Exigences pour les fournisseurs dans les locaux d'Euroclear

Toute personne travaillant chez Euroclear doit respecter le code de conduite professionnelle dont les principes ont été traduits dans ces exigences.

Si vous avez des questions concernant ces exigences, veuillez contacter compliance@euroclear.com.

1. Conduite éthique

1.1 Conformez-vous aux normes les plus élevées en matière d'équité, de probité et d'intégrité.

1.2 Respectez la lettre et l'esprit des lois et règlements en vigueur dans les juridictions où nous exerçons nos activités.

1.3 Efforcez-vous d'assurer une communication complète, pertinente, loyale et transparente avec les clients et les actionnaires d'Euroclear.

1.4 Ne commettez aucune discrimination à l'égard d'une personne, en raison notamment de son âge, ses origines, son sexe, sa religion, son handicap ou son orientation sexuelle.

1.5 N'adoptez pas un comportement pouvant être interprété comme une forme de :

- **a.** violence ; ou
- **b.** harcèlement sexuel (comportement verbal, non verbal ou physique à caractère sexuel) ; ou
- **c.** harcèlement moral (conduite abusive et répétée, qu'elle qu'en soit l'origine, qui se manifeste notamment par un comportement, des paroles, des intimidations, des actes, des gestes et des écrits unilatéraux, portant atteinte de manière intentionnelle à la personnalité, à la dignité, à l'intégrité physique ou psychologique d'une personne) ; ou
- **d.** intimidation (« bullying »). Le terme « bullying » désigne tout acte imprévisible ou inopportun visant à humilier, déstabiliser ou dévaloriser une personne.

1.6 Sauf autorisation spéciale, la consommation de boissons alcoolisées est interdite dans les locaux de travail.

1.7 La consommation, l'achat, la vente et la possession de drogues sont interdits dans les locaux d'Euroclear.

1.8 Traitez avec les régulateurs d'Euroclear de manière ouverte et coopérative et dans le respect des lois en vigueur.

1.9 Ne commettez pas et ne dissimulez pas des actes frauduleux ou illégaux. Faites part de vos soupçons ou preuves d'activités frauduleuses à votre point de contact à Euroclear.

1.10 Vous-même, ainsi que les membres de votre famille et vos proches, ne devez jamais accepter de cadeaux d'une valeur unitaire supérieure à 100 euros (ou équivalente), en raison de votre position au sein d'Euroclear, sans l'autorisation préalable de votre point de contact à Euroclear. Les sommes d'argent en espèces, quel que soit leur montant, doivent toujours être refusées. Vous pouvez accepter les invitations à déjeuner ou à dîner qui vous sont faites dans le cadre normal de vos relations d'affaires.

1.11 Signalez toutes les sollicitations de la presse et des médias, y compris les demandes de rédaction d'un article ou d'interview sur votre expérience au sein d'Euroclear ou concernant tout développement d'activité lié à Euroclear, à l'équipe Euroclear Corporate Communications avant d'engager une discussion avec un journaliste.

1.12 Respectez le code vestimentaire d'Euroclear lorsque vous travaillez dans les locaux de l'entreprise. Le style Euroclear est « sport-chic ». Néanmoins, une tenue de ville standard convient mieux lorsque vous rencontrez des clients extérieurs sur place ou si vous devez assister à une réunion d'affaires en externe.

1.13 Ne signez jamais de documents officiels qui pourraient engager la responsabilité d'Euroclear (par ex. : factures, contrats avec des fournisseurs, etc.) et ne demandez jamais de devis à des fournisseurs au nom d'Euroclear.

1.14 La fraude fiscale consiste en une violation intentionnelle des lois ou règlements fiscaux et est strictement interdite. Vous ne devez pas coopérer, directement ou indirectement, avec des clients d'Euroclear qui cherchent à se soustraire à leurs obligations fiscales. Vous n'êtes pas autorisé à répondre à des demandes de clients, ni à contacter des clients afin de leur donner un conseil en matière de fiscalité, à moins d'avoir consulté un membre du service Corporate Tax d'Euroclear ou un fiscaliste de la division juridique d'Euroclear.

1.15 Si vous avez connaissance ou si vous soupçonnez qu'une société Euroclear ne respecte pas les lois, règlements et directives, signalez-le immédiatement à votre point de contact à Euroclear.

1.16 Veuillez consulter et vous conformer aux fiches d'information appropriées incluant (mais n'étant pas limitées à): la protection des données, le droit de la concurrence, le blanchiment des capitaux & financement du terrorisme et la prévention de l'abus de marché. La liste complète des directives d'entreprise est disponible sur Pulse+

2. Exigences en matière de sécurité

2.1 Laptops Euroclear et télétravail

a. Seuls les laptops autorisés utilisant des configurations et des logiciels autorisés peuvent être connectés au réseau informatique d'Euroclear.

b. Les utilisateurs ne doivent pas installer de logiciels non autorisés ou modifier les paramètres de sécurité des logiciels Euroclear.

c. Avant de laisser l'appareil sans surveillance, l'utilisateur doit verrouiller son écran.

d. Il est fortement recommandé aux utilisateurs à distance de connecter leur laptop au réseau d'entreprise une fois par semaine (à distance ou au bureau). Il est néanmoins obligatoire de se connecter en local au moins une fois par mois afin que les logiciels essentiels puissent être mis à jour.

e. Les utilisateurs doivent prendre toutes les précautions raisonnables pour éviter qu'une autre personne n'espionne leur écran (shoulder surfing) lorsqu'ils travaillent sur leur laptop d'entreprise dans un espace public (par ex. dans le train).

f. Les laptops ne doivent jamais être laissés sans surveillance dans les espaces publics.

g. Les utilisateurs ne doivent pas s'adonner à des activités illégales ou contraires à l'éthique lorsqu'ils utilisent des laptops Euroclear.

h. Les utilisateurs doivent immédiatement contacter le Help Desk d'Euroclear à l'extension 2424 (Nordics Local CT Service Desk) en cas de perte ou de vol de leur laptop.

2.2 Bring your own device

a. Euroclear offre à des utilisateurs autorisés la possibilité d'accéder à leurs e-mails et calendrier professionnel en utilisant leur appareil mobile personnel (pour des raisons de sécurité et de compatibilité).

b. Tous les utilisateurs doivent signer le Document d'accord pour les utilisateurs finaux et se conformer à l'ensemble de ses dispositions. Une fois que l'accès a été autorisé par Euroclear, l'utilisateur doit enregistrer son ou ses appareils. Veuillez vous reporter à la procédure de mise en œuvre relative au Bring Your Own Device (BYOD) pour de plus amples détails.

c. L'utilisateur doit supprimer de l'appareil toutes les données Euroclear à la fin de son contrat de travail ou lorsque l'accès au service lui est retiré.

d. L'utilisateur final doit vérifier les éléments suivants :

- Un profil de sécurité doit être installé sur l'appareil personnel afin qu'une série de contrôles puisse être appliquée, à savoir : utilisation obligatoire d'un code PIN (au moins 6 caractères) pour déverrouiller l'appareil, verrouillage automatique de l'appareil en cas d'inactivité pendant 2 minutes, etc.
- Le système d'exploitation (version iOS) ne doit jamais être inférieur à la version recommandée par Euroclear.
- Les notifications du personnel de support d'Euroclear doivent être immédiatement appliquées.

e. L'utilisateur final doit immédiatement contacter le Help Desk d'Euroclear à l'extension 2424 (Nordics Local CT Service Desk) en cas de perte ou de vol de son appareil. Les opérateurs d'Euroclear tenteront, à distance, de verrouiller et d'effacer de l'appareil les données Euroclear ainsi que les propres données de l'utilisateur, sur demande expresse de ce dernier.

2.3 Messagerie d'entreprise

a. La messagerie d'entreprise Euroclear doit être utilisée avec discrétion et intégrité professionnelles.

b. Les utilisateurs ne doivent ni ouvrir ni sauvegarder sur le disque les e-mails comportant une pièce jointe provenant d'une source inconnue ; ces e-mails doivent être supprimés. L'utilisateur final doit alerter l'équipe CIRT (cirt@euroclear.com) s'il reçoit un e-mail suspect ou une pièce jointe, et ne doit pas les ouvrir.

c. Les informations d'entreprise, de clients et de tiers ne doivent pas être envoyées ou transférées vers des comptes e-mails privés.

d. Les utilisateurs ne doivent pas, délibérément ou par imprudence, propager des logiciels malveillants ou un programme malveillant intentionnellement écrit qui pourraient endommager les réseaux/systèmes d'Euroclear ou ceux appartenant à un tiers.

2.4 Utilisation d'Internet

a. La connexion à Internet est uniquement autorisée par le biais d'installations autorisées et sécurisées fournies par Euroclear.

b. L'utilisateur final doit rester vigilant à l'égard de la menace de virus informatiques. Toute personne suspectant qu'un programme malveillant a été introduit par le biais d'une activité Internet doit immédiatement en informer l'équipe CIRT (cirt@euroclear.com).

c. Les utilisateurs ne sont pas autorisés à utiliser les services Internet pour charger ou transférer les données détenues ou traitées par Euroclear en dehors de l'exercice normal de ses activités. Cela inclut l'utilisation de la messagerie par Internet, les réseaux sociaux, les sites d'hébergement vidéo/audio et les clouds, tels que Dropbox, Google Drive, etc.

2.5 Support amovible

a. Afin de réduire le risque de vol/fuite de données, Euroclear a désactivé les ports USB sur les laptops. Dans les cas exceptionnels, Euroclear peut fournir à l'utilisateur final des clés USB chiffrées sécurisées.

b. L'utilisateur final doit immédiatement contacter le Euroclear Help Desk à l'extension 2424 (Nordics Local CT Service Desk) en cas de perte ou de vol du support amovible.

c. L'utilisateur final doit restituer le support amovible dès qu'il n'en a plus besoin.

d. Le stockage des données sensibles sur les clés USB est interdit.

2.6 Contrôle d'accès et informations d'authentification

a. Le mot de passe doit être facile à mémoriser, mais néanmoins difficile à deviner par les autres (par ex., nom du partenaire, enfants, etc.).

b. L'identifiant et les mots de passe de l'utilisateur ne doivent jamais être partagés et en aucun cas, un employé ne peut emprunter l'identité d'un autre utilisateur.

c. Les mots de passe ne doivent pas être portés à la connaissance d'autres personnes et ne doivent jamais être enregistrés par écrit ou conservés dans un endroit non sécurisé.

d. Si une personne suspecte que son mot de passe a été découvert, elle doit le modifier immédiatement et contacter le Euroclear Help Desk à l'extension 2424 (Nordics Local CT Service Desk).

e. Les mots de passe ne doivent jamais être archivés en texte clair dans des fichiers, tels que docs, scripts, macros etc.

2.7 Lignes directrices relatives au Clear Desk

a. L'utilisateur final doit sécuriser les documents de nature sensible lorsqu'il est loin de son bureau pendant une longue période et à la fin de la journée de travail.

b. Aucun document ne doit être laissé dans les salles de réunion. Il incombe à l'organisateur de la réunion de récupérer tous les documents qui traînent, de nettoyer les white boards et de retirer du tableau les feuilles mobiles utilisées.

2.8 Sécurité physique

a. Portez en permanence votre badge Euroclear de manière visible et comme il se doit dans les locaux d'Euroclear.

b. Annoncez et accompagnez toujours vos visiteurs. Pour annoncer vos visiteurs à Bruxelles (visitors.brussels@euroclear.com).

c. Veillez à ce que personne ne vous suive de près afin d'accéder de manière non autorisée aux locaux d'Euroclear (tailgating).

d. Veuillez signaler toute activité suspecte de ce type aux agents de sécurité (Bruxelles 1200).

2.9 Exigences spécifiques pour les profils admin GTS et GBS

a. Les règles suivantes sont applicables à la communauté du personnel responsable du développement et du support des systèmes d'entreprise :

- Toute activité de navigation doit être effectuée à partir de comptes utilisateurs standard, jamais à partir de compte privilégiés.
- L'utilisateur doit veiller à ce que tous les logiciels téléchargés soient soumis à vérification et à un screening de logiciels malveillants avant l'installation.
- Les logiciels doivent être téléchargés à partir de sites fournisseurs légitimes.

- Il est interdit à l'utilisateur d'accéder à Internet en dehors de canaux définis et approuvés et d'accéder directement à Internet à partir des serveurs de production.

2.10 Sensibilisation et formation en matière de sécurité

a. L'utilisateur doit avoir un état d'esprit orienté sécurité, protéger les données et actifs et compléter tous les modules de sensibilisation obligatoires (sécurité, risque et conformité) dans les délais impartis.

3. Hygiène et sécurité

Dans les locaux d'Euroclear

3.1 Veillez à ce que vos actes ne mettent pas en danger vos collègues ni vous-même.

3.2 Respectez toutes les procédures locales en cas d'urgence.

3.3 Familiarisez-vous avec le système d'alerte incendie et les procédures d'évacuation, y compris les issues de secours des zones que vous fréquentez et les points de rassemblement désignés.

3.4 Participez aux exercices d'évacuation et suivez les procédures d'évacuation requises.

3.5 N'utilisez pas votre équipement électrique personnel dans les locaux sans autorisation préalable et assurez-vous qu'il a passé les tests requis pour les appareils portables.

Matériel, équipement et substances

3.6 Ne déplacez pas les meubles et autres équipements, à moins d'avoir reçu la formation et les instructions à cet effet.

3.7 Ne retirez pas et ne détérioriez pas les équipements et autres appareils fournis pour assurer la protection de l'hygiène et de la sécurité.

3.8 Ne réalisez pas vous-même de réparations sur les installations ou équipements, à moins d'avoir reçu la formation et les instructions à cet effet.

3.9 Utilisez toujours le matériel, les équipements, les subs tances dangereuses, les équipements de transport, les moyens de production ou dispositifs de sécurité conformément aux formations et instructions que vous avez reçues.

3.10 En cas d'exposition à des substances dangereuses pour la santé dans le cadre de vos fonctions, veillez à respecter les exigences de contrôle des substances dangereuses pour la santé.

Que faut-il signaler ?

3.11 Signalez à votre point de contact à Euroclear tous les dommages et risques encourus en matière d'hygiène et de sécurité.

3.12 Informez votre point de contact à Euroclear de toute situation ou question professionnelle qui représente soit un danger grave et imminent, soit une faille dans les mesures d'hygiène et de sécurité prises par Euroclear.

3.13 Signalez immédiatement à votre point de contact à Euroclear tous les accidents, incidents (y compris les « quasi-accidents »), évènements dangereux et maladies à déclaration obligatoire.

3.14 Signalez immédiatement toute défaillance électrique d'un équipement ou matériel électrique portable. L'équipement ou le matériel en question devront être débranchés et un avertissement approprié sera fixé dessus.