



POLITIQUE INFORMATIQUE
CHARTRE INFORMATIQUE

1 PRÉAMBULE

La présente charte définit les conditions d'accès aux ressources informatiques de BUPDOS-ONG, ainsi que les règles d'utilisation de celles-ci. Elle a notamment pour objet de préciser les droits et devoirs des Utilisateurs.

Elle a également pour objet de sensibiliser les Utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent aux Utilisateurs le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un Utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale, personnelles, ainsi que celle de l'Organisation BUPDOS-ONG.

2 CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout Utilisateur du système d'information et de communication de BUPDOS-ONG dans l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

La charte est diffusée à l'ensemble des Utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet de BUPDOS-ONG. Elle est systématiquement remise à tout nouvel agent.

Des actions de communication internes sont organisées régulièrement afin d'informer les Utilisateurs des pratiques recommandées. Toutefois les utilisateurs ne peuvent s'appuyer sur l'absence éventuelle d'actions de communication sur une période donnée pour s'autoriser des déviences.

On désignera sous le terme « **Utilisateur** » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de BUPDOS-ONG et à les utiliser, à savoir : membres du conseil d'administration, employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels, etc.

Les termes « **Outils Informatiques et de Communication** » recouvrent tous les équipements informatiques et de télécommunications de BUPDOS-ONG.

3 REGLES D'UTILISATION DU SYSTEME D'INFORMATION

Chaque Utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle, dans les conditions définies par BUPDOS-ONG.

3.1 Les modalités d'intervention du service de l'informatique interne

Le service de l'informatique interne assure le bon fonctionnement et la sécurité des réseaux et moyens informatiques de BUPDOS-ONG. Le personnel de ce service dispose d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques et respectent les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à traiter dans le cadre de leurs fonctions.

3.2 L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'Utilisateur lors de son arrivée au sein de BUPDOS-ONG. Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont personnels et confidentiels.

Actuellement, le mot de passe doit être composé de 8 caractères minimum combinant majuscules, minuscules, chiffres et caractères spéciaux. Il ne doit comporter ni le nom, prénom, date de naissance ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement tous les 6 mois. À défaut, l'Utilisateur risque d'assister à un blocage de son compte.

L'authentification prévoit une restriction de l'accès au compte mise en place par le service de l'informatique interne (Verrouillage du compte après 3 échecs).

3.3 Les règles de sécurité

Tout Utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne de BUPDOS-ONG toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe à un tiers.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas enregistrer ses mots de passe dans son navigateur sans mot de passe maître.
- Ne pas stocker ses mots de passe dans un fichier clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes.
- Ne pas utiliser le même mot de passe pour des accès différents.
- Ne pas s'envoyer par courriel ses propres mots de passe.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramètres du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier ou détruire les logiciels propriétés de BUPDOS-ONG.
- Verrouiller son ordinateur avant de quitter son poste de travail même pour un temps limité.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Effectuer des sauvegardes régulières et enregistrer les copies sur disque dur externe, CD ou DVD.
- S'interdire toute copie de données sur un support externe sans l'accord du supérieur hiérarchique.
- Ne pas mener d'actions engageant la responsabilité juridique ou financière de l'ONG en répondant par exemple à un courriel.

Règles de sécurité propres au smartphone :

- N'installer que des applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...) par ailleurs éviter d'installer les applications qui demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement.
- En plus du code PIN qui protège sa carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès à son terminal et le configurer pour qu'il se verrouille automatiquement.

En tout état de cause, l'utilisateur doit séparer les usages personnels des usages professionnels :

- Ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles.
- Ne pas héberger de données professionnelles sur ses équipements personnels (clés USB, téléphone...) ou sur des moyens personnels de stockage en ligne.
- Éviter de connecter des supports amovibles personnels (clés USB, disques durs externes...) aux ordinateurs de l'ONG.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au système d'information de BUPDOS-ONG sans l'accord préalable du service informatique interne.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre BUPDOS-ONG et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

4 MOYENS INFORMATIQUES ET MESURES DE CONTROLE

4.1 Configuration du poste de travail

Dans le cas où BUPDOS-ONG met à disposition un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions, l'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications, sans y avoir été autorisé par l'équipe informatique interne.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « Équipement Nomade »).
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de nouveaux logiciels (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord du service informatique interne.

4.2 Équipements nomades et procédures spécifiques

Équipements Nomades

On entend par « **Équipements Nomades** » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc...).

Sauf réserve technique particulière, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, il est recommandé qu'il soit physiquement attaché à l'aide d'un antivol.

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté, de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Procédures spécifiques

L'utilisateur doit renseigner et signer un registre manuel ou digital, tenu par le service informatique interne, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (ex : vidéoprojecteur, hautparleur audio). Il en assure la garde et la responsabilité et doit informer le responsable informatique en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou la plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

4.3 Internet

Les Utilisateurs peuvent consulter uniquement les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

4.4 Messagerie électronique

Conditions d'utilisation

La messagerie mise à disposition des Utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est interdite.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique interne, et validées par la direction générale :

- Volumétrie de la messagerie,
- Taille maximale de l'envoi et de la réception d'un message,
- Nombre limité de destinataires simultanés lors de l'envoi d'un message,
- Gestion de l'archivage de la messagerie.

Les Utilisateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'Utilisateur dans ce cadre doivent être impérativement effacés.

Courriel non sollicité

BUPDOS-ONG dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir des messages de type commercial, newsletters, abonnements ou autres, et à ne s'abonner qu'à un nombre limité de listes de diffusion, notamment si celles-ci ne relèvent pas du cadre strictement professionnel.

Contenu du courriel

Il est strictement interdit à l'Utilisateur d'ouvrir des pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que leur envoient habituellement leurs contacts.

De même, si des liens figurent dans un courriel, il est fortement recommandé aux Utilisateurs de passer leur souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). L'Utilisateur pourra ainsi en vérifier la cohérence.

En tout état de cause, l'Utilisateur doit respecter les règles suivantes :

- Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles (par exemple : code confidentiel et numéro de carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer les données des personnes concernées. Il s'agit d'attaques par hameçonnage ou « fishing ».
- Ne pas ouvrir et ne pas relayer de messages de type chaînes de lettre, appels à la solidarité, alertes vitales, etc.

4.5 Téléchargements

Si l'Utilisateur télécharge du contenu numérique à partir de sites internet dont la confiance n'est pas assurée, il prend le risque d'enregistrer sur son ordinateur des programmes qui contiennent des virus. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de sa machine pour notamment espionner les actions réalisées sur son ordinateur, voler ses données personnelles, lancer des attaques.

Afin de veiller à la sécurité de sa machine et de ses données, l'Utilisateur doit respecter les règles suivantes :

- Télécharger ses programmes sur les sites des éditeurs ou autres sites de confiance.
- Penser à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires.
- Rester vigilant concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens.
- Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

4.6 Paiements sur internet

Avant d'effectuer un paiement en ligne, il est nécessaire que l'Utilisateur procède aux vérifications suivantes sur le site Internet :

- Contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de son navigateur Internet, de préférence Google Chrome ou Mozilla Firefox mis à jour régulièrement (remarque : ce cadenas n'est pas visible sur tous les navigateurs).
- S'assurer que la mention « https:// » apparaît au début de l'adresse du site Internet.
- Vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

4.7 Téléphone

Dans certains cas, BUPDOS-ONG met à disposition des Utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles.

L'utilisation du téléphone à titre privé est rigoureusement proscrite.

Des restrictions d'utilisation par les Utilisateurs des téléphones fixes sont mises en place en tenant compte de leurs missions. À titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

BUPDOS-ONG peut mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Des statistiques globales et individuels sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

L'utilisation du téléphone privé pour les activités professionnelles doivent se faire uniquement selon les accréditations/autorisations de l'utilisateur concerné. Ces accréditations/ autorisations sont définis par le service ressources humaines et mis en application conjointement par le service informatique et ressources humaines

4.8 Déplacements professionnels

L'emploi des équipements nomades facilite les déplacements professionnels mais fait peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'ONG.

C'est pourquoi, les Utilisateurs sont tenus de respecter les règles suivantes :

Avant de partir en mission :

- N'utiliser que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission et ne contenant que les données nécessaires.
- Sauvegarder ces données, pour les retrouver en cas de perte.
- Activer un filtre de protection pour son ordinateur si l'Utilisateur compte profiter des trajets pour travailler.
- Apposer un signe distinctif (par exemple, une pastille de couleur) sur ses appareils pour s'assurer qu'il n'y a pas eu d'échange pendant le transport,
- Vérifier que ses mots de passe ne sont pas préenregistrés.

Pendant la mission :

- Garder ses appareils, supports et fichiers avec soi, pendant son voyage comme pendant le séjour (ne pas les laisser dans un bureau ou un coffre d'hôtel).
- Désactiver les fonctions Wi-Fi et Bluetooth de ses appareils.
- Retirer la carte SIM et la batterie s'il est contraint de se séparer de son téléphone.
- Informer son entreprise en cas d'inspection ou de saisie de son matériel par des autorités étrangères.
- Ne pas utiliser les équipements reçus à titres gratuits s'il ne peut pas les faire vérifier par un service de sécurité de confiance.
- Éviter de connecter ses équipements à des postes qui ne sont pas de confiance (par exemple : si l'utilisateur a besoin d'échanger des documents lors d'une présentation commerciale, utiliser une clé USB destinée uniquement à cet usage et effacer ensuite les données avec un logiciel d'effacement sécurisé).
- Refuser la connexion d'équipements appartenant à des tiers à ses propres équipements (smartphone, clé USB, ...)

Après la mission :

- Effacer l'historique des appels de navigation.
- Changer les mots de passe que l'utilisateur a utilisés pendant le voyage.
- Faire analyser ses équipements après la mission s'il le peut.
- Ne jamais utiliser les clés USB qui peuvent avoir été offertes lors de ses déplacements (salons, réunions, voyages...) : elles sont susceptibles de contenir des programmes malveillants.