CHARTE ADMINISTRATEUR RÉSEAUX ET SYSTÈMES D'INFORMATION DE L'ÉTAT

Annexe à l'Arrêté Ministériel n° 2018-281
du 4 avril 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.377

DU 13 AVRIL 2018

1. INTRODUCTION

La présente Charte complète la Charte des systèmes d'information de l'État et s'inscrit dans la logique de la Politique de Sécurité des Systèmes d'Information de l'État. Elle a pour objet de formaliser les règles spécifiques de déontologie et de sécurité applicables d'une part, aux fonctionnaires et agents non titulaires de l'État et d'autre part, aux tiers appelés à réaliser des missions pour le compte de l'Administration, lorsqu'ils exercent, au sens de la présente Charte, des fonctions « d'Administrateur réseaux et systèmes d'information ».

Ces personnes disposent, dans le cadre de leur mission, d'accès privilégiés et de droits spécifiques sur les systèmes d'information. À ce titre elles sont responsables, à leur niveau, du bon fonctionnement et de la sécurité des systèmes d'information de l'État.

Dans le cadre de leur activité, les Administrateurs réseaux et systèmes d'information peuvent être amenés à avoir accès à des informations et/ou données appartenant à d'autres utilisateurs, que ces informations présentent ou non un caractère confidentiel, au sens de l'article 18 de la loi n° 1.430 du 13 juillet 2016 relative à la préservation de la sécurité nationale ou du secret professionnel.

La présente Charte précise donc les droits et devoirs de tout Administrateur réseaux et systèmes d'information et sa bonne application garantit une administration saine des systèmes d'information de l'État, dans le respect de la législation en vigueur.

2. DÉFINITIONS

1- « système d'information » : Est qualifié de système d'information, tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

2- « Administrateur réseaux et systèmes d'information » désigne, au sens de la présente Charte, toute personne ayant en charge le bon fonctionnement du système d'information et/ou disposant d'accès privilégiés et de droits spécifiques permettant de modifier des systèmes d'information, des réseaux, des applications, des infrastructures et/ou des postes de travail. Ces droits étendus, dont il a besoin pour réaliser sa mission au niveau organisationnel ou technique peuvent permettre d'accéder à des données Utilisateurs ou Administrés de l'État liées au périmètre qu'il administre dans le cadre de sa mission. Dans la suite de la Charte, le terme « Administrateur » fait référence au terme « Administrateur réseaux et systèmes d'information ».

3- « Données Utilisateurs ou Administrés » désignent toutes les informations circulant ou accessibles depuis les systèmes d'information de l'État ou transitant sur ces systèmes d'information, et/ou générées par les utilisateurs.

4- « Services informatiques » : Entité informatique autre que la Direction Informatique au sein d'un service de l'État, qui gère sous sa responsabilité un système d'information.

3. PERSONNES CONCERNÉES

La présente Charte est applicable aux fonctionnaires et agents non titulaires de l'État qui interviennent sur les systèmes d'information de l'État en qualité d'Administrateur, quel que soit leur grade.

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

L'administrateur possède une compétence reconnue pour gérer tout ou partie des réseaux et des systèmes d'information. Cette compétence peut-être initiale ou acquise par le biais de formations spécifiques.

L'Administrateur peut être, sans que cette liste soit limitative selon les exigences de son périmètre d'action, Administrateur de base(s) de données, Administrateur d'annuaire, Administrateur de messagerie, Administrateur de système(s), Administrateur de réseau(x), Administrateur d'équipements, Administrateur de services Voix, Administrateur sécurité, Administrateur de sites internet, Administrateur d'application, Exploitant de production, Technicien Support, soit à temps plein, soit à temps partiel, soit épisodiquement.

4. RESPONSABILITÉS ET PRÉROGATIVES DE L'ADMINISTRATEUR

Pour assurer un fonctionnement optimal des systèmes d'information, l'Administrateur est doté de droits d'accès ou d'habilitations spécifiques sur les ressources de son périmètre de gestion. À ce titre :

- ✓ L'Administrateur a le droit d'accéder aux informations privées à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations ;

✓ L'Administrateur a le droit de mettre en place des procédures appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies dans la Politique de Sécurité des Systèmes d'Information de l'État, annexée à l'arrêté ministériel n° 2017-56 du 1er février 2017 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 ;

✓ L'Administrateur a le droit d'établir des procédures de surveillance de toutes les tâches exécutées sur les machines lui permettant de vérifier la bonne application des règles ;

✓ L'Administrateur est responsable de la configuration, supervision, maintenance opérationnelle et de la sécurité, et de l'évolution de ces procédures. Il s'assure de la sécurité et de la confidentialité des données qu'il manipule, collecte, traite, stocke, sauvegarde ou archive ;

✓ L'Administrateur est responsable de la protection de ses droits d'accès privilégiés, il veille à bien fermer sa session Administrateur après usage et à appliquer toute politique de protection de son poste ou des équipements auxquels il accède de par sa mission. Pour les tâches courantes d'utilisateur il utilise un poste Utilisateur (différent du poste Administrateur) et son accès Utilisateur non privilégié, mis à disposition par l'administration dans le cadre de la mise en œuvre de la politique de sécurité des systèmes d'information de l'État ;

✓ L'Administrateur peut procéder à des contrôles dans le cadre de sa mission (surveillance et détection d'anomalies sur les réseaux et systèmes d'information). Lesdits contrôles doivent être effectués conformément aux exigences suivantes :

- tous les contrôles sont non nominatifs ;
- lorsque ces contrôles permettent de déceler une anomalie ou un dysfonctionnement, l'Administrateur peut alors effectuer des vérifications complémentaires plus approfondies (liste des émetteurs ou destinataires des données, contenu des messages professionnels, etc.). Si ces vérifications permettent d'identifier formellement une personne en charge, l'Administrateur informe cette dernière et lui demande de prendre les mesures de correction nécessaires, en lui proposant son aide.

✓ Dans tous les cas, y compris en cas de nuisance volontaire avérée ou de réelle mise en danger du système d'information par un Utilisateur ou Administré, l'Administrateur informe sans délai sa hiérarchie et l'Agence Monégasque de Sécurité Numérique.

5. DEVOIRS GÉNÉRAUX DE L'ADMINISTRATEUR

✓ L'Administrateur s'engage à prendre connaissance et à respecter strictement, dans le respect des procédures formalisées ou des cas prévus par la législation en vigueur :

- les guides et bonnes pratiques liées à son activité ;
- l'obligation de confidentialité, de discrétion et de diligence ;
- les règles d'accès définies (physique et/ou logique) aux données, aux locaux, aux bases ou autres éléments auxquels il doit avoir accès ;
- les règles de péremption, de conservation, d'isolement ;
- toutes règles adaptées à l'usage envisagé des données, le type de données (trafic ou autres données métiers) ;
- les règles visant à gérer des risques liés à la perte, circulation, conservation, utilisation ou autre action visant ces données ;
- toutes les règles pouvant être fixées par sa hiérarchie ;
- l'interdiction de partage de ses propres accès (physique et/ou logique) ;
- le secret de sécurité nationale, tel que prévu par la loi n° 1.430 du 13 juillet 2016 relative à diverses mesures relatives à la sécurité nationale ;
- le secret des correspondances.

✓ Lors de ses interventions, l'Administrateur n'utilise jamais ses accès étendus sur demande d'une personne non identifiée ou sans légitimité ; il remonte à son supérieur hiérarchique toute demande lui paraissant inappropriée ;

✓ Il exerce ses droits d'accès privilégiés dans la limite nécessaire à l'exercice de sa mission. Il modifie les configurations et les droits d'accès uniquement dans le respect des procédures d'administration ou d'exploitation définies par sa hiérarchie ;

✓ Il n'effectue des accès au contenu marqué comme « privé » ou protégé par tout autre droit ou liberté légalement protégés qu'en présence de l'utilisateur ou avec son autorisation, à l'exception des cas d'atteinte à la sécurité où une simple information à l'utilisateur suffit ;

✓ Il n'a pas à connaître les mots de passe des utilisateurs pour mener à bien sa mission, et ne doit donc jamais demander à un utilisateur la communication de son mot de passe, il doit expliquer ce principe de façon claire aux utilisateurs et le leur rappeler si nécessaire. Ainsi, si une authentification d'un utilisateur est nécessaire, il invitera l'utilisateur à saisir son mot de passe. Toutefois, si des utilisateurs communiquent tout de même leur mot de passe, l'Administrateur doit les inviter à le changer en leur indiquant la marche à suivre ;

✓ Il n'utilise pas ses droits étendus de sa propre initiative pour contourner des mesures de sécurité établies au sein de l'État ou agir de manière inappropriée par rapport à sa mission ;

✓ Il veille à maintenir la traçabilité (par exemple l'historique sur la machine) de ses actions (il ne désactive pas les mécanismes de traçabilité) et ne porte pas atteinte à l'intégrité des fichiers de journalisation, nécessaires à la détection et/ou résolution des incidents et à toute investigation ultérieure (preuve). Il veille également ce que toute action sur le système, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, soit expliquée dans des documents auxquels les utilisateurs et/ou la Direction informatique peuvent se référer ;

✓ Il n'utilise que des logiciels autorisés par l'État. Toute installation de logiciel ne faisant pas partie de ceux déjà autorisés doit être préalablement approuvée par sa hiérarchie dans le respect des procédures internes de validation. L'Administrateur refuse toute installation logicielle non autorisée.

6. DEVOIRS SPÉCIFIQUES DE L'ADMINISTRATEUR

✓ L'Administrateur doit mettre en place des bonnes pratiques (telles que communément mises en œuvre dans le secteur privé ou public exerçant des activités similaires, et recouvrant le niveau de vigilance et précaution de l'homme de l'art) visant à limiter au maximum :

- toute intrusion susceptible de modifier, détruire ou révéler de l'information à des tiers ;
- toute introduction de données ou de programmes malveillants ;
- tout usage abusif, illicite ou malintentionné (divulgation, interception, modification, réémission, perte, destruction, altération, de messages ou données, usurpation d'identité, répudiation, attaque de système, inondation systèmes, atteinte à l'intégrité ou authenticité des données, etc…) des outils du système d'information.

✓ Il doit signaler tout problème de sécurité potentiel ou avéré qu'il détecte auprès de sa hiérarchie et de l'Agence Monégasque de Sécurité Numérique (A.M.S.N.). Dans ce cas, sa hiérarchie et/ou la direction compétente ayant la responsabilité de la gestion du système d'information décidera d'isoler, de suspendre ou d'arrêter, selon les cas, les comptes des utilisateurs, les flux à risque, les équipements ou les ressources informatiques en cas de menace jugée importante pouvant compromettre le fonctionnement normal et la sécurité du système d'information ou des réseaux. Il trace et documente ses actions autant que les circonstances l'exigent ;

✓ En cas d'incident de sécurité avéré, tel que tentative d'intrusion, attaque virale, usurpation d'identité, vol de matériel ou d'information, il en informe sans délai l'Agence Monégasque de Sécurité Numérique, sa hiérarchie ainsi que la direction informatique de l'État ou le service informatique. Aucune action de l'administrateur qui pourrait avoir pour conséquence de détruire ou corrompre des éléments de preuve ne doit être engagée sans validation de l'Agence Monégasque de Sécurité Numérique ;

✓ Il respecte strictement les règles de sécurité des identifiants et authentifiants des comptes privilégiés (complexité du mot de passe, fréquence de modification, règles de constitution de l'identifiant). À ce titre, les droits confiés à un Administrateur sont personnels, confidentiels et incessibles ;

- ✓ Il est rappelé que toute action sur les systèmes d'information de l'État fait l'objet d'une journalisation permettant son imputabilité ;
- ✓ L'information, le conseil, l'alerte et la mise en garde auprès de la Direction informatique de l'État ou du service informatique, font partie de la mission de l'Administrateur ;
- ✓ L'Administrateur assure une veille générale des systèmes d'information relevant de sa responsabilité et informe la Direction Informatique ou le service informatique de l'État de tout dysfonctionnement qu'il pourrait constater ;
- ✓ Dans le cadre de l'exercice de ses missions, l'Administrateur a obligation de veiller au respect des droits de propriété intellectuelle et à la protection des informations nominatives conformément aux dispositions de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;
- ✓ L'Administrateur tient régulièrement informé sa hiérarchie des dispositions qu'il prend en application de la présente Charte.

7. ÉVOLUTION DE LA CHARTE

Chaque Administrateur destinataire de la présente Charte est invité à transmettre au Secrétariat Général du Gouvernement toute proposition de modification ou d'ajout dont il a pu constater l'intérêt dans le cadre de ses missions d'Administrateur.

8. SANCTIONS

Toute utilisation des systèmes d'information, par un Administrateur dûment formé par la Direction Informatique et l'Agence Monégasque de Sécurité Numérique à l'application de cette Charte, 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 outre, tout acte effectué par les Administrateurs dûment formés par la Direction Informatique et l'Agence Monégasque de Sécurité Numérique à l'application de cette Charte, en connaissance de cause et allant à l'encontre des dispositions de la Charte des systèmes d'information de l'État et de la présente Charte, est considéré comme un acte de malveillance qui pourra également être sanctionné 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'Administrateur des systèmes d'information et ce, indépendamment d'une mesure de suspension des fonctions conformément aux règles qui lui sont applicables.

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

9. ENTRÉE EN VIGUEUR

La présente Charte figure en annexe de l'arrêté ministériel n° 2018-281 du 4 avril 2018 et entre en vigueur à compter du lendemain de la publication au Journal de Monaco dudit arrêté ministériel.

imprimé sur papier PEFC

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