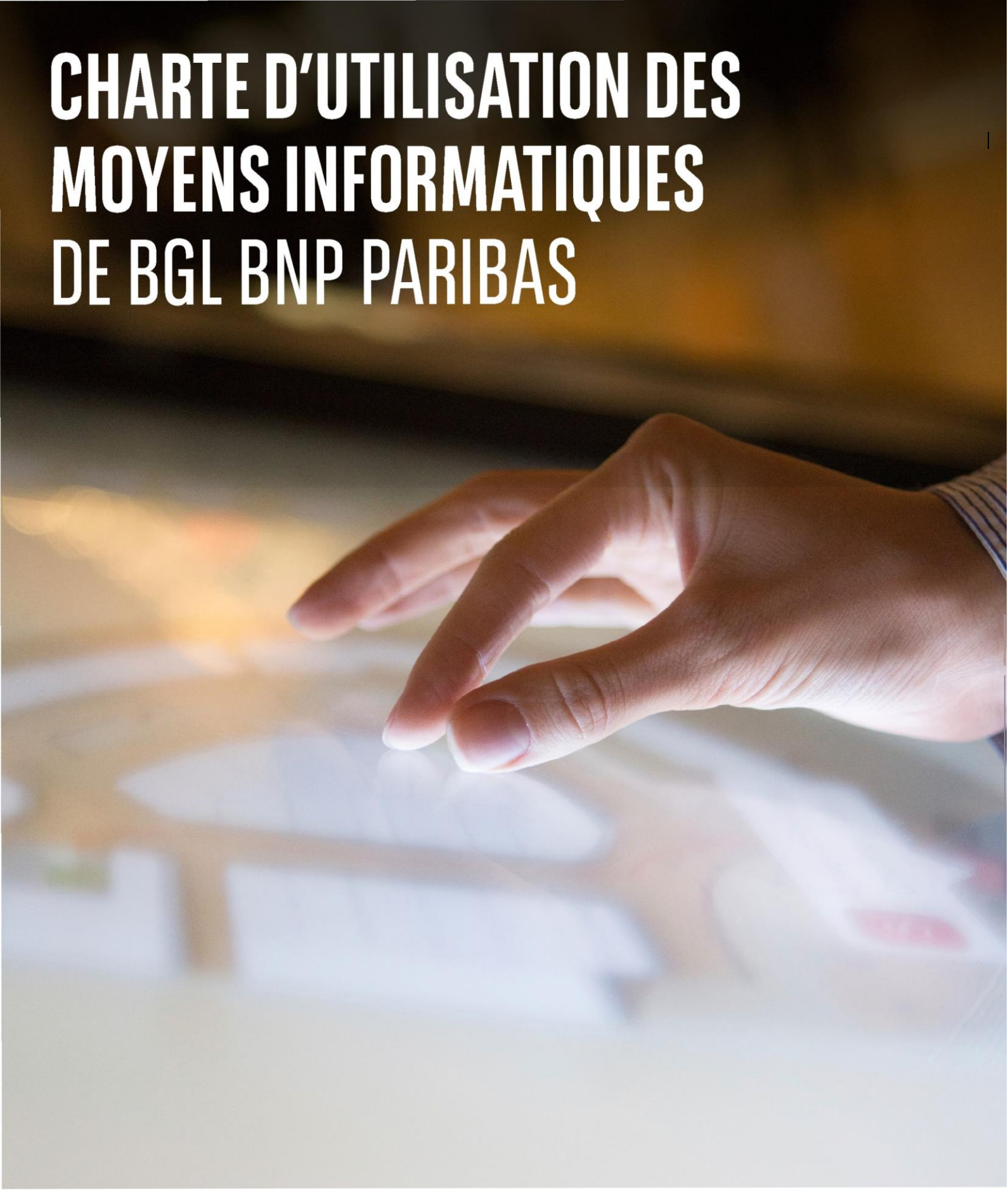
CHARTE D'UTILISATION DES MOYENS INFORMATIQUES DE BGL BNP PARIBAS



BGL
BNP PARIBAS

La banque
d'un monde
qui change

Cette charte fait partie du règlement d'ordre intérieur de la Banque. Elle est applicable à tous les collaborateurs internes et externes de la Banque. Par collaborateurs externes nous entendons entre autres les stagiaires, les intérimaires, les prestataires externes et les consultants.

Les présentes règles s'appliquent à tout utilisateur des moyens informatiques de la Banque :

- Est dénommé utilisateur tout collaborateur faisant usage de moyens informatiques mis à sa disposition au sein et pour le compte de la Banque.
- Sont considérés comme moyens informatiques, toutes les ressources informatiques, téléinformatiques et systèmes d'information : matériels fixes ou nomades, logiciels, systèmes de communication en interne ou en externe, ainsi que les fichiers - quels que soient leurs supports - mises à la disposition des utilisateurs par la Banque.
- Sera désigné par "moyen d'accès", tout dispositif permettant l'usage des moyens informatiques par un utilisateur (identifiant, mot de passe, code PIN ...)

Dans la présente Charte, nous entendons par :

- **Matériel informatique (hardware)** : les systèmes informatiques de la Banque, à savoir les unités centrales de traitement, le matériel de télécommunication (téléphone, fax, vidéoconférence, ...), les systèmes décentralisés et les équipements qui y sont liés, tels que les ordinateurs individuels (PC et Laptops), les « smartphones » (ex : « Blackberry » ou « iPhone »), les imprimantes, les tablettes et les terminaux;
- **Logiciel (software)** : les programmes (tels que les traitements de texte, les tableurs et les applications métiers) qui sont utilisés sur le matériel informatique et ce, que la Banque en ait la propriété ou en ait acquis le droit d'utilisation;
- **Fichiers** : tous les recueils des informations et des données de la Banque, repris sur un support pouvant faire l'objet d'une lecture automatisée et ce, que la Banque en ait la propriété ou en ait acquis le droit d'utilisation.

1. Moyens informatiques

1. L'utilisateur est personnellement responsable de l'usage qu'il fait des moyens informatiques de la Banque qui sont mis à sa disposition dans le cadre de l'exercice de son contrat de travail ou de sa mission. L'utilisateur doit faire bon usage de ces moyens informatiques dans le cadre de son activité professionnelle ou à des fins personnelles à l'intérieur ou à l'extérieur de la Banque. Cette utilisation ne doit pas porter atteinte à l'exécution normale de son contrat de travail ou de sa mission, ni aux intérêts de la Banque, de sa clientèle ou de ses salariés.

   Il s'engage à respecter les présentes règles. Le caractère contraignant des règles énoncées dans la présente Charte découle en particulier de la législation applicable en matière de secret professionnel, de protection des données personnelles, de la vie privée et de droits d'auteur. (Voir la liste des lois et règlementations luxembourgeoises et européennes auxquelles cette Charte se réfère en page 7 de ce document).

2. L'utilisation des moyens informatiques est exclusivement réservée aux collaborateurs qui y sont expressément autorisés. Les autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

3. Les moyens informatiques mis à la disposition des collaborateurs de la Banque sont en principe destinés à un usage purement professionnel. Néanmoins, la Banque reconnaît un droit d'usage privé résiduel, lorsqu'il est justifié par la nécessité ou par un intérêt accepté dans les usages. Il sera fait usage de ce privilège pour raisons privées de manière raisonnable à condition que cet usage soit réduit au minimum et ne porte pas préjudice à la Banque, à ses activités, à ses clients, aux autres entreprises du groupe auquel appartient la Banque et aux marchés sur lesquels la Banque est active. Les dossiers, fichiers et e-mail émis, crées ou stockés par un collaborateur sont présumés avoir un caractère professionnel, sauf si le collaborateur les a identifiés comme « privés » ou « personnels ». La transformation et le classement de dossiers, fichiers ou e-mails de nature professionnelle en information privée est interdite. La Banque pourra accéder en cas de besoin motivé et autorisé par le DPO, à toute information, conformément aux procédures en vigueur.

4. L'utilisation illicite ou la manipulation des moyens informatiques d'une manière qui aurait pour conséquence l'accès à des informations non autorisées, la saturation, le spamming (lettres en chaîne, etc.) ou des indisponibilités de ressources ou services pour les autres utilisateurs est interdite. Cela vaut également pour les sites de jeux en ligne et de paris. De même l'utilisation du matériel informatique à des fins qui auraient des caractéristiques offensantes, insultantes, racistes, pornographiques, pédophiles, diffamatoires ou qui relèveraient de harcèlement moral ou sexuel est interdite. De tels agissements sont passibles de poursuites judiciaires.

5. Pour accéder aux logiciels et aux fichiers, l'utilisateur dispose de moyens d'accès. L'utilisation de l'identifiant attribué à un tiers est formellement interdite. Le code PIN ou mot de passe doit être choisi par l'utilisateur lui-même selon les recommandations en vigueur et doit rester secret; l'utilisateur doit le protéger, ne pas le communiquer à des tiers et le modifier périodiquement. Si l'utilisateur soupçonne ou constate que son code PIN ou mot de passe est connu d'un tiers, il est dans l'obligation de le modifier immédiatement et de signaler l'incident à son responsable hiérarchique ou à la fonction Compliance. L'utilisateur ne doit pas quitter son poste de travail en laissant accessible une session en cours. Tout supérieur hiérarchique doit veiller à la stricte application de cette règle.

   En fin de journée, l'utilisateur doit arrêter son poste de travail en faisant « Shut Down » ou « Log off ».

6. Toute copie - intégrale ou partielle – de logiciels ou de fichiers de la Banque est interdite, sauf aux fins qui sont expressément précisées dans le contrat de licence conclu par la Banque ou une société du groupe auquel la Banque appartient. En cas d'autorisation prévue par le contrat de licence, la copie – intégrale ou partielle – de logiciels ou de fichiers dont la Banque a la propriété ou a acquis le droit d'utilisation ne peut être effectuée que par des collaborateurs qui y sont expressément autorisés par la direction informatique compétente.

7. Seuls les moyens informatiques en ce compris les logiciels fournis par ou au nom de la Banque et approuvés par la Banque, peuvent être utilisés. L'installation et/ou la mise en service de matériel informatique ne peuvent être effectuées que par des collaborateurs autorisés par la direction informatique compétente ou désignés à cet effet.

8. Les utilisateurs autorisés et désignés à cet effet qui importent des logiciels ou des données dans leur système informatique (ordinateurs portables et tablettes inclus), notamment au moyen de clés USB, de CD-ROM, de DVD, ou par voie électronique (par exemple, via le réseau Internet ou par e-mail), seront considérés comme responsables des conséquences que cette importation pourrait avoir sur les autres logiciels et sur les autres données. Ils doivent utiliser les programmes de détection de virus approuvés par la Banque et s'assurer que les logiciels et les données importés ne contiennent pas de code malveillant. La non-utilisation de ces programmes de détection des virus doit faire l'objet d'une autorisation explicite de la direction informatique.

9. Les moyens informatiques ne peuvent être mis à la disposition de tiers, sauf accord de la direction informatique compétente. Sur demande de la Banque, ou au plus tard lorsqu'il quitte la Banque, l'utilisateur a l'obligation de désinstaller de son ordinateur privé (à domicile) tout logiciel et tout fichier que la Banque aurait mis à sa disposition et de restituer à la Banque tout matériel informatique qui lui aurait été confié.

10. Les moyens informatiques ne peuvent être déplacés de l'endroit où ils se trouvent, sauf accord de la direction informatique compétente, à l'exception du matériel destiné à un usage mobile tel que PC portables, tablettes numériques, « smartphones » (p.ex. « Blackberry » ou « iPhone »).

11. L'utilisation des moyens informatiques, doit toujours faire l'objet de soins attentifs. Tout dysfonctionnement ou tout événement anormal doit être signalé immédiatement à Infoline. Si un collaborateur utilise les moyens informatiques en dehors de la Banque, tant la Banque que le collaborateur doivent prendre les mesures nécessaires pour exclure dans toute la mesure du possible tout risque d'usage abusif ou de détournement. Tout usage abusif ou détournement éventuel (par exemple vol) doit être immédiatement signalé à la hiérarchie et à Infoline.

Tout média contenant des informations classées confidentielles ou secrètes doit faire l'objet de mesures de protection assurant la confidentialité des informations qui y sont stockées. Il est interdit de conserver sur le disque dur du PC des données confidentielles non protégées par un système de chiffrement approuvé par la direction informatique compétente.

Sont à considérer comme informations confidentielles ou secrètes, entre autres, les données clients protégées par le secret professionnel, les données à caractère personnel au sens de la législation applicable en matière de protection des données personnelles, ainsi que de façon plus générale les données concernant les clients, les collaborateurs ou la Banque qui ne sont pas destinées à des tiers et dont la divulgation peut porter préjudice à la Banque, au Groupe et/ou à leurs clients. Le stockage de ces informations doit se faire uniquement sur les répertoires sécurisés définis par la hiérarchie et/ou sur des médias autorisés.

Il est défendu de prendre des notes concernant des informations confidentielles sur des équipements privés.

12. Après utilisation, les appareils et médias informatiques amovibles (comme des médias USB) doivent être conservés dans une armoire sécurisée.

13. La moindre présomption ou constatation de la présence d'un virus informatique doit être immédiatement signalée à la hiérarchie et à Infoline.

14. Les moyens d'accès à l'ordinateur portable et/ou la tablette et la connexion à distance au système de la Banque doivent être gardés séparément de l'ordinateur portable et/ou de la tablette.

15. La mise en œuvre de réseaux sans fil (par ex. WiFi) à l'intérieur de la Banque n'est pas autorisée sans analyse et autorisation préalables de la direction informatique compétente.

16. Il est interdit de laisser prendre le contrôle à distance de sa station de travail par un intervenant n'appartenant pas à l'équipe de support informatique de la Banque (Infoline). Seule une autorisation formelle et écrite (mail ou courrier à l'intéressé et copie à la Sécurité Informatique) d'un membre de la direction informatique permet, à titre exceptionnel, d'y déroger.

Dans ce cas précis, le collaborateur se doit de surveiller toutes les actions de l'intervenant. Il informera immédiatement le membre de la direction informatique ayant autorisé cette dérogation de toute anomalie constatée.

17. Il est interdit de procéder sans autorisation à des prises de vue photographiques ou des enregistrements vidéo à l'intérieur des locaux de la Banque. Le fait de disposer d'un appareil (« smartphone » ou simple téléphone portable) de la Banque muni de la fonction photographique ne vaut pas autorisation de photographier ou d'enregistrer des vidéos.

2. Réseau Internet

1. Les connexions au réseau Internet mises à la disposition des collaborateurs par la Banque et l'utilisation par les collaborateurs du réseau Internet pour accéder aux messageries instantanées, aux réseaux sociaux, aux forums de discussion sont en principe destinées à des fins professionnelles.

2. Néanmoins, la Banque reconnaît un droit d'usage privé résiduel, lorsqu'il est justifié par un intérêt accepté dans les usages. Il sera fait usage de ce privilège pour raisons privées de manière raisonnable à condition que cet usage soit réduit au minimum et ne porte pas préjudice à la Banque, à ses activités, à ses clients, aux autres entreprises du groupe auquel appartient la Banque et aux marchés sur lesquels la Banque est active.

3. Les collaborateurs utilisant des logiciels ou des données en provenance du réseau Internet doivent veiller à respecter la législation en matière de droits d'auteur.

4. Les collaborateurs ne doivent pas utiliser le réseau Internet pour inciter à importer et diffuser des photos, des lettres en chaîne ou autres éléments non professionnels. En même temps, des appels reçus via Internet pour diffuser par voie électronique des photos, des lettres en chaîne ou d'autres productions doivent être ignorés.

5. Chaque collaborateur est entièrement responsable des actions (consultations, saisies, publications) qu'il effectue sur le réseau Internet. Certaines actions sur Internet peuvent générer une fuite d'informations sensibles préjudiciable à la Banque. Pour faire notamment appel à un outil de traduction en ligne, les collaborateurs doivent vérifier qu'aucune donnée confidentielle ne soit sélectionnée – l'utilisation d'outils de traduction internes est à privilégier.

Il ne faut pas télécharger des fichiers disponibles via des liens sur des sites Web, dont on ne connaît ni leur source, ni leur but pour éviter le risque d'importation de logiciels malveillants dans les systèmes informatiques de la Banque.

3. Messagerie électronique

Les messageries électroniques entrent dans le champ des moyens informatiques et à ce titre leur utilisation obéit aux règles indiquées ci-dessus.

Dans cette section, nous entendons par :

- **E-mail externe :** tout courriel échangé avec une adresse en dehors de la Banque et qui transite par le réseau public Internet.
- **E-mail interne :** par opposition à l'e-mail externe, un message interne transite uniquement par les serveurs et le réseau protégé du Groupe BNP PARIBAS.

1. L'e-mail externe transite par le réseau Internet. Ce réseau est public et non protégé. L'e-mail externe ne constitue donc pas un canal de communication adéquat pour échanger des informations internes, confidentielles ou secrètes avec des clients ou des tiers. Il ne doit donc jamais être utilisé à cette fin sauf si les messages sont protégés par un système de chiffrement approuvé par IT Sécurité des systèmes d'information.

2. L'utilisation inadéquate du courrier électronique augmente le risque d'importation de virus dans les systèmes informatiques de la Banque et peut entraîner une surcharge du réseau. Il est important de rester prudent lors de la réception de documents attachés et de ne les ouvrir que si l'expéditeur est connu et identifié.

3. Le contenu d'un document pouvant être modifié lors de son transit au travers d'Internet, ce canal de communication n'est pas adéquat pour échanger des documents qui, selon le contexte dans lequel ils sont envoyés, pourraient engager de manière contractuelle la Banque. L'utilisation du courrier électronique en vue de la mise en œuvre d'engagements contractuels, doit obligatoirement être précédée d'un accord écrit par lequel l'entité compétente de la Banque et le tiers se mettent d'accord sur l'utilisation du courrier électronique pour l'exécution des contrats. Les e-mails utilisés pour la mise en œuvre du contrat devront être conservés pendant une durée identique à celle applicable aux copies papier d'un contrat. Exemple : Acceptation d'ordres clients par e-mail.

4. Bien que le contenu d'un simple e-mail n'ait pas de valeur légale pour la conclusion d'un contrat, il est quand-même susceptible de servir de preuve ou au moins de commencement de preuve par écrit dans le cadre d'actions en justice. La responsabilité de la Banque peut dès lors être mise en cause sur la base d'informations échangées par e-mail, d'autant plus que certains juges reconnaissent le courrier électronique au même titre que l'écrit sur support papier.

5. La teneur d'un e-mail envoyé par un collaborateur de la Banque contribue à l'image de l'entreprise. Tout message contenant des informations non professionnelles ou un contenu inopportun est susceptible de porter atteinte à la réputation de la Banque et pourrait même aller jusqu'à engager la responsabilité de la Banque en cas de préjudice subi par un tiers ou un client.

6. Le courrier électronique est un outil professionnel et ne peut être utilisé en principe qu'à des fins professionnelles. Les messages privés doivent donc rester exceptionnels. Seront considérés comme messages privés les messages comportant dans leur sujet la mention « [PRIVE] » ou « [PRIVATE] ».
Les collaborateurs n'utiliseront pas le courrier électronique pour mener des activités contraires aux intérêts de la Banque.

Il est défendu d'envoyer des documents professionnels de nature confidentielle à son adresse email privée.

Le système de courrier électronique ne peut pas être utilisé pour envoyer des messages dont le contenu présente un caractère illégal, déplacé ou offensant, des chaînes de messages, pour participer à des concours et/ou paris ou pour mener des activités commerciales à titre personnel.

7. Les règles et les normes qui régissent les communications tant écrites que téléphoniques s'appliquent également aux communications utilisant le réseau Internet.

8. Les collaborateurs ne peuvent en aucun cas utiliser le réseau Internet comme instrument de marketing à des fins de "spamming" (publipostage électronique non sollicité).

9. En cas de doute sur les points qui précèdent, il est recommandé aux collaborateurs de consulter la fonction Compliance.

4. Téléphonie

1. L'enregistrement de conversations téléphoniques des collaborateurs sur le lieu de travail peut être effectué par la Banque conformément à la législation applicable. La Banque peut notamment enregistrer les conversations téléphoniques lorsque cela est nécessaire pour fournir la preuve d'une communication ou transaction commerciale avec des clients ou des tiers. Les collaborateurs concernés sont informés préalablement à la mise en place du dispositif.

5. Accès en cas d'absence

1. En cas d'absence prévisible, le collaborateur doit mettre une réponse automatique d'absence sur sa messagerie. Il peut également donner accès à sa boîte e-mail à un collègue pendant son absence en configurant Outlook (fonction autoforward ou délégation d'accès à sa mailbox).

Pour rappel : la transmission du mot de passe à une autre personne n'est en aucun cas autorisée!

Si le collaborateur n'a rien prévu, le DPO sera considéré par défaut comme suppléant et analysera au cas par cas la recevabilité des éventuelles demandes d'accès en fonction des lois et règlements en vigueur. Les messages marqués comme «[PRIVE] » ou « [PRIVATE] » ne seront ni consultés, ni transmis sans accord du collaborateur.

2. En cas d'absence définitive ou prolongée et/ou non prévue du collaborateur, sa hiérarchie peut demander (demande motivée) au DPO d'accéder à ses fichiers et de transmettre les fichiers professionnels. Après vérification que la demande est bien recevable en fonction des lois et règlements en vigueur, le DPO extraira les fichiers professionnels concernés. Les fichiers identifiés comme «[PRIVE] » ou « [PRIVATE] » ne seront ni consultés, ni transmis sans l'accord du collaborateur.

6. Contrôles

1. Les activités des utilisateurs réalisées au moyen du matériel informatique de la Banque y compris l'utilisation de l'e-mail et de l'Internet, sont tracées, analysées et enregistrées (fichiers « logs » ou de journalisation, etc...) dans les limites autorisées par la législation en vigueur

2. L'utilisation de ces traces d'audit (« logs ») est nécessaire aux fins des intérêts légitimes poursuivis par la Banque, et plus particulièrement pour assurer la protection des biens de la Banque, le bon fonctionnement et la sécurité des systèmes et réseaux informatiques et de communication électronique ainsi que la protection des données traitées.

3. Des contrôles réguliers sont réalisés sur les connexions et tentatives de connexion par les services informatiques en charge d'assurer la sécurité des réseaux et des systèmes, afin de garantir :

- L'utilisation normale des ressources et le cas échéant identifier les usages contraires aux règles de confidentialité ou de sécurité des données,
- La protection d'informations dont la divulgation pourrait porter préjudice à la banque ou à ses clients.

Les administrateurs système, qui de par leur fonction, sont amenés à accéder à ces informations sont tenus au secret professionnel et ne peuvent exploiter ces données que dans le but d'assurer le bon fonctionnement technique et la sécurité des installations

4. Des contrôles ponctuels et gradués de l'utilisation du matériel informatique et des applications peuvent être réalisés par la Cellule Anti-Fraude sur base de l'accord du DPO. De même, des filtrages systématiques de l'e-mail et de l'internet, qui peuvent également être complétés par des contrôles réalisés par la Cellule Anti-fraude sur base de l'accord du DPO, sont effectués. Ces contrôles sont réalisés en accord avec les politiques et les procédures de la Banque et la législation en vigueur

Les enregistrements des activités sont également susceptibles d'être fournis sur requête du parquet ou des autorités de contrôle.

Principales lois et règlementations luxembourgeoises et européennes applicables

Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Art.28 de la CONSTITUTION DU GRAND-DUCHÉ DE LUXEMBOURG garantissant l'inviolabilité du secret des correspondances.

Règlement grand-ducal du 21 décembre 2004 déterminant les services de communications électroniques et les services postaux ainsi que la nature, le format et les modalités de mise à disposition des données dans le cadre de l'article 41 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Loi modifiée du 5 avril 1993 relative au secteur financier en particulier l'article 41 relatif au secret professionnel.

Loi modifiée du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données.

Loi du 11 août 1982 concernant la protection de la vie privée.

Loi du 01 Août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

CODE PENAL

Section VII.4 - De certaines infractions en matière informatique. (L. 15 juillet 1993)

Art. 509-1. (L. 14 août 2000) Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros.

Art. 509-2. (L. 15 juillet 1993) Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

Art. 509-3. (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

Violation de secret d'affaires ou de fabrication, **Article 309** du Code Pénal.

Violation du secret professionnel, **Article 458** du Code Pénal.

Violation du secret des correspondances, **Article 460** du Code Pénal.

Vol ou recel d'informations, **Article 505** du Code Pénal, etc.

BGL
BNP PARIBAS

La banque
d'un monde
qui change