Arrêté Ministériel n° 2015-703 du 26 novembre 2015 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

Vu la loi n° 975 du 12 juillet 1975 portant statut des fonctionnaires de l'État, modifiée ;

Vu l'ordonnance souveraine n° 6.365 du 17 août 1978 fixant les conditions d'application de la loi n° 975 du 12 juillet 1975, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu la délibération du Conseil de Gouvernement en date du 11 novembre 2015 ;

ARRÊTONS :

ARTICLE PREMIER.

Outre les obligations définies aux articles 7 à 11 de la loi n° 975 du 12 juillet 1975, modifiée, susvisée, les fonctionnaires relevant des services exécutifs mentionnés à l'article 44 de la Constitution sont tenus de respecter les dispositions de la Charte des systèmes d'information de l'État annexée au présent arrêté.

Les agents publics des services exécutifs mentionnés à l'article 44 de la Constitution qui ne sont pas régis par les dispositions de la loi n° 975 du 12 juillet 1975, modifiée, susvisée, sont également soumis au respect des dispositions de ladite Charte.

ART. 2.

Le Secrétaire Général du Ministère d'État et le Directeur des Ressources Humaines et de la Formation de la Fonction Publique sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le vingt-six novembre deux mille quinze.

Le Ministre d'État,
M. ROGER

CHARTE DES SYSTÈMES D'INFORMATION DE L'ÉTAT

Annexe à l'arrêté ministériel n° 2015-703 du 26 novembre 2015

TABLE DES MATIÈRES

1. DISPOSITIONS GÉNÉRALES

1.1. Préambule, définitions et objectifs

1.1.1. Préambule

L'utilisation des systèmes d'information de l'État tels que déterminés par la présente Charte s'effectue conformément aux règles destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance et, de manière générale, dans le respect des dispositions constitutionnelles, légales et réglementaires applicables.

1.1.2. Définitions

Dans le cadre de la présente charte, les termes ou expressions ci-dessous auront la signification suivante :

- « **accès distant** » : il s'agit d'un accès à partir d'un site extérieur et quel que soit le lieu de cet accès (domicile, etc.) aux systèmes d'information qui ne sont pas présents sur le moyen informatique local, et ce grâce à une technologie d'accès à distance (exemple : citrix) ;
- « **espace collaboratif** » : il s'agit d'un espace dédié à la collaboration entre différents acteurs ;il peut notamment prendre la forme d'un site internet, ou d'un serveur partagé. Cet espace a pour fonction de centraliser tous les outils liés à la conduite d'un projet, la gestion des connaissances ou au fonctionnement d'une organisation afin de les mettre à disposition des différents acteurs. L'objectif d'un espace collaboratif est de faciliter et d'optimiser la communication entre les différents acteurs d'une entité ou d'un projet ;
- « **information nominative** » : toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ;
- « **matériel nomade** » : moyens et ressources informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de l'Administration tels que par exemple ordinateur portable, téléphone mobile, Personal Digital Assistant (PDA), tablettes et autres accessoires (disquette, disque dur, carte mémoire, CDRom, clé USB, équipement réseaux, équipement sans fil, carte de communication à distance), et autres existants ou à venir ;
- « **systèmes d'information de l'État** » : ressources et moyens informatiques et moyens de communication électronique des services exécutifs de l'État, recouvrant tout matériel informatique (câblage, périphérique (tel que imprimantes simples ou multifonctions, webcam, etc.), disquette, disque dur, carte mémoire, CD-Rom, clé USB, ordinateur, tablette, PDA, photocopieurs, scanner, serveurs, baies de stockage, équipements réseau etc.) et toute ressource informatique de toute nature (telle que logiciels, applications, bases de données, etc., et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau, ainsi les moyens de communication électronique recouvrant internet et les télécommunications (tels que téléphones, équipement sans fil, carte de communication sans fil, terminaux portables, le matériel nomade, messagerie, forum, sites web, etc.) ;
- « **Administration** » : autorités relevant des services exécutifs de l'État au sens de l'article 44 de la Constitution, se trouvant placés sous l'autorité du Ministre d'État. Il s'agit en d'autres termes de l'administration gouvernementale ;
- « **Service Informatique Habilité** » : entité informatique autre que la Direction Informatique au sein d'un service de l'État, qui gère sous sa responsabilité un système d'information et/ou qui utilise certaines applications fournies par la Direction Informatique.

1.1.3. Objectifs

La présente Charte, rédigée dans l'intérêt des utilisateurs, manifeste la volonté de l'État d'assurer un développement sécurisé de l'accès et de l'utilisation de ses systèmes d'information. À cet égard, elle a pour objectif de poser les règles de déontologie et de sécurité applicables aux utilisateurs lorsqu'ils font usage des systèmes d'information de l'État.

La Charte est complétée par un document « Foire aux Questions » (FAQ) qui recense des questions réponses et un « guide d'utilisation du poste de travail » ayant pour objet de préciser, de manière pratique, à ses destinataires les règles de bon usage des systèmes d'information de l'État. Ce guide est destiné aux utilisateurs du parc informatique géré par la Direction Informatique. Des documents spécifiques pourront être établis par ailleurs par le service informatique habilité.

1.2. Personnes concernées

La présente Charte est applicable aux fonctionnaires et agents non titulaires de l'État lorsqu'ils utilisent les systèmes d'information de l'État.

Au sens de la présente Charte, l'utilisateur est tout fonctionnaire ou agent non titulaire de l'État, y compris les stagiaires, qui fait usage des systèmes d'information de l'État.

Elle est également applicable aux tiers appelés à réaliser des missions pour le compte de l'Administration.

1.3. Équipements et services concernés

1.3.1. Sont visés par la présente Charte les équipements suivants :

- l'ensemble des systèmes d'information définis ci-avant qui sont la propriété de l'État ou que ce dernier détient en licence ou en location et qui sont mis à la disposition des utilisateurs à des fins professionnelles, tels que notamment par exemple sans que cette liste ne soit limitative les postes de travail, les logiciels, les téléphones, existants ou à venir, etc.
- l'ensemble des systèmes d'information tels que définis à la présente Charte qui sont la propriété personnelle de l'utilisateur notamment smartphone et tablette et autres équipements qui seraient autorisés à l'avenir, et pour lesquels celui-ci a obtenu l'accord préalable de sa hiérarchie pour les utiliser dans le cadre de son activité professionnelle.

1.3.2. Sont visés par la présente Charte les services suivants :

Les bases de données et leur contenu, les applications informatiques, la messagerie électronique permettant l'échange de courriers et de documents, Intranet, Internet et toutes leurs applications, la téléphonie, ainsi que tout autre réseau d'information ou de communication existant ou à venir.

Les utilisateurs ne deviennent en aucun cas propriétaire des systèmes d'information de l'État mis à leur disposition.

1.4. Usages concernés

La présente Charte s'applique à tous les types d'usages, quels que soient leur fréquence ou leur périodicité et qu'ils aient lieu :

- dans les locaux de l'Administration ;
- dans le cadre d'un usage dit « nomade », c'est-à-dire l'usage des systèmes d'information pour des déplacements professionnels en-dehors des locaux de l'Administration, et quel qu'en soit le lieu ;
- dans le cadre d'un accès distant (y compris la messagerie).

2. RÈGLES D'UTILISATION

2.1. Conditions générales d'utilisation

2.1.1. Accès et identification

L'accès aux systèmes d'information de l'État est déterminé par l'autorité hiérarchique de l'utilisateur qui l'accorde en fonction des nécessités du service.

L'autorisation, la suppression et la suspension de l'accès aux systèmes d'information de l'État sont effectuées par la Direction Informatique ou le service informatique habilité, à la demande expresse de l'autorité hiérarchique du service de l'utilisateur.

Tout usage des systèmes d'information de l'État est réputé avoir été réalisé par le bénéficiaire de l'identification d'accès qui en sera pleinement responsable, sauf s'il démontre qu'il n'était en réalité pas l'utilisateur.

- *Constitution des identifiants et des codes confidentiels*

  Chaque utilisateur est doté d'un ou plusieurs identifiants et codes confidentiels permettant l'accès aux systèmes d'information de l'État, de manière nomade ou non, et qui peuvent prendre diverses formes et notamment login, mots de passe, cartes à puce, clé USB, etc. sans préjudice de l'introduction par l'administration, de nouveaux moyens d'authentification des utilisateurs qui seront soumis aux mêmes règles.

  Ces identifiants et codes confidentiels sont strictement personnels et permettent à chaque titulaire de se connecter sur tout poste informatique et d'utiliser les ressources en local.

  L'utilisateur s'interdit :

  - d'utiliser un identifiant ou un code confidentiel/mot de passe autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
  - de supprimer, masquer ou modifier son identité ou son identifiant ;
  - d'user de son droit d'accès pour accéder à un poste de travail autre que le sien, à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation de sa hiérarchie.

- *Renouvellement et modification des identifiants et des codes confidentiels*

  En cas de communication ou de risque de communication, d'oubli, de perte ou de vol de ses identifiants et codes confidentiels, l'utilisateur, après avoir avisé sans délai la Direction Informatique ou le service informatique habilité, devra en demander le renouvellement.

  Il devra également, selon les cas, soit apporter sa collaboration à l'Administration, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

  Un code confidentiel/mot de passe doit être modifié selon une fréquence déterminée le cas échéant par l'Administration et notamment par la Direction Informatique ou le service informatique habilité, et spécifiée s'il y a lieu, dans le guide d'utilisation du poste de travail.

2.1.2. Intégrité des outils

Les équipements et services et plus généralement les systèmes d'information de l'État, mis à la disposition de l'utilisateur, sont exclusivement installés, configurés et paramétrés par la Direction Informatique ou le service informatique habilité ou les prestataires dûment désignés à cet effet. Il est strictement interdit à l'utilisateur de les modifier notamment par l'ajout de logiciels ou de matériels.

En cas de nécessité de services et après autorisation donnée par la hiérarchie conformément à la procédure prévue à l'article 3, la Direction Informatique ou le service informatique habilité ou les prestataires dûment désignés à cet effet sont seuls habilités à procéder à l'installation de logiciels ou matériels nécessaires pour l'exercice des fonctions confiées à l'utilisateur.

L'utilisateur s'engage, de manière générale, à ne pas porter atteinte à l'intégrité et à la conservation des bases de données de l'Administration, en respectant les finalités des outils mis à sa disposition.

Il s'interdit, notamment et en particulier, de charger ou de transmettre, sciemment, des fichiers contenant des virus ou des données altérées.

2.1.3. Gestion des absences et accès aux systèmes d'information

Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation du service, telles que définies par la hiérarchie et le cas échéant, avec le concours la Direction Informatique ou du service informatique habilité.

À cette fin, en cas d'absence, l'utilisateur doit mettre en œuvre l'une des procédures suivantes, telles que définies par le guide d'utilisation du poste de travail :

- le message d'absence, en précisant de préférence le nom de la personne à contacter durant ladite absence ;
- le système de délégation.

Le système de reroutage des messages peut être également utilisé exclusivement vers un destinataire au sein du service ou vers la messagerie du service.

Par ailleurs, afin d'assurer le bon fonctionnement du service, en cas de nécessité professionnelle ou pour des raisons d'urgence, la Direction Informatique ou le service informatique habilité pourra être saisi par le chef de Service en cas d'absence de l'utilisateur, afin d'accéder directement à l'aide de comptes Administrateur aux différents dossiers et répertoires stockées dans le Bureau Windows de l'utilisateur, courriers électroniques et plus généralement à tous documents à caractère professionnel de l'utilisateur.

2.1.4. Gestion des départs

Lors de la cessation de ses fonctions, l'utilisateur doit remettre à sa hiérarchie et en bon état général de fonctionnement, les éléments des systèmes d'information qui lui ont été mis à disposition (ordinateurs, périphériques, mobiles, PDA, carte d'accès, moyens d'authentification à distance, badges, supports de stockage, etc.).

Le compte messagerie de l'utilisateur est supprimé le jour de son départ, ses identifiants et codes confidentiels sont également désactivés à la même échéance. Toutefois, si la nécessité du service le justifie, le Secrétaire Général du Gouvernement pourra autoriser, sur demande du Chef de Service, le maintien de la messagerie pour un temps raisonnable qui ne saurait excéder six mois.

Les documents identifiés comme étant « PRIVÉ » au sens des dispositions des articles 2.2.2 et 2.2.3 devront être supprimés par l'utilisateur avant son départ, sauf en cas de procédure judiciaire en cours ou pour les besoins d'une enquête administrative. Il pourra conserver une copie à titre personnel de ces seuls documents.

2.1.5. Protection de la propriété intellectuelle

L'utilisation des systèmes d'information de l'État implique le respect des droits de propriété intellectuelle.

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- utiliser les logiciels, applications, dans les conditions de la licence souscrite par l'Administration ;
- ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels l'Administration ne posséderait pas un droit d'usage ;
- ne pas reproduire et utiliser les bases de données, pages web ou autres créations de l'Administration ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet ;
- ne pas copier et remettre à des tiers des créations appartenant à des tiers ou à l'Administration sans s'assurer de l'autorisation du titulaire des droits qui s'y rapportent.

2.1.6. Protection des informations nominatives

L'utilisation des systèmes d'information de l'État peut donner lieu à la mise en œuvre par l'État de traitements d'informations nominatives dans le respect des dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée.

L'utilisateur doit, dans l'exercice de ses fonctions, respecter les finalités de ces traitements d'informations nominatives et s'abstenir de communiquer des informations nominatives à des tiers extérieurs à l'Administration, sauf autorisation de sa hiérarchie et dans le respect des dispositions légales et réglementaires en vigueur.

La sauvegarde des intérêts et de la sécurité de l'État nécessite le respect, par l'utilisateur, d'une obligation générale et permanente de confidentialité laquelle résulte des devoirs généraux des fonctionnaires et agents de l'État en matière de secret professionnel, de discrétion professionnelle et de réserve inhérents à leur statut, à l'égard des informations ou données dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions.

Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ou données ;
- n'accéder qu'aux informations en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations ou données réservées à d'autres utilisateurs ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve, de devoir de discrétion, de confidentialité en usage au sein de l'Administration.

L'attention de l'utilisateur est attirée sur les risques liés à la diffusion de contenus d'information et de données sur internet, en particulier au sein des réseaux sociaux et sur les blogs. Il est donc strictement interdit de diffuser la moindre information nominative, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de confidentialité, sur internet.

La diffusion de toute donnée ne peut être réalisée que dans les conditions dans lesquelles le fonctionnaire ou l'agent non titulaire de l'État peut être délié de son obligation de discrétion professionnelle.

L'utilisation de procédés de cryptage est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés. Il est interdit d'utiliser des moyens de cryptologie autres que ceux expressément autorisés par l'Administration.

2.1.7. Enregistrements et vidéoprotection

L'Administration peut, à titre exceptionnel, recourir à des outils techniques d'enregistrements vidéo et sonores dans le but d'enregistrer les réunions professionnelles. Dans ce cas, les utilisateurs en sont informés.

Par ailleurs, les utilisateurs sont informés de la possibilité pour l'Administration de mettre en place, selon les règles en vigueur, un dispositif de vidéoprotection dans ses locaux ou à l'extérieur de ses locaux à des fins de sécurité et de prévention des atteintes aux biens et/ou aux personnes.

2.2. Conditions particulières d'utilisation des équipements et services

2.2.1. Principes de base

- *Utilisation à des fins professionnelles*

Dans tous les cas, et quelles que soient les conditions effectives d'utilisation, l'usage des systèmes d'information de l'État est réservé à l'exercice de son activité professionnelle.

- *Utilisation à des fins privées*

Toutefois, un usage personnel est toléré pour répondre aux nécessités de la vie courante et familiale, sous réserve qu'il :

- soit occasionnel et raisonnable tant dans la fréquence que dans la durée ;
- ne perturbe pas le bon fonctionnement du service et des systèmes d'information de l'État ;
- ne compromette pas l'activité de l'utilisateur ;
- ne porte pas atteinte aux devoirs généraux des fonctionnaires et agents de l'État ;
- ne porte pas atteinte à l'ordre public ;
- ne poursuive pas un but lucratif ou même ludique.

L'Administration se réserve le droit de limiter ou de suspendre cette tolérance en cas d'abus.

- *Utilisation des systèmes d'information personnels à des fins professionnelles*

L'utilisateur ne peut utiliser des systèmes d'information qui sont sa propriété personnelle à des fins professionnelles, sauf accord formel du Chef de service et sous réserve, le cas échéant des prescriptions techniques exigées par la Direction Informatique ou le service informatique habilité.

À ce titre, le Chef de Service, saisi d'une telle demande par un fonctionnaire ou par un agent non titulaire de l'État relevant de son autorité, doit en informer la Direction Informatique ou le service informatique habilité afin qu'il puisse examiner les conditions dans lesquelles l'utilisation à des fins professionnelles des systèmes d'information personnels peut être envisagée. Dans ce cadre, les éventuels coûts notamment en matière de télécommunication sont supportés par l'utilisateur.

2.2.2. Poste de travail fixe ou portable

- *Utilisation à des fins professionnelles*

Le poste de travail est par principe d'usage strictement professionnel.

- *Utilisation à des fins privées*

Il est possible de créer un répertoire privé au sein du disque dur de l'ordinateur, sous réserve qu'il soit identifié sous le terme « PRIVÉ ». Ainsi, tous les répertoires informatiques ne portant pas cette mention, sont considérés comme professionnels.

Par ailleurs, aucune information à caractère professionnel ne peut être stockée dans le répertoire informatique « PRIVÉ ».

Le caractère « PRIVÉ » de l'usage des systèmes d'information interdit, par principe, à l'Administration d'accéder aux contenus ou données stockées.

Toutefois, l'utilisateur est informé que :

- ces éléments peuvent faire l'objet de copie dans le cadre d'une maintenance du poste de travail nécessitant la restauration des données locales ;
- un administrateur réseau ou système d'exploitation ou toute autorité spécialement « habilitée », accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information, ce notamment dans le cadre d'opérations de maintenance ;
- l'Administration peut, dans tous les cas, pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé.

2.2.3. Messagerie

- *Utilisation à des fins professionnelles*

L'adresse « électronique » est strictement professionnelle. Elle ne doit donc pas être utilisée dans un autre contexte, et notamment diffusée sur des sites internet (chats, forums, blogs, etc.), sans rapport avec l'activité professionnelle.

L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est également réservée à un usage strictement professionnel. Elle est basée sur un principe d'autodiscipline des utilisateurs, destiné à s'assurer d'une part, de la pertinence et de la nécessité d'une telle inscription et d'autre part, des conséquences de celle-ci (fréquence de réception des messages, poids des messages, encombrement des réseaux, etc.).

Sont interdits :

- l'utilisation de l'adresse électronique personnelle de l'utilisateur dans le cadre de l'activité professionnelle de l'utilisateur ;
- le reroutage de la messagerie professionnelle vers la messagerie personnelle de l'utilisateur ou vers tout autre destinataire extérieur à l'Administration, sauf dérogation accordée par le chef de service et portée à la connaissance de la Direction Informatique ou du service informatique habilité ;
- les comportements pouvant inciter les tiers à lui adresser des messages non sollicités ou des fichiers douteux, qu'il devra détruire en cas de réception fortuite.

Dans l'hypothèse où l'utilisateur recevrait, régulièrement ou non, des messages non sollicités ou qui seraient manifestement illicites, il en préviendra la Direction Informatique ou le service informatique habilité afin qu'ils puissent prendre les mesures nécessaires en fonction des obligations légales, des possibilités techniques et des contraintes économiques.

L'utilisateur doit être vigilant sur la nature des messages électroniques qu'il envoie ou qu'il échange car ils peuvent engager sa responsabilité personnelle ou dévoiler des informations confidentielles.

La transmission d'informations par l'utilisateur à des tiers doit se faire dans le respect de son obligation de discrétion professionnelle et de son devoir de réserve qui s'imposent à lui.

- *Utilisation à des fins privées*

Afin qu'un message soit présumé comme non-professionnel, l'utilisateur doit mentionner le terme « PRIVÉ » dans la zone « objet » du message. À cet égard, l'utilisateur est tenu d'informer son destinataire de cette règle, afin qu'il applique également la mention « PRIVÉ » dans sa réponse.

Le recours aux pièces jointes est à éviter dans les cas d'un usage non professionnel.

Sans préjudice des règles applicables au secret des correspondances, un message, adressé ou reçu par l'utilisateur à partir d'une adresse électronique attribuée pour des raisons professionnelles et ne portant pas, dans la zone objet, la mention « PRIVÉ » est considéré comme professionnel.

Par ailleurs, aucune information à caractère professionnel ne peut être émise ou reçue via un courrier électronique identifié comme « PRIVÉ ».

Le caractère « privé » de l'usage des systèmes d'information interdit, par principe, à l'Administration d'accéder aux contenus ou données émis, reçus ou échangés via la messagerie.

Toutefois, l'utilisateur est informé que :

- ces éléments peuvent faire l'objet de conservation technique dans le cadre des procédures de backup ou de plans de continuité ou reprise d'activité mises en œuvre au sein de l'Administration ;
- un administrateur réseau ou système d'exploitation ou toute autorité spécialement « habilitée », accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information, ce notamment dans le cadre d'opérations de maintenance ;
- l'Administration peut, dans tous les cas, pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé.

Dans le cadre de son obligation de réserve, l'utilisateur s'abstient de tenir des propos inappropriés sur la politique conduite par le Gouvernement Princier et de faire état de ses opinions politiques.

2.2.4. Internet / Intranet et réseaux sociaux

2.2.4.1 Internet / Intranet

L'accès à des applications en ligne (sites web, web Radio, web TV, blogs, forums, chats, applications existantes ou à venir etc.) est strictement réservé à un usage professionnel.

L'utilisateur ne doit en aucune manière se livrer à la consultation, au chargement, téléchargement, au stockage, à la publication ou à la diffusion de fichiers, y compris vidéos ou musicaux, et de messages électroniques, dont le contenu présente un caractère injurieux, diffamatoire, pornographique ou raciste etc. et ce sans que cette liste ne soit exhaustive, sauf dans le cadre d'une mission liée à la recherche et à la poursuite d'infractions. Ceci s'applique tant aux fichiers qu'aux messages électroniques, avec ou sans pièces attachées et à toute forme de communication quelle que soit la forme des contenus (sonores, audiovisuels, multimédias ou logiciel).

L'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en termes de sécurité et/ou d'image pour l'Administration. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

2.2.4.2 Réseaux sociaux

- *Utilisation à des fins professionnelles*

Dans le cadre de la sphère professionnelle ou de la communication institutionnelle du Gouvernement, l'usage des réseaux sociaux est strictement encadré.

À ce titre, l'utilisateur doit :

- respecter toute procédure qui aura été définie par l'Administration ;
- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de l'Administration ;- respecter les conditions générales d'utilisation du réseau social et l'ensemble des dispositions applicables ;
- utiliser uniquement les outils de communication de l'Administration, selon les instructions qui lui ont été données et valoriser la visibilité du site web ou du réseau social de l'Administration ;
- s'abstenir de diffuser toute information confidentielle ou toute information commerciale sensible relative à l'Administration ;
- respecter son devoir de réserve ;
- s'assurer de la préservation de l'ordre public et prendre toutes précautions utiles.

En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra immédiatement consulter son supérieur hiérarchique.

Toute habilitation spécifique donnée pourra être retirée, modifiée ou suspendue par le Ministre d'État ou le Secrétaire Général du Gouvernement.

L'utilisation d'un réseau social par un service administratif doit faire l'objet d'une autorisation préalable du Ministre d'État ou du Secrétaire Général du Gouvernement.

- *Utilisation à des fins privées*

Dans le cadre de la sphère privée, en dehors de l'exercice de ses fonctions, l'utilisateur est libre d'utiliser les réseaux sociaux et d'y accéder à partir de son poste de travail et en dehors de son travail. Cependant il s'interdit de communiquer toute information à caractère professionnel, en particulier des informations confidentielles, des informations sensibles relatives à l'Administration, des informations relatives aux conditions de travail, à l'organisation générale, au calendrier d'événements et déplacements, à la rémunération, etc.

L'utilisateur est toutefois autorisé à faire mention de son appartenance à l'Administration et à faire état de son grade et de son service de rattachement.

Dans tous les cas, l'utilisateur doit respecter son devoir de réserve et son obligation de discrétion professionnelle. À ce titre, il s'abstient de tenir des propos inappropriés sur la politique conduite par le Gouvernement Princier.

2.2.5. Téléphonie fixe

- *Utilisation à des fins professionnelles*

Le téléphone fixe mis à disposition de l'utilisateur est destiné à un usage professionnel tant pour les appels émis que pour les appels reçus.

- *Utilisation à des fins privées*

Un usage privé en est toutefois toléré dans la mesure où il demeure raisonnable et ne perturbe ni sa propre activité professionnelle ni celle de ses collègues.

2.2.6. Équipements « nomades »

Les matériels dits « nomades » sont mis à la disposition de l'utilisateur par la Direction Informatique ou le service informatique habilité.

L'utilisateur en assure la garde et la responsabilité. Il assiste ou procède lui-même selon les cas à toutes les démarches (dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit (perte ou vol par exemple).

Lorsque qu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser, à l'exclusion de tout autre, les identifiants et codes confidentiels qui lui seront remis.

L'utilisation de systèmes d'information nomades et/ou à distance impose à l'utilisateur un niveau de surveillance et de confidentialité renforcée.

Il doit notamment veiller à ce que des tiers non-autorisés ne puissent accéder à ces ressources et éléments accessoires, les utiliser ou accéder à leurs contenus.

En cas d'incident avéré mais aussi en cas de doute, il doit immédiatement en aviser sa hiérarchie et la Direction Informatique (Cf. Guide d'utilisation du poste de travail) ou le service informatique habilité.

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser les identifiants et codes confidentiels qui lui seront remis et aucun autre. En termes de sécurité et de confidentialité, l'utilisateur est soumis aux mêmes obligations que celles visées pour la gestion des identifiants et codes confidentiels et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées.

Il devra aviser, sans délai, la Direction Informatique ou le service informatique habilité de la perte ou du vol des identifiants et codes confidentiels.

Par ailleurs, l'utilisateur se doit d'adopter une attitude de prudence, de confidentialité, de sécurité et de réserve au regard des informations et des ressources du système d'information de l'État.

2.2.7. Espace collaboratif

L'Administration privilégie, autant que faire se peut, le partage et la mutualisation des connaissances, et peut être ainsi amenée à mettre en place des espaces collaboratifs de travail. À ce titre, un espace collaboratif de travail peut par exemple prendre la forme d'un outil spécifique, d'une plateforme collaborative, ou d'une base de données partagée, etc.

La qualité des informations ainsi disponibles est un objectif élevé et chaque utilisateur s'engage à être attentif à la pertinence des informations diffusées au sein de ces espaces.

Par souci de qualité, de responsabilité et de protection de l'ensemble des informations et données contenues dans les systèmes d'informations de l'État, l'utilisation de ces mêmes espaces peut faire objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

Aux mêmes fins, l'Administration peut mettre en place des outils de marquage de tout ou partie des éléments des bases de données constituées dans ce cadre, pour éviter notamment toute extraction. Les utilisateurs seront avertis de la présence de tels outils.

3. SÉCURITÉ ET VIGILANCE

3.1. Généralités

L'utilisateur s'engage à user des systèmes d'information de façon loyale et à être vigilant en signalant toute anomalie ou intrusion. L'utilisateur est tenu d'informer, sans délai, sa hiérarchie et la Direction Informatique ou le service informatique habilité de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les systèmes d'information.

L'utilisateur doit utiliser les systèmes d'information dans le respect des procédures et méthodologies qui lui sont adressées (notes de Direction, livrets des procédures, livrets des préconisations, manuels utilisateurs, guide d'utilisation du poste de travail, etc.) et s'engage à user exclusivement les services d'accès sécurisés mis à sa disposition.

L'utilisateur pourra être invité à prendre des mesures d'urgence ou de sécurité spécifique, qu'il s'engage à appliquer sans le moindre délai.

À des fins de précaution, certaines configurations peuvent être verrouillées par la Direction Informatique ou le service informatique habilité (poste de travail, accès internet, etc.).

La mise en place d'outils de sécurité par la Direction Informatique ou le service informatique habilité ne doit pas, toutefois, dispenser les utilisateurs d'une obligation de vigilance à cet égard.

En effet, tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des systèmes d'information mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information de l'État.

L'utilisateur s'interdit également de :

- modifier les systèmes d'information de l'État notamment par l'ajout de logiciels, progiciels, même gratuits, ou de matériels pour quelque raison que ce soit ;
- modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;
- mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage ;
- utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- effectuer des opérations pouvant nuire aux relations internes ou externes de l'État.

Dans le cas où des logiciels ou matériels non installés semblent nécessaires à l'utilisateur pour l'exercice de sa mission, la procédure à respecter est la suivante :

- l'utilisateur doit transmettre une demande par note à son chef de service afin d'en saisir son département de tutelle ;
- la demande doit être ensuite relayée au Secrétariat Général du Gouvernement qui saisit la Direction Informatique ou le service informatique habilité ;
- le traitement et l'analyse de la demande sont effectués par la Direction Informatique ou le service informatique habilité en relation avec la Direction de l'Administration Électronique et de l'Information aux Usagers, en tenant compte de la nature du besoin et des impératifs de sécurité ;
- le Secrétariat Général du Gouvernement notifie la décision au Département concerné.

D'une manière générale, toute installation ou utilisation de matériels non expressément autorisée conformément à cette procédure est interdite.

En cas de violation de la présente Charte ou de risque d'atteinte à la sécurité des systèmes d'information de l'État ou dans tous les cas d'intérêt public, l'Administration pourra, à titre conservatoire, prendre toutes mesures de sécurité consistant à effectuer des contrôles renforcés, suspendre, bloquer, retirer, supprimer le(s) droit(s) de l'utilisateur sur tout ou partie des moyens informatiques et de communication électronique ainsi que des espaces collaboratifs et réseaux sociaux.

3.2. Traçabilité

Dans le cadre des règles d'engagement de la responsabilité de la puissance publique, l'Administration peut mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des systèmes d'information.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils (« traces ») est strictement interdit.

3.3. Filtrage

Dans le cadre des règles d'engagement de la responsabilité de la puissance publique l'Administration peut procéder à la mise en place d'outils de filtrage (filtrage des contenus, des URL, protocolaire, proxy, etc.) permettant d'analyser les conditions d'utilisation des systèmes d'information de l'État, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet. À ce titre, l'utilisation de Webmail est notamment interdite.

Il est précisé que ces outils, en ce qu'ils portent entre autre sur l'accès à internet, permettent un contrôle des connexions des utilisateurs.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

3.4. Mesures d'urgence et plan de reprise d'activité

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, l'Administration peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la reprise de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené à la demande de l'Administration à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, le basculement sur un système informatique de relève, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, déplacement sur des sites de secours tiers, etc.).

4. MAINTENANCE ET CONTRÔLE DE SÉCURITÉ

4.1. Opérations de maintenance

La mise à disposition et l'utilisation des systèmes d'information de l'État impliquent nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

L'objectif de ces opérations est d'assurer le bon fonctionnement et la sécurité des systèmes d'information de l'État.

Les utilisateurs sont informés des opérations de maintenance lorsqu'elles sont susceptibles d'affecter leur activité ou leurs accès.

Elles peuvent être réalisées sous la forme d'une « prise de main à distance ».

Les opérations de « prise de main à distance » sont effectuées en accord avec l'utilisateur qui pourra être présent téléphoniquement, devant son poste de travail informatique.

À cette occasion, la Direction Informatique ou le service informatique habilité peut être amené à prendre connaissance de l'ensemble des éléments présents sur le poste de l'utilisateur et notamment des messages électroniques émis ou reçus par l'utilisateur ainsi qu'à examiner en détail le journal de ses connexions, et cela qu'il s'agisse d'un usage professionnel ou privé.

Si à l'occasion d'opérations de maintenance la Direction Informatique ou le service informatique habilité identifie une utilisation anormale et/ou un contenu illicite ou préjudiciable, il en informe sa hiérarchie et celle de l'utilisateur.

Les fonctionnaires et agents de la Direction Informatique ou du service informatique habilité sont tenus de respecter le secret professionnel, l'obligation de discrétion professionnelle et la confidentialité des informations auxquelles ils accèdent. Ils ne peuvent utiliser leurs droits d'accès étendus qu'à des fins strictement professionnelles.

4.2. Opérations de contrôle de sécurité

Les opérations de contrôle de sécurité se distinguent des opérations de maintenance en ce qu'elles portent sur la sécurité et le bon fonctionnement des systèmes d'information et sur la vérification du respect des dispositions de la présente Charte.

À ce titre, elles répondent à des finalités statistiques, de traçabilité, d'optimisation, de sécurité, ou de détection des abus.

Ainsi, l'Administration se réserve le droit, notamment de :

- vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
- contrôler l'origine licite des logiciels installés ;
- conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, l'Administration se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;
- vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;
- procéder à toutes copies utiles pour faire valoir ses droits.

Les opérations de contrôle ciblé d'un utilisateur sont effectuées par une « prise de main à distance » ou sur site, en présence de l'utilisateur devant son poste de travail informatique ou dûment appelé. Il est informé que dans ce cadre, les autorités habilitées peuvent notamment être amenées à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail, ainsi qu'à ouvrir tout message figurant sur sa messagerie et à vérifier l'ensemble des connexions dudit utilisateur.

Ces opérations de contrôle de sécurité relèvent des fonctions de la Direction Informatique ou du service informatique habilité, qui a la charge de la qualité, de la protection et de la sécurité des systèmes d'information fournis aux utilisateurs.

Les agents relevant de ces services (administrateur réseau ou système d'exploitation ou toute autorité spécialement « habilitée ») sont tenus de respecter le secret professionnel, l'obligation de discrétion professionnelle et la confidentialité des informations auxquelles elles accèdent. Ils ne peuvent utiliser leurs droits d'accès étendus qu'à des fins strictement professionnelles.

En ce qui concerne l'usage des services Internet, il peut être contrôlé a posteriori et peut porter sur le temps de connexion par poste ou sur les sites les plus consultés par l'utilisateur. En cas de perturbation induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, la Direction Informatique ou le service informatique habilité est habilité à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

Si en cas d'opérations de contrôle, les services de la Direction Informatique ou du service informatique habilité identifient un faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité de l'Administration, ou réalisent une utilisation anormale, ou identifient un contenu illicite ou préjudiciable, le Directeur Informatique ou le responsable du service informatique habilité en informera sa hiérarchie, laquelle saisira le Secrétariat Général du Gouvernement qui se réserve le droit de mettre à la disposition des services compétents les traces individuelles des connexions incriminées.

Pour des raisons de sécurité des systèmes d'information de l'État, tout matériel ou logiciel installé illicitement ou en violation de la présente charte pourra être supprimé ou désactivé par les intervenants de la Direction Informatique ou du service informatique habilité, dès le constat de leur présence sur le poste de travail ou autre matériel.

4.3. Conservation, sauvegarde et archivage électronique

Chaque utilisateur doit veiller au respect de la politique de conservation et d'archivage mise en œuvre par l'Administration.

Les traces mentionnées au point 3.2 sont conservées pendant les durées nécessaires à la réalisation de la finalité pour laquelle elles sont collectées, à l'issue desquelles elles sont détruites.

Ces traces valent preuve de l'utilisation des systèmes d'information. Ces traces peuvent faire l'objet d'un traitement statistique. Ces traces peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

Elles peuvent aussi être communiquées à l'utilisateur, pour les seules informations qui le concerne directement et individuellement, en application de la loi sur la protection des informations nominatives.

Les éléments du répertoire et les messages identifiés comme étant « PRIVÉ », qui seraient techniquement conservés, sont conservés sous la seule et entière responsabilité de l'utilisateur.

5. RESPONSABILITÉ ET SANCTIONS

Toute utilisation des systèmes d'information de l'État en méconnaissance des règles de la présente Charte est constitutive d'une faute, qui pourra être sanctionnée conformément au régime disciplinaire applicable, sans préjudice d'une action juridictionnelle qu'elle soit de nature administrative, civile ou pénale.

En tout état de cause, l'Administration pourra prendre toute mesure conservatoire qu'elle jugera utile quant à l'accès et à l'utilisation par l'utilisateur des systèmes d'information et ce, indépendamment d'une mesure de suspension des fonctions conformément aux règles qui lui sont applicables.

L'utilisateur est informé que la multiplication de fautes dans l'utilisation des systèmes d'information constitue une circonstance aggravante.

6. DÉROGATION

Toute demande de dérogation aux termes de la présente Charte doit être présentée, par écrit, au Ministre d'État qui se réserve le droit de l'accepter ou de la refuser.

7. ENTRÉE EN VIGUEUR

La présente Charte figure en annexe de l'arrêté ministériel n° 2015-703 du 26 novembre 2015.

Elle se substitue à la précédente Charte en date du 1er novembre 2007.

La présente charte entre en vigueur à compter du lendemain de la publication au Journal de Monaco de l'arrêté ministériel précité.