

## CONDITIONS PARTICULIÈRES ONLINE BANKING

Helpdesk Online Banking: 02 548 28 00 ou helpdesk@triodos.be

### Art. 1. Définitions

- 1.1 La Banque : la succursale belge de Triodos Bank nv, société anonyme de droit néerlandais, dont le siège social est établi à Nieuweroordweg 1 - 3704 AB Zeist - Pays-Bas, inscrite au registre du commerce d'Utrecht sous le numéro 62 451, et dont la succursale belge est située Rue Haute 139 boîte 3 à 1000 Bruxelles, TVA BE 0450.507.887, RPM Bruxelles, info@triodos.be, www.triodos.be.
- 1.2 Le Titulaire : la personne physique et/ou morale à qui appartient un produit Triodos.
- 1.3 L'Utilisateur : la personne désignée en cette qualité par le Titulaire ainsi que le Titulaire lui-même lorsqu'il a un accès Online Banking.
- 1.4 Conditions Particulières : les Conditions particulières Online Banking.
- 1.5 Online Banking : nom collectif pour les services électroniques bancaires Internet Banking et Mobile Banking.
- 1.6 Internet Banking : le service électronique bancaire relatif aux comptes Triodos accessible par internet au travers d'un navigateur web.
- 1.7 App : l'application mobile "Triodos Banking BE" à télécharger auprès de l'App Store d'Apple ou le Play Store de Google. L'App requiert un Appareil mobile pour pouvoir y être installée.
- 1.8 Appareil mobile : tout smartphone, tablette, ou autres appareils assimilables, ayant une caméra ainsi qu'une fonctionnalité de géolocalisation, et sur lesquels pourraient être installée l'App.
- 1.9 Mobile Banking : le service électronique bancaire relatif aux comptes Triodos accessible au travers de l'App.
- 1.10 Le Nom d'Utilisateur : un nom unique, attribué par la Banque et qui, avec le Mot de passe, donne accès à Online Banking.
- 1.11 Mot de passe : une série de lettres et de chiffres strictement confidentielle et personnelle qui, avec le Nom d'Utilisateur, donne accès à Online Banking et qui est utilisé notamment pour signer en toute sécurité les transactions.
- 1.12 Digipass : Le Digipass est un module physique de sécurité qui, avec le Code PIN, permet l'accès à Online Banking et qui génère une signature électronique afin notamment de signer en toute sécurité les transactions.
- 1.13 Code PIN : code strictement confidentiel et personnel qui, avec le Digipass, donne accès à Online Banking et qui est utilisé notamment pour signer en toute sécurité les transactions.
- 1.14 Code secret : code strictement confidentiel et personnel qui, avec l'App, donne accès à Mobile Banking et qui est utilisé notamment pour signer en toute sécurité les transactions en Mobile Banking.
- 1.15 Ordre(s) : un ordre de paiement envoyé à la Banque au moyen d'Online Banking (des virements vers des comptes nationaux avec ou sans date-mémo, des nouveaux ordres permanents, des modifications à des ordres permanents existants, des virements vers des pays dans la zone SEPA avec ou sans date-mémo).

### Art. 2. Généralités

- 2.1 Les présentes Conditions Particulières sont d'application aux relations entre le Titulaire, le(s) Utilisateurs et la Banque en ce qui concerne Online Banking.
- 2.2 Les Conditions Générales de la Banque sont également d'application aux relations contractuelles entre la Banque et le Titulaire et/ou l'Utilisateur. Le Titulaire et/ou l'Utilisateur déclarent en avoir pris connaissance et en accepter les dispositions.
- 2.3 Dans la mesure où les présentes Conditions Particulières dérogent aux dispositions des Conditions générales de la Banque, les Conditions Particulières prévaudront.

- 2.4 Le Titulaire et/ou l'Utilisateur s'engagent à respecter strictement toutes les instructions de la Banque concernant Online Banking.
- 2.5 La Banque se réserve le droit de modifier ou de compléter les dispositions des présentes Conditions Particulières. Ces modifications seront communiquées par support durable (lettre, extrait de compte, communications électroniques, e-mail, ...) au Titulaire. Le Titulaire a le droit de mettre fin, par support durable et sans frais, au contrat Online Banking, dans les deux mois qui suivent cet avis. Après cette période de deux mois, les Conditions Particulières modifiées sont considérées comme définitivement acceptées. En cas de nouvelles fonctionnalités, le Titulaire peut donner son accord explicite pour accéder immédiatement à Online Banking.
- 2.6 Le Titulaire est tenu d'informer chaque Utilisateur autre que lui du contenu des Conditions Générales et des présentes Conditions Particulières et de leurs modifications ainsi que de toute autre instruction émanant de la Banque et de veiller à ce qu'il les respecte.

### **Art. 3. Accès au service Online Banking**

- 3.1 Internet Banking est proposé sur Internet. En plus de la possession d'au moins une des trois combinaisons suivantes :
- 1) Nom d'Utilisateur et Mot de passe
  - 2) Digipass et Code PIN
  - 3) App et Code Secret
- l'Utilisateur doit disposer d'un ordinateur ou d'un autre appareil répondant aux exigences techniques suivantes :
- accès Internet
  - un navigateur Internet. Sur [www.triodos.be](http://www.triodos.be) vous trouverez quels navigateurs sont supportés.
- 3.2 Mobile Banking est proposé via l'App. L'Utilisateur doit disposer d'un appareil mobile répondant aux exigences techniques suivantes :
- un accès Internet
  - la version la plus récente de App
  - la version la plus récente possible du système d'exploitation de l'appareil mobile. Sur [www.triodos.be](http://www.triodos.be) vous trouverez pour quels systèmes d'exploitation l'App est disponible.
- 3.3 Pour Online Banking, la Banque Triodos procure une aide à la clientèle via un service d'assistance téléphonique au numéro 02 548 28 00, via l'adresse e-mail [helpdesk@triodos.be](mailto:helpdesk@triodos.be), ou via tout moyen de communication électronique disponible au sein d'Online Banking. Cette assistance constitue une obligation de moyen de la Banque Triodos et ne peut garantir une utilisation effective.

### **Art. 4. Accès – Sécurité**

- 4.1 Le Nom d'Utilisateur et le Mot de passe, le Digipass et le Code PIN, ou l'App et le Code secret donnent accès à Internet et Mobile Banking. Ceux-ci sont strictement personnels et non-transmissibles. L'Utilisateur s'engage à ne jamais les noter sous une forme aisément reconnaissable ou utilisable par d'autres personnes.
- 4.2 Le Titulaire et/ou l'Utilisateur sont tenus de conserver la plus stricte confidentialité en ce qui concerne le Nom d'Utilisateur, le Mot de passe, le Code PIN et le Code secret. Ils ne peuvent en aucun cas être transmis à des tiers y compris les membres de leur famille, les personnes habitant sous le même toit, les (co-)Titulaires, les (co-)Utilisateurs et mandataires.
- 4.3 Le Titulaire et/ou l'Utilisateur ne permettront à un tiers d'accéder à son ordinateur ou son appareil mobile qu'après avoir clôturé complètement leur session Internet ou Mobile Banking. Dans le cas de l'ordinateur, ils s'assureront que le Mot de passe n'est pas sauvegardé dans leur navigateur Internet. Dans le cas d'appareils mobiles offrant la reconnaissance faciale ou des empreintes digitales, ils s'assureront qu'il n'y ait que leur propre visage ou empreintes qui soient configurés sur l'appareil mobile et non ceux d'un tiers. Ils ne laisseront jamais leur ordinateur ou appareil mobile sans surveillance durant une session d'Internet ou Mobile Banking.
- 4.4 Le Titulaire et/ou l'Utilisateur s'engagent à prendre les mesures de précaution nécessaires afin d'éviter tout risque de fraude. À cette fin, il est nécessaire de :
- Sécuriser le réseau sans fil utilisé au moyen d'un mot de passe personnel, autre que le mot de passe standard du fournisseur.
  - Vérifier que la session Internet Banking s'effectue dans le cadre d'une liaison sécurisée avec la Banque Triodos.

- S'assurer de l'intégrité de son appareil mobile en ne procédant pas à des opérations de "Root" sur les systèmes d'exploitation Android ou de "Jailbreak" sur les systèmes d'exploitation iOS (c'est-à-dire les appareils de la marque Apple).

Pour plus d'information sur la sécurité informatique, consultez <http://safeonweb.be>

- 4.5 L'accès à Online Banking se fait sous l'entière responsabilité de l'Utilisateur. Ce dernier est par ailleurs tenu à une vigilance accrue en cas d'accès à Internet ou Mobile Banking dans un lieu public ou sur un autre appareil mobile.
- 4.6 Il est fortement recommandé que le Titulaire et/ou l'Utilisateur sécurisent de manière suffisante leurs appareils avant toute utilisation d'Online Banking, au moyen d'un logiciel antivirus, un firewall, de l'utilisation d'applications autorisées, sans élévation des privilèges de l'Utilisateur, verrouillage d'écran de l'Appareil mobile.
- 4.7 Toutes les communications relatives à des tentatives d'hameçonnage (phishing) ou de cybercriminalité doivent être transmises à l'adresse e-mail [phishing@triodos.be](mailto:phishing@triodos.be).

#### **Art. 5. Ordres de paiement – limites**

- 5.1 Avant de donner un Ordre, l'Utilisateur veillera à ce que les limites, telles que mentionnées sous le point 5.2, soient respectées et à ce que le compte soit suffisamment provisionné. La Banque se réserve le droit de refuser l'exécution d'Ordres de virement en cas de provision insuffisante sur le compte.
- 5.2 Pour les Ordres de paiement, certaines limites transactionnelles sont d'application et peuvent varier en fonction du profil du Titulaire et/ou de l'Utilisateur. Plus de détails sur ces limites se trouvent sur [www.triodos.be](http://www.triodos.be). Le Titulaire peut faire modifier ces limites dans le cadre des conditions imposées par la Banque.
- 5.3 Les Ordres ont la même force juridique que des Ordres écrits et signés par le Titulaire et/ou l'Utilisateur.
- 5.4 L'Utilisateur est responsable de l'exactitude de ses Ordres. La Banque ne peut être tenue de vérifier l'exactitude des données de l'Ordre.
- 5.5 Sauf convention contraire, à partir du moment où l'Ordre est réceptionné par la Banque, ni le Titulaire ni l'Utilisateur ne peuvent le révoquer ni l'annuler.
- 5.6 Il est dérogé à l'alinéa qui précède concernant les domiciliations, ordres permanents et virements avec date-mémo qui peuvent être révoqués dans la condition de l'article 6.5 des Conditions Générales en matière de services de paiement.
- 5.7 Tout Ordre doit être validé avant de pouvoir être exécuté par la Banque. Les délais (cut-off time) dans lesquels les Ordres sont traités par la Banque sont repris dans la liste des tarifs de paiements.
- 5.8 La Banque conserve un enregistrement interne des transactions pendant 5 ans à dater de l'exécution des Ordres. La Banque est toujours censée être responsable pour le traitement de ces données. En cas de contestation d'un Ordre que l'Utilisateur a exécuté via Online Banking, la Banque s'engage à fournir la preuve que l'Ordre a été correctement enregistré et comptabilisé et qu'il n'a pas été influencé par un incident technique ou un défaut quelconque, à la condition que le Titulaire ait informé la Banque de la contestation dans les 3 mois de la communication au Titulaire des informations relatives à cette transaction. La mise par écrit ou la reproduction par la Banque des Ordres, ainsi que des autres données enregistrées par la Banque, vaut preuve à part entière entre le Titulaire et la Banque, et ce jusqu'à preuve du contraire à fournir par le Titulaire.

#### **Art. 6. Modifications des paramètres**

- 6.1 L'Utilisateur peut modifier ou accéder à ses paramètres du compte et certaines données personnelles via Online Banking.
- 6.2 Le Titulaire est responsable des modifications introduites dans Online Banking tant par lui-même que par les Utilisateurs.
- 6.3 La Banque se réserve à tout moment le droit de refuser de tenir compte d'une modification lorsqu'elle estimera pour des raisons de sécurité ou autres, qu'un ordre écrit est nécessaire.
- 6.4 Les modifications effectuées via Online Banking ont la même force juridique que si elles avaient été communiquées par un écrit signé, sous réserve de l'application de l'article 6.3.

## **Art. 7. Echange d'informations avec la Banque**

- 7.1 Online Banking peut offrir un service de communication électronique qui permet un échange d'informations entre la Banque et l'Utilisateur de manière sécurisée.
- 7.2 Le Titulaire est responsable des communications électroniques transmises tant par lui-même que par les Utilisateurs.
- 7.3 La Banque se réserve à tout moment le droit de refuser de tenir compte d'une communication transmise par le service de communication électronique, lorsqu'elle estimera pour des raisons de sécurité ou autres, qu'une communication écrite est nécessaire.
- 7.4 Les informations communiquées via le service de communication électronique ont la même force juridique que si elles avaient été communiquées par un écrit signé, sous réserve de l'application de l'article 4.
- 7.5 Conformément aux Conditions Générales, le Titulaire et/ou l'Utilisateur peuvent recevoir leurs extraits de compte sous format électronique via Online Banking.

## **Art. 8. Obligation de notification**

- 8.1 Le Titulaire et l'Utilisateur ont l'obligation d'avertir immédiatement la Banque :
- en cas de perte, de vol, de détournement, d'usage abusif, de falsification d'un Digipass, ainsi que de l'App ou l'appareil mobile sur lequel l'App est installée ;
  - si le Titulaire et/ou l'Utilisateur savent ou supposent que le Nom d'Utilisateur et/ou le Mot de passe et/ou le Code PIN et/ou le Code secret est (sont) connu(s) par des tiers ;
  - si le Titulaire et/ou l'Utilisateur constate des irrégularités comme, par exemple, un Ordre donné par une personne non habilitée.

Le Titulaire et/ou l'Utilisateur peuvent en avvertir la Banque par e-mail ou téléphone au numéro du Helpdesk. Après avoir reçu l'avertissement, la Banque est habilitée à bloquer l'accès à Online Banking.

## **Art. 9. Responsabilité**

- 9.1 La Banque supporte la responsabilité de l'envoi du Digipass, du Code PIN et du Mot de passe.
- 9.2 Dès le premier accès à Online Banking, toutes les manipulations effectuées par un Utilisateur sont effectuées pour le compte et au risque du Titulaire et ce jusqu'au moment où l'usage est dénoncé conformément à l'article 8, hormis l'application des dispositions ci-après.
- 9.3 Jusqu'au moment de la notification, conformément à l'article 8, le Titulaire supporte, à concurrence de 50 EUR, les pertes liées à tout usage non autorisé, abusif ou incorrect du Nom d'Utilisateur et Mot de Passe, du Digipass et du Code PIN, ou de l'App et le code secret, ainsi que pour toutes autres irrégularités qui pourraient être constatées.
- Par dérogation avec l'alinéa précédent, si le Titulaire et/ou l'Utilisateur a agi avec négligence grave ou de manière frauduleuse, tel que notamment le non-respect des dispositions de l'article 4, le Titulaire sera tenu de l'intégralité des pertes mentionnées ci-dessus.
- En cas de vol, détournement, usage abusif, ou autres irrégularités (cf. article 8.1), le Titulaire et/ou l'Utilisateur est tenu de faire immédiatement, à la requête de la Banque, une déclaration auprès de la police et de collaborer en tous points de vue à l'enquête de la police.
- 9.4 Après la déclaration conformément à l'article 8, le Titulaire n'est plus responsable des conséquences de l'usage non autorisé, abusif ou incorrect du Nom d'Utilisateur et Mot de passe, du Digipass et du Code PIN, ou de l'App et le Code secret, sauf si la Banque fournit la preuve que l'Utilisateur a agi de manière frauduleuse.
- 9.5 En dérogation à cette disposition et sauf cas de fraude de l'Utilisateur, le Titulaire n'est pas responsable lorsque la transaction a été effectuée sans identification électronique.
- 9.6 Sauf en cas de faute grave ou intentionnelle de sa part, la Banque ne peut être tenue responsable pour le dommage direct ou indirect causé au Titulaire, à l'Utilisateur ou à un tiers et qui résulterait :
- de l'indisponibilité partielle ou totale d'Online Banking;
  - de la non-exécution ou l'exécution tardive d'un Ordre;

- de la déformation, la non-réception ou la réception tardive, la transmission incorrecte ainsi que la prise de connaissance ou la modification d'un Ordre par des personnes non habilitées;
- du fonctionnement incorrect ou incomplet du programme, de l'installation informatique du Titulaire, de la Banque ou de tiers et/ou du réseau de données, dont Internet, utilisé par le Titulaire;
- d'un usage incorrect d'Online Banking, dont le non-respect des instructions données par la Banque.

9.7 La Banque Triodos peut suspendre temporairement l'accès à Online Banking afin d'apporter des améliorations ou des modifications. Dans la mesure du possible, l'Utilisateur en est informé préalablement.

9.8 Ces dispositions s'appliquent sans préjudice des dispositions particulières prévues à l'article 6 des Conditions Générales de la Banque en matière de Services de paiement.

#### **Art. 10. Résiliation d'Online Banking**

10.1 Si le Titulaire souhaite mettre fin à l'utilisation d'Online Banking par un Utilisateur, il est tenu d'en informer la Banque par écrit ou communication électronique au sein d'Online Banking. La fin de l'utilisation n'est effective qu'à partir de la date mentionnée par la Banque dans sa confirmation écrite.

10.2 Le Titulaire et/ou l'Utilisateur peuvent en tout temps résilier par écrit Online Banking. La résiliation ne prend effet qu'à partir de la date de réception de la résiliation par la Banque.

10.3 La Banque peut également résilier en tout temps Online Banking moyennant le respect d'un préavis de 1 mois.

10.4 La Banque a le droit de bloquer l'utilisation d'Online Banking dans les cas suivants :

- lorsque le Titulaire et/ou l'Utilisateur ne respectent pas les procédures de sécurité ;
- en cas de présomption d'usage abusif, frauduleux ou d'accès non autorisé d'un tiers à Online Banking ;
- en cas de contrat de crédit, en raison du risque sensiblement accru que le Titulaire soit dans l'incapacité de s'acquitter de son obligation de paiement, notamment en cas de faillite, liquidation ou toute autre procédure similaire.

Dans ces cas, la Banque informe le Titulaire et/ou l'Utilisateur, selon les modalités convenues par e-mail, téléphone ou courrier, du blocage d'Online Banking et des raisons de ce blocage et ce, si possible avant qu'Online Banking ne soit bloqué et au plus tard immédiatement après.

10.5 À partir de la date de résiliation, tous les Ordres non-exécutés sont caducs et l'Utilisateur n'est plus habilité à utiliser le Nom d'Utilisateur, le Digipass, ou l'App.

#### **Art. 11. Frais**

11.1 Pour l'utilisation d'Online Banking, la Banque pourra mettre à charge du Titulaire des frais qu'elle portera au débit de son compte. Le tarif peut en être obtenu sur demande ou peut être consulté sur [www.triodos.be/DocumentCenter/Tarifs](http://www.triodos.be/DocumentCenter/Tarifs) et Conditions. Le tarif est en outre communiqué au Titulaire lors de son inscription à Online Banking.

11.2 La Banque se réserve le droit de modifier les tarifs. Toute modification tarifaire sera portée à la connaissance du Titulaire 15 jours avant leur entrée en vigueur. Au cas où le Titulaire ne serait pas d'accord avec cette modification, il peut résilier Online Banking avec effet immédiat.

11.3 Les frais relatifs au réseau de communication, comme les frais d'abonnement à Internet, ainsi que les frais d'acquisition, d'installation, de mise à jour et de fonctionnement de son appareil mobile et de l'App sont à charge du Titulaire et/ou l'Utilisateur.

#### **Art. 12. Droits**

12.1 Tous les droits, y compris les droits d'auteur et de propriété, relatifs à Online Banking et aux programmes y afférents appartiennent à la Banque ou à ses fournisseurs. La Banque ne fournit au Titulaire qu'un droit d'usage non-exclusif et non-transmissible des programmes.

#### **Art. 13. Données personnelles**

- 13.1 En ce qui concerne le traitement et l'échange de données personnelles conformément au Règlement européen n° 2016/679, il est renvoyé à la Charte vie privée, dont le Titulaire déclare avoir pris connaissance.

**Art. 14. Traitement des plaintes et litiges**

- 14.1 Les dispositions des Conditions Générales relatives aux plaintes sont également applicables aux plaintes liées à Online Banking.
- 14.2 Toute plainte du Titulaire et/ou de l'Utilisateur concernant Online Banking doit être adressée le plus rapidement possible à la connaissance de la Banque et adressée par écrit à l'adresse suivante : Banque Triodos, Complaints Management, Rue Haute, 139/3, à 1000 Bruxelles ou [complaints@triodos.be](mailto:complaints@triodos.be).
- 14.3 Lorsque la plainte n'est pas traitée à la pleine satisfaction du Titulaire et/ou de l'Utilisateur, il peut s'adresser à l'ombudsman du secteur financier : Ombudsfin, l'Ombudsman en Conflits Financiers, North Gate II, Boulevard du Roi Albert II, 8, 1000 Bruxelles, tél. 02 545 77 70, [ombudsman@ombudsfin.be](mailto:ombudsman@ombudsfin.be), [www.ombudsfin.be](http://www.ombudsfin.be).
- 14.4 Tout Titulaire et/ou Utilisateur peut également adresser sa plainte à la Direction Générale du Contrôle et de la Médiation près du SPF Economie, PME, Classes Moyennes et Energie, City Atrium, Rue du Progrès, 50, à 1210 Bruxelles, tél. 0800 120 33, fax 0800 120 57, [info.eco@economie.fgov.be](mailto:info.eco@economie.fgov.be). Un formulaire peut être téléchargé sur le site <http://economie.fgov.be>.
- 14.5 Les relations entre la Banque et le Titulaire et/ou l'Utilisateur sont soumises au droit belge. Tout litige entre la Banque et le Titulaire et/ou l'Utilisateur concernant Online Banking sera porté devant les cours et tribunaux de l'arrondissement judiciaire de Bruxelles lorsque cela est permis par les règles du droit judiciaire.