COSOB

لـجنــة تــنــظــيـم عــمــلـيــات الـبــورصـــة و مــراقــبـــتــهــا

Tasqamut n usuddes d toessast n temhilin n tbursa

Commission d'**O**rganisation et de **S**urveillance des **O**pérations de **B**ourse

Charte d'Utilisation Du Système d'Information au sein de la COSOB

Novembre 2021

Sommaire

Introduction

La plupart des institutions aujourd'hui mettent à la disposition de leurs salariés des moyens informatiques pour l'exécution de la mission qu'elles leur confient.

L'objectif principale de cette charte est de réguler l'utilisation des moyens informatiques, limiter les responsabilités pénales et civiles, et de préserver les ressources informatiques de la COSOB. Elle a également pour objectif de sensibiliser les utilisateurs et d'éviter tous forme d'abus dans l'usage des outils informatiques.

Il sera fait état d'un ensemble de règles précisant les droits et obligations des utilisateurs du système d'information de la COSOB selon la réglementation en vigueur .

Enfin, cette charte pourrait constituer une référence en cas de conflit.

Champs d'application

La présente charte concerne les ressources informatiques et les services internet de la COSOB ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le Réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau;
- Ordinateurs portables;
- Imprimantes simples ou multifonctions;
- Scanner;
- Tablettes;
- Les appareils téléphoniques mobiles.

Elle s'applique à l'ensemble des utilisateurs tous statuts confondus, et concerne notamment les utilisateurs permanents ou temporaires (stagiaires, prestataires, fournisseurs, sous-traitants,..) qui utilisent les moyens informatiques de la commission auxquels il est possible d'accéder au système d'information à distance directement ou à partir du Réseau de la COSOB.

Titre I : Accès et usage des ressources informatiques

- L'utilisation des ressources informatiques ainsi que du Réseau pour y accéder n'est autorisé que dans le cadre exclusif de l'activité professionnelle des utilisateurs;
- Toute autorisation prend fin, lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifié.

1 : Règles d'utilisation, de sécurité et de bon usage

- Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès;
- L'utilisation de ces ressource doit être rationnelle, afin d'en éviter la saturation ou leur détournement à des fins personnelles;
- Tout utilisateur doit s'abstenir de nuire à l'image de marque de l'institution par une mauvaise utilisation des outils informatiques;
- L'utilisateur doit respecter les consignes de l'administrateur système et du responsable informatique;
- Il doit suivre les règles en vigueur au sein de la COSOB;
- Il doit choisir des mots de passe sûrs :

- Ne pas les divulguer;
- Ne pas les écrire sur un document papier;
- Ne jamais les communiquer à un tiers;
- Ne jamais prêter son compte;

- Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité;
- Il doit protéger ses fichiers;
- Il lui appartient de protéger ses données et base de données en utilisant, régulièrement, les différents moyens de sauvegarde;
- Il ne doit pas laisser un document affiché sur l'écran de visualisation après exploitation;
– Il ne doit pas tenter de lire, modifier, copier ou détruire des données, sans qu'il n'y soit habilité;
– Il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers un matériel dont il a l'usage;
- Il ne doit pas utiliser un support de donnés externe (disquette, flash disk, CD, etc.), sans autorisation;
- Il ne doit pas laisser traîner des supports magnétiques (disquettes, CD, flash disk, etc.);
- Il doit respecter les modalités de raccordement du matériel au Réseau de la COSOB;

- Il ne doit, en aucun cas, déplacer le matériel et/ou modifier la configuration des systèmes, sauf s'il est habilité;
– Il ne doit pas quitter son poste de travail, sans fermer la session en laissant des ressources ou services accessibles;
– Il doit utiliser les guides d'utilisation du matériel informatique.

2 : Conditions de confidentialité

- L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leurs sont propre;
- Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs;
- L'utilisateur ne doit pas divulguer des informations à caractère générale ou spécifique;
- L'utilisateur doit appliquer le secret professionnel absolu sur toutes les données qu'il pourrait recevoir.

3: Respect de la législation concernant les logiciels

- Toute installation d'un logiciel est soumise aux règles en vigueur;
- Il est strictement interdit d'installer un logiciel sur un système sans s'être assuré, préalablement, que les droits de licence le permettent;
- Il est strictement interdit d'effectuer des copies de logiciels commerciaux, quel qu'en soit l'usage.

4 : Préservation de l'intégrité des systèmes informatiques

- L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et du Réseau;
- En cas de coupure électrique prolongée, il est impératif de procéder à l'arrêt du système.

5 : Mesures de sécurité à appliquer lors des déplacements

- Le missionnaire doit prendre toute les précautions nécessaires de sécurité selon la réglementation en vigeur;

- Il est strictement interdit d'utiliser des (ordinateurs, tablettes.) publics ou partagés pour accéder au compte de messagerie professionnelle de la COSOB;

- Le missionnaire doit garder sur lui, en permanence, son appareil téléphone mobile ou laptop ainsi que les supports de stockage;

- Le missionnaire doit informer la hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger;

- Il est strictement interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles.

Titre II. Usage des services Internet (web, messagerie, appareil téléphonique mobile, réseaux sociaux)

- Dans le cadre de l'accomplissement de leur travail au sein de la COSOB, les employés peuvent être appelés à utiliser Internet;
- Ce service est accessible à des fins strictement professionnelles. Néanmoins, une utilisation raisonnable et occasionnelle à des fins personnelles, est permise sous certaines conditions;

6 : Utilisation d'Internet

- L'employeur fournit aux travailleurs habilités l'accès à Internet à des fins professionnelles.

Les règles suivantes s'appliquent à tout employé autorisé à utiliser Internet :

- L'utilisation d'Internet est limitée à des fins professionnelles. L'exploration d'Internet dans une optique d'apprentissage et de développement personnel est, toutefois, tolérée, mais ne doit en rien porter atteinte au bon fonctionnement du Réseau ou à la productivité de l'employé;

L'employeur peut, à tout moment, limiter ou interdire cet usage privé;

- L'accès à Internet ne peut se faire qu'en utilisant son propre compte (login name). L'utilisation d'un autre compte n'est, par conséquent, pas autorisée;
- L'accès à Internet ne peut être utilisé à des fins prohibées, décrites au point 10 ci-dessous;
- Il est strictement interdit d'accéder aux sites dont le contenu est illégal, immoral, offensant ou inapproprié;
- les publications impliquant la COSOB sur internet doivent être validées avant toute publication;
- Aucune publication ni communication n'est valable sans l'accord préalable de la COSOB.

7 : Utilisation du courrier électronique

- La destination première du système de courrier électronique est exclusivement professionnelle. L'employeur en tolère, toutefois, l'usage exceptionnel à des fins privées,

à condition que cet usage soit occasionnel, se déroule en-dehors des heures de travail, n'entrave en rien la bonne conduite des affaires de la COSOB ou la productivité;

- En aucun cas, le courrier électronique ne pourra être utilisé à l'une des fins prohibées décrites au point 10 ci-dessous.

8 : Appareil téléphonique mobile

- En aucun cas, l'appareil téléphonique mobile ne pourra être utilisé à l'une des fins prohibées décrites au point 10;
- Faire l'inventaire des appareils téléphonique mobiles personnels ou ceux dont la COSOB est propriétaire qui sont utilisés pour accéder a la messagerie professionnelle de la COSOB;
- Prendre les précautions nécessaires à l'utilisation des appareils téléphonique mobile selon les mêmes consignes de politique de sécurité observées l'ors de l'utilisation des PC et laptops;
- Changer le mot de passe de la messagerie professionnelle de la COSOB après chaque connexion au réseau internet wifi public ou après un déplacement;
- Vider historique après chaque connexion au réseau wifi public;
- Ne pas laisser l'appareil téléphonique mobile ou le remettre à une autre personne;
- En cas de vol ou de perte de l'appareil téléphonique mobile, signaler au service informatique pour modifier les différents identifiants.

9. Réseaux sociaux

- En aucun cas, le réseau social ne pourra être utilisé à l'une des fins prohibées décrites au point 10 ci-dessous;
- La COSOB se réserve le droit d'interdire, restreindre, bloquer, ou de suspendre à ses employés l'accès à tout site de réseau social ou à une partie de site de réseau social;
- Les utilisateurs de réseau social ne doive pas divulguer d'informations personnelles sensibles, c'est-à-dire : adresse personnelle, informations financières, numéro de téléphone etc;
- Ne pas utiliser des emails de la COSOB pour créer des comptes sur les réseaux sociaux;
- Les employés doivent utiliser des mots de passe différents de ceux utilisés pour accéder aux ressources et documents de la COSOB;
- Se méfier des liens partagés ou des pièces jointes, notamment via des services de messagerie directe offerts dans les réseaux sociaux.

10 : Activités prohibées

Il est strictement interdit d'utiliser le système de courrier électronique, l'accès à Internet et, plus généralement, l'infrastructure informatique de la COSOB pour :

- La diffusion d'informations confidentielles relatives à l'employeur;

- Accéder aux sites dont le contenu est illégal, immoral, offensant ou inapproprié;
- La diffusion ou le téléchargement (piratage) de données ou de logiciels protégés par le droit de la propriété intellectuelle, en violation des lois applicables;
- La participation à une activité professionnelle annexe;
- L'envoi de messages dont le contenu est susceptible de porter atteinte à la dignité d'autrui
- L'envoi ou la réception sollicitée de message comprenant des annexes à volumes importants sauf pour besoin professionnel;
- La propagation intentionnellement d'un virus;
- L'utilisation du service « chat » et des jeux;

Cette énumération n'est pas limitative;

Titre III. Contrôle et sanctions

11 : Finalités du contrôle de l'utilisation des technologies en Réseau

- L'employeur est attaché au principe du respect de la vie privée des travailleurs sur le lieu de travail.

Les objectifs visées par ce contrôle sont, notamment :

- La prévention et la répression de faits illicites ou diffamatoires;
- La sécurité et / ou le bon fonctionnement technique des systèmes informatiques, du Réseau de la COSOB ainsi que la protection physique des installations de la COSOB;
- Le respect de bonne foi des principes et règles d'utilisation des technologies en Réseau, tels que définis par la présente charte.

12 : Mesures de contrôle et d'individualisation

12.1. Mesures de contrôle

12.1.1. Contrôle de l'utilisation d'Internet

- L'employeur maintient automatiquement une liste générale des sites Internet consultés via le réseau de la COSOB, indiquant la durée et le moment des visites. Cette liste ne fait pas directement mention de l'identité de l'employé. Elle doit être régulièrement évaluée par l'employeur, dans le cadre des objectifs visés dans le point 12.

12.1.2. Contrôle du courrier électronique

- Sur la base d'indices généraux (tels la fréquence, le nombre, la taille, les annexes, etc.), des messages électroniques, certaines mesures de contrôle pourront être prises par l'employeur vis-à-vis de ces messages, dans le cadre des objectifs cités dans le point 12;

- Si l'employeur juge qu'il est fait un usage anormal ou interdit du système de courrier électronique, il procédera, dans le cadre des objectifs cités dans le point 12, à l'identification du travailleur concerné, dans le respect de la procédure d'individualisation décrite au point 12.2 ci-dessous.

12.2. Mesures d'individualisation

- Par "individualisation", on entend le traitement des données collectées lors d'un contrôle, en vue de les attribuer à un employé identifié ou identifiable;
- Des sanctions appropriées seront prises dès que l'individualisation sera faite.

13. Analyse et contrôle de l'utilisation des ressources

- Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges *via* le Réseau peuvent être analysés et contrôlés dans le respect de la législation applicable.

14. Sanctions

- Les infractions à la présente charte informatique sont sanctionnées conformément aux dispositions du titre III du règlement intérieur de la COSOB (cf. Annexe).

15. Modification

- Le contenu de la charte informatique est susceptible d'être modifié, selon les mêmes règles de son élaboration.

Annexe

Catégorie de la Sanction		Liste des infractions
Faute du premier degré	1	L'envoi ou la réception de messages comprenant des annexes à volumes importants à l'exception des messages professionnels et après accord de la hiérarchie.
	2	De la propagation intentionnelle d'un virus
	3	L'utilisation du service « chat » et des jeux
	4	Utilisation abusive des moyens informatiques de la COSOB
	5	Connaissance d'informations détenues par d'autres utilisateurs
	6	Perturbations au bon fonctionnement des systèmes informatiques et du Réseau
	7	Modification de la configuration système du poste
	8	Déplacement du matériel informatique
	9	Mauvaise manipulation lors du raccordement du matériel informatique
	10	De ne pas restituer des données
	11	De ne pas sauvegarder les données
Faute du deuxième degré	1	La diffusion d'informations confidentielles relatives à l'employeur
	2	Accéder aux sites dont le contenu est illégal, immoral, offensant ou inapproprié
	3	La diffusion ou le téléchargement (piratage) de données ou de logiciels protégés par le droit de la propriété intellectuelle, en violation des lois applicables
	4	La participation à une activité professionnelle annexe
	5	Installation de logiciel piraté
	6	Nuire à l'image de l'institution par une mauvaise utilisation des outils informatiques
Faute du troisième degré	1	Envoi de messages dont le contenu est susceptible de porter atteinte à la dignité d'autrui
	2	Publications d'informations impliquant la COSOB sans l'accord préalable de la COSOB