Le Responsable de la certification AFAQ Engagement de service ®	Le Représentant du CLUSIR-LR
Nom : Pascal PREVOST	Nom : Christian FERRAND
Fonction : Responsable de la Branche Services	Fonction : Président
Date : 10/05/2001	Date : 13 mai 2001
Visa : 	Visa : 

Table des matières

I. Le domaine d'application

Le présent référentiel a pour objectif de servir de référence à l'attribution de la marque AFAQ Service Confiance ®aux activités de sauvegarde à distance des données informatiques. Il définit un ensemble d'engagements de service pris par le prestataire portant sur :

- la sécurité des échanges de données,
- la sécurité du stockage des données,
- la contractualisation des résultats concernant la sauvegarde des données et leur restauration éventuelle.

Le présent référentiel définit également les exigences relatives à la maîtrise et au contrôle du respect des engagements. Tous les points présentés dans le présent référentiel doivent être intégralement respectés.

Le présent référentiel s'inscrit dans le cadre de la sécurité des systèmes d'information et concerne plus précisément la sauvegarde à distance des données numériques des disques durs des ordinateurs de bureau ou portables et des serveurs via les réseaux de télécommunications. La sécurité des données constitutives du système d'information de l'entreprise représente un enjeu stratégique. L'altération de ces données peut compromettre l'activité de l'entreprise en cas de sinistre, de vol de matériel, d'acte de malveillance. Le référentiel permet de répondre aux exigences de sécurité des systèmes d'information selon 3 critères : disponibilité, intégrité, confidentialité.

L'élaboration d'un référentiel AFAQ Service Confiance ® sur la sauvegarde à distance de données numériques est motivée par un double constat. En premier lieu, force est de constater que les utilisateurs de postes de travail de type micro-ordinateur ne font que très rarement, voire jamais de sauvegardes de leurs données sensibles. En second lieu, il n'existe pas de normes, ni de référentiels concernant la sauvegarde des données. Par conséquent, aucun référentiel universel n'a été défini sur ce thème. En outre, la sécurité des systèmes d'information s'inscrit dans le cadre d'obligations légales de protection de certaines données.

De trop nombreuses entreprises, en particulier les TPE ou les PME-PMI, sous-estiment les risques informatiques ce qui constitue une menace pour leur pérennité. Le référentiel AFAQ Service Confiance ® contribuera à les sensibiliser aux risques en dotant la communauté d'un référentiel universel, simple, compréhensible et accessible aux « non techniciens » permettant ainsi aux prescripteurs potentiels (Secrétariat d'Etat aux PME, au commerce et à l'artisanat, Secrétariat d'Etat à l'Industrie, Chambres de commerce et d'industrie, Chambres des métiers, Ordres professionnels, banques, assurances...) de jouer un rôle incitatif vis à vis des entreprises en termes de sauvegarde de leurs données.

II. Le contexte général

L'élaboration du présent référentiel est une initiative du CLUSIRLR (Club de la Sécurité des Systèmes d'Information Régional- Languedoc Roussillon) - association loi de 1901 - 10, rue du Professeur Jean Granier 34000 Montpellier.
Le CLUSIR-LR est une structure régionale de relais des actions du CLUSIF (Club de la Sécurité des Systèmes d'Information Français) qui a néanmoins sa propre autonomie. Il offre un cadre dans lequel les acteurs dans le domaine de la sécurité des systèmes d'information, responsables et prestataires de services se rencontrent, échangent leurs points de vue, travaillent et progressent ensemble.
Le rôle du CLUSIR-LR est de favoriser activement les échanges entre utilisateurs et offreurs pour qu'ils puissent partager leurs expériences et leur connaissance de l'offre et de la demande. Il participe avec un certain nombre d'acteurs de la sécurité à la promotion de la sécurité et fait valoir les besoins et contraintes des utilisateurs auprès des instances dirigeantes.

En perspective au présent référentiel, il importe de souligner que la révolution de la société de l'information avec l'explosion d'Internet, des Intranet et Extranet, la croissance considérable des services en ligne dans le monde entier, particulièrement en France et en Europe, et l'accroissement de la bande passante offerte sur les réseaux de télécommunication sont évidemment autant de facteurs favorables à l'interconnexion des micro-ordinateurs et des serveurs. A terme, Internet devrait pouvoir satisfaire tous les besoins d'un utilisateur professionnel ou d'un particulier, en termes de services en ligne ; le développement du commerce électronique en est un exemple évident. L'information devient un enjeu pour la stratégie de développement de l'entreprise.

Les prestataires présents sur le marché de la sauvegarde à distance de données numériques pourront faire certifier par AFAQ leurs engagements sur la base de ce référentiel. Les utilisateurs de ces services disposeront ainsi d'un élément de différenciation des prestataires, la démarche volontaire des prestataires permettant alors d'orienter le choix des utilisateurs.
La certification prévoit une identification claire des bénéficiaires des engagements (toutes les entreprises sont concernées) et des prestataires de service (les candidats à la certification de leurs engagements.

II.1. La sécurité, une nécessité souvent sous-estimée voire négligée.

Les éléments sont réunis pour cette explosion des services, des réseaux, de la communication, des transactions électroniques donc du commerce électronique au sens large. Mais, quid de la sécurité ? Cette sécurité, pourtant indispensable à tout utilisateur, quel que soit le matériel, les logiciels, les applications ou données utilisés! Cette sécurité, besoin élémentaire non satisfait car relevant du syndrome classique de "l'accident qui n'arrive qu'aux autres" et de la confiance excessive dans la technologie.

L'accroissement de la capacité des disques durs des micro-ordinateurs accroît corrélativement la fragilité du système d'information de l'utilisateur face à des risques informatiques en croissance sensible et liés en particulier à l'usage de réseaux ouverts.

Dans le même temps, les lecteurs de disquettes standards ont toujours une capacité de 1,44 méga-octets faisant ainsi croître considérablement le rapport capacité du disque/capacité de la disquette. Ce constat implique de nouvelles réponses au problème de sauvegarde des données que l'on ne peut plus satisfaire raisonnablement avec des disquettes. Certes, en fonction des configurations, des solutions de type streamer ou disque dur externe, lecteur de bandes, sauvegarde au niveau d'un serveur de réseau local, graveur de CD-ROM, disquette de grande capacité... peuvent être mises en œuvre.

Ces solutions éprouvées sont pertinentes dans certains cas ; les unes peuvent être lourdes à mettre en œuvre, d'autres s'adressent à des architectures déjà conséquentes (plusieurs postes connectés sur un réseau local avec une solution de sauvegarde locale) ou à des réseaux d'entreprise. Rarement ces solutions répondent à la problématique d'un micro-ordinateur isolé ou d'un nombre limité de micro-ordinateurs en environnement professionnel et a fortiori d'un micro-ordinateur en environnement domestique. Toutes ces solutions requièrent une intervention active de l'utilisateur.

Quand bien même une solution de sauvegarde locale d'un micro-ordinateur indépendant ou d'un réseau au niveau du serveur serait-elle mise en place, elle ne répond que partiellement à la sécurité du système d'information car la copie de sauvegarde, lorsqu'elle est faite (ce qui est loin d'être une généralité!), n'est la plupart du temps pas délocalisée.

Une question mérite par conséquent d'être posée :

Pourquoi les utilisateurs de postes de travail ne sauvegardent-ils pas leurs données alors qu'elles représentent pour eux une valeur inestimable ?

Nous venons de le voir, il y a parfois inadéquation entre le besoin et l'offre technique. Mais la raison principale tient au fait que jusqu'à présent les offres techniques n'étaient pas entièrement automatisées. Or une opération de sauvegarde est perçue par l'utilisateur d'une part, comme une contrainte n'apportant pas de valeur ajoutée à l'activité principale cœur de métier de l'entreprise, d'autre part comme une perte de temps.

II.2. Les risques ne sont pas des concepts, ils sont une réalité.

La banalisation et la vulgarisation des technologies conduisent progressivement les utilisateurs de ces technologies à en occulter les risques même pour les professionnels avertis. La confiance absolue en la technique risque de conduire à la perte irrémédiable des données sensibles (fichier client, fichier médical, comptabilité...) en cas de sinistre, de vol de matériel, de manipulation hasardeuse, de virus, d'actes de malveillance... La valeur des données est sans commune mesure avec la valeur des matériels ; leur altération peut compromettre l'activité de l'entreprise. En effet, il est prouvé statistiquement que dans les deux ans qui suivent un sinistre majeur (perte totale du système d'information), une entreprise sur deux dépose son bilan.

L'avènement du tout numérique sur les réseaux et l'explosion du « e-business » avec Internet favorisent désormais une offre de service en ligne dans le domaine de la sécurité des systèmes d'information (SI). L'enjeu est d'importance car il s'agit de banaliser, de démocratiser et de rendre accessible à toutes les entreprises une offre de services dans le domaine de la sécurité des SI, ce qui jusqu'à une époque récente n'était guère envisageable que pour les grands systèmes.

II.3. La cible : les entreprises concernées.

L'identification des entreprises passe par leur segmentation en fonction de leur taille au sens de l'INSEE. Il y a en France 2 925 200 entreprises (source INSEE 1995) qui se répartissent en 3 segments :

1. très petites entreprises (TPE) et indépendants 2 720 436 (93%)
2. PME 190 138 (6,5%)
3. grands comptes 14 626 (0,5%)

<u>Les TPE et les indépendants (moins de 10 salariés).</u>

Le premier segment comprend notamment les professions libérales, les artisans, les commerçants. Il s'agit certainement de la population la plus exposée aux risques des TIC (Technologies de l'Information et de la Communication) et paradoxalement la moins outillée et la moins convaincue des actions à entreprendre.

Il convient également de citer certaines catégories d'utilisateurs tels que les télétravailleurs, les cadres "nomades" utilisateurs de micro-ordinateurs portables, les entreprises de type SOHO (Small Office Home Office).

<u>Les PME et les grands comptes.</u>

Les deuxième et troisième segments du marché des entreprises méritent également une attention particulière: il s'agit des entreprises disposant de plusieurs sites géographiques dispersés sur un vaste territoire et concernées par la mise en place d'un intranet. Sur ce type de réseau, des services de sécurité peuvent être proposés dans les mêmes conditions que sur le Web. Ce segment semble peut-être mieux armé que le segment précédent mais il s'agit dans bon nombre de cas d'une simple apparence masquant une réalité contrastée.

II.4. Les prescripteurs.

Le point commun aux prescripteurs potentiels est le souci de la pérennité de l'activité industrielle ou commerciale des entreprises. Sous cet angle là, la problématique du risque des Systèmes d'Information est novatrice : ce risque devient un paramètre au même titre que le risque financier, commercial, technique... dans le business plan d'une start-up, dans l'évolution d'une activité de l'entreprise, dans la gestion quotidienne de l'entreprise tout simplement et dans la relation du chef d'entreprise avec son banquier, son assureur, ses autorités de tutelle.

Les prescripteurs potentiels peuvent être :

- Le Secrétariat d'Etat aux PME, au commerce et à l'artisanat.
- Le Secrétariat d'Etat à l'Industrie.
- Les Chambres de Commerce et d'Industrie (CCI) .
- Les Ordres professionnels.
- Les Chambres des métiers.
- Les Pépinières d'entreprises.
- Les Banques.
- Les Assurances.
- Les Centres de gestion agréés.
- Les Sociétés de capital risque.

...

Au delà de la sensibilisation à la sécurité des Systèmes d'Information, l'objectif est de faire prendre conscience à une communauté la plus large possible que la pérennité des activités de toute nature et des entreprises en général est liée au fonctionnement de systèmes souvent mal maîtrisés, et dans tous les cas, vulnérables.

II.5. Les enjeux.

Il s'agit de sensibiliser les entreprises à la sécurisation de leurs systèmes d'information. De trop nombreuses entreprises, en particulier les TPE ou les PME-PMI, sous-estiment les risques informatiques par manque de moyens ou d'informations, ce qui constituent une menace pour leur pérennité.

Au delà de cette sensibilisation, l'enjeu majeur réside dans l'assimilation de la sécurité des Systèmes d'Information à un facteur de risque pouvant affecter la pérennité de l'entreprise et la continuité de son activité.

Les actions de sensibilisation traditionnelles ont montré leurs limites car la problématique était abordée sous un angle technique ou méthodologique sans que des prescripteurs externes au domaine puisse jouer un rôle incitatif fort, les outils faisant défaut.

L'approche par le référentiel AFAQ Service Confiance ® permet de dépasser ces limites en dotant la communauté des entreprises d'un référentiel universel, simple, compréhensible et accessible aux « non techniciens » permettant ainsi aux institutions de jouer pleinement leur rôle de prescripteur.

Par ailleurs, les certifications de type ISO9000 semblent ne pas prendre suffisamment en compte cet aspect sécurité et qualité des données sauf cas très spécifiques car le plus souvent les données constituant un système d'information ne sont pas comprises dans le périmètre de certification. Aucun référentiel universel n'a par conséquent été défini sur le thème fondamental de la qualité et la sécurité du système d'information de l'entreprise. Il s'agit pourtant d'un des éléments sur lequel reposent de nombreux processus et, in fine, la mémoire et la pérennité de l'entreprise.

II.6. L'offre technique.

Proposer un référentiel déconnecté des réalités technologiques n'aurait guère de sens. Le présent référentiel AFAQ Service Confiance ® est d'autant plus crédible qu'il fait référence à une offre technique disponible sur le marché.

Aujourd'hui, la mise en œuvre d'un service de sauvegarde à distance sur un réseau numérique est désormais possible. Sur le continent nord américain, de nombreuses sociétés proposent de tels services sur Internet via des réseaux téléphoniques classiques ou par des liaisons RNIS / ISDN depuis déjà plusieurs années. Un opérateur de télécoms américain (USWest) propose sur Internet une solution de backup distant (E-Backup) à ses clients moyennant un abonnement mensuel. En France une offre est disponible depuis le début de l'année 1999 et de nombreuses sociétés proposent un tel service. L'objet n'est pas d'assurer la promotion de telle ou telle firme, ni de tel ou tel produit, c'est la raison pour laquelle aucune entreprise de service, ni aucun produit ne seront cités ici. Toutefois, le point commun à ces services est qu'ils sont entièrement automatisés, accessibles à tout utilisateur d'un matériel informatique sans investissement et sans compétence particulière.

L'objectif d'un système de sauvegarde à distance de données numériques est de réaliser automatiquement la sauvegarde des données contenues sur le ou les disques des systèmes informatiques de l'abonné à ce système de sauvegarde et d'externaliser ces sauvegardes de façon à pouvoir disposer d'une copie de sauvegarde valide permettant la reconstruction complète du système d'information de l'abonné en cas de sinistre majeur, de panne ou de dysfonctionnement quelconque. Il s'agit pour le système automatisé de sauvegarde de se substituer à l'utilisateur du système informatique pour faire les opérations de sauvegarde selon une fréquence à définir au cas par cas.

Le système central de sauvegarde comprend un système de traitement qui assure les interfaces avec les systèmes informatiques des abonnés via des réseaux de communications numériques et un système d'archivage situé dans un lieu géographique différent du système de traitement qui assure l'archivage des fichiers sauvegardés en vue d'une restauration éventuelle.
Une connexion est établie entre le système informatique de l'abonné et le système de traitement en mettant en œuvre des fonctions d'identification et d'authentification. Les fichiers à sauvegarder sont ensuite sélectionnés selon qu'ils ont été modifiés ou non depuis la dernière opération de sauvegarde. Ces fichiers font l'objet d'un traitement anti-virus et un traitement de décontamination le cas échéant. Ils sont ensuite chiffrés et compressés pour être transmis au système de traitement qui les transmettra ensuite vers le système d'archivage. Un compte-rendu d'exécution des opérations est alors transmis au système informatique de l'abonné pour l'informer du déroulement des opérations.

Pour de plus amples informations sur le détail des fonctionnalités de ces services de sauvegarde à distance, on pourra se référer à l'annexe (point IX du document).

III. Le contexte réglementaire.

Le présent référentiel s'inscrit dans le cadre de la Certification de Services prévue par les articles L.115-27 à L. 115-33 et R. 115-1 à R. 115-12 du Code de la Consommation.
Au plan normatif, il apparaît qu'il n'existe pas de normes, ni de référentiels concernant la sauvegarde des données, si ce n'est une norme concernant l'archivage électronique sur disque optique numérique de type WORM (Write Once Read Many) qui ne répond pas à la problématique du processus de sauvegarde systématique des données des disques d'ordinateurs (Norme française NF Z 42 - 013 - Archivage électronique - Recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes).

Enfin, les critères d'évaluation de la sécurité des systèmes d'information ITSEC (Information Technology Security Evaluation Criterias) ou la norme ISO 15408 traitant de la sécurité des systèmes d'information n'abordent pas la problématique de la sauvegarde des données numériques ; la démarche consistant à évaluer le niveau de sécurité d'un produit ou d'un système informatique afin de mettre en place une politique cohérente de sécurité.

En termes législatif, il importe de mentionner les textes ayant trait à la sécurité des systèmes d'information qui s'inscrit dans le cadre d'obligations légales de protection de certaines données :

- La loi 78-17 (Informatique et Libertés) du 6 janvier 1978 définit les obligations légales de sécurité concernant tout traitement d'informations nominatives et notamment l'art. 29 sur les précautions à prendre pour préserver la sécurité des informations.
- La convention européenne n°108 du 28 janvier 1981 consacre son art. 7 à la sécurité des données.
- La loi 92-1336 du 16.12.92 prévoit dans son art. 226-17 de lourdes sanctions pénales pour défaut de sécurité dans le traitement d'informations nominatives.
- La loi 78-17 (Informatique et Libertés) du 6 janvier 1978 définit les obligations légales de sécurité concernant tout traitement d'informations nominatives et notamment l'art. 29 sur les précautions à prendre pour préserver la sécurité des informations.
- Le code pénal traite dans ses articles 323-1 à 323-7 des atteintes aux systèmes de traitement automatisé de données.
- Le décret n°98-101 du 24 février 1998 définit les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.
- Le décret n°98-102 du 24 février 1998 définit les conditions dans lesquelles sont agrées les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.
- Le décret n°99-199 du 17 mars 1999 définit les catégories de moyens et de prestations de cryptologie par lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

IV. Les engagements de service.

1. Un prestataire de service parfaitement identifié.
2. Une description précise de la prestation proposée dans un contrat de service en termes d'obligation de résultat par le prestataire.
3. Une description précise des moyens mis en œuvre par le prestataire pour atteindre les objectifs de résultat définis dans le contrat de service.
4. Un archivage de vos données chiffrées (cryptées) dans un lieu sûr.
5. Une hot-line client pour répondre à toutes vos attentes.
6. Une analyse systématique et régulière de vos besoins.
7. Une réponse à vos réclamations en 48 heures maximum.
8. Une évaluation régulière de la satisfaction des clients.
9. Un interlocuteur unique par client.
10. Un respect systématique des délais.
11. Un service disponible en permanence.
12. Un personnel compétent et régulièrement formé à votre service.
13. Une information systématique du client sur l'exécution de la prestation de sauvegarde.
14. Une information immédiate du client, sous forme de message d'alerte, en cas de détection de virus, sur son site, dans ses fichiers.
15. Une information immédiate du client, sous forme de message d'alerte, en cas de détection d'incident ou d'anomalie.
16. Une évaluation régulière des prestations par un organisme indépendant.
17. Une restauration de vos données à la demande.

Voir tableaux ci-après.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
1. Un prestataire de service parfaitement identifié.	Identification du prestataire. Le prestataire indique clairement les informations ci-dessous qui doivent être communiquées au client : - nom commercial, - adresse géographique de son siège social, - nom de l'entité juridique responsable des échanges de données, - adresse géographique complète où un représentant du prestataire peut-être joint, - jours et horaires d'accueil téléphonique ; durant ces périodes, l'accueil ne peut être assuré par un répondeur, - numéros d'enregistrements légaux ou professionnels, - adresse électronique, numéro d'enregistrement TVA, - nom des personnes habilitées à avoir accès aux informations suivantes : contenu du contrat, nature des données à sauvegarder, modalités de sauvegarde, clés de chiffrement, données elles-mêmes. L'ensemble de ces informations concerne le prestataire qui assume la responsabilité de l'ensemble de la prestation. Dans l'hypothèse où le prestataire ferait appel à un sous-traitant pour tout ou partie de la prestation, le prestataire en informe le client et lui demande son approbation Le prestataire précise dans le contrat de service la mention suivante : « Le prestataire garantit qu'en aucun cas les informations du client ne seront accessibles à qui que ce soit sans son autorisation expresse ». Par ailleurs, le prestataire fait explicitement référence aux articles 323-1 à 323-7 du code pénal traitant des atteintes aux systèmes de traitement automatisé de données.	Contrat de service décrivant précisément tous ces points. Dossier client.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
2. Une description précise de la prestation proposée dans un contrat de service en termes d'obligation de résultat par le prestataire	Description de la prestation dans un contrat de service Le contrat de service doit comprendre au minimum les éléments suivants : - Identification du système à sauvegarder. - Identification des données à sauvegarder (taille, organisation...). - Dates et horaires des sauvegardes ou fréquence. - Engagement de restauration des données. - Obligations contractuelles du client et du prestataire. - Définition de la prestation et en garantir l'exécution dans le cadre d'un contrat de service. - Engagement de performance de réalisation de sauvegarde (immobilisation de la donnée) et de restauration en fonction du volume. - Traçabilité de l'exécution de la prestation en apportant les preuves, étape par étape. - Description des résultats de l'exécution dans un document référencé dans le contrat, selon une périodicité à définir avec le client. - Information du client en temps réel de tout événement concernant l'exécution de la prestation. - Mesure régulière de l'exécution de la prestation (comptes rendus d'exécution des sauvegardes et des restaurations), selon une périodicité à définir avec le client. Le contrat de service fait explicitement référence au présent référentiel qui lui est annexé. A l'expiration du contrat de service, le prestataire s'engage à restituer au client ses données sous une forme et un support préalablement définis dans le contrat de service; par ailleurs, le prestataire s'engage à détruire les données archivées du client sur le site du prestataire à la fin dudit contrat de service.	Contrat de service décrivant précisément tous ces points. Dossier client.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
3. Une description précise des moyens mis en œuvre par le prestataire pour atteindre les objectifs de résultat définis dans le contrat de service.	Information du client sur les moyens mis en œuvre pour assurer la prestation Description des moyens techniques et humains, garanties en terme de sécurité des équipements et description des composants techniques. Description des menaces que doit contrer le système du prestataire, description des mesures de sécurité prévues et justification de leur adéquation aux menaces potentielles. Le prestataire s'engage à faire bénéficier le client des progrès techniques permanents dans le domaine de l'informatique et des télécommunications. ● Moyens humains : Correspondant nommément désigné par le prestataire pour répondre aux sollicitations du client. ● Moyens matériels : - Système informatique de l'abonné comprenant notamment un ou plusieurs disques. - Réseau numérique de communication. - Système central de sauvegarde comprenant deux sites géographiques distincts reliés par un réseau numérique de communication : - Système de traitement des données transmises. Système d'archivage comprenant des mémoires de masses de grande capacité. - Chiffrement (cryptage). ● Moyens logiciels : - Anti-virus dans le système informatique du client. - Chiffrement (cryptage). - Compression des données. - Sauvegarde automatique.	Contrat de service décrivant précisément tous ces points. Dossier client.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
4. Un stockage de vos données chiffrées (cryptées) dans un lieu sûr.	L'opération de stockage consiste à mettre en mémoire les données traitées. Elle peut être réalisée par l'intermédiaire d'un robot ou d'un automate de gestion de cartouches magnétiques, par un système de gestion mécanique de multiples disques (juke-box). Le système de stockage est localisé dans une chambre forte du type de celles qui sont utilisées dans le domaine bancaire. Cette chambre forte est adaptée à résister à de nombreuses agressions et elle est dotée de nombreuses alarmes et de nombreux moyens de surveillance. En dehors des opérations d'installation ou de maintenance, aucune personne n'est habilitée à pénétrer dans la chambre forte. Les fichiers à sauvegarder font l'objet d'une opération de chiffrement avec un système de chiffrement à clé publique ou privé conforme à la législation en vigueur. L'opération de chiffrement consiste à substituer à un ensemble de données que l'on veut protéger un texte inintelligible pour quiconque ne connaît pas l'algorithme et les paramètres de chiffrement.	Contrat de service. Dossier client.
5. Une hot-line client pour répondre à toutes vos attentes.	Le prestataire met à la disposition de ses clients une hot-line, accessible selon des horaires et des modalités précisés dans le contrat de service, afin de répondre à toutes questions et sollicitations des clients concernant la prestation. Le prestataire s'engage à résoudre dans un délai fixé contractuellement tout dysfonctionnement intervenant dans le déroulement de la prestation. En aucun cas le délai d'intervention ne doit excéder 12 heures. Les appels des clients sont enregistrés dans une base de données, ils sont horodatés. Chaque réponse apportée à un appel client est également enregistrée et horodatée.	Contrat de service. Dossier client avec la copie d'un fichier informatique précisant l'heure de début de l'intervention, l'heure de fin ainsi que la nature de l'intervention. Réponse au client.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
6. Une analyse systématique et régulière de vos besoins.	Le prestataire met en place un dispositif d'analyse systématique et régulier des besoins des clients en leur adressant par exemple un questionnaire d'évaluation de leurs besoins selon une périodicité annuelle. D'autres moyens d'évaluation des besoins pourront être mis en œuvre comme par exemple : - un entretien personnalisé régulier, - un contact sur site, - une revue de contrat initial … Chaque questionnaire envoyé à un client est enregistré et daté. Les réponses des clients sont également enregistrées. Elles font l'objet d'une analyse et d'un traitement permettant d'optimiser les prestations et plus généralement de répondre aux besoins exprimés.	Questionnaire client. Compte rendu d'entretien clients. Compte rendu de revue de contrat.
7. Une réponse à vos réclamations en 48 heures maximum.	Le prestataire met en place une organisation définie dans le contrat de service pour gérer les réclamations des clients. Chaque réclamation fait l'objet d'un enregistrement et d'un traitement aboutissant à une réponse écrite au client dans un délai de 48 heures. Les réclamations des clients sont enregistrées dans une base de données, elles sont horodatées. Les réclamations font l'objet d'une analyse et d'un traitement ayant pour objectif d'apporter une solution au problème posé. Chaque réponse apportée à une réclamation d'un client est également enregistrée et horodatée. Le prestataire met en place un indicateur de performance relatif au respect du délai de réponse aux réclamations	Courrier de réclamation du client. Courrier de réponse du prestataire. Taux de réponse aux réclamations dans les délais

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
8. Une évaluation régulière de la satisfaction des clients.	Le prestataire défini les modalités d'une enquête de satisfaction des clients afin de mesurer le niveau de satisfaction des clients, par rapport au respect des engagements de service par le prestataire. La périodicité de ces enquêtes est précisée dans le contrat de service, à savoir tous les 6 mois. Une analyse des points forts et des points faibles est réalisée, ainsi que la mise en œuvre et le suivi d'un plan d'amélioration. Le prestataire procède à l'enquête de satisfaction des clients sur un panel représentatif de ces derniers. Chaque enquête de satisfaction envoyée à un client est enregistrée et datée. Les réponses des clients sont également enregistrées. Elles font l'objet d'une analyse et d'un traitement permettant d'optimiser les prestations et plus généralement de répondre aux besoins exprimés.	Questionnaire de satisfaction. Résultats d'enquête de satisfaction

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
9. Un interlocuteur unique par client.	Le prestataire désigne pour chaque client un correspondant nommément désigné. Il communique au client toutes les informations concernant ce correspondant (nom, adresse, n° de téléphone, n° de fax, adresse e-mail, heures de présence, boîte vocale en cas d'absence) : toutes ces informations sont consignées dans le contrat de service.	Contrat de service décrivant précisément tous ces points. Dossier client.
10. Un respect systématique des délais.	Le prestataire s'engage contractuellement à effectuer les prestations décrites dans le contrat de service en respectant les horaires de début des opérations ainsi que leur durée définis en accord avec le client. Le prestataire met en place un indicateur de performance relatif au respect des délais.	Contrat de service décrivant précisément tous ces points. Le dossier client contient la copie d'un fichier informatique précisant pour chaque opération l'heure de début de la prestation ainsi que sa durée. Nombre mensuel d'interventions hors délais contractuels
11. Un service disponible en permanence.	Outre son engagement de moyens conformément à l'engagement n° 3, le prestataire s'engage sur leur disponibilité aux heures convenues pour les opérations de sauvegarde du système du client mais aussi en cas de demande d'une opération de restauration des données de la part du client. Le service du prestataire est disponible 24 heures sur 24 et 7 jours sur 7. En cas d'indisponibilité le client est prévenu immédiatement afin de ne pas perturber le déroulement de la prestation de service. Le prestataire met en place un indicateur de performance relatif à la disponibilité de son service.	Contrat de service décrivant précisément tous ces points. Dossier client. Taux mensuel d'indisponibilité du service

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
12. Un personnel compétent et régulièrement formé à votre service.	Le prestataire s'assure que son personnel a bien les compétences requises pour réaliser les tâches dont il a la responsabilité et assure le maintien de ses compétences. Il s'engage à ce que l'information soit bien diffusée de manière appropriée au sein de son entreprise. Le prestataire s'engage sur la mise en œuvre d'un plan annuel de formation portant sur les exigences relatives aux engagements de service du présent référentiel. Il s'engage à ce que tout nouveau personnel soit formé sur les engagements du présent référentiel. Toutes les formations suivies par les personnels seront enregistrés dans un document spécifique. Chaque employé signe impérativement un engagement de confidentialité relativement à ces activités au sein de l'entreprise de service qui l'emploie.	Document d'information sur les systèmes exploités à la disposition des personnels employés par le prestataire. Pour chaque poste de travail, description d'un plan de formation. Description précise du cursus suivi pour tout titulaire d'un poste de travail. Attestations de formation suivie par les personnels. Engagement de confidentialité du personnel.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
13. Une information systématique du client sur l'exécution de la prestation de sauvegarde.	A l'issue de chaque opération de sauvegarde des données du client, le prestataire s'engage à adresser au client un compte-rendu d'exécution de l'opération précisant : ● le résultat de la sauvegarde, ● le résultat de l'éventuelle détection de virus, ● le résultat de l'éventuelle décontamination, ● la fin des opérations de réception des fichiers, ● la liste des fichiers sauvegardés, ● les heures de début et de fin de la sauvegarde. L'information se fait par tout moyen précisé dans le contrat de service en accord avec le client (fax, e-mail, message émis par le système de sauvegarde sur l'imprimante du client). Le prestataire s'engage à prévenir le client lorsque les fichiers devant être sauvegardés sont stockés dans le centre de sauvegarde du prestataire. L'information se fait par tout moyen précisé dans le contrat de service en accord avec le client (appel téléphonique, fax, e-mail, message émis par le système de sauvegarde sur l'imprimante du client).	Contrat de service décrivant précisément tous ces points. Dossier client. Compte-rendu d'exécution.
14. Une information immédiate du client, sous forme de message d'alerte, en cas de détection de virus, sur son site, dans ses fichiers	Lors de l'opération de sauvegarde des fichiers, le prestataire s'engage à informer immédiatement le client si un virus a été détecté dans lesdits fichiers sur le site du client. L'information se fait par tout moyen précisé dans le contrat de service en accord avec le client (fax, e-mail, message émis par le système de sauvegarde...) Corrélativement à la détection d'un virus, le prestataire peut mettre en œuvre des fonctions de décontamination des données du client à sa demande. La détection d'un virus sur le site du client entraîne l'arrêt des opérations de sauvegarde.	Contrat de service décrivant précisément tous ces points. Dossier client. Compte-rendu d'incident.

Engagement de service	Détail de l'engagement	Documents de référence et enregistrement
15. Une information immédiate du client, sous forme de message d'alerte, en cas de détection d'incident ou d'anomalie.	Dans l'hypothèse où un incident ou une anomalie survient au cours de la sauvegarde, le prestataire s'engage à en informer le client dans un délai de 2 heures par tout moyen précisé dans le contrat de service en accord avec le client (fax, e-mail, message émis par le système de sauvegarde sur l'imprimante du client).	Contrat de service décrivant précisément tous ces points. Dossier client. Compte-rendu d'incident.
16. Une évaluation régulière des prestations réalisées par un organisme indépendant.	Lors de la mise en œuvre du service de sauvegarde à distance, une vérification de conformité est réalisée, dans un délai d'un mois, par un organisme indépendant afin de vérifier si la prestation respecte les engagements du présent référentiel. Par la suite, une vérification de conformité semestrielle des prestations de service de sauvegarde à distance est réalisée par le même organisme indépendant afin de vérifier si la prestation respecte toujours les engagements du présent référentiel. Un relevé des écarts éventuels par rapport au présent référentiel est effectué et consigné dans un dossier de vérification de conformité. Le résultat de chaque vérification de conformité est communiqué au client ainsi qu'au prestataire. Si aucun écart n'est constaté à l'issu de la vérification de conformité, l'organisme indépendant délivre à l'entreprise évaluée un document de conformité valable pour une période de 6 mois, jusqu'à la vérification de conformité semestrielle suivante. Ces vérifications de conformité ne donnent lieu à aucune facturation pour le client.	Résultats de vérification de conformité. Dossier client.
17. Une restauration de vos données à la demande	Le prestataire s'engage à restaurer les données du client sur sa demande. La demande du client est conforme aux clauses du contrat de service.	Contrat de service décrivant précisément tous ces points. Dossier client.

V. Les dispositions d'organisation.

Le prestataire d'un service de sauvegarde à distance de données numériques a défini une organisation qui lui permet d'assurer la continuité du respect de ses engagements de service.
Le prestataire désigne un RSSI (Responsable Sécurité des Systèmes d'Information) et précise ses attributions. Ses autres responsabilités, s'il en a, ne doivent pas d'interférer avec la Sécurité des Systèmes d'Information (par exemple on considère souvent qu'il n'est pas sain qu'un administrateur systèmes soit également RSSI).

V.1. Responsabilité.

Le prestataire a défini les responsabilités de toute personne dont l'activité a une incidence sur le respect des engagements de service dans un organigramme, ainsi que dans les définitions de fonctions correspondantes. Il convient de préciser que lesdites responsabilités sont définies par écrit.
Le contrat de service de sauvegarde / restauration doit comporter une description précise de la prestation afin de retracer fidèlement l'exécution des processus techniques mis en œuvre.
Le prestataire garantie la confidentialité des données qui lui sont confiées par engagement. Il garantit la mise en œuvre d'une application informatique nécessaire à la protection des données confiées et des mesures adaptées au contrôle de la fiabilité des matériels et des logiciels, de la capacité de résistance aux atteintes accidentelles ou volontaires.

V.2. Organisation documentaire.

L'organisation documentaire comporte d'une part les documents de référence servant à mettre en œuvre les différents éléments du référentiel et d'autre part les enregistrements apportant la preuve de cette mise en œuvre.

Les principaux documents et enregistrement sont définis dans le chapitre IV, au regard de chaque engagement de service concerné.

Le contrat de service doit définir avec la plus grande précision les obligations du prestataire et particulièrement les points suivants :

- Description de la prestation.
- Définition de la prestation et garantie de son exécution.
- Information du client sur les moyens mis en œuvre par le prestataire.
- Information du client sur les résultats de l'exécution de la prestation.
- Désignation d'un interlocuteur client unique.
- Gestion des réclamations des clients.
- Analyse des besoins des clients.
- Evaluation de la satisfaction des clients.

Les documents à disposition du personnel réalisant de prestation de service de sauvegarde à distance de données numériques sont les suivants :

- Document d'exploitation précisant les modalités techniques de fonctionnement des systèmes mis en œuvre pour réaliser la prestation.
- Contrat de service
- Dossier nominatif par client précisant les contraintes spécifiques à chaque client
- Planning d'exécution des opérations de sauvegarde
- Document de suivi des opérations de sauvegarde dans lequel sont consignés tous les événements concernant la sauvegarde
- Document de suivi des opérations de restauration dans lequel sont consignés tous les événements concernant la restauration

La traçabilité de l'exécution des différentes opérations techniques automatisées est réalisée grâce à l'impression de fichiers « log » qui sont des fichiers internes au système informatique. Ces fichiers permettent d'obtenir, par impression sur des documents référencés prévus à cet effet, une liste d'opérations avec pour chaque opération des informations caractérisant l'opération et notamment un compte rendu d'exécution de l'opération.

Les documents sont établis, diffusés et mis à jour selon des dispositions définies par écrit.
La liste des enregistrements et leurs modalités de gestion sont définis par écrit.
D'une façon générale, toute modification des dispositions prises dans le cadre du référentiel (changement de personne, d'organisation, de matériels, de logiciels…) doit être portée sans délai à la connaissance du client, accompagnée des justifications nécessaires établissant que cette modification n'amoindrit pas la sécurité.

V.3. Formation du personnel.

Chaque prestataire d'un service de sauvegarde à distance de données numériques assure et maintien à jour l'information et les compétences de son personnel.

La formation concernant les engagements relatifs au présent référentiel est assurée dans le cadre d'une structure spécialisée dans le domaine de la sécurité des systèmes d'information.

Afin de s'assurer de la bonne mise en œuvre des pratiques liées aux engagements du présent référentiel, le prestataire s'assure que :

- le personnel a bien les compétences requises pour réaliser les tâches dont il a la responsabilité et assure le maintien de ces compétences,
- l'information est bien diffusée de manière approprié au sein de l'entreprise prestataire,
- la formation nécessaire est bien dispensée afin d'assurer une garantie sur le maintien du respect des engagements.

L'entreprise prestataire doit mettre en œuvre un plan annuel de formation portant sur les exigences ci-dessus et plus particulièrement :

- l'accueil téléphonique pour la mise en œuvre des garanties, du traitement des réclamations et erreurs de l'offre de service après-vente,
- la formation de tout nouveau personnel sur les engagements relatifs au présent référentiel,
- les formations sont enregistrées.

VI. Les modalités de suivi et de pilotage du respect des engagements

VI.1. Les audits internes

Le prestataire d'un service de sauvegarde à distance de données numériques réalise un audit interne deux fois par an (dont un avant l'audit de certification).

Ces audits internes permettent la vérification du respect :

- des engagements,
- des dispositions d'organisation décrites dans le présent référentiel.

L'organisation de l'audit interne est placée sous la responsabilité du responsable qualité qui établit le programme d'audit et désigne les auditeurs internes.
Ces audits sont réalisés par des personnes qualifiées et indépendante de l'activité auditée.
Pour être qualifiés, les auditeurs internes doivent avoir suivi une formation à l'audit qualité.
Les audits s'effectuent selon des supports définis. Les éventuels écarts relevés lors d'un audit interne font l'objet d'un plan d'amélioration, mis en œuvre et suivi par le responsable qualité.

VI.2. Le traitement et le suivi des réclamations clients

Toute réclamation fait l'objet d'un enregistrement puis d'une réponse écrite dans un délai de **48 heures**.

VI.3. Les enquêtes de satisfaction

Des enquêtes sont réalisées au moins **2 fois par an** pour évaluer la satisfaction des clients quant au respect de chacun des engagements de service du présent référentiel..
Une analyse des points fort et des points faibles est réalisée, ainsi que la mise en œuvre et le suivi d'un plan d'amélioration.

VI.4. Le bilan annuel

Un bilan est effectué au moins **1 fois par an**. Ce bilan a pour objet :

- d'examiner l'ensemble des données reflétant la qualité de ce service et le respect des engagements à partir de l'analyse :
  - des indicateurs mis en place :
    - taux de réponse aux réclamations dans les délais,
    - taux mensuel d'indisponibilité du service,
    - nombre mensuel de dysfonctionnements,
    - nombre mensuel d'interventions hors délais contractuels
  - des enquêtes de satisfaction,
  - des audits internes,
  - des réclamations,
  - des besoin en formation.
- de fixer des plans d'actions correspondants fixant les mesures correctives qu'il convient d'entreprendre pour remédier aux écarts constatés.

Le bilan annuel est diffusé à l'ensemble du personnel concerné.

VII. Les modalités de communication.

Les modalités de communication ci-dessous s'appuient sur l'article 10 du décret n°95-354 du 30 mars 1995 (article R115-10 du code de la consommation) et sur l'avis du Conseil National de la Consommation relatif à la certification de service (BOCCRF du 31/12/1998).

Lorsque le prestataire d'un service de sauvegarde à distance de données numériques fait référence à la certification, il doit distinguer 2 types de supports :

1. Supports de communication sur la certification de service :

Il s'agit :

. Du certificat AFAQ

. De tout support dont l'objet est la certification de service

Ces supports mentionnent obligatoirement :

- le domaine d'activité donnant lieu à des engagements de service certifiés,
- le logo « **AFAQ Service Confiance ®** »,
- l'adresse d'AFAQ : « BP 40 - 92224 BAGNEUX CEDEX »,

- le nom du référentiel : « **Sauvegarde à distance de données numériques** » et son code REF-118-01,
- les principaux engagements de service certifiés :

Un prestataire de service parfaitement identifié.
Une description précise de la prestation proposée dans un contrat de service en termes d'obligation de résultat par le prestataire.
Une description précise des moyens mis en œuvre par le prestataire pour atteindre les objectifs de résultat définis dans le contrat de service.
Un archivage de vos données chiffrées (cryptées) dans un lieu sûr.
Une hot-line client pour répondre à toutes vos attentes.
Une analyse systématique et régulière de vos besoins.
Une réponse à vos réclamations en 48 heures maximum.
Une évaluation régulière de la satisfaction des clients.
Un interlocuteur unique par client.
Un respect systématique des délais.
Un service disponible en permanence.
Un personnel compétent et régulièrement formé à votre service.
Une information systématique du client sur l'exécution de la prestation de sauvegarde.
Une information immédiate du client, sous forme de message d'alerte, en cas de détection de virus dans ses fichiers.
Une information immédiate du client, sous forme de message d'alerte, en cas de détection d'incident ou d'anomalie.
Une évaluation régulière de vos prestations par un organisme indépendant.
Une restauration de vos données à la demande.

Le prestataire d'un service de sauvegarde à distance de données numériques assure une information systématique de ses clients et de ses prospects concernant les engagements de service au moyen d'un support de communication, tel que :

- une plaquette envoyée à tous ses clients ou prospects,
- une lettre d'information adressée 4 fois par an à ses clients,
- une information disponible sur le site Internet du prestataire de service.

2. Supports de communication institutionnelle ou d'information générale sur l'entreprise.

Sur tout autre document de communication à caractère institutionnel ou d'information générale sur l'entreprise (carte de visite, papier à entête…) doivent apparaître au minimum les éléments suivants :

- le logo « **AFAQ Service Confiance ®** »,
- l'adresse d'AFAQ : « BP 40 - 92224 BAGNEUX CEDEX »,
- le nom du référentiel : « **Sauvegarde à distance de données numériques** », ou son code REF-118-01
- lorsque le support le permet, il est préconisé de faire figurer un extrait de la liste des principaux engagements de service ou les modalités d'obtention des supports de communication sur la certification de service.

Cette communication s'effectue dans le respect du « Règlement d'utilisation de la marque AFAQ Engagement de Service ® et AFAQ Service Confiance ® » (DG/J/0649).

VIII. Le glossaire.

- Fichier "Log" : Du verbe anglais "TO LOG" qui signifie "consigner".
  Fichier dans lequel sont enregistrés les événements successifs au déroulement d'un programme afin d'obtenir une trace.
- Sauvegarde : Ensemble de mesure physiques ou opérationnelles permettant d'assurer la protection des données par copie de celles-ci sur un autre support.
- Back-up : (Secours de).
  Qualifie une procédure, une méthode ou un ordinateur utilisé en cas de défaillance de la procédure, de la méthode ou de l'ordinateur principal.
- Virus informatique : Série d'instructions regroupées sous forme d'un programme capable de se reproduire dans un ordinateur et d'infecter d'autres programmes.
- Authentification : Vérification qu'un utilisateur ou un système est bien celui qu'il prétend être.
- Identification : Vérification de l'identité d'un utilisateur ou d'un système.
- Chiffrement (Cryptage) : Le chiffrement consiste à substituer à un ensemble de données que l'on veut protéger un texte inintelligible pour quiconque ne connaît pas l'algorithme et les paramètres de chiffrement.

IX. Annexe : un exemple de prestation de sauvegarde à distance.

Il importe de préciser que les fonctions décrites ci-après explicitent les caractéristiques d'un dispositif et d'un procédé de sauvegarde à distance de données numériques qui peuvent être proposés par des prestataires de services certifiés **AFAQ Service Confiance ®** sur la base des engagements de service du présent référentiel.

Liste des fonctions

1. Déclenchement automatique de l'exécution de la prestation
2. Numérotation automatique sur un réseau de télécommunications
3. Sécurisation de la connexion par identification et authentification des deux parties : le client et le prestataire.
4. Identification des fichiers modifiés depuis la précédente sauvegarde.
5. Sélection automatique des fichiers à sauvegarder.
6. Lecture automatique des données à sauvegarder.
7. Détection automatique de virus informatique dans les fichiers à sauvegarder.
8. Décontamination automatique de tous les fichiers si un virus a été détecté.
9. Sécurisation des données par chiffrement (cryptage).
10. Réduction de la taille des données par compression.
11. Transmission automatique des données sur un réseau de télécommunications.
12. Réception des données et traitement par le système central du prestataire.
13. Archivage et stockage sécurisés automatiques des données dans un lieu distant.
14. Transmission automatique d'un accusé de réception des données au système informatique du client par le système central du prestataire.
15. Transmission automatique d'un compte rendu d'exécution de la prestation au système informatique du client par le système central du prestataire.
16. Transmission automatique d'une information de détection d'anomalie au système informatique du client par le système central du prestataire .
17. Marquage automatique des fichiers sauvegardés.
18. Déclenchement automatique de l'opération de restauration sur demande du client.
19. Numérotation automatique sur un réseau de télécommunication.
20. Sécurisation de la connexion par identification et authentification des deux parties : le client et le prestataire.
21. Traitement automatique de la demande restauration par le système central de sauvegarde.
22. Recherche automatique des fichiers du client dans le système central du prestataire.
23. Sélection automatique des fichiers à restaurer.
24. Lecture automatique des données à restaurer.
25. Transmission automatique des données sur un réseau de télécommunications.
26. Décompression automatique des données.
27. Déchiffrement automatique des données.

Fonction	Détail de la fonction	Eléments de suivi
1. Déclenchement automatique de l'exécution de la prestation.	Déclenchement automatique de l'opération de sauvegarde : Le système de déclenchement automatique de l'opération de sauvegarde comprend par exemple la liste des numéros de téléphone ou des adresses IP des abonnés au service de sauvegarde à distance ou du système central de gestion des sauvegardes. Il comprend également pour chaque abonné un calendrier horaire, quotidien, hebdomadaire, mensuel et annuel des sauvegardes à réaliser. Le déclenchement s'opère en scrutant, par exemple, l'horloge universelle et en la comparant, pour chaque abonné, aux heures et dates prévues de sauvegarde de ses données. Le déclenchement consiste à émettre le numéro de téléphone ou l'adresse IP de l'abonné ou du système central de sauvegarde vers un système de numérotation automatique sur un réseau numérique.	Les éléments nécessaires au déclenchement automatique de la sauvegarde seront définis dans le contrat de service : - N° Téléphone. - Adresse IP. - Mode de déclenchement.
2. Numérotation automatique sur un réseau de télécommunications.	Commande de numérotation : Le système de numérotation automatique établit la connexion entre le système central de gestion des sauvegardes et le système informatique de l'abonné au service de sauvegarde.	Le fichier "Log" contient le numéro de téléphone appelé ou l'adresse IP auquel l'applicatif se connecte.
3. Sécurisation de la connexion par identification et authentification des deux parties : le client et le prestataire.	Identification et authentification du système à sauvegarder : Lors de l'établissement de la connexion, le système d'identification d'accès identifie le système informatique de l'abonné puis authentifie son identité de façon à accepter ou à refuser la sauvegarde des données du système informatique de l'abonné. Il vérifie si le système informatique auquel il est connecté est identique à celui qui a été utilisé lors de la précédente sauvegarde.	Protocole de reconnaissance entre Prestataire / Client et Client / Prestataire : - Reconnaissance des systèmes (N° d'identification) - Authentification des mots de passe (codes secrets client et prestataire).

Fonction	Détail de la fonction	Eléments de suivi
4. Identification des fichiers modifiés depuis la précédente sauvegarde.	Accès aux attributs des fichiers pour reconnaître les données modifiées depuis la précédente sauvegarde : Lorsque le système informatique de l'abonné est identifié et authentifié, le système d'accès aux attributs des fichiers effectue la lecture des attributs de tous les fichiers du ou des disques du système informatique de l'abonné pour reconnaître les données modifiées depuis la précédente sauvegarde.	Inscription du déclenchement de lecture des attributs dans le fichier "Log".
5. Sélection automatique des fichiers à sauvegarder.	Création de table de sauvegarde : Lorsque le système d'accès aux attributs des fichiers détecte un fichier modifié depuis la dernière sauvegarde, ce fichier est référencé dans la table de sauvegarde.	Liste de la table de sauvegarde dans le fichier "Log".
6. Lecture automatique des données à sauvegarder.	Lecture des données à sauvegarder : Après détection des fichiers à sauvegarder référencés dans la table de sauvegarde, chaque fichier fait l'objet d'une lecture des données.	Inscription du déclenchement de lancement de la lecture des fichiers à sauvegarder dans le fichier "Log".
7. Détection automatique de virus informatique dans les fichiers à sauvegarder.	Détection de virus informatique : Tous les fichiers à sauvegarder font l'objet d'une opération de détection de virus informatique avec un logiciel antivirus mis à jour des derniers virus identifiés.	Inscription de début de détection de virus dans le fichier "Log". Inscription des informations suivantes dans le fichier log : le nom de l'antivirus, sa version et la version de la dernière mise à jour.
8. Décontamination automatique de tous les fichiers si un virus a été détecté.	Décontamination des fichiers : Dès qu'un virus informatique est détecté dans un fichier, non seulement ce fichier est décontaminé mais l'ensemble des fichiers du ou des disques du système informatique de l'abonné fait l'objet d'une décontamination. (Sécurité étendue).	Inscription des événements (virus détectés, décontamination, rapport) au cours du déroulement de la détection de virus dans le fichier "Log".

Fonction	Détail de la fonction	Eléments de suivi
9. Sécurisation des données par chiffrement (cryptage).	Chiffrement des données (cryptage) : Lorsque tous les doutes sont levés quant à l'existence d'un virus informatique ou que l'opération de décontamination s'est déroulée avec succès, les fichiers à sauvegarder font l'objet d'une opération de chiffrement avec un système de chiffrement à clé publique ou privé conforme à la législation en vigueur. L'opération de chiffrement consiste à substituer à un ensemble de données que l'on veut protéger un texte inintelligible pour quiconque ne connaît pas l'algorithme et les paramètres de chiffrement. Le chiffrement utilise préférentiellement des modifications mathématiques de codes comportant des permutations, des substitutions et/ou des décalages ou factorisation de très grands nombres.	Inscription de fin de détection de virus dans le fichier "Log". Inscription du résultat de détection de virus dans le fichier "Log". Inscription du déclenchement de lancement du "cryptage" sur les fichiers à sauvegarder dans le fichier "Log".
10. Réduction de la taille des données par compression.	Compression des données : Le système de compression des données a pour objectif de réduire la taille des fichiers à sauvegarder sans perte d'information de façon à optimiser la durée de la transmission sur le réseau numérique.	Inscription, dans le fichier "Log", du déclenchement du lancement de la "compression des données" sur les fichiers à sauvegarder
11. Transmission automatique des données sur un réseau de télécommunications.	Transmission sur un réseau : Lorsque toutes les opérations qui précèdent ont été réalisées, le système de transmission transmet sur le réseau numérique sélectionné par le prestataire toutes les données à sauvegarder vers le système central de sauvegarde, externe au système informatique du client et délocalisé en n'importe quel point du territoire.	Inscription du début de transmission des données dans le fichier "Log" : - Date et heure de début de transmission. - Nombre de fichiers à transmettre. - Volume total des données à transmettre.

Fonction	Détail de la fonction	Eléments de suivi
12. Réception des données et traitement par le système central du prestataire.	Traitement des données : Au niveau du système central de sauvegarde, les données reçues font l'objet d'un traitement qui consiste à organiser l'archivage des données en fonctions des consignes de l'abonné. Les données seront partitionnées par client et transmises par un réseau numérique vers un système d'archivage situé dans un lieu différent du système de traitement des données.	Inscription de fin de transmission des données dans le fichier "Log" : - Date et heure de fin de transmission. - Nombre et liste des fichiers transmis. - Nombre et liste des fichiers non transmis. - Volume total des données transmises. - Consignation des "informations abonnées" sur les fichiers sauvegardés dans le fichier "Log".
13. Archivage et stockage sécurisés automatiques des données dans un lieu distant.	Archivage et stockage sécurisés des données : L'opération d'archivage consiste à mettre en mémoire les données traitées. Elle peut être réalisée par l'intermédiaire d'un robot ou d'un automate de gestion de cartouches magnétiques, par un système de gestion mécanique de multiples disques (juke-box). Le système d'archivage est localisé dans une chambre forte du type de celles qui sont utilisées dans le domaine bancaire. Cette chambre forte est adaptée à résister à de nombreuses agressions et elle est dotée de nombreuses alarmes et de nombreux moyens de surveillance de type connus. En dehors des opérations d'installation ou de maintenance, aucune personne n'est habilitée à pénétrer dans la chambre forte. Pour des raisons de sûreté de fonctionnement les réseaux et les mémoires de masse sont dupliquées de façon à assurer une disponibilité permanente du système d'archivage en cas de panne.	Inscription du déclenchement de transfert des données partitionnées vers un lieu sécurisée dans le fichier "Log" : - Lieu. - Nom. - Catalogue. Les caractéristiques de la sécurité mise en œuvre pour le lieu d'archivage doivent être spécifiées dans le contrat de service : - Mode de stockage. - Personnes habilitées. - Protection contrôle d'accès. - Protection incendie. - Protection électrique.

Fonction	Détail de la fonction	Eléments de suivi
14. Transmission automatique d'un accusé de réception des données au système informatique du client par le système central du prestataire.	Emission de signal de réception : Cette opération consiste, pour le système de traitement du prestataire, à émettre, dès la fin de l'archivage des données, un accusé de réception au système informatique de l'abonné pour marquer la fin de la réception des données par le système d'archivage.	Inscription de la fin de transfert des données partitionnées vers un lieu sécurisé dans le fichier "Log". Inscription du début et fin d'envoi d'un accusé de réception vers l'abonné dans le fichier "Log".
15. Transmission automatique d'un compte rendu d'exécution de la prestation au système informatique du client par le système central du prestataire.	Création, émission et affichage de compte-rendu : L'opération de création de compte-rendu consiste à réaliser un tableau comportant les informations représentatives de la sauvegarde effectuée. L'émission de compte-rendu consiste à créer sur le ou les disques du système informatique de l'abonné un fichier comportant les informations suivantes : ● résultat de la sauvegarde, ● résultat de la détection de virus, ● résultat de la décontamination, ● liste des fichiers sauvegardés, ● heures de début et de fin de la sauvegarde, ● décalage de l'horloge avec le temps universel. Cette opération d'émission de compte-rendu comprend également l'affichage des information sur le moniteur et/ou l'imprimante du système informatique de l'abonné.	Inscription dans le fichier "log" du début et de fin de création du compte-rendu des opérations de sauvegarde. Inscription dans le fichier "log" du début et de fin de l'envoi du compte-rendu des opérations de sauvegarde. Le compte rendu contient toute les informations relatives au déroulement de la sauvegarde depuis le début le déclenchement de la sauvegarde jusqu'à l'émission du compte-rendu.
16. Transmission automatique d'une information de détection d'anomalie au système informatique du client par le système central du prestataire .	Emission de message : Le système d'émission de message est adapté à émettre des messages de compte-rendu d'exécution de la sauvegarde mais aussi à émettre des messages de défaut à destination du système informatique de l'abonné, si le système informatique de l'abonné n'était pas alimenté électriquement par exemple.	Inscription dans le fichier "log" du résultat de l'envoi du compte-rendu des opérations de sauvegarde.

Fonction	Détail de la fonction	Eléments de suivi
17. Marquage automatique des fichiers sauvegardés.	Modification d'attribut : L'opération de modification d'attributs des fichiers sauvegardés consiste à modifier les attributs des fichiers qui ont été sauvegardés. Les nouveaux attributs correspondent à un fichier transmis dans sa dernière version et se substituent aux anciens. Ces attributs sont, par le fonctionnement même du système informatique, modifiés à chaque modification du fichier auquel ils sont liés et l'information de transmission de la dernière version, information utilisée par le système de reconnaissance de données modifiées, est ainsi éliminée des modifications dudit fichier.	Inscription des attributs des fichiers sauvegardés dans la "table d'attributs" du système de sauvegarde. Le fichier « Log » contient les attributs des fichiers sauvegardés : - Nom de fichier. - Taille du fichier. - Date et heure de sauvegarde.
18. Déclenchement automatique de l'opération de restauration sur demande du client.	Déclenchement de l'opération de restauration : Le système de déclenchement de l'opération de restauration est activé par un message du système informatique du client du service de sauvegarde. Ce message consiste à émettre le numéro de téléphone ou l'adresse IP du système central de gestion des sauvegardes vers un système de numérotation automatique sur un réseau numérique. Le message comprend les modalités de l'opération de restauration (on line ou CD-ROM, fichiers à restaurer).	Les éléments nécessaires au déclenchement automatique de la restauration seront définis dans le contrat de service : - N° Téléphone. - Adresse IP. - Mode de déclenchement.
19. Numérotation automatique sur un réseau de télécommunication.	Commande de numérotation : Le système de numérotation automatique établit la connexion entre le système central de gestion des sauvegardes et le système informatique de l'abonné au service de sauvegarde.	Le fichier "Log" contiendra le numéro de téléphone appelé ou l'adresse IP auquel l'applicatif se connecte.

Fonction	Détail de la fonction	Eléments de suivi
20. Sécurisation de la connexion par identification et authentification des deux parties : le client et le prestataire.	Identification et authentification du système à sauvegarder : Lors de l'établissement de la connexion, le système d'identification d'accès identifie le système central de gestion des sauvegardes puis authentifie son identité de façon à accepter ou à refuser l'opération de restauration. Réciproquement, le système central vérifie si le système informatique auquel il est connecté est habilité à demander une opération de restauration.	Protocole de reconnaissance entre Prestataire / Client et Client / Prestataire : - Reconnaissance des systèmes (N° d'identification) - Authentification des mots de passe (codes secrets client et prestataire).
21. Traitement automatique de la demande restauration par le système central de sauvegarde.	Traitement de la demande de restauration : Lorsque le système informatique de l'abonné et le système central sont identifiés et authentifiés, la demande de restauration est traitée puis est transmise par un réseau numérique vers le système d'archivage (situé rappelons le dans un lieu différent du système de traitement des données).	Inscription de la date et heure de la demande de restauration par l'abonné dans le fichier "Log". Inscription dans le ficher "Log" du contenu de la restauration : - Date et heure de la sauvegarde. - Nombre de fichiers. - Volume total des données.
22. Recherche automatique des fichiers du client dans le système central du prestataire.	Accès aux attributs des fichiers stockés : Au niveau du système d'archivage et de stockage, le système d'accès aux attributs des données partitionnées du client effectue la lecture des attributs des fichiers archivés du client.	Inscription dans le fichier "Log" de la date et de l'heure de lecture des attributs.
23. Sélection automatique des fichiers à restaurer.	Création de table de restauration : Lorsque le système d'accès aux attributs des fichiers détecte un fichier à restaurer mentionné dans le message de demande de restauration , ce fichier est référencé dans la table de restauration.	Liste de la table de sauvegarde dans le fichier "Log".

Fonction	Détail de la fonction	Eléments de suivi
24. Lecture automatique des données à restaurer.	Lecture des données à restaurer : Après détection des fichiers à restaurer référencés dans la table de restauration, chaque fichier fait l'objet d'une lecture des données.	Inscription du déclenchement de lancement de la lecture des fichiers à sauvegarder dans le fichier "Log".
25. Transmission automatique des données sur un réseau de télécommunications.	Transmission sur un réseau : Lorsque toutes les opérations qui précèdent ont été réalisées, le système de transmission transmet sur le réseau numérique sélectionné par le prestataire toutes les données à restaurer vers le système informatique de l'abonné au service de sauvegarde. Une autre variante consiste à transférer les données du client sur tout support magnétique (CD-ROM, bande, cassette…) à sa convenance et à lui transmettre le support par voie postale ou transporteur spécialisé.	Inscription du début de transmission des données dans le fichier "Log" : - Date et heure de début de transmission. - Nombre de fichiers à transmettre. - Volume total des données à transmettre.
26. Décompression automatique des données.	Décompression des données : Le système de décompression des données a pour objectif de restaurer les données dans leur format initial.	Inscription du déclenchement de lancement du "décompression des données" sur les fichiers à sauvegarder dans le fichier "Log".
27. Déchiffrement automatique des données.	Déchiffrement des données : L'opération de déchiffrement a pour objectif de rendre les données à nouveau intelligibles et exploitables par l'abonné au service de sauvegarde.	Inscription du déclenchement de lancement du déchiffrement sur les fichiers à sauvegarder dans le fichier "Log".