LPTSP

Politique Générale des Services de Confiance

Version 1.1

Date d'entrée en vigueur : 16/06/2021

Technopole de l'Aube en Champagne - 2, rue Gustave Eiffel 10430 Rosières-près-Troyes - France
Tél. : +33 (0)3 25 43 90 78 – Fax : +33 (0)9 81 40 30 08 – www.lex-persona.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

Table des matières

1 Introduction

1.1 Présentation générale

Dans le cadre de son offre de Services de confiance, Lex Persona est amenée à gérer, traiter et partager avec ses clients, partenaires et fournisseurs un capital informationnel onéreux et précieux.

Afin de fournir à ses clients des Services de confiance à des niveaux élevés de sécurité et de traçabilité, Lex Persona définit et met en œuvre des mesures de sécurité afin de :

- Garantir la disponibilité, la confidentialité, l'intégrité de l'information et des moyens de preuve et de contrôle ;
- Garantir le respect des différents codes de conduite adoptés par Lex Persona concernant l'utilisation et la gestion des technologies de l'information et des télécommunications ;
- Se conformer aux lois, règlements, normes nationales et internationales en vigueur en matière de sécurité de l'information ;
- Répondre aux attentes des clients et des partenaires qui dans le cadre des projets émettent des exigences en matière de sécurité de l'information.

Le présent document décrit les mesures mises en œuvre pour répondre aux exigences énumérées dans [ETSI_319401] et constitue le socle de base sur lequel s'appuient les politiques spécifiques des différents Services de confiance de Lex Persona.

1.2 Définitions

Abonné : Entité légale, ayant contracté avec Lex Persona pour bénéficier d'un Service de confiance.

Service de confiance : Service de confiance, opéré par Lex Persona, sous la responsabilité du LPTSP Board.

1.3 Acronymes

AC	Autorité de Certification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
LCR	Liste des Certificats Révoqués
LPTSP Board	Lex Persona Trust Service Provider Board
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
PSI	Politique de la Sécurité de l'Information de Lex Persona

UUID	Universally Unique Identifier (identifiant unique)

1.4 Documents associés

1.4.1 Documents normatifs

[EIDAS]	Règlement nº 910/2014 du 23 juillet 2014 sur l'identification électronique et les Services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive nº 1999/93/CE. http://www.europa.eu
[ETSI_319401]	ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.01_60/en_319401v020201p.pdf
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. https://www.cnil.fr/fr/reglement-europeen-protection-donnees

1.4.2 Procédure de sauvegarde

[PR_SAVE]	Procédure de Sauvegarde des Services de Confiance.

1.4.3 Procédure d'archivage

[PR_ARCHI]	Procédure d'Archivage des Services de Confiance.

2 Responsabilité concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Lex Persona est chargée de la mise en place et de la mise à disposition aux personnes et entités concernées par ses Services de confiance, ainsi qu'au public, des informations devant être publiées (tel que défini par les normes applicables).

Ces informations, dont la présente politique générale, sont publiées sur le site de publication suivant : https://pki2.sunnystamp.com/repository.

2.2 Informations devant être publiées

Les informations devant être publiée dépendent des différents Services de confiance et sont par conséquent listées dans la politique spécifique de chaque Service de confiance.

2.3 Délais et fréquences de publication

Les informations liées au service sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations délivrées et les engagements, moyens et procédures de Lex Persona.

Lex Persona garantit la disponibilité et l'intégrité des informations publiées.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est libre d'accès en lecture.

L'accès en modification au système de publication des informations est strictement limité aux fonctions internes habilitées de Lex Persona et requiert une authentification forte.

3 Gestion des risques

3.1 Analyse de risques

Avant le lancement d'un Service de confiance, Lex Persona effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques, métier et commerciaux. Cette analyse de risque met en exergue, en particulier, les systèmes « critiques » du service.

Suite à cette analyse de risque, Lex Persona sélectionne et met en œuvre des mesures de traitement du risque et les procédures opérationnelles associées en alignant le niveau de sécurité sur le degré de risque.

Les risques résiduels identifiés sont acceptés durant le processus d'homologation du service.

Cette analyse de risque est revue régulièrement, a minima annuellement, et lors de toute évolution significative d'un système ou d'une composante d'un Service de confiance.

3.2 Homologation

Pour un Service de confiance qualifié, le système d'information du service doit être homologué préalablement à la fourniture dudit service. L'analyse de risque est approuvée par la direction de Lex Persona, qui accepte ainsi les éventuels risques résiduels identifiés ; cette phase correspond à l'homologation du système d'information du service.

Cette homologation doit être prononcée au moins tous les trois ans.

Pour un Service de confiance certifié mais non qualifié, la fourniture du service peut être préalable à son homologation.

3.3 Politique Générale de la Sécurité de l'Information

Lex Persona dispose d'une PSI qui est approuvée par la direction.

La PSI est un document de référence, commun à l'ensemble des Services de confiance, qui fixe les enjeux, les principes de gouvernance et les fondamentaux de sécurité. Les directives de sécurité associées définissent les exigences de sécurité à mettre en œuvre ; ces dernières peuvent être définies pour tout ou partie des services et du système d'information de Lex Persona.

La PSI est systématiquement communiquée à l'ensemble des collaborateurs de Lex Persona, et transmise aux sous-traitants concernés ; elle est aussi portée à la connaissance des organismes de certification et de l'organe de contrôle national (ANSSI).

Lex Persona demeure responsable de la conformité globale avec les exigences prévues dans sa PSI, même lorsque certaines fonctions sont mises en œuvre par des sous-traitants. Lex Persona s'assure de la mise en œuvre effective des mesures prévues dans la PSI.

La PSI est revue annuellement ainsi qu'à l'occasion d'un changement majeur du SI, afin de maintenir sa pertinence et son exhaustivité.

Tout changement au niveau de la PSI susceptible d'avoir un impact sur le niveau de sécurité d'un Service de confiance doit être approuvé par le comité de pilotage du service. Les modifications apportées à la PSI sont communiquées aux parties prenantes concernées.

4 Mesures de sécurité non techniques

4.1 Mesures de sécurité physique

4.1.1 Situation géographique et construction des sites

L'ensemble des ressources matérielles des Services de confiance sont hébergées dans deux *datacenters* hautement sécurisés qui respectent les règlements et normes en vigueur et qui fournissent une protection robuste contre les accès non autorisés. Le *datacenter* principal est certifié ISO 27001.

Ces deux *datacenters* sont localisés sur le territoire français et sont séparés l'un de l'autre par une distance en ligne droite supérieure à 100 km.

4.1.2 Accès physique

L'accès au site d'hébergement des Services de confiance est contrôlé et est strictement limité aux seules personnes autorisées à pénétrer dans les locaux. Les personnes non autorisées doivent toujours être accompagnées par des personnes autorisées.

4.1.3 Alimentation électrique et climatisation

Lex Persona assure que les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences des Services de confiance en matière de disponibilité de leurs fonctions.

La baie dédiée à l'infrastructure de Lex Persona dispose d'une alimentation électrique redondante.

4.1.4 Vulnérabilité aux dégâts des eaux

Lex Persona respecte les exigences de protection contre les dégâts des eaux afin de respecter les exigences des Services de confiance en matière de disponibilité de leurs fonctions.

Les *datacenters* sont situés hors zone inondable. Des systèmes de détection de fuites d'eau sont en place.

4.1.5 Prévention et protection incendie

Les risques d'incendie ont été pris en compte pour l'installation des Services de confiance afin de respecter les exigences des Services de confiance en matière de disponibilité de leurs fonctions.

4.1.6 Conservation des supports

Les différents supports utilisés par les Services de confiance sont stockés de manière sécurisée.

Les documents papiers sont conservés par Lex Persona dans des locaux fermés à clés et sont stockés dans un coffre-fort fermé à clé, que seul le responsable ou les personnes autorisées peuvent ouvrir.

Lex Persona assure que les différentes informations nécessaires intervenant dans l'activité des Services de confiance sont listées, et les besoins en sécurité sont définis. Les supports correspondant à ces informations sont gérés en fonction de leur besoin en sécurité.

Lex Persona met en œuvre les moyens nécessaires pour que les supports soient protégés contre l'obsolescence et la détérioration pendant la période de temps durant laquelle les Services de confiance s'engagent à conserver ces informations.

4.1.7 Mise hors service des supports

En fin de vie, les supports sont détruits de manière sécurisée ou réinitialisés en vue d'une réutilisation.

4.1.8 Sauvegardes hors site

Des sauvegardes hors site sont mises en œuvre par les Services de confiance vers un site de secours afin d'assurer une reprise des fonctions des Services de confiance le plus rapidement possible après incident, conformément aux engagements des différents services en matière de disponibilité.

Le site de secours offre un niveau de sécurité au moins équivalent au site principal et garantit notamment que les informations sauvegardées hors site sont protégées en confidentialité et en intégrité au même niveau que sur le site principal.

La procédure de sauvegarde hors site est détaillée dans [PR_SAVE].

4.2 Mesures de sécurité procédurales

4.2.1 Rôles de confiance

Les rôles de confiance suivants sont définis :

- **Security Officer** : Personne chargée de la mise en œuvre et du contrôle de la politique de sécurité des composantes des services. Elle gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Elle est habilitée à prendre connaissance des archives et des journaux d'évènements ;
- **System Operator** : Personne responsable de l'exploitation des applications pour les fonctions mises en œuvre par les composantes et notamment de l'administration fonctionnelle des applications ;
- **System Auditor** : Personne en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. ;
- **System Administrator** : Personne chargée de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Elle assure l'administration technique des systèmes et des réseaux des composantes ;
- **HSM Administrator** : Personne chargée de l'administration des HSM utilisés par les Services de confiance ;
- **Key Holder** : Personne qui assure la confidentialité, l'intégrité et la disponibilité des parts de secrets qui lui sont confiées et qui sont liées à la génération et à la protection des clés privées mises en œuvre par les Services de confiance au sein des HSM.

Les rôles de confiance sont définis et attribués de telle sorte qu'il n'y ait aucun conflit d'intérêt possible entre ces rôles.

4.2.2 Nombre de personnes requises par tâche

En fonction des opérations réalisées, une ou plusieurs personnes avec des rôles différents sont requises.

4.2.3 Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement d'un Service de confiance doit avoir préalablement reçu le rôle correspondant.

L'accès physique est autorisé aux seules personnes qualifiées. L'accès logiciel est protégé par des politiques de sécurité fortes.

4.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les cumuls des rôles suivants par une même personne physique sont interdits :

- Security Officer et System Administrator ;

- Security Officer et HSM Administrator ;
- System Operator et System Administrator ;
- System Operator et HSM Administrator.

4.3 Mesures de sécurité vis-à-vis du personnel

4.3.1 Qualifications, compétences et habilitations requises

Tout le personnel de Lex Persona contribuant aux Services de confiance est soumis à une clause de confidentialité et a notamment signé la charte de sécurité.

Les fonctions demandées à chaque membre du personnel sont compatibles avec ses compétences. Le personnel d'encadrement dispose de l'expertise nécessaire et est familier des procédures de sécurité.

Le LPTSP Board informe toute personne intervenant dans les rôles de confiance :

- Des responsabilités relatives aux services qui lui incombent ;
- Des procédures liées à la sécurité du système et au contrôle du personnel qu'elle doit respecter.

4.3.2 Procédures de vérification des antécédents

Le personnel travaillant pour l'une des composantes des Services de confiance est soumis à une procédure de vérification des antécédents lors de leur prise de fonction. Ces vérifications sont revues tous les 2 ans.

Les vérifications portent sur les points suivants :

- Les éventuelles condamnations en justice de la personne ne devront pas être contraires à ses fonctions ;
- Les rôles de confiance de la personne ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de ses tâches.

4.3.3 Exigences en matière de formation initiale

Le recrutement du personnel des Services de confiance permet de vérifier que chacun dispose de la formation initiale adéquate à la réalisation de ses fonctions.

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met œuvre et doit respecter.

4.3.4 Exigences et fréquence en matière de formation continue

Le personnel recevra une formation adaptée préalablement aux évolutions des Services de confiance (procédures, organisation, application, etc.) concernant la ou les composantes sur lesquelles il intervient.

D'autre part, le personnel des Services de confiance participe annuellement à des séances de formation sur la sécurité des systèmes d'information.

4.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

4.3.6 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation d'un Service de confiance, le LPTSP Board peut lui interdire l'accès aux composantes sur lesquelles elle intervenait.

En outre, si les faits sont avérés, le LPTSP Board pourra prendre à son encontre toutes sanctions disciplinaires adéquates.

4.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences de la section 4.3 sont applicables aux prestataires externes.

4.3.8 Documentation fournie au personnel

Tout le personnel des Services de confiance a accès à des procédures et manuels complémentaires concernant leurs fonctions et leurs responsabilités.

4.4 Procédure de constitution des données d'audit

4.4.1 Type d'évènements à enregistrer

Les événements ci-dessous sont enregistrés de manière manuelle ou automatique :

- Création / modification / suppression de comptes utilisateur et des données d'authentification correspondantes ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes ;
- Les accès physiques ;
- Les actions de maintenance et de changement de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction des supports.

4.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'événements sont systématiquement analysés afin de détecter tout événement anormal (cf. 4.4.8). Les Security Officers sont notifiés de manière journalière des événements significatifs.

4.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés pendant au moins un mois sur site avant d'être archivés pendant une période de conservation indiquée dans la politique spécifique de chaque Service de confiance.

4.4.4 Protection des journaux d'évènements

Le mode de conservation des journaux d'événements protège leur intégrité et leur disponibilité. Ils ne sont accessibles qu'au personnel autorisé à les exploiter.

4.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux d'évènement sont régulièrement sauvegardés et exportés sur le site de secours.

4.4.6 Système de collecte des journaux d'évènements

Sans objet.

4.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

4.4.8 Évaluation des vulnérabilités

Pour détecter les vulnérabilités et plus généralement les anomalies, Lex Persona met en place les contrôles suivants :

- Notification automatique en cas d'ouverture de la baie contenant les équipements des Services de confiance ;
- Analyse quotidienne des journaux d'événements des Services de confiance ;
- Vérification de la disponibilité du site de publication toutes les heures ;
- Réalisation régulière de tests d'intrusion et de scans de vulnérabilités sur les équipements et serveurs des Services de confiance.

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Les vulnérabilités pouvant affecter le système sont étudiées et traitées, par le déploiement de correctifs ou de mesures palliatives, dans des délais cohérents avec la criticité de la menace.

La non application d'un correctif de sécurité disponible est motivée (par exemple, l'introduction de vulnérabilités additionnelles ou d'instabilités considérées supérieures au bénéfice du correctif) et tracée.

Les vulnérabilités critiques affectant le système sont prises en compte dans les 48 heures suivant leur découverte.

4.5 Archivage des données

4.5.1 Types de données à archiver

Les données archivées des Services de confiance sont, au minimum, les suivantes :

- Toutes les versions des CGU, politiques et pratiques ;
- Les accords contractuels entre les Services de confiance et les Abonnés ;
- Les certificats permettant d'identifier les Services de confiance (AC, UH, répondeurs OCSP et LCR) ;
- Les journaux d'évènements des différentes composantes ;
- Les rapports d'audit.

Les données à archiver qui sont spécifiques aux différents Service de confiance sont décrites dans leur politique spécifique.

4.5.2 Période de conservation des archives

La période de conservation des archives est précisée dans la politique de chacun des Services de confiance.

4.5.3 Protection des archives

Les archives, qu'elles soient au format papier ou électronique, sont conservées de façon à garantir leur intégrité et leur confidentialité afin que seules les personnes autorisées puissent y accéder. L'accès aux serveurs d'archivage se fait par des personnes autorisées via un tunnel VPN et nécessite une authentification forte non rejouable avec certificats et OTP.

Les données à archiver sont envoyées pour archivage sur 2 serveurs différents situés sur 2 sites différents, puis stockées signés de manière à garantir leur intégrité et leur authenticité.

4.5.4 Procédure de sauvegarde des archives

Les archives sont périodiquement sauvegardées sous forme électronique et sont exportées sur le site de secours (4.1.1) en conservant le même niveau de sécurité en matière d'intégrité et de confidentialité.

4.5.5 Exigences d'horodatage des données

Voir 5.5.

4.5.6 Système de collecte des archives

Le système de collecte des archives est uniquement interne et est détaillé dans [PR_ARCHI].

4.5.7 Procédures de récupération et de vérification des archives

Les archives, qu'elles soient au format papier ou électronique, peuvent être récupérées dans un délai inférieur à 2 jours ouvrés suite à l'acceptation par Lex Persona de la demande de récupération de l'archive.

Les détails sur les procédures de récupération et de vérification des archives sont décrits dans [PR_ARCHI] et la politique du service concerné.

4.6 Reprise suite à la compromission et sinistre

4.6.1 Procédures de remontée et de traitement des incidents et des compromissions

Lex Persona met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

Une activité anormale peut être le signe d'un incident de sécurité potentiel, par exemple de type intrusion réseau. Toute activité anormale est détectée et remontée aux exploitants. Dans ce but, les composantes matérielles et logicielles sont constamment supervisées et les journaux d'événements sont analysés automatiquement et de façon régulière.

Chaque service de Confiance dispose d'un PCA qui décrit la procédure à exécuter en cas d'incident majeur affectant le bon fonctionnement des Services de confiance.

Un incident majeur tel que la perte, la suspicion de compromission, la compromission ou encore le vol d'une clé privée (AC, UH…), est immédiatement notifié au LPTSP Board qui peut alors décider, si cela est nécessaire, de demander la révocation du certificat concerné.

Dans ce cas, le LPTSP Board notifiera dans les plus brefs délais, et au maximum dans les 24 heures, le point de contact identifié sur le site https://www.ssi.gouv.fr et, concernant les services certifiés ou qualifiés, l'organisme de certification.

En cas d'incident majeur de sécurité ayant un impact important sur des données à caractère personnel, le LPTSP Board notifiera la CNIL et les entités concernées (personnes morales ou physiques) sans délai.

Si l'un des algorithmes utilisés, ou des paramètres associés, devient insuffisant pour son utilisation prévue restante, Lex Persona publiera l'information sur son site Internet et révoquera les certificats concernés.

4.6.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données)

Le PCA définit les procédures de reprise en cas de corruption des ressources informatiques ainsi que les procédures visant à assurer la disponibilité des composantes critiques des Services de confiance.

4.6.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Ce point est couvert par le PCA des Services de confiance.

D'une manière générale, si la clé privée d'une composante est compromise, soupçonnée d'être compromise, perdue ou détruite :

- Le LPTSP Board, après enquête, demande la révocation du ou des certificats concernés ;
- La procédure de révocation est appliquée, avec un arrêt immédiat des services exploitant la clé compromise.
- Les porteurs dont le certificat a été révoqué, les entités avec lesquelles Lex Persona a passé des accords ou d'autres formes de relations établies, sont notifiés dans les plus brefs délais de la révocation ;
- Lex Persona publie sur son site de publication toutes les informations nécessaires (description de l'incident, plan d'action, etc.) ;
- Le LPTSP Board prévient directement et sans délai le point de contact de l'ANSSI https://www.ssi.gouv.fr.

Des mesures similaires sont prises si la robustesse de l'algorithme de la clé privée ou celle des paramètres associés devient insuffisante.

4.6.4 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité de l'activité d'un Service de confiance suite à un sinistre est traitée par le PCA/PRA de ce service qui permet de basculer sur le site de secours. Pour cela le Service de confiance dispose, pour le site principal et le site de secours, d'une architecture redondée pour ses fonctions critiques et gère un stock de matériel de rechange afin de réagir rapidement en cas de de panne matérielle.

Les opérations de bascule et de restauration sont réalisées par des personnes ayant les rôles de confiance adéquats. Les PCA et PRA sont testés au moins une fois par an.

4.7 Fin de vie

Chaque Service de confiance dispose d'une procédure de fin de vie qui lui est propre et qui est vérifiée et maintenue à jour régulièrement.

En cas de cessation définitive de l'activité d'une composante, la procédure de fin de vie correspondante est appliquée.

Chaque procédure de fin de vie est conçue de manière à minimiser l'impact sur les Abonnés et les utilisateurs des Services de confiance et vise à permettre le maintien dans le temps de la vérification des éléments à valeur probante produits par ces services.

5 Mesures de sécurité techniques

5.1 Mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques

Les mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques sont décrites dans les politiques spécifiques des Services de confiance.

5.2 Mesures de sécurité des systèmes informatiques

5.2.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Lex Persona définit les objectifs de sécurité suivants :

- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès, notamment pour implémenter les principes de moindres privilèges, de contrôle multiple et de séparation des rôles) ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- La gestion des droits des utilisateurs est mise en œuvre en prenant en compte les différents rôles identifiés dans le présent document (cf. 4.2.1). Des procédures assurent que l'octroi et le retrait des habilitations s'effectue en accord avec la gestion des ressources humaines ;
- Identification et authentification forte des utilisateurs pour l'accès aux systèmes ;
- Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée ;
- Les informations sensibles sont protégées contre la divulgation, y compris en cas de réutilisation de ressources par des personnels non autorisés ;
- Protection contre toute tentative non autorisée et / ou irrégulière d'accès aux ressources (physique et / ou logique) ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent.

5.2.2 Niveau de qualification des systèmes informatiques

Pas d'exigence.

5.3 Mesures de sécurité liées au développement des systèmes

5.3.1 Mesures de sécurité liées au développement des systèmes

Tous les développements réalisés par Lex Persona et affectant les Services de confiance sont documentés et réalisés via un processus de manière à en assurer la qualité.

La configuration du système des composantes ainsi que toute modification et mise à niveau est documentée et contrôlée.

Lex Persona opère un cloisonnement entre l'environnement de développement et les environnements de préproduction et de production.

5.3.2 Mesures liées à la gestion de la sécurité

Les configurations et les mises à jour des applications sont effectuées de manière sécurisée par le personnel compétent apparaissant dans les rôles de confiance.

5.3.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

5.4 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein des Services de confiance.

Le réseau et ses systèmes sont protégés contre les attaques via des mesures et des objectifs de sécurité identifiés dans l'analyse de risques (3.1).

Le SI est segmenté en réseaux ou zones en fonction de l'analyse de risque, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services.
Les mêmes contrôles de sécurité sont appliqués à tous les systèmes partageant la même zone.
Les accès et les communications sont restreints entre les réseaux et les zones et définis au strict nécessaire pour le fonctionnement du service.

Les connexions et les services inutiles sont explicitement interdits ou désactivés.
Les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la PSI et des politiques et pratiques des Services de confiance.

L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné.
Les systèmes utilisés pour l'administration de la mise en œuvre de la PSI ne doivent pas être utilisés à d'autres fins.

Les systèmes de production du service sont séparés des systèmes utilisés pour le développement et les tests.

La communication vers les HSM n'est établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.

Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service est effectuée par une personne ou une entité ayant les compétences, les outils, l'éthique et l'indépendance nécessaires. Cette analyse donne lieu à un rapport.

Un test d'intrusion sur les systèmes du service est réalisé lors de la mise en place du Service de confiance et après toute évolution majeure de l'infrastructure ou des applications. Ce test est effectué par une personne ou une entité ayant les compétences, les outils, l'éthique et l'indépendance nécessaires, et donne lieu à un rapport.

5.5 Horodatage / Système de datation

Les différents serveurs utilisés par les Services de confiance sont synchronisés au moins une fois par jour avec la même source de temps UTC.

6 Audit de conformité et autres évaluations

6.1 Fréquences et circonstances des évaluations

Avant la première mise en service d'une composante d'un Service de confiance certifié ou qualifié, ou suite à toute modification significative au sein d'une composante, Lex Persona fait procéder à un audit de conformité de cette composante vis-à-vis de sa politique et de ses pratiques déclarées.

Lex Persona réalise des audits internes annuellement, et fait réaliser tous les 2 (deux) ans, par un organisme accrédité, un audit de certification ou de qualification.

6.2 Identités et qualifications des évaluateurs

Lex Persona s'engage à mandater des auditeurs qui sont compétents en sécurité des systèmes d'information et en particulier dans le domaine d'activité de la composante contrôlée.

6.3 Relations entre évaluateurs et entités évaluées

Pour les audits internes, l'auditeur sera nommé par le LPTSP Board et pourra appartenir à Lex Persona, mais devra nécessairement être indépendant du Service de confiance audité.

Pour l'audit de certification, l'auditeur ne devra pas appartenir à Lex Persona ou présenter un quelconque conflit d'intérêt.

6.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante du service (contrôles ponctuels) ou sur l'ensemble de l'architecture du service (contrôles périodiques) ; ils visent à vérifier le respect des engagements et pratiques définies dans la politique du service, ses pratiques déclarées et dans les procédures internes associées.

6.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, des écarts sont levés et Lex Persona propose et implémente des corrections et des actions correctives, avec un planning dépendant de la criticité des impacts des écarts.

Le choix de la mesure à appliquer est effectué par le LPTSP Board et doit respecter ses politiques de sécurité internes.

Un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.

En cas de réussite, le LPTSP Board confirme à la composante contrôlée la conformité aux exigences des politiques et des procédures internes.

6.6 Communication des résultats

Les résultats des audits sont tenus à la disposition de l'organisme de certification et de l'organe de contrôle national.

7 Autres problématiques métiers et légales

7.1 Tarifs

Se référer à la politique de chaque Service de confiance.

7.2 Responsabilité financière

7.2.1 Couverture par les assurances

Lex Persona a souscrit une assurance en responsabilité civile professionnelle couvrant ses prestations de prestataire de Services de confiance auprès d'une compagnie d'assurance.

7.2.2 Autres ressources

Lex Persona dispose des ressources financières suffisantes pour assurer la fourniture de ses Services de confiance conformément à leurs engagements.

7.2.3 Couvertures et garantie concernant les entités utilisatrices

Se référer à la politique de chaque Service de confiance.

7.3 Confidentialité des données professionnelles

7.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les procédures internes des services ;
- Les clés privées mis en œuvre par les composantes des services ;

- Les données d'activation de ces clés privées ;
- Les journaux d'événements des composantes ;
- Les rapports d'audit.

D'autres informations peuvent être classées comme confidentielles ; se référer à la politique de chaque Service de confiance pour plus d'information.

7.3.2 Informations hors du périmètre des informations confidentielles

Se référer à la politique de chaque Service de confiance.

7.3.3 Responsabilités en termes de protection des informations confidentielles

Lex Persona s'engage à traiter les informations confidentielles dans le respect de la législation et de la réglementation en vigueur sur le territoire français.

7.4 Protection des données personnelles

7.4.1 Politique de protection des données personnelles

Lex Persona s'engage à collecter et utiliser les données personnelles en respectant la législation et la réglementation européenne en vigueur relative à la protection des données à caractère personnel.

7.4.2 Informations à caractère personnel

Se référer à la politique de chaque Service de confiance.

7.4.3 Informations à caractère non personnel

Sans objet.

7.4.4 Responsabilité en termes de protection des données personnelles

Lex Persona respecte, pour le traitement et la protection des données à caractère personnel, la loi française nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi nº 2004-801 du 6 août 2004 [CNIL], et au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 [RGPD].

7.4.5 Notification et consentement d'utilisation des données personnelles

Les données personnelles ne sont jamais utilisées, sans le consentement exprès et préalable de la personne, à d'autres fins que celles définies :

- Dans la politique, les pratiques et les CGU du service ;
- Dans l'accord de souscription ou tout accord contractuel.

7.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Les données personnelles peuvent être mis à la disposition de la justice en cas de besoin pour servir de preuve dans le cadre d'une procédure judiciaire.

7.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

7.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par Lex Persona sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerces et de services, dessins et modèles, signes distinctifs et droits d'auteur est sanctionnée par le Code de la propriété intellectuelle.

Lex Persona détient tous les droits de propriété intellectuelle et est propriétaire des documents publiés sur son site.

7.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes des Services de confiance sont les suivantes

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par les politiques et pratiques du service, et les documents qui en découlent ;
- Respecter et appliquer les procédures internes ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par Lex Persona (cf. section 6) et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles ou aux Abonnés ;
- Documenter leurs procédures internes de fonctionnement ;
- Mettre en œuvre les moyens techniques et humains nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité ;
- Avoir des pratiques non-discriminatoires dans leurs politiques et leurs procédures.

7.6.1 LPTSP Board

Le LPTSP Board est représenté par LEX PERSONA. Il est composé des membres suivants :

- Le responsable du LPTSP Board qui est un représentant légal de LEX PERSONA ;

- Des intervenants spécialisés dans le management de la sécurité des systèmes d'information et nommés par le responsable du LPTSP Board.

Les obligations du LPTSP Board sont les suivantes :

- Approuver des politiques et pratiques des services et de leurs évolutions ;
- Conduire l'audit des Services de confiance ;
- Définir et attribuer les rôles de confiance ;
- Gérer la relation contractuelle avec les entités tierces intervenant dans les Services de confiance.

7.7 Limite de garantie

Se référer à la politique de chaque Service de confiance.

7.8 Limite de responsabilité

Se référer à la politique de chaque Service de confiance.

7.9 Indemnités

Sans objet.

7.10 Durée et fin anticipée de validité d'une politique de service

7.10.1 Durée de validité

Se référer à la politique de chaque Service de confiance.

7.10.2 Fin anticipée de validité

Sauf mention contraire, une politique reste en application jusqu'à son remplacement par une nouvelle version.

7.10.3 Effets de la fin de validité et clauses restant applicables

Se référer à la politique de chaque Service de confiance.

7.11 Notification individuelles et communications entre les participants

Après validation, le LPTSP Board publie toute nouvelle version sur le site de publication.

7.12 Amendements

7.12.1 Procédures d'amendements

Le LPTSP Board est responsable de la création, l'approbation, la maintenance et la modification des politiques et pratiques des services.

Seuls les changements mineurs tels que la correction de fautes d'orthographe ou d'erreurs ne remettant pas en cause le sens de la politique peuvent être réalisés par le LPTSP Board sans nécessiter de notification.

7.12.2 Mécanisme et période d'information sur les amendements

Lors de tout changement important, le LPTSP Board informera les acteurs au travers d'un communiqué distribué par voie électronique ou sur son site Internet. Si besoin, une communication par courrier postal pourra être réalisée.

7.12.3 Circonstances selon lesquelles l'OID doit être changé

Si le LPTSP Board juge qu'un changement important est nécessaire, et qu'il a un impact majeur sur le service, il publiera une nouvelle version, portant un nouvel OID.

7.13 Dispositions concernant la résolution de conflits

Les politiques et pratiques des Services de confiance sont soumises au droit français.

Le LPTSP Board met en place une procédure de gestion des incidents qui intègre le règlement des différends.

7.14 Juridictions compétentes

L'ensemble des documents contractuels est soumis à la législation et à la réglementation en vigueur sur le territoire français.

7.15 Conformité aux législations et réglementations

Les politiques et pratiques des services sont conformes à la législation et à la réglementation en vigueur sur le territoire français.

7.16 Dispositions diverses

7.16.1 Accord global

Sans objet.

7.16.2 Transfert d'activités

Sans objet.

7.16.3 Conséquences d'une clause non valide

Sans objet.

7.16.4 Application et renonciation

Sans objet.

7.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

7.17 Autres dispositions

Lex Persona s'assure que les activités qu'elle réalise dans le cadre de ses Services de confiance sont non discriminatoires.