamais remise.

Décision de sécurité convoyeur : autorisation accordée pour assurer, durant le transport, la garde des informations ou des supports classifiés.

Déclassement : modification, par abaissement, du niveau de classification d'informations ou supports classifiés.

Déclassification : suppression de la classification d'informations ou supports classifiés à quelque niveau que ce soit.

Disponibilité : propriété d'une information ou d'un traitement d'être utilisable à la demande par une personne ou par un système.

Dossier d'habilitation : dossier constitué en vue de l'habilitation d'une personne. Il comporte la demande d'habilitation établie par l'autorité demanderesse et attestant le besoin d'en connaître, la notice individuelle renseignée par l'intéressé et une photographie d'identité récente.

Donnée : toute représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

Engagement de responsabilité : document en deux volets signés par le titulaire de l'habilitation lors de sa prise et de sa cessation de fonction. L'engagement a pour but de rappeler à cette personne la responsabilité pénale qui lui incombe du fait de son habilitation. La signature de l'encart central du formulaire de l'engagement de responsabilité par l'intéressé vaut prise de connaissance de la décision.

Homologation de sécurité : déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le système d'information (SI) opère dans les conditions approuvées par l'autorité d'homologation.

Identification : mention figurant sur un support d'information et précisant le numéro de l'exemplaire ainsi que son numéro d'enregistrement.

Imputabilité : capacité à identifier l'auteur d'une action.

Information : tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, à un enregistrement ou à un traitement.

Information ou support classifié : procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier présentant un caractère de secret de sécurité nationale.

Intégrité : propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.

Lieux abritant des éléments classifiés : locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau.

Marquage : opération consistant à apposer sur un support classifié les mentions précisant son niveau de classification, le numéro d'exemplaire, le numéro d'enregistrement, la pagination pour un document papier et, le cas échéant, la destination exclusivement nationale.

Matériel classifié : objet, équipement, installation, système ou substance présentant un caractère de secret de la sécurité nationale et qui nécessite une protection appropriée au niveau *« Très Secret de Sécurité Nationale »*, *« Secret de Sécurité Nationale »* ou *« Confidentiel-Sécurité Nationale »*.

Mise en éveil : démarche initiée par l'autorité d'habilitation auprès de la personne à habiliter pour la sensibiliser à ses vulnérabilités découvertes au cours de l'enquête administrative.

Mise en garde : démarche initiée par l'autorité d'habilitation visant à sensibiliser l'officier de sécurité du service employeur d'une personne sur l'existence d'éléments pouvant présenter un risque de vulnérabilité de la personne à habiliter.

Non-répudiation : impossibilité de nier la participation au traitement d'une information.

Notice individuelle : formulaire destiné à recueillir les renseignements nécessaires à l'habilitation d'une personne. Elle doit être renseignée par l'intéressé lui-même et constitue un élément majeur du dossier d'habilitation. Elle est exploitée par l'autorité chargée de prononcer la décision et par les services enquêteurs.

Officier de sécurité : nommé par le responsable du service employeur, il est le correspondant de l'Agence Monégasque de Sécurité Numérique et de la Direction de la Sûreté Publique. Il a pour mission, sous les ordres de son autorité d'emploi et en fonction des modalités propres à chaque structure, de fixer les règles et consignes de sécurité à mettre en œuvre concernant les personnes et les informations ou supports classifiés et d'en contrôler l'application. Il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret de sécurité nationale. Il est chargé de la gestion des habilitations et, en liaison avec la Direction de la Sûreté Publique, du contrôle des accès aux zones abritant des éléments du secret de sécurité nationale.

Personne habilitée : est habilitée, au sens de l'article 18 de la loi n° 1.430 du 13 juillet 2016, la personne qui, par son état, sa profession, sa fonction ou sa mission, temporaire ou permanente, est habilitée à avoir accès à une information classifiée et a le besoin d'en connaître.

Plan d'urgence : document établi par un organisme détenteur d'informations ou supports classifiés, prévoyant, en cas de circonstances exceptionnelles, les modalités d'évacuation ou de destruction des supports d'information.

Procédure d'habilitation : procédure visant à s'assurer qu'une personne peut, sans risque pour la sécurité nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l'exercice de ses fonctions.

Qualification d'un produit de sécurité : reconnaissance formelle que le produit de sécurité évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.

Reclassement : modification, par relèvement, du niveau de classification d'informations ou de supports classifiés.

Refus d'habilitation : décision prise par l'autorité d'emploi, au vu de l'avis de sécurité ou de tout autre élément recueilli sur une personne, de ne pas habiliter cette personne.

Réseau de sécurité : ensemble des moyens humains, matériels et organisationnels qui permettent l'acheminement en toute sécurité des informations ou supports classifiés à un niveau déterminé (et en deçà), entre un ensemble de correspondants habilités.

Responsable de la classification : autorité émettrice d'informations qui leur attribue, en fonction de leur contenu, un niveau de classification approprié.

Renouvellement d'habilitation : procédure déclenchée à la fin de validité d'un avis de sécurité concernant une personne déjà habilitée en vue d'obtenir un avis actualisé. Ce nouvel avis permettra de prononcer une décision d'habilitation au profit de la personne qui présente encore le besoin d'en connaître.

Retrait d'habilitation : décision prise par l'autorité d'emploi, au vu d'éléments nouveaux de vulnérabilité, de supprimer l'habilitation d'une personne.

Sensibilisation : instruction périodiquement prodiguée aux personnes habilitées ou susceptibles d'être habilitées et destinée à leur faire prendre conscience des enjeux de la protection du secret de la sécurité nationale, des sanctions judiciaires et administratives encourues et de la nécessité d'appliquer les mesures de sécurité prescrites.

Support : tout moyen matériel, quelles qu'en soient la forme et les caractéristiques physiques, permettant de recevoir, de conserver ou de restituer des informations ou des données.

Système d'information : ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des informations.

Timbre : mention figurant sur un support d'information précisant son niveau de classification et, le cas échéant, son usage national exclusif. Le timbre possède des caractéristiques définies (dimensions, aspect).

Vulnérabilité : fait relatif à la situation d'une personne et qui amoindrit les garanties qu'elle présente pour la protection des informations ou supports classifiés. Il s'agit d'une fragilité qui peut donner lieu à des pressions de diverses natures et qui doit être prise en compte pour accorder avec ou sans restriction, pour refuser ou pour retirer l'accès aux informations ou supports classifiés.

APPENDICES

TABLE DES APPENDICES

APPENDICE 1

PRINCIPAUX TEXTES DE RÉFÉRENCE

1. Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la Sécurité Nationale.

2. Ordonnance du 23 juin 1902 établissant une Direction de la Sûreté publique.

3. Ordonnance Souveraine n° 16.605 du 10 janvier 2005 portant organisation des Départements ministériels, modifiée.

4. Ordonnance Souveraine n° 765 du 13 novembre 2006 relative à l'organisation et au fonctionnement de la Direction de la Sûreté Publique, modifiée.

5. Ordonnance souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.

6. Ordonnance souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique.

APPENDICE 2

GUIDE DE CLASSIFICATION

RECOMMANDATIONS POUR L'ÉLABORATION DES REGLES RELATIVES À LA PROTECTION DU SECRET DE SECURITE NATIONALE.

Il revient au Ministre d'Etat et à chaque Conseiller de Gouvernement-Ministre, pour ce qui relève de leurs attributions, de définir dans une note particulière :

a) Les conditions d'emploi des niveaux de classification *« Secret de Sécurité Nationale »* et *« Confidentiel-Sécurité Nationale »*. Il fixe notamment :

- le champ d'application de chacun des niveaux « Secret de Sécurité Nationale » et « Confidentiel-Sécurité Nationale » et dresse la nomenclature des informations ou catégories d'informations qui devront être couvertes par le secret de sécurité nationale ;

- les critères objectifs à considérer pour apprécier le caractère secret de l'information (par exemple l'importance dans l'organisation et la politique de sécurité, le domaine concerné, la nature de la source...) ;

- les autorités responsables de la classification.

b) Les informations ou catégories d'informations qui doivent être classifiées au niveau « Très Secret de Sécurité Nationale ».

Les éléments définis dans l'article 18 de la loi n° 1.430 du 13 juillet 2016, peuvent être pris comme référence pour procéder à la classification au niveau le plus pertinent.

Il est rappelé que la décision de classifier une information est un acte important par les contraintes qu'il induit en matière de protection et les conséquences qu'il peut générer. Une sur-classification engendre une inflation de documents protégés, dévalorise la notion de secret et s'accompagne de surcoûts. A l'inverse, une sous-classification ne garantit pas à l'information une protection suffisante.

APPENDICE 3

RÈGLES DE PROTECTION DES INFORMATIONS OU SUPPORTS PORTANT UNE MENTION PARTICULIERE (PAR EX DIFFUSION RESTREINTE)

La mention particulière n'est pas un niveau de classification mais une mention de protection. Son objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

1. Teneur des informations de la mention particulière

L'application de cette mention relève de la nécessité d'éviter la divulgation, dans le domaine public, d'informations dont le regroupement ou l'exploitation pourraient :

- conduire à la découverte d'une information classifiée ;
- porter atteinte à la sécurité ou à l'ordre public, au renom des institutions, à la vie privée de leurs membres ;
- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics.

2. Condition d'emploi de la mention particulière

Il appartient à chaque autorité des administrations de l'Etat, chef d'établissement ou chef de service, de décider si la diffusion d'une information doit être restreinte ou non et de la mention à attribuer.

3. Elaboration et marquage

Les documents à mention particulière doivent être identifiés sur la première page avec les références de l'organisme émetteur, la date d'émission et le numéro d'enregistrement.

Ils doivent porter le marquage suivant :

- sur chaque page, le timbre approprié apposé au milieu du haut de la page ;
- pour les messages et autres documents informatiques, la mention approprié rappelée en début de chaque page.

4. Expédition et circulation

La transmission des documents à mention particulière peut être effectuée vers l'extérieur sous double enveloppe, l'enveloppe intérieure portant la mention particulière et les références du document, l'enveloppe extérieure ne comportant que les indications nécessaires à la transmission.

5. Conservation, destruction et reproduction

Les documents marqués d'une mention particulière sont enregistrés au départ et à l'arrivée selon les règles appliquées à tout document administratif non classifié.

Ils doivent être conservés dans des meubles fermant à clés.

Leur destruction a lieu sous la responsabilité des détenteurs, sans mention particulière sur les documents d'enregistrement du courrier.

Leur reproduction doit rester limitée aux seuls besoins du service.

6. Sécurité des systèmes d'information

Les systèmes d'information destinés au traitement, au stockage ou à la transmission des informations à mention particulière font l'objet d'une homologation de sécurité. L'Agence Monégasque de Sécurité Numérique définit les règles applicables à ces systèmes d'information.

Lorsque l'urgence de leur traitement ou de leur transmission est plus importante que la protection de leur confidentialité, des informations à mention particulière peuvent, à titre exceptionnel, être traitées ou transmises sur des systèmes n'ayant pas fait l'objet d'une homologation de sécurité au niveau adéquate.

7. Exemple de mention particulière :

- confidentiel médical ;
- confidentiel personnel ;
- diffusion restreinte.

APPENDICE 4

LES TYPES DE MESURES DE PROTECTION PHYSIQUE

L'ensemble des mesures de sécurité relatif à la protection physique est destiné à garantir l'intégrité des bâtiments et des locaux spécifiquement dédiés aux informations ou supports classifiés ainsi que la fiabilité des meubles dans lesquels ils sont conservés, afin d'éviter toute perte, dégradation ou compromission.

Le niveau de classification des informations et supports détermine les menaces et les vulnérabilités à prendre en compte et conditionne le dispositif de protection.

Les mesures de protection physique mettent en œuvre des moyens techniques ou humains et reposent sur une organisation particulière, coordonnant l'ensemble. Elles comprennent :

- des mesures statiques à base de dispositifs matériels. Elles constituent l'essentiel des moyens de protection (murs, clôtures, portes, armoires fortes...) et de détection (radar volumétrique, contact d'ouverture, détecteur sismique...) et assurent la protection passive et active. Elles incluent aussi l'installation de systèmes de contrôle d'accès hiérarchisés selon le besoin d'en connaître (tels que badge ou lecteur biométrique) ;

- des mesures dynamiques mettant en jeu des personnes (gardes, rondes de surveillance, filtrage, éléments d'intervention présents sur le site ou extérieurs) qui contribuent à la détection par des actions de surveillance et assurent l'intervention adéquate en cas d'intrusion ;

- des mesures technologiques nouvelles dont l'emploi devra être parfaitement connu, testé par les utilisateurs et, le cas échéant, complété par des procédés mécaniques plus traditionnels ;

- des dispositifs technologiques nouveaux dont l'emploi devra être parfaitement connu, testé par la Direction de la Sûreté Publique ou l'Agence Monégasque de Sécurité Numérique.

Les mesures de protection physique font l'objet d'un suivi rigoureux et de toute mise à jour nécessaire pour préserver l'efficacité de l'ensemble du dispositif de sécurité.

APPENDICE 5

LES BARRIÈRES DE PROTECTION PHYSIQUE ET LEUR RÉPARTITION EN CLASSES

Les barrières sont réparties en classes indiquant leur degré de résistance à une tentative d'intrusion. Chacune des barrières est répartie en quatre classes, de la moins fiable à la plus sûre. Un contrôle d'accès et une procédure d'intervention s'imposent pour toutes les classes.

1. Classes du bâtiment et/ou de l'emprise

- **Classe 4** : enceinte protégée (clôture d'une hauteur supérieure à 2,15 m ou, dans le cas où les murs du bâtiment constituent l'enceinte, protection de toutes les ouvertures situées à moins de 5,50 m au-dessus du niveau du sol) mais absence de gardes permanents ou de dispositif de détection alarme.

- **Classe 3** : protection de la classe 4 + gardes permanents effectuant des rondes de surveillance dans les locaux et l'emprise ou dispositif de détection-alarme relié à un élément d'intervention extérieur (service de police, société de gardiennage).

- **Classe 2** : protection de la classe 3 + dispositifs de détection-alarme (éclairage, télésurveillance, vidéosurveillance, détection périmétrique ou périphérique) + présence de gardes permanents.

- **Classe 1** : protection de la classe 2 + dispositifs de détection-alarme pour les locaux (détection périphérique ou volumétrique) ou les meubles (détection ponctuelle) + traçabilité des accès (registre et vidéosurveillance).

Les dispositifs électroniques de filtrage ne peuvent pas à eux seuls garantir l'intégrité des accès aux bâtiments et/ou aux emprises. Ils doivent obligatoirement être complétés par des systèmes mécaniques de fermeture activés en dehors des heures normales d'occupation des bâtiments.

2. Classes du local

Les parois ainsi que les plafonds et les sols des locaux doivent avoir une résistance suffisante.

- **Classe d** : local avec porte à serrure mécanique ordinaire, équipée d'une sûreté à clé dont, si possible, l'ébauche est protégée, et fenêtres sans protection.

• **Classe c** : local avec porte à serrure mécanique de haute sécurité (multipoints), équipée d'une sûreté à clé dont l'ébauche est protégée et fenêtres protégées lorsqu'elles sont situées à moins de 5,5 m d'un lieu accessible (sol, toit, corniche, descente d'eau pluviale, promontoire).

La protection des fenêtres doit être assurée :

- soit par des barres en acier de 2 cm de diamètre au moins, espacées de 11 cm au plus ;

- soit par un vitrage anti-effraction. Les fenêtres doivent être alors munies d'un dispositif de limitation d'ouverture de manière à empêcher toute intrusion.

• **Classe b** : local avec porte renforcée (en bois plein ou recouverte de feuilles d'acier) équipée d'un système anti-dégondage, à serrure mécanique de haute sécurité avec détecteur ou compteur d'ouverture ; les autres ouvertures doivent être protégées comme pour la classe c.

• **Classe a** : chambre forte dont la porte est au minimum équipée des systèmes de sécurité des armoires fortes de classe B. Les parois des locaux doivent avoir une résistance au moins équivalente à 15 cm de béton.

3. Classes du meuble

Les meubles de sécurité destinés à la conservation des informations ou supports classifiés se répartissent en trois classes et ne pourront pas être ouverts frauduleusement sans effraction. Ils sont donc conçus pour que toute tentative d'ouverture illégitime laisse des traces visibles. Ils seront dotés par défaut de serrure mécanique satisfaisant à la norme maximale de sécurité de leur pays de conception.

• **Classe C** : armoire dite forte, à un ou deux battants, à structure métallique d'au moins 2 millimètres d'épaisseur, munie d'une serrure mécanique à combinaison silencieuse et à manœuvre discrète qui permet de s'affranchir de la conservation des clés. Les battants doivent posséder un système d'accrochage du côté du pivot interdisant le démontage des portes en cas de sectionnement des gonds, lorsque le meuble est condamné. Les pênes, inaccessibles de l'extérieur, ne doivent pas pouvoir être démontés.

• **Classe B** : armoire forte de structure identique à la classe C, complété par les dispositifs suivants :

- un renforcement de la structure de la zone située derrière les organes essentiels (148) dont la présence peut être vérifiée visuellement par démontage du foncet de porte (face intérieure de la porte) ;

- un dispositif délateur, à déclenchement mécanique et thermique, bloquant définitivement les mécanismes d'ouverture en cas de tentative d'ouverture illégitime ;

- un plombage du foncet de porte (face intérieure de la porte) permettant de détecter aisément un démontage ;

- un système à clé interdisant l'accès au dispositif de changement de la combinaison pour les modèles mécaniques ;

- un système d'asservissement, interdisant la sortie des pênes de la porte principale lorsque l'autre battant n'est pas fermé, s'il ne s'agit pas d'une porte à battant unique ;

- un dispositif qui interdise aux pênes de la porte principale, une fois sortis, de se rétracter à moins que la combinaison soit à nouveau composée ;

- un compteur d'ouverture non falsifiable et non réutilisable, sans dispositif de remise à zéro et protégé par le foncet ;

- une serrure mécanique à combinaison silencieuse et à manœuvre discrète est à recommander. L'emploi d'une serrure électronique peut être autorisé s'il est justifié. Elle doit alors être de haut de gamme, posséder une mémoire permettant son audit, éventuellement pouvoir être paramétrée pour n'être ouverte que dans des plages horaires choisies, comporter un dispositif permettant à un usager de déclencher une alarme auprès d'un service de sécurité lorsque l'ouverture est effectuée sous la menace ;

- le meuble équipé d'une combinaison électronique devra comporter une serrure mécanique à clé facilement permutable en supplément. Cette clé devra être prisonnière de la serrure tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis portes fermées ;

- un système de tringlerie métallique en acier assurant sur la porte principale une répartition géographique de plusieurs pênes horizontaux et verticaux. Si une poignée actionne ce système, elle doit posséder un point de rupture pour éviter un effort trop conséquent sur la tringlerie ;

- les portes seront dépourvues de toute plaque de propreté et de tout enjoliveur.

• **Classe A** : coffre-fort blindé sur toutes ses faces, d'un poids minimum à vide de 500 kilogrammes ou, à défaut, fixé au mur, au sol ou sur une plaque métallique dont la plus petite dimension est supérieure à la plus grande dimension des issues du local.

Ce meuble devra comporter tous les systèmes de sécurité de la classe B et, en plus :

- une ou plusieurs serrures pouvant s'adapter à un nouveau jeu de clés (serrures mécaniques dites à clé) facilement permutable ;

- au moins une serrure dont la clé reste prisonnière du mécanisme tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis porte fermée.

D'une manière générale, la marque et le numéro de série du meuble sont estampillés de façon apparente et inaltérable, à l'extérieur de celui-ci, sur des parties fixes et sur des parties mobiles. Le numéro de série et l'année de fabrication de chaque serrure figurent sur celles-ci.

TABLEAUX DE COMBINAISON

DES CLASSES

Les tableaux suivants indiquent les différentes combinaisons possibles entre les classes des trois barrières afin d'obtenir un niveau de sécurité minimal en fonction de chacune des classifications.

TABLEAU 1

Niveau *« Très Secret de Sécurité Nationale »*

CLASSE DU BÂTIMENT ou de l'emprise	CLASSE DU LOCAL			
	a	b	c	d
1	C	B	Interdit	Interdit
2	B	A	Interdit	Interdit
3	A	Interdit	Interdit	Interdit
4	Interdit	Interdit	Interdit	Interdit

TABLEAU 2

Niveau *« Secret de Sécurité Nationale »*

CLASSE DU BÂTIMENT ou de l'emprise	CLASSE DU LOCAL			
	a	b	c	d
1	C	C	Interdit	Interdit
2	C	C	Interdit	Interdit
3	C	C	Interdit	Interdit
4	Interdit	Interdit	Interdit	Interdit

TABLEAU 3

Niveau *« Confidentiel-Sécurité Nationale »*

CLASSE DU BÂTIMENT ou de l'emprise	CLASSE DU LOCAL			
	a	b	c	d
1	C	C	C	C
2	C	C	C	C
3	C	C	C	B
4	C	C	B	Interdit

APPENDICE 6

NOTICE INDIVIDUELLE D'HABILITATION

CONFIDENTIEL PERSONNEL

Photographie d'identité du candidat

NOTICE INDIVIDUELLE
ZONE RÉSERVÉE A L'ORGANISME DEMANDEUR

Organisme demandeur : _____

Procédure d'habilitation demandée : ☐ Admission ☐ Renouvellement ☐ Révision

Habilitation : ☐ Très Secret _____ ☐ Secret _____ ☐ Confidentiel _____

Autorité de décision à laquelle l'avis de sécurité doit être envoyé : _____

Grade ou qualité, prénom et nom de l'officier de sécurité : _____ Signature de l'officier de sécurité :

Date : _____

ZONE RÉSERVÉE AU CANDIDAT A L'HABILITATION

Nom de famille *(de jeune fille suivi d'épouse X... pour les femmes mariées) (EN LETTRES MAJUSCULES)* : _____ Prénoms *(indiquer en premier le prénom usuel)* : _____

Date de naissance : _____ Sexe : ◯ M ◯ F Surnom ou alias éventuels : _____

Lieu de naissance

Ville : _____ Code postal :

Pays : _____ Code commune :

Nationalité

Nationalité(s) à la naissance : _____ Nationalité(s) actuelle(s) : _____

Année d'acquisition de la nationalité actuelle : Année d'arrivée dans le pays : Pays d'origine : _____

Domicile actuel

N°, rue : _____ Commune : _____

Depuis le : _____ Code postal : Code commune :

N° de téléphone : _____ Email : _____

Domicile précédent *(si changement d'adresse depuis moins de six mois)* ☐ Cocher si sans objet

N°, rue : _____ Commune : _____

Du : _____ Au : _____ Code postal : Code commune :

Résidence secondaire ou occasionnelle *(y compris à l'étranger)* ☐ Cocher si sans objet

N°, rue : _____ Commune, pays : _____

Depuis le : _____ Code postal : Code commune :

N° de téléphone : _____ Email : _____

Situation professionnelle actuelle ◯ Civil ◯ Militaire

Fonction - Profession : _____

Grade - Fonction : _____

Unité d'appartenance : _____

Département d'origine : _____ Département d'emploi : _____

Organisme d'affectation : _____ Depuis le : _____

Adresse professionnelle : _____

Tph professionnel : _____ Email professionnel : _____

Emploi(s) successif(s) durant les cinq dernières années *(si nécessaire, utiliser l'espace "Renseignements complémentaires" en page 6)*

Etablissement ou organisme d'emploi / adresse *(N°, rue, commune, pays si étranger).*	Emploi ou fonction	Code postal	Période Du :	Période Au :

Habilitation déjà détenue *(en Principauté ou dans un autre pays, précisez lequel)* ☐ Cocher si sans objet

Niveau d'habilitation : _____ Depuis le : _____

Niveau d'études et culture générale

DIPLOMES OBTENUS OU NIVEAU EQUIVALENT	Langues étrangères – Langue	Langues étrangères – Degré de connaissance

Situation de famille actuelle

☐ Célibataire ☐ En instance de mariage ☐ Marié(e) ☐ Veuf(ve) ☐ Séparé(e) ☐ Divorcé(e) ☐ En instance de remariage

☐ Remarié(e) ☐ Concubinage ☐ PACS ☐ Autre situation Nombre d'enfants :

Date et lieu de mariage ou de la présente situation : Date : _____ Lieu *(ville,pays)* : _____

Précisions sur la situation actuelle *(qu'il y ait ou non cohabitation)* : _____

Documents administratifs

	Numéro	Autorité de délivrance	Date de délivrance
Carte nationale d'identité			
Passeport *(préciser si privé, de service ou diplomatique)*			

Voyages et séjours à l'étranger durant les cinq dernières années *(en partant du plus récent).* ☐ Cocher si sans objet

Pays - Période*(date de début et de fin)* **- Adresse***(n'indiquer l'adresse que pour les séjours d'une durée de plus de six mois)*	Motif *(professionnel, familial, touristique, ...)*

Enfants *(si nécessaire, utiliser l'espace "Renseignements complémentaires" en page 6).*
Ne pas mentionner ici les enfants du conjoint nés d'une précédente union.

☐ Cocher si sans objet

Nom et prénoms	Sexe	Date de naissance	Lieu de naissance	Code postal	Code commune	Nationalité	Eventuel domicile distinct *(N°, rue, commune, pays si étranger)*

Parents du candidat

	Père	Mère *(nom de jeune fille suivi du nom d'épouse)*
Nom		
Prénom(s)		
Date de naissance		
Lieu de naissance		
Code postal - code commune	-	-
Nationalité(s) à la naissance		
Nationalité(s) actuelle(s)		
Date d'arrivée dans le pays de résidence actuel		
Pays d'origine		
Année d'acquisition de la nationalité actuelles		
N° de carte nationale d'identité ou de passeport		
Adresse du domicile actuel ou du dernier domicile avant le décès *(préciser date du décès)* *(N°, rue, commune, pays si étranger)*		
Nom et adresse de l'employeur actuel ou du dernier employeur *(N°, rue, commune, pays si étranger)*		

CONJOINT*

☐ Cocher si sans objet

*Il s'agit de la personne visée dans le cadre "situation de famille actuelle" en deuxième page.

Nom de famille *(de jeune fille suivi d'épouse X... pour les femmes mariées) (EN LETTRES MAJUSCULES)* : _____ Prénoms *(indiquer en premier le prénom usuel)* : _____

Date de naissance : _____ Sexe : ○M ○F Surnom ou alias éventuels : _____

Lieu de naissance

Ville : _____ Code postal : _____

Pays : _____ Code commune : _____

Nationalité

Nationalité(s) à la naissance : _____ Nationalité(s) actuelle(s) : _____

Année d'acquisition de la nationalité actuelle : _____

Année d'arrivée dans le pays : _____ Pays de naissance : _____

Domicile actuel ☐ Si même domicile que le candidat, cocher et ne pas renseigner.

N°, rue : _____ Commune : _____

Depuis le : _____ Code postal : _____ Code commune : _____

N° de téléphone : _____ Email : _____

Résidence secondaire ou occasionnelle *(y compris à l'étranger)* ☐ Cocher si sans objet ou si même résidence secondaire que le candidat.

N°, rue : _____ Commune, pays : _____

Depuis le : _____ Code postal : _____ Code commune : _____

N° de téléphone : _____ Email : _____

Documents administratifs

	Numéro	Date de délivrance	Autorité de délivrance
Carte nationale d'identité			
Passeport *(préciser si privé, de service ou diplomatique)*			

Niveau d'études et culture générale

DIPLOMES OBTENUS OU NIVEAU EQUIVALENT	Langues étrangères	
	Langue	Degré de connaissance

Situation professionnelle actuelle ○ Civil ○ Militaire

Fonction - Profession : _____

Grade - Fonction : _____

Unité d'appartenance : _____

Département d'origine : _____ Département d'emploi : _____

Organisme d'affectation : _____ Depuis le : _____

Adresse professionnelle : _____

Tph professionnel : _____ Email professionnel : _____

Voyages et séjours à l'étranger durant les cinq dernières années *(en partant du plus récent)*. ☐ Cocher si sans objet

Pays - Période*(date de début et de fin)* **- Adresse***(n'indiquer l'adresse que pour les séjours d'une durée de plus de six mois)*	Motif *(professionnel, familial, touristique, ...)*

Enfants *(ne mentionner que les enfants du conjoint nés d'une précédente union).* ☐ Cocher si sans objet

Nom et prénoms	Sexe	Date de naissance	Lieu de naissance	Code postal	Code commune	Nationalité	Eventuel domicile distinct *(N°, rue, commune, pays si étranger)*

Parents du conjoint du candidat	Père	Mère *(nom de jeune fille suivi du nom d'épouse)*
Nom		
Prénom(s)		
Date de naissance		
Lieu de naissance		
Code postal / code commune	-	-
Nationalité(s)à la naissance		
Nationalité(s)actuelle(s)		
Date d'arrivée dans le pays de résidence actuel.		
Pays d'origine		
Année d'obtention de votre nationalité		
N° de carte nationale d'identité ou de passeport		
Adresse du domicile actuel ou du dernier domicile avant le décès *(N°, rue, commune, pays si étranger)*		
Nom et adresse de l'employeur actuel ou du dernier employeur		

Renseignements de sécurité

Répondre par **OUI** ou par **NON** aux questions suivantes :

1. Pensez-vous, vous-même ainsi que votre conjoint(e) ou concubin(e) :

a) avoir été sollicité(e) en dehors de vos attributions professionnelles pour fournir des informations à caractère sensible ?

b) que des pressions ont été exercées sur vous, ou sur des membres de votre famille, à la suite d'un incident survenu sur le territoire étranger ?

c) avoir été l'objet d'approches de la part d'un service de renseignement ou de sécurité étranger ?

En cas de réponse positive, décrire les circonstances.

2. Avez-vous des proches parents résidant à l'étranger ou êtes-vous en relations suivies, à titre professionnel ou privé, avec des ressortissants étrangers ?

Si la réponse est positive, identifiez les personnes concernées (nom, prénom, date et lieu de naissance, nationalité)

3) Souhaitez-vous évoquer un point particulier avec le service chargé de l'instruction du dossier ?

Renseignements complémentaires (éventuellement) ☐ Cocher si sans objet

ATTESTATION DU CANDIDAT

Je soussigné(e) (nom, prénom) : _____

a) Reconnais avoir été informé(e) de la définition de l'habilitation à laquelle je suis candidat(e) et de sa portée. Ainsi, il m'a été indiqué que la décision d'habilitation, si elle est favorable, m'autorise, en fonction de mon besoin d'en connaître, à accéder aux informations ou supports classifiés au niveau précisé dans cette décision ainsi qu'au(x) niveau(x) inférieur(s). Il m'a également été précisé que la présente demande d'habilitation déclenche une procédure destinée à vérifier qu'il m'est possible, sans risque pour la sécurité nationale ou pour ma propre sécurité, de connaître des informations ou supports classifiés dans l'exercice de mes fonctions.

b) Reconnais être informé(e) :
- du caractère obligatoire des réponses qui me sont demandées ;
- de ce qu'en l'absence de réponse aux questions posées, aucune décision ne pourra être prise quant à mon éventuelle habilitation ;
- de ce que je dispose d'un droit d'accès et de rectification, en application de la loi n°1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives.

c) Certifie l'exactitude des renseignements que j'ai fournis dans la présente notice et admets avoir été informé(e) que je m'expose, en cas d'altération frauduleuse de la vérité aux dispositions législatives ;

d) Déclare avoir été dûment avisé(e) qu'en vertu des dispositions législatives et réglementaires relatives à la protection du secret, l'habilitation à laquelle je me porte candidat(e) engage ma responsabilité et fait naître à ma charge des obligations, parmi lesquelles :
- garantir la sécurité des informations et supports classifiés auxquels je peux avoir accès par le strict respect de la réglementation applicable ;
- répondre, pénalement et administrativement, de tout acte de malveillance, d'imprudence, de négligence ou d'inattention ayant pour résultat qu'une information ou un support classifié dont je suis le dépositaire ait été détruit(e), détourné(e), soustrait(e), reproduit(e) ou porté(e) à la connaissance soit du public, soit d'une personne non qualifiée*.

*Loi n°1.430 du 13 juillet 2016

Fait à : _____ Signature du candidat : _____

Date :

imprimé sur papier PEFC

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO