Table des Matières

Avant-propos du Directeur Général 3

Section 1. Introduction 4

Section 2. Politique d'acquisition de matériel informatique 4

2.1 Objectif visé par la politique: 4

2.2 Achat de matériel informatique. 4

2.3 Transfert du matériel informatique:. 4

2.4 Responsabilité de l'utilisateur du matériel 5

Section 3. Politique d'acquisition de logiciels 5

3.1 Objectif visé par la politique: 5

3.2 Achat de logiciel: 5

3.3 Développement de logiciels:. 5

3.4 Installation du logiciel: 6

Section 4: Politique sur la sécurité des technologies de l'information 7

4.1 Objectif visé par la politique: 7

4.2 Accès physique 7

4.3 Contrôles environnementaux 8

4.4 Sécurité de l'information 8

4.5 Codes d'identification des utilisateurs et mots de passe 9

4.6 Détection d'intrusion 10

4.7 Classification de l'information 10

Section 5. Utilisation d'Internet 11

5.1 Objectif visé par la politique 11

5.2 Limite des responsabilités de l'Agence en matière d'utilisation d'Internet par le personnel: 11

5.3 Devoir de diligence des employés: 11

5.4 Le principe de respect ou de protection de vie privée ne s'applique pas en matière d'utilisation du système informatique de l'agence 11

5.5 Blocage de contenus inappropriés: 12

5.6 Activités interdites: 12

5.7 Jeux et logiciels de divertissement: 12

5.8 Copie illégale: 12

5.9 Accès à Internet: 12

5.10 Détection des virus: 12
5.11 Usage personnel acceptable 13
5.12 Utilisation inacceptable d'Internet 13
5.13 Sécurité: 13
5.14 Infraction 14
Section 6. Politique sur les courriers électroniques 14
6.1 Objectif visé par la politique: 14
6.2 Aucun principe de respect de vie privée ne s'applique: 14
6.3 Utilisation acceptable du courrier électronique: 14
6.4 Utilisation inacceptable du courrier électronique: 14
6.5 Sécurité des courriels : 15
6.6 Pieds de page standard pour les courriels: 15
Section 7. Politique du site Web 15
7 .1 Objectif visé par la politique 15
7.2 Principes directeurs 16
7.3 Les paramètres de l'hébergement du site Web: 16
Section 8. Politique sur les contrats de services TIC 17
8.1 Objectif visé par la politique:. 17
8.2 Types de contrats de services informatiques : 17
8.3 Responsabilités en matière d'étude de dossier et d'approbation de contrat de services informatiques 17
FORMULAIRE D'ACCEPTATION DES POLITIQUES ET PROCÉDURES EN MATIERE DE TECHNOLOGIE DE L'INFORMATION 18

Avant-propos du Directeur Général

La technologie de l'information est devenue omniprésente et vitale pour le succès de presque toutes les entreprises. Des changements majeurs se sont produits dans la production, le stockage et l'utilisation de l'information, avec un impact profond sur le travail, l'interaction sociale, l'éducation et la gouvernance. Pour la plupart des organisations, l'information et les outils utilisés pour la manipuler sont devenus des atouts importants, dont l'utilisation efficace est primordiale au succès de l'organisation. Toutefois, cette dépendance à l'égard de la technologie de l'information signifie également que les données et les systèmes doivent être protégés contre les menaces qui peuvent entraîner des pertes financières ou nuire à la réputation.

En tant qu'institution chargée de la mise en œuvre du Programme de Coopération Monétaire de la CEDEAO, l'AMAO s'engage à un respect strict des normes les plus élevées dans ses contributions aux travaux techniques, politiques, statistiques, institutionnels et juridiques visant à créer les conditions nécessaires à la réalisation de l'Union économique et monétaire de la CEDEAO. A cet égard, l'Agence a la responsabilité de veiller à ce que ses systèmes informatiques et ses informations soient utilisés efficacement à son profit, respectent les normes les plus élevées d'intégrité et de disponibilité et réduisent au minimum le risque de perte financière ou d'atteinte à sa réputation.

Le présent manuel des politiques et procédures en matière de technologies de l'information décrit les politiques et procédures pour définir les processus, les rôles et les responsabilités nécessaires à la prestation de services informatiques fiables et durables à l'Agence. J'attends de tous les membres du personnel qu'ils en prennent connaissance et qu'ils se conforment à ses dispositions.

Momodou Bamba Saho
Directeur Général

Section 1. Introduction

Le Manuel des Politiques et Procédures de l'Agence Monétaire de l'Afrique de l'Ouest (AMAO) sur les Technologies de l'Information et de Communication (TIC) décrit les politiques et procédures pour définir les processus, les rôles et les responsabilités nécessaires à la prestation de services informatiques fiables et durables à l'Agence.

L'Agence fera en sorte que toutes les politiques de technologie de l'information et de communication (TIC) soient à jour et pertinentes. Par conséquent, de temps à autre, il sera nécessaire de mettre à jour et de modifier certaines sections de ces politiques et procédures, ou d'en ajouter de nouvelles au besoin.

Ces politiques et procédures s'appliquent à tous les employés de l'Agence.

Section 2. Politique d'acquisition de matériel informatique

2.1 Objectif visé par la politique: La présente politique fournit des lignes directrices sur l'acquisition de matériel informatique à l'intention de l'Agence afin de s'assurer qu'il soit approprié, rentable et, le cas échéant, compatible avec d'autres matériels utilisés par l'Agence. La présente politique vise à réduire au minimum les différences entre les matériels utilisés au sein de l'Agence.

2.2 Achat de matériel informatique: L'achat de tous les ordinateurs de bureau, serveurs, ordinateurs portables, périphériques informatiques et appareils mobiles doit respecter cette politique. Le système informatique comprenant les serveurs, les ordinateurs de bureau, les ordinateurs portables et les périphériques informatiques doit fonctionner sous le système d'exploitation Windows et s'intégrer au matériel et aux logiciels existants. Tout changement par rapport aux exigences ci-dessus doit être autorisé par le chef de l'unité informatique. Les membres du personnel professionnel auront le choix entre un ordinateur de bureau *(desktop)* ou un ordinateur portable. Tous les achats de matériel informatique doivent être conformes aux dispositions du Règlement financier et des règles de gestion financière en vigueur dans l'agence.

L'unité de technologie de l'information et de communication demandera des devis aux fournisseurs, gérera l'achat de l'équipement, installera et prendra en charge le nouveau matériel. Le matériel informatique qui n'est pas acquis officiellement par l'Agence n'est pas pris en charge par le service de support technique de l'Agence. En raison des restrictions de licence et de garantie, l'unité TIC ne doit pas installer de logiciels appartenant à l'Agence sur du matériel non approuvé. L'unité informatique n'est pas non plus responsable des réparations de ces dispositifs.

2.3 Transfert du matériel informatique: À l'exception du matériel informatique mobile affecté au personnel, les employés ne peuvent pas retirer du matériel de l'Agence ou transférer du matériel à d'autres endroits de l'Agence sans l'approbation au préalable du responsable des TIC. Avant tout transfert d'un équipement, l'employé et/ou son superviseur responsable du matériel doit communiquer avec l'unité de TIC pour l'en informer. Seul le personnel informatique responsable du matériel informatique est autorisé à déplacer les équipements matériels de leur emplacement initial vers un nouvel emplacement.

2.4 Responsabilité de l'utilisateur du matériel: Les utilisateurs doivent éviter de d'exposer les PC à des vibrations ou à des chocs excessifs. Des chocs violents pendant l'utilisation d'un PC peuvent endommager le disque dur. La fumée, la chaleur, les champs magnétiques et la poussière excessive peuvent également endommager les équipements réseau. Tous les PC doivent être connectés à des onduleurs protégés par des parasurtenseurs.

Section 3. Politique d'acquisition de logiciels

3.1 Objectif visé par la politique: Les logiciels non autorisés, même ceux qui semblent être fournis par des fournisseurs connus ou des entreprises fiables, peuvent introduire des virus et des programmes de Troie qui aident les pirates informatiques à obtenir illégalement des données sensibles, personnelles et confidentielles. La protection des ordinateurs, des systèmes, des données et des communications de l'Agence contre les accès non autorisés et la protection contre la perte de données est d'une importance capitale.

En permettant aux employés d'installer des logiciels sur les appareils informatiques de l'Agence, l'Agence s'expose au risque de conflits de versions de fichiers système ou de bibliothèques qui peuvent empêcher l'exécution des programmes, à l'introduction de logiciels malveillants à partir de logiciels infectés, aux violations des droits d'auteur dues à des logiciels non autorisés et aux programmes qui peuvent être utilisés pour pirater le réseau de l'Agence. Ces risques nécessitent des politiques y relatives.

3.2 Achat de logiciel: Tout achat de logiciel doit être initié par le chef de l'unité informatique. Tous les achats de logiciels doivent provenir de fournisseurs réputés, être appuyés par les garanties nécessaires et être compatibles a l'infrastructure technologique de l'Agence. Tous les achats de logiciels doivent être conformes aux dispositions du Règlement financier et des règles de gestion financière en vigueur dans l'Agence. Le budget pour l'acquisition de nouveaux logiciels doit inclure le coût du logiciel ainsi que les coûts connexes comme l'installation, la formation, les mises à jour, les produits de tiers qui peuvent être nécessaires au fonctionnement du logiciel et le coût de tout matériel ou équipement spécialisé requis.

Dans le cas où un logiciel libre et ouvert ou freeware est requis, l'approbation du responsable de l'unité informatique doit être obtenue avant le téléchargement ou l'utilisation de ce logiciel. Tous les logiciels libres ou gratuits doivent être compatibles avec les systèmes matériels et logiciels de l'Agence. Toute modification aux dispositions ci-dessus doit être autorisée par le chef de l'unité informatique.

3.3 Développement de logiciels: L'unité des TIC peut agir à titre de conseiller ou participer à des projets de développement de logiciels en tant que gestionnaire de projet ou fournir des ressources techniques lorsqu'elles sont disponibles ou entreprendre le développement, si la compétence nécessaire dans ce domaine est disponible. . Aucun département utilisateur ne peut engager des consultants pour concevoir et mettre au point des systèmes sans consultation et le consentement du chef de l'unité informatique et du directeur général.

3.3 Licences de logiciels

3.3.1 Aucun logiciel ne doit être installé sur l'équipement de l'Agence sans les licences appropriées ou

autres formes d'autorisation du titulaire du droit d'auteur. L'acquisition, la duplication ou l'utilisation non autorisée de copies de logiciels est interdite. Tout employé qui acquiert, copie ou utilise des copies non autorisées de logiciels sur le matériel informatique de l'Agence est passible de mesures disciplinaires. Les logiciels privés ne doivent pas être inclus dans la liste des logiciels approuvés pour les employés. Lorsqu'un employé a connaissance d'un manquement à l'utilisation d'un logiciel conformément à la présente politique, il doit en aviser immédiatement le chef de l'unité informatique.

3.3.2 L'unité informatique se réserve le droit de refuser l'installation d'une application logicielle en cas de doute sur la légalité du logiciel. Le chef de l'unité informatique tient un répertoire des logiciels approuvés qu'il ou elle compare à toute demande d'installation de logiciels.

3.3.3 L'Unité des TIC se réserve le droit de refuser le service et/ou de débrancher tout système qui ne respecte pas cette politique.

3.3.4 Lorsqu'un employé a connaissance d'un manquement à l'utilisation du logiciel conformément à la présente politique, il est tenu d'en informer immédiatement le responsable de l'unité informatique. Si le manquement n'est pas signalé et qu'il a pu être établi que l'employé a caché l'information à dessein, il pourra faire objet de sanctions disciplinaires.

3.3.5 Le responsable de l'unité informatique est chargé d'effectuer deux fois par an un audit logiciel de l'ensemble des systèmes de l'Agence afin de s'assurer que les droits d'auteur des logiciels et les accords de licence sont respectés.

3.4 Installation du logiciel:

3.4.1 Seul le personnel de l'unité informatique est habilité à installer des applications logicielles dans les systèmes informatiques de l'Agence. Il s'agit notamment des ordinateurs portables appartenant à l'Agence et d'autres dispositifs informatiques portables placés sous le contrôle du personnel. En aucun cas le logiciel ne doit être installé ou copié par un autre employé. L'unité informatique se réserve le droit de désinstaller tout logiciel non approuvé, installé sans autorisation sur un ordinateur de l'Agence.

3.4.2 Pour qu'un logiciel spécifique soit installé sur un poste de l'Agence, le personnel demandeur doit obtenir l'approbation du chef de l'unité informatique.

3.4.3 Seuls les logiciels obtenus conformément à la présente politique doivent être installés sur les ordinateurs de l'Agence.

3.4.4 Tous les logiciels en utilisation dans l'Agence doivent être enregistrés auprès du titulaire des droits d'auteur lorsque cela est requis. L'AMAO sera le propriétaire enregistré de tous ces logiciels.

Section 4: Politique sur la sécurité des technologies de l'information

4.1 Objectif visé par la politique: La présente politique fournit des lignes directrices pour la protection et l'utilisation des biens et des ressources de la technologie de l'information au sein de l'Agence. La vaste gamme d'information disponible sur le réseau de l'Agence et sur Internet, ainsi que la nature et les risques associés à l'utilisation d'Internet soulèvent des préoccupations quant à la sécurité, l'intégrité, la confidentialité, la surveillance ainsi que l'utilisation appropriée des renseignements sur l'Agence. L'absence d'une protection adéquate de l'information expose l'Agence à des risques financiers et de d'image.

La présente politique énonce les principes directeurs et le détail des responsabilités nécessaires pour protéger l'intégrité, la confidentialité et la disponibilité des systèmes d'information de l'Agence et pour atténuer les risques liés au vol, à la perte, à l'utilisation abusive ou à l'endommagement de ces systèmes.

4.2 Accès physique

4.2.1 Les privilèges d'accès physique à toutes les salles de serveurs, aux centres de données et sites de sauvegarde externes de l'Agence doivent être documentés et gérés par le responsable de l'unité TIC. Il tient un registre des entrées et sorties de la salle serveur pour ainsi documenter les déplacements des employés et des prestataires externes, à destination et en provenance de la salle informatique de l'Agence. Le registre des visiteurs devrait être revu régulièrement par le responsable de l'unité informatique.

4.2.2 L'accès restreint aux salles serveurs, aux centres de données et aux sites de sauvegarde distants ne doit être accordé qu'aux employés dont les responsabilités professionnelles exigent l'accès à ces installations.

4.2.3 Le processus d'attribution des clés d'accès aux salles de serveurs, centres de données ou sites de sauvegarde doit être approuvé par le responsable de l'unité informatique.

4.2.4 Les dispositifs d'accès sécurisé tels que les clés, les cartes d'accès ou les combinaisons de serrures ne doivent être ni partagés ni prêtés à des tiers par des utilisateurs autorisés.

4.2.5 Les clés et cartes d'accès perdues ou volées doivent être signalées immédiatement au responsable de l'unité informatique.

4.2.6 Toutes les salles de serveurs, les centres de données et les installations de sauvegarde doivent être fermés à clé lorsqu'ils ne sont pas occupés par un membre du personnel autorisé

4.2.7 Le chef de l'unité informatique doit examiner périodiquement les droits d'accès à la carte et/ou aux clés pour les installations informatiques et retirer l'accès aux personnes qui n'en ont plus besoin.

4.3 Contrôles environnementaux

4.3.1 Un système de climatisation adéquat, des extincteurs d'incendie et un système de contrôle d'humidité doivent être installés, pour protéger l'infrastructure technologique, notamment dans le centre de données, afin d'éviter des dommages que peut causer la chaleur à long terme et d'éventuelles défaillances d'équipement.

4.3.2 Tous les équipements et systèmes dans les installations du réseau doivent être raccordés à une source ininterrompue de courant afin d'éviter les surtensions, les baisses de tension et les dommages éventuels aux données, aux logiciels et au matériel.

4.4 Sécurité de l'information

4.4.1 Toutes les données contenues dans les systèmes du réseau de l'Agence doivent être sauvegardées. Il incombe au responsable de l'unité informatique de veiller à ce que les sauvegardes de données soient effectuées et à ce que les données sauvegardées soient conservées en lieu sûr.

4.4.2 Les données gardées et gérées sur le disque local des utilisateurs dans les départements et unités sont exclues du système de sauvegarde ci-dessus mentionné, à moins que les départements et unités n'aient conclu des accords spécifiques avec l'unité informatique. Il est rappelé à tous les membres du personnel qu'ils sont individuellement responsables de la sauvegarde des données conservées localement sur leur ordinateur de bureau ou portable et qu'ils sont fortement encouragés à effectuer régulièrement des sauvegardes de tous les fichiers personnels. Il est également rappelé aux employés que l'information qu'ils produisent dans le cadre de leur travail est la propriété de l'Agence et que toutes les données sensibles et précieuses doivent être stockées sur le réseau de l'Agence.

4.4.3 Les sauvegardes complètes de toutes les données de l'Agence doivent être effectuées chaque semaine. Les sauvegardes complètes sont conservées pendant trois mois avant d'être effacées.

4.4.4 Les sauvegardes différentielles de toutes les données de l'Agence doivent être effectuées quotidiennement. Les sauvegardes différentielles sont conservées pendant un mois avant d'être supprimées.

4.4.5 Les sauvegardes devraient être stockées dans une installation hors site sécurisée pour assurer la reprise en cas de panne et la continuité de service

4.4.6 Le responsable de l'unité informatique est chargé de tester les procédures de récupération des données et de s'assurer de leur bon fonctionnement.

4.4.7 Tous les équipements de l'Agence doivent être munis d'un logiciel antivirus. Il incombe au

responsable de l'unité informatique d'installer tous les logiciels antivirus et de veiller à ce que le logiciel reste à jour.

4.4.8 L'Agence doit préparer et mettre en œuvre un plan de continuité des opérations. Ce plan doit être testé au moins deux fois par année afin de de s'assurer de son efficacité pour permettre une reprise sur panne rapide grâce à la récupération des données de sauvegarde stockées hors site. Le Directeur général est responsable de sa mise en œuvre.

4.5 Codes d'identification des utilisateurs et mots de passe

4.5.1 Chaque employé recevra un code d'identification d'utilisateur unique pour permettre l'accès aux ressources informatique de l'Agence et devra utiliser un mot de passe, renouvelable tous les six mois, afin d'y accéder. Le code d'identification de l'utilisateur doit être conforme à une convention de nomenclature définie par l'Agence.

4.5.2 Tous les mots de passe devraient être assez complexes et difficiles à deviner pour les personnes non autorisées. Les employés devraient choisir des mots de passe d'au moins huit caractères et contenant une combinaison de lettres majuscules et minuscules, de chiffres, de signes de ponctuation et d'autres caractères spéciaux. Aucun mot de passe par générique ne doit être autorisé sur un système ou un appareil.

4.5.3 Les employés ne doivent pas communiquer leurs mots de passe à d'autres employés. Lorsqu'il est nécessaire que plusieurs employés partagent un seul mot de passe, par exemple ceux qui travaillent en collaboration sur un projet, il faut obtenir l'approbation du chef de l'unité informatique.

4.5.4 Le responsable de l'unité informatique est responsable de la délivrance du code d'identification de l'utilisateur et du mot de passe initial pour tous les employés. Ce mot de passe initial doit être changé le plus rapidement possible par l'employé.

4.5.5 Les employés devraient prendre des mesures pour éviter les escroqueries par phishing et d'autres tentatives de piratage visant à voler des mots de passe et d'autres renseignements de nature délicate. Tous les employés recevront une formation sur la façon de reconnaître ces attaques.

4.5.6 Lorsqu'un employé oublie son mot de passe ou qu'il est " verrouillé " des systèmes en raison de tentatives d'ouverture de session antérieures infructueuses, le responsable de l'unité informatique a la responsabilité d'émettre un nouveau mot de passe provisoire après une demande officielle de l'employé. L'employé sera tenu de changer le mot de passe lorsqu'il ou elle se connecte en utilisant ce mot de passe provisoire.

4.6 Détection d'intrusion

4.6.1 L'unité informatique doit mettre en œuvre des processus pour les systèmes d'exploitation, la comptabilité des utilisateurs et l'audit des logiciels sur tous les systèmes hôtes et serveurs.

4.6.2 L'unité informatique doit mettre en œuvre des fonctions d'alerte pour les pare-feu et autres contrôles d'accès au périmètre du réseau.

4.6.3 L'enregistrement de la vérification des pare-feux et des autres contrôles d'accès au périmètre du réseau doit être examiné quotidiennement à partir des systèmes de contrôle d'accès au périmètre.

4.6.4 L'unité informatique doit examiner les registres d'audit des serveurs et des hôtes sur le réseau interne protégé au moins une fois par semaine.

4.6.5 L'unité des technologies de l'information doit vérifier au moins une fois par semaine les outils d'intrusion basés sur l'hôte et examiner les rapports d'incident pour déceler les symptômes qui pourraient indiquer une activité intrusive ou un incident.

4.6.6 L'unité informatique doit collaborer avec les chefs de service et les responsables d'unité pour former les employés à signaler au responsable de l'unité informatique les anomalies dans le rendement du système et les signes d'actes illicites.

4.7 Classification de l'information

Toutes les informations de l'Agence et toute information obtenue de tiers sont classées dans l'une des quatre catégories indiquées ci-dessous :

4.7.1 Public : Il s'agit d'informations dont la publication a été approuvée et qui devraient être accessibles à tout le monde sans exclusion. Il s'agit des rapports annuels, des bulletins, des revues économiques, des brochures et autres publications disponibles sur le site Web de l'Agence.

4.7.2 Utilisation interne : Il s'agit d'informations notamment accessibles uniquement au personnel de l'AMAO dont la divulgation à l'extérieur de l'Agence serait inappropriée. Celles-ci comprennent les correspondances internes, les documents, les procès-verbaux des réunions et le matériel de formation des Comités ad 'hoc, Groupes de travail et tout autre Comité, ainsi que les données des Banques centrales membres. Ces informations ne seraient en principe pas marquées, mais devraient être traitées avec soin en tout temps et ne devraient pas être divulguées, sans autorisation, à des tiers.

4.7.3 Restreint : Ces informations ne sont en principe accessibles qu'à certains membres du personnel qui ont un besoin légitime d'y accéder. Il s'agit notamment des procès-verbaux des réunions du Comité de direction et certaines données personnelles des employés.

4.7.4 Confidentiel : Il s'agit d'informations accessibles uniquement à certains membres du personnel. Cela peut s'appliquer aux informations dont la perte ou la divulgation aurait des conséquences préjudiciables pour l'Agence. Elles devraient donc être soumises à des normes les plus rigoureuses en matière de confidentialité, d'intégrité et de disponibilité restreinte. Il s'agit notamment des mots de passe d'administrateur, des correspondances sensibles, des délibérations du Comité des Gouverneurs et correspondances juridiques, des publications non encore autorisées à la diffusion et les données personnelles des employés.

Il n'est pas nécessaire d'étiqueter l'information en fonction de l'utilisation publique ou interne. Toutefois, les informations confidentielles et à diffusion restreinte devraient être marquées par les Chefs de département ou d'unité responsables de l'information.

Section 5. Utilisation d'Internet

5.1 Objectif visé par la politique: La politique a pour objet de définir les utilisations appropriées d'Internet par les employés de l'Agence. Tous les employés qui utilisent le réseau informatique de l'AMAO pour accéder à Internet doivent se conformer strictement aux directives concernant l'utilisation appropriée des ressources du réseau.

5.2 Limite des responsabilités de l'Agence en matière d'utilisation d'Internet par le personnel: L'AMAO n'est pas responsable du matériel consulté ou téléchargé par les employés à partir d'Internet. Internet est un réseau mondial d'ordinateurs qui contient des millions de pages d'informations. Les utilisateurs sont avertis que plusieurs de ces pages contiennent du matériel offensif da tout genre y compris de la pornographie, et d'autre contenus inappropriés. . En général, il est difficile d'éviter ces contenus lors de l'utilisation d'Internet. Même les demandes de recherche anodines ou inoffensives peuvent mener à des sites à contenu très répréhensible. Les employés qui divulguent leurs renseignements personnels (y compris leur adresse électronique) sur Internet le font à leurs propres risques.

5.3 Devoir de diligence des employés: Les employés de l'AMAO doivent s'efforcer de faire en sorte que chaque communication électronique soit fiable et exacte. Ils devront veiller à la qualité de tout ce qu'ils écrivent qu'il s'agisse de la rédaction des courriels et autres documents électroniques ou de toute autre communication écrite. Les employés doivent garder à l'esprit que tout ce qui est créé ou stocké dans les systèmes informatiques de l'Agence pourra être consulté par l'Agence a tout moment que cela sera nécessaire.

5.4 Le principe de respect ou de protection de vie privée ne s'applique pas en matière d'utilisation du système informatique de l'agence. L'équipement informatique et les comptes confiés aux employés ont pour but de les aider dans l'exercice de leurs fonctions. Les employés ne devraient pas s'attendre à la protection de la vie privée dans tout ce qu'ils créent, stockent, envoient ou reçoivent sur les systèmes informatiques de l'Agence.

L'Agence peut surveiller les messages sans préavis.

5.5 Blocage de contenus inappropriés: L'Agence peut utiliser des logiciels pour identifier des sites Internet offensants ou d'avance sexuelle explicites. Ces sites peuvent être interdits d'accès à l'Agence. Dans le cas où le personnel rencontrerait du matériel offensant ou d'avance sexuelle explicites pendant qu'il navigue sur Internet, il ou elle devrait immédiatement se déconnecter du site, que le site ait été bloqué ou non par l'Agence.

5.6 Activités interdites: Le système de courriel de l'Agence ne doit pas être utilisé pour la création, la distribution, le téléchargement, la visualisation ou le stockage de messages perturbants ou offensants, y compris des commentaires offensants sur la race, le sexe, les handicaps, l'âge, l'orientation sexuelle, les croyances et pratiques religieuses, les convictions politiques ou l'origine nationale. Les employés qui reçoivent des e-mails comportant ce contenu de la part d'un employé de l'AMAO doivent immédiatement signaler l'incident au responsable de l'unité informatique.

5.7 Jeux et logiciels de divertissement: Les employés ne peuvent pas utiliser les installations Internet de l'Agence pour télécharger des jeux ou tout autre logiciel de divertissement. Les employés ne peuvent pas jouer à des jeux sur Internet pendant les heures de travail.

5.8 Copie illégale: Les employés ne peuvent pas copier illégalement des documents protégés par la loi sur les droits d'auteur ou mettre ces documents à la disposition d'autres personnes aux fins de copie. Les employés sont responsables du respect des lois sur les droits d'auteur et des licences qui peuvent s'appliquer aux logiciels, fichiers, images, documents, messages et autres éléments qu'ils téléchargent ou copient. Le personnel ne devrait pas autoriser ou télécharger de matériel pour lequel des frais d'inscription sont exigés sans avoir obtenu au préalable la permission écrite expresse de l'Agence.

5.9 Accès à Internet: Afin d'assurer la sécurité et d'éviter la propagation de virus, les employés qui accèdent à Internet au moyen d'équipement relié au réseau de l'Agence doivent le faire à travers un pare-feu Internet approuvé. Il est strictement interdit de contourner le pare-feu de l'Agence.

5.10 Détection des virus: Les fichiers téléchargés à partir de sources extérieures à l'Agence, y compris les disques privés, les pièces jointes aux courriels, les fichiers téléchargés à partir d'Internet, des médias sociaux, des groupes de discussion ou d'autres services et fichiers en ligne fournis par les clients et les fournisseurs, peuvent contenir des virus informatiques dangereux qui peuvent endommager le réseau de l'Agence. Les employés ne doivent pas télécharger de fichiers à partir d'Internet, accepter des pièces jointes à des courriels provenant de l'extérieur ou utiliser des disques provenant de sources autres que celles de l'Agence sans avoir préalablement analysé le matériel à l'aide du logiciel antivirus approuvé par l'Agence. Toute suspicion qu'un virus a été introduit dans le réseau de l'Agence sera portée à la connaissance du responsable de l'unité informatique.

5.11 Usage personnel acceptable: Les systèmes informatiques de l'AMAO sont destinés à un usage professionnel. Toutefois, lorsque certains critères sont remplis, les employés peuvent utiliser Internet pour des activités personnelles sur une base limitée. Toute utilisation personnelle d'Internet par le biais du réseau AMAO est soumise aux restrictions suivantes:

i. Il ne doit ni dégrader ni entraver le rendement normal au travail.
ii. Il ne doit pas faire encourir de coûts directs à l'AMAO.
iii. Étant donné que l'utilisation de l'équipement et des installations de l'AMAO peut être perçue par d'autres comme représentant l'AMAO, les employés ne doivent pas utiliser Internet à des fins qui pourraient avoir une répercussion négative sur l'Agence ou ses employés.
iv. Les opinions personnelles exprimées au cours des activités de communication en ligne devraient inclure un avis de non-responsabilité selon lequel elles ne reflètent pas les positions officielles de l'Agence.
v. L'utilisation personnelle des installations Internet de l'Agence est limitée aux utilisateurs autorisés et ne s'étend pas aux membres de la famille ou à d'autres connaissances.
vi. Il est interdit d'envoyer ou de recevoir des fichiers ou des documents susceptibles d'engager la responsabilité légale de l'AMAO ou de l'embarrasser.

5.12 Utilisation inacceptable d'Internet: Les employés ne doivent pas utiliser Internet de l'AMAO pendant les heures de travail ou le temps personnel pour:

i. Accédez, récupérez ou imprimez du texte et des graphiques qui font entorse à la Politique d'utilisation acceptable
ii. Se livrer à des activités illégales ou à d'autres activités qui pourraient de quelque façon que ce soit discréditer l'Agence.
iii. S'engager dans des activités commerciales personnelles, y compris offrir des services ou de la marchandise à vendre, acheter en ligne sans rapport avec les activités professionnelles et faire de la publicité commerciale personnelle.
iv. Entreprendre toute activité qui compromettrait la sécurité des systèmes, des ressources ou des réseaux.
v. S'engager dans toute activité de collecte de fonds, endosser tout produit ou service, participer à toute activité de lobbying ou s'engager dans toute activité politique active.
vi. Accéder ou transmettre du matériel pornographique.

5.13 Sécurité: Les employés de l'AMAO qui identifient ou perçoivent un problème de sécurité réel ou soupçonné doivent en informer immédiatement l'unité de technologie de l'information. Les employés de l'AMAO ne doivent pas révéler le mot de passe de leur compte à des tiers ni permettre à une autre personne, employée ou non, d'utiliser leur compte. De même, les employés ne doivent pas utiliser les comptes d'autres employés.

Les employés ne doivent pas tenter de contourner ou de détourner les mesures de sécurité sur le réseau AMAO ou tout autre système connecté ou accessible par Internet.

L'accès aux ressources du réseau AMAO sera retiré à tout utilisateur identifié comme présentant un risque de sécurité ou ayant des antécédents avérés de problèmes de sécurité.

5.14 Infraction: Tout employé qui contrevient à ces politiques ou aux lois locales applicables alors qu'il utilise le réseau AMAO est sujet à la perte des privilèges du réseau et à toute autre mesure disciplinaire jugée appropriée.

Section 6. Politique sur les courriers électroniques

6.1 Objectif visé par la politique: Le courriel est largement utilisé à l'Agence et constitue souvent le principal moyen de communication avec les partenaires. Cependant, une mauvaise utilisation du courrier électronique peut présenter des risques juridiques, de confidentialité et de sécurité. Il est donc important que les employés comprennent l'utilisation appropriée du courrier électronique. La présente politique sur le courrier électronique a pour but d'assurer l'utilisation appropriée des systèmes de courrier électronique et de sensibiliser les employés à ce qui constitue une utilisation acceptable et inacceptable du système de courrier électronique de l'Agence. La présente politique énonce les exigences minimales relatives à l'utilisation du courrier électronique au sein de l'Agence.

6.2 Aucun principe de respect de vie privée ne s'applique: La confidentialité des courriels ne peut être garantie. Pour des raisons de sécurité, les messages transmis par le biais du système de messagerie électronique ou de l'infrastructure des réseaux de l'AMAO sont la propriété de cette dernière et peuvent donc être inspectés par l'Agence au besoin.

6.3 Utilisation acceptable du courrier électronique:

6.3.1 Les employés de l'AMAO ne sont pas autorisés à transmettre des courriels officiels confidentiels ou des pièces jointes à des comptes personnels gérés par des fournisseurs publics de courrier électronique ou de services Internet lorsque l'information pourrait être compromise.

6.3.2 Les employés de l'AMAO peuvent faire un usage personnel limité du courrier électronique. Toute utilisation occasionnelle ne doit pas interférer avec les fonctions officielles, doit avoir un effet minimal sur l'Agence et doit se conformer au Code de conduite du personnel de l'AMAO.

6.3.3 Les employés de l'AMAO ne doivent pas envoyer, transmettre, recevoir ou stocker des informations officielles confidentielles ou sensibles utilisant des dispositifs mobiles non autorisés par l'AMAO. Les exemples d'appareils mobiles incluent, mais ne sont pas limités aux ordinateurs portables, smartphones, tablettes, etc.

6.4 Utilisation inacceptable du courrier électronique: il est formellement interdit de faire usage du courrier électronique de l'AMAO aux fins suivantes:

i. Envoyer des courriels destinés à intimider ou à harceler.

ii. Mener des affaires personnelles.
iii. Mener des activités de lobbying ou de campagne politique.
iv. Violer les lois sur le droit d'auteur en distribuant de façon inappropriée des œuvres protégées.
v. Les utilisateurs du système ne doivent pas se faire passer pour qui que ce soit d'autre lorsqu'ils envoient des courriels, sauf s'ils sont autorisés à envoyer des messages à un autre employé lorsqu'ils jouent un rôle de soutien administratif.
vi. Envoyer des messages qui véhiculent des contenus malveillants, provocateurs, ethniques, discriminatoires ou racistes ou d'autres contenus religieux à polémique.

Afin d'éviter toute perturbation ou dégradation indue des communications sur les réseaux et de l'efficacité du fonctionnement des systèmes de courriel, les employés ne doivent pas:

i. Envoyer ou transmettre des lettres en chaîne.
ii. Envoyer des messages non sollicités à de grands groupes, sauf si cela est nécessaire dans le cadre de la conduite des opérations officielles.
iii. Envoyer ou transférez des e-mails susceptibles de contenir des virus

6.5 Sécurité des courriels :

6.5.1 Tous les courriels entrants et sortants doivent être scrutés à la recherche de virus et d'autres contenus malveillants.

6.5.2 Une politique d'analyse de contenu doit être mise en place pour permettre d'utiliser de filtres de blocage de courriel entrant ou sortant contenant des messages provocateurs, ethniques, discriminatoires ou racistes ou tout autre contenu religieux à polémique. Le filtre de contenu est revu et mis à jour tous les trimestres.

6.5.3 Certaines pièces jointes (avec des extensions telles que .EXE, .HTML et autres fichiers avec des extensions suspectes) dans les messages électroniques doivent être interdites et/ou explicitement bloquées par un logiciel d'analyse de contenu.

6.6 Pieds de page standard pour les courriels: Pieds de page standard pour les courriels: Ce pied de page devrait être inséré dans tous les courriels envoyés à l'extérieur de l'Agence concernant toute information confidentielle relative à l'Agence.

"Ce courriel et les autres fichiers qui y sont transmis sont confidentiels et sont destinés uniquement à l'usage de la personne ou de l'entité à laquelle ils sont adressés. Si vous n'êtes pas le destinataire prévu, sachez que vous avez reçu ce courriel par erreur et que toute utilisation, diffusion, transmission, impression ou copie de ce courriel est strictement interdite. Si vous avez reçu ce courriel par erreur, veuillez en informer immédiatement l'Agence Monétaire de l'Afrique de l'Ouest par le courrier suivant..... et procéder à sa suppression."

Section 7. Politique du site Web

7 .1 Objectif visé par la politique: Les entreprises, les organismes gouvernementaux et les particuliers du

monde entier utilisent Internet comme outil médiatique pour communiquer avec leurs partenaires. Etant donné le rôle de l'Agence dans la conduite du processus d'intégration monétaire en Afrique de l'Ouest, il est important que nos partenaires obtiennent les dernières informations sur les activités de l'Agence via le site web de l'Agence. Cette politique fournit des lignes directrices pour s'assurer que le contenu est affiché sur le site Web de l'Agence en temps opportun et avec exactitude. Il précise également les responsabilités en matière de fourniture et de modification du contenu du site Web.

7.2 Principes directeurs

7.2.1 Fiabilité: Le site web de l'Agence est une source officielle d'information sur le projet d'intégration monétaire de la CEDEAO. Son contenu serait utilisé par les banques centrales membres, les gouvernements, les citoyens de la CEDEAO et d'autres acteurs dans la conduite de leurs propres activités. Par conséquent, le contenu du site Web doit être exact et soigneusement vérifié avant publication.

7 .2.3 Actualisation. Il est important que le contenu du site soit le plus actuel possible afin d'être d'une grande utilité. Par conséquent, le contenu du site web doit être mis à jour régulièrement.

7.2.4 Site bilingue. Le contenu du site Web devrait être disponible en français et en anglais.

7.2.5 Image: Le site Web de l'Agence doit avoir un aspect uniforme pour assurer une image cohérente et uniforme de l'Agence.

7.3 Les paramètres de l'hébergement du site Web:

7.3.1 Le registre du site web doit contenir au minimum les données suivantes:

i. Liste des noms de domaine enregistrés auprès de l'Agence
ii. Dates de renouvellement des noms de domaine
iii. Liste des fournisseurs de services d'hébergement
iv. Date d'expiration de l'hébergement

7.3.2 La mise à jour du registre sera assurée par le responsable de l'unité informatique.Le responsable de l'unité informatique est également tenu de procéder au renouvellement des éléments inscrits au registre.

Contenu du site Web Tout contenu du site Web de l'Agence doit être exact, approprié et à jour. Cette responsabilité sera assumée par Direction. Les personnes suivantes sont autorisées à apporter des modifications au site Web de l'Agence:

i. Directeur Général
ii. Le responsable de l'unité informatique
iii. Les chefs de département et les responsables d'unités sur les informations relatives à leurs fonctions

Section 8. Politique sur les contrats de services TIC

8.1 Objectif visé par la politique: Cette politique établit des lignes directrices pour tous les contrats de services TIC conclus au nom de l'Agence.

8.2 Types de contrats de services informatiques : Les contrats de services informatiques suivants peuvent être conclus pour le compte de l'AMAO:

- Fourniture de services informatiques généraux
- Fourniture de matériel et de logiciels réseau
- Réparation et entretien des équipements informatiques
- Fourniture de logiciels d'entreprise
- Fourniture de téléphones mobiles et de plans de données
- Conception et maintenance du site web

8.3 Responsabilités en matière d'étude de dossier et d'approbation de contrat de services informatiques

8.3.1 Tout contrat en matière de services informatiques doit être examiné par le responsable de l'unité informatique et le Conseiller juridique de l'Agence avant leur conclusion. Apres examen du dossier et sur proposition de recommandation d'exécution du responsable de l'unité informatique, le dossier est approuvé par le Directeur général.

8.3.2 Tous les contrats, obligations et renouvellements de services informatiques doivent être consignés dans un registre tenu à cet effet par le responsable de l'unité informatique.

8.3.3 Lorsqu'un renouvellement d'un contrat de services informatiques est nécessaire, dans le cas où l'accord est substantiellement inchangé par rapport à l'accord précédent, ce renouvellement peut être autorisé par le responsable de l'unité informatique.

8.3.4 Lorsqu'un renouvellement d'un contrat de services informatiques est requis, dans le cas où l'accord a substantiellement changé par rapport à l'accord précédent, il doit d'abord être examiné par le responsable de l'unité informatique et le Conseiller juridique de l'Agence avant sa conclusion. Une fois l'accord examiné et la recommandation d'exécution reçue, l'accord doit être approuvé par le Directeur général.

8.3.5 En cas de litige relatif à la fourniture de services informatiques couverts par une convention de services informatiques, il doit être renvoyé au Directeur Général qui sera chargé de régler ce litige.

FORMULAIRE D'ACCEPTATION DES POLITIQUES ET PROCÉDURES EN MATIERE DE TECHNOLOGIE DE L'INFORMATION

Après avoir lu cette politique, veuillez signer le formulaire de couverture et le soumettre à l'Unité des TIC de l'Agence aux fins de classement. En apposant sa signature ci-dessous, la personne qui demande l'accès aux ressources informatiques de l'Agence accuse réception des politiques et procédures en matière de technologie de l'information et s'engage à les respecter. De plus, le soussigné reconnaît également avoir lu et compris la présente politique avant de signer le présent formulaire. L'accès aux ressources du réseau de l'Agence ne sera pas accordé tant que ce formulaire d'accusé de réception n'aura pas été signé par le directeur du département ou le responsable de l'unité. Une fois rempli, le formulaire est classé dans le dossier des ressources humaines de l'employé (pour les employés permanents), ou dans un dossier spécifiquement dédié à l'accès au réseau (pour les contractuels, etc.), et gardé par le service informatique. Ces formulaires d'acceptation font l'objet d'une vérification interne.

DECLARATION

Je soussigné (e)…….. déclare avoir lu et compris les Politiques et procédures régissant la technologie de l'information au sein de l'AMAO et accepte de me conformer à celles-ci.

Nom _____

Signature _____Date _____

Chef de Département/Unité Signature _____Date _____