UBIFRANCE
L'Agence française pour le développement international des entreprises

CHARTE

UTILISATION DU SYSTEME D'INFORMATION

LIVRET DES PROCEDURES

Table des matières

1 PREAMBULE

1. Ubifrance a déployé une charte d'utilisation du système d'information.

2. Afin de faciliter la bonne compréhension de cette charte, Ubifrance a rédigé et diffusé un document intitulé « Guide juridique », dont l'objectif est de présenter les règles de droit qui ont présidé à la rédaction de cette charte.

3. Le présent document intitulé « Livret des procédures » est le pendant technique du « Guide juridique ».

4. Il s'agit d'un document technique permettant l'implémentation pratique de l'ensemble des recommandations qui peuvent figurer non seulement dans la charte du système d'information mais également dans le guide juridique détaillé.

5. Ce livret, bien qu'il s'efforce d'être exhaustif, ne saurait cependant être considéré comme limitatif.

6. En effet, compte tenu de la multiplicité des causes pouvant affecter l'usage régulier des ressources informatiques et de communication électronique, il appartient à tout utilisateur d'adopter en toutes circonstances un comportement prudent et avisé en sollicitant au besoin l'aide de la Direction du système d'information.

7. Chaque utilisateur est supposé avoir pris connaissance du présent livret des procédures accessible sur l'Intranet d'Ubifrance.

2 PORTEE ET EVOLUTION

8. Ce livret des procédures est par nature évolutif car il doit permettre de répondre aux évolutions des technologies disponibles, des méthodes et des procédures ainsi que des nouvelles menaces envers le système d'information.

9. De ce fait, il ne peut pas définir des obligations générales et permanentes, le présent livret n'est donc annexé ni à la charte du système d'information ni au règlement intérieur.

10. Il est donc modifié de manière régulière, la version la plus à jour étant la version opposable.

11. Ubifrance fera ses meilleurs efforts pour informer les utilisateurs des évolutions apportées à ce livret. Cependant, l'utilisateur est invité à le consulter régulièrement.

12. Chaque utilisateur est également invité à transmettre à la Direction des systèmes d'information toute proposition de modification ou d'ajout dont il a pu constater l'intérêt dans le cadre de sa pratique des ressources informatiques et de communication électronique.

13. Le livret des procédures n'empêche pas Ubifrance de prendre toutes mesures pour remédier à une situation d'urgence ou à un risque dans la continuité du service.

14. Le livret des procédures pourra faire l'objet d'adaptations spécifiques en fonction des catégories d'utilisateurs concernés.

3 CHAMP D'APPLICATION

3.1 Personnes concernées

15. Les procédures d'utilisation et de sécurité doivent être respectées par l'ensemble des utilisateurs des ressources informatiques et de communication d'Ubifrance, c'est-à-dire notamment :

- les salariés d'Ubifrance ;
- les stagiaires et agents auxiliaires (vacataires,...) ;
- le personnel des prestataires externes intervenant sur les sites d'Ubifrance ;
- de manière générale toute personne qui utilise les ressources informatiques et de communication électronique, sur site et hors site.

16. Tout utilisateur qui fait intervenir des personnes tierces à Ubifrance qui seront amenées à utiliser les ressources informatiques et de communication, devra suivre et faire accepter à cette personne une procédure spécifique d'autorisation par la Direction des systèmes d'information.

3.2 Moyens concernés

17. Le livret vise :

- les équipements individuels et collectifs appartenant à Ubifrance ou à des loueurs, mis à disposition par Ubifrance ;
- les ressources informatiques et de communication personnelles à l'utilisateur et utilisées dans le cadre de son activité professionnelle devant suivre la procédure suivante :
    - demande d'autorisation écrite motivée auprès de la Direction des systèmes d'information mentionnant :
        - les références techniques des ressources (nom de produit, date et version),
        - les droits de l'utilisateur sur lesdites ressources,
        - la durée d'utilisation au sein d'Ubifrance.

3.3 Usages concernés

18. Les ressources informatiques et de communication sont utilisées soit :

- dans les locaux d'Ubifrance quels qu'ils soient et les Directions interrégionales ;
- dans le cadre d'un usage dit nomade ;

- en accès distant quel que soit le lieu de la connexion.

19. En toute hypothèse, l'utilisation des ressources informatiques et de communication électronique nécessite une attention et une vigilance particulière de l'utilisateur.

20. Les équipements individuels doivent être restitués en bon état après usage et lors du départ de l'utilisateur.

4 CONDITIONS D'ACCES ET D'IDENTIFICATION

4.1 Installation

21. Chaque utilisateur est informé que l'installation et la mise en œuvre des ressources informatiques et de communication qui lui sont allouées s'effectuent en fonction de leur disponibilité au sein d'Ubifrance et du profil de l'utilisateur.

22. La création des droits d'accès nécessite le respect préalable des phases suivantes :

- remplir la fiche des mouvements.

4.2 Droits d'accès

23. L'étendue du droit d'accès n'est pas la même pour tous les utilisateurs. Les niveaux d'accès sont définis en fonction des besoins du service et des fonctions de chaque utilisateur.

24. En conséquence, il est interdit d'essayer :

- d'accéder par un moyen détourné à une zone non accessible par le droit d'accès ;
- de modifier un document si vous n'y êtes pas autorisé.

25. Le droit d'accès d'un utilisateur au système d'information et de communication est donné à titre personnel et est incessible.

26. La communication par un utilisateur de son droit d'accès à toute autre personne est interdite.

27. Chaque utilisateur est responsable de l'utilisation qui sera faite de son droit d'accès aux ressources informatiques et de communication.

28. Ce droit d'accès disparaît lorsque son titulaire quitte Ubifrance, quelle qu'en soit la cause (cessation du contrat de travail, fin de mission, mutation, …).

4.3 Authentification

29. Cette procédure permet de garantir l'identité de l'utilisateur et l'intégrité des informations.

30. Les informations communiquées pour la mise en œuvre des procédures d'authentification sont confidentielles. Leur divulgation à des personnes non habilitées à les connaître porte atteinte à la sécurité du système d'information et de communication.

4.4 Gestion des mots de passe

31. Chaque utilisateur doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à un ou plusieurs environnements informatiques ainsi qu'à la messagerie.

32. A cet égard, chaque utilisateur doit :

- choisir des mots de passe sûrs, n'ayant aucun lien avec son environnement familier, (date de naissance, immatriculation de votre véhicule, surnom…) ;
- choisir des mots de passe constitués au minimum de 8 caractères alphanumériques dont au moins un chiffre, une majuscule, une minuscule et un caractère spécial ;
- changer de mots de passe régulièrement, aux dates et dans les délais fixés par Ubifrance et à tout le moins tous les trois (3) mois ;
- protéger ses fichiers par des mots de passe avec l'aide éventuel d'un administrateur.

33. Chaque utilisateur est personnellement responsable des mots de passe qu'il a choisis.

34. A ce titre, il s'engage à :

- ne jamais communiquer ses mots de passe à un tiers ;
- mémoriser ses mots de passe et donc ne jamais garder d'informations de connexion papier récapitulant ses codes et accès ;
- changer immédiatement ses mots de passe en cas de doute sur la confidentialité.

4.5 Paramétrage des postes de travail

35. Le poste de travail de l'utilisateur constitue un outil à usage exclusif qui doit être protégé des intrusions.

36. Il convient de :

- paramétrer la mise en veille automatique des postes de travail avec demande du mot de passe pour réactivation du poste après quinze minutes d'inactivité maximum ;
- utiliser son poste de travail après saisie de son mot de passe (pas de connexion au réseau et applications inutile) ;
- verrouiller sa session avant de quitter son poste de travail.

37. Par ailleurs, l'utilisateur s'engage :

- à ne pas arrêter anormalement son poste de travail connecté au système d'information sans l'accord d'un administrateur ;

- à ne pas interrompre sciemment le fonctionnement normal du système d'information et de communication connecté au réseau.

38. Il est strictement interdit à l'utilisateur d'installer tout logiciel ou matériel périphérique sur son poste de travail ou dans toute autre partie du système d'information d'Ubifrance compte tenu :

- des risques d'incompatibilité avec d'autres composants, de modifications de fichiers du système, de ralentissement, voire de blocage et occasionner la perte de contrôle du poste ;
- de la nécessité de respecter le nombre de licences et leurs modalités d'utilisation concédées à Ubifrance.

39. Il est interdit d'introduire toute disquette ou autre support numérique (notamment clef USB et disque dur externe) provenant de l'extérieur, contenant des fichiers de données et/ou logiciels d'applications sans la validation d'un informaticien de la DSI ou à défaut des responsables informatiques locaux.

40. En cas de besoin, une autorisation expresse devra être sollicitée auprès de la Direction des systèmes d'information et seul un informaticien de la DSI pourra y procéder.

5 REGLES DE NOMMAGE

41. Les règles de nommage des éléments électroniques notamment messages, fichiers et répertoires doivent respecter la charte stylistique et graphique d'Ubifrance en matière de transmission et de contenu des messages.

42. Par dérogation à l'usage exclusif à des fins professionnelles, toute utilisation du système d'information et de communication à des fins personnelles doit être résiduelle.

43. Tout message et fichier à caractère privé, reçu ou émis, et tout répertoire à caractère privé doivent comporter la mention « PRIVÉ » en caractères majuscules.

44. Cette mention « PRIVÉ » sera reportée en objet pour les messages et en intitulé pour les fichiers et les répertoires.

45. Tout message et/ou fichier et/ou répertoire ne comportant pas cette mention est réputé avoir un caractère professionnel et pourra donc être ouvert sans que cela constitue une violation du secret des correspondances privées.

46. Tel est le cas notamment :

- des initiales de l'utilisateur,
- du prénom de l'utilisateur,
- mes documents.

6 GESTION DES ABSENCES ET DES DEPARTS

6.1 Gestion des absences

47. L'utilisation de la messagerie et de l'agenda permet l'optimisation du travail au sein d'Ubifrance et une mutualisation de l'information concernant les disponibilités de chacun des utilisateurs.

48. Chaque utilisateur devra grâce à la messagerie et à l'agenda notifier ses périodes de présence et d'absence par la création d'un message automatique d'absence indiquant la durée de son absence et les coordonnées d'un autre utilisateur pouvant être contacté en son absence.

49. En raison du caractère professionnel de la messagerie électronique, il est important de s'assurer de la continuité du traitement des messages en cas d'absence pour cause de maladie ou de congés.

50. Quelles que soient la cause et la durée de l'absence de l'utilisateur, Ubifrance peut :

- accéder aux éléments présents au sein des ressources informatiques et de communication électronique mises à la disposition de l'utilisateur concerné, en ce qu'ils sont présumés professionnels,
- accéder, sous certaines conditions, aux fichiers, répertoires et messages informatiques clairement dénommés « PRIVÉ ».

6.2 Gestion des départs

51. Lors de son départ d'Ubifrance, l'utilisateur doit remettre l'ensemble des moyens informatiques et de communications électroniques, y inclus les matériels nomades, à la Direction du système d'information dans un bon état de fonctionnement.

52. Le jour du départ de l'utilisateur, un inventaire sera établi contradictoirement entre l'utilisateur et le Directeur des systèmes d'information précisant l'état du matériel restitué.

53. En cas de détérioration, Ubifrance se réserve le droit de demander à l'utilisateur, le paiement du prix du matériel endommagé évalué le jour de sa restitution.

54. L'utilisateur quittant Ubifrance devra supprimer tous messages, répertoires, fichiers à caractère personnel.

55. A défaut de destruction par l'utilisateur, Ubifrance détruira ces fichiers, dossiers, répertoires à caractère personnel le jour suivant le départ de l'utilisateur sans en garder copie.

56. Il appartient à l'utilisateur de faire suivre ses messages à caractère personnel en communiquant sa nouvelle adresse à ses interlocuteurs.

57. Lors de son départ, l'utilisateur s'interdit de protéger quelconque élément par un code d'accès ou un mécanisme de protection quelconque.

58. A l'annonce du départ d'un utilisateur, Ubifrance peut modifier les droits d'accès et les conditions d'utilisation des ressources informatiques et de communication électronique de ce dernier.

59. Lors de son départ, l'utilisateur perd tout droit d'accès au système d'information et de communication sauf décision contraire de l'autorité hiérarchique de l'utilisateur et de la Direction des systèmes d'information et s'interdit donc tout accès non autorisé au système d'information et de communication d'Ubifrance.

7 PRESERVATION DE LA CONFIDENTIALITE ET DU SECRET

60. Tout utilisateur du système d'information est tenu à une obligation de discrétion et de confidentialité qui porte notamment sur les fichiers, messages et bases de données. Chaque utilisateur doit veiller à ce que les tiers non autorisés n'aient pas connaissance de données confidentielles.

61. La transmission de données confidentielles ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur,
- indication de la mention « CONFIDENTIEL », en lettres majuscules, dans l'objet du message.

62. Chaque utilisateur s'engage à n'accéder qu'aux seules informations ayant un rapport direct avec son activité et s'interdit de prendre connaissance d'informations réservées à d'autres utilisateurs.

63. Par ailleurs, l'utilisateur s'interdit :

- de quitter son poste de travail en laissant une session ouverte,
- de laisser un document affiché sur l'écran de visualisation après exploitation.

64. L'utilisation de procédés de cryptage destinés à rendre inintelligible un message transmis est rendue possible grâce aux moyens de cryptologie expressément autorisés par la Direction du système d'information.

65. En toute hypothèse, l'utilisation de procédés de cryptage est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés.

66. Il est interdit d'utiliser des moyens de cryptologie personnels, ce qui emporte en particulier l'interdiction de télécharger des logiciels de cryptologie disponibles sur Internet.

8 DISPONIBILITE DU SYSTEME D'INFORMATION

8.1 Gestion de l'utilisation des ressources

67. La Direction du système d'information a le pouvoir de modifier la priorité ou de stopper une tâche utilisateur, si une exploitation excessive des ressources, au-delà des capacités moyennes de celles-ci, nuit aux autres utilisateurs, (par exemple des éditions trop importantes des tris ou sélections trop larges ou des traitements trop lourds).

68. Les ressources informatiques et de communication d'Ubifrance sont partagées entre un nombre important d'utilisateurs.

69. Chaque utilisateur doit agir en vue d'une utilisation optimum des ressources, et notamment, déporter toute utilisation monopolisant des ressources importantes, au-delà des capacités moyennes de celles-ci, en dehors des heures ouvrables, par exemple lancer une importante édition ou un traitement particulièrement long pendant l'heure du déjeuner.

70. Le cas échéant, une planification des tâches consommatrices de ressources informatiques est préparée avec un administrateur.

8.2 Gestion de la continuité d'activité

71. Toute intervention nécessitant une indisponibilité, même légère, du système d'information et de communication est communiquée aux utilisateurs concernés et, si possible, planifiée à l'avance.

72. La Direction du système d'information rétablira les ressources informatiques et de communication dans les meilleurs délais et s'attachera à optimiser la prestation, afin de minimiser la gêne occasionnée par celle-ci.

8.3 Reprise et restauration

73. Il existe des procédures de reprise automatique des applications en cas d'interruption accidentelle de l'exploitation, notamment :

- des procédures de reprise à chaud : points de reprise ou de check points programmés et utilisation du journal avant ;
- des procédures de reprise à froid : points de reprise ou check points programmés et utilisation du journal après.

74. Toutes les procédures automatiques et/ou manuelles doivent être consignées dans un document écrit et tenu à jour.

75. Ce document est disponible auprès des administrateurs des systèmes d'information.

9 MOBILITE ET MATERIELS MIS A DISPOSITION PAR UBIFRANCE

76. Il est de la responsabilité des utilisateurs des ressources informatiques et de communication nomades de tout faire pour garantir la sécurité de celles-ci.

77. Chaque utilisateur doit respecter les règles suivantes :

- s'informer, auprès de la Direction du système d'information des mesures particulières de sécurité et de sûreté à observer en fonction de sa destination, s'il s'agit d'un pays étranger ;

- adopter la plus stricte discrétion sur Ubifrance et ses activités au sein de celle-ci lorsqu'il est dans des lieux publics, notamment les trains, gares, aéroports, avions, salons professionnels, restaurants et parties communes des hôtels, notamment ne pas travailler sur ou discuter d'éléments confidentiels, secrets, sensibles ou stratégiques en de tels lieux ;

- ne pas discuter d'informations confidentielles, secrètes, sensibles ou stratégiques au téléphone, particulièrement si la conversation se déroule dans un lieu public ; ne pas faire directement référence au nom d'Ubifrance dans ses conversations, ni faire mention d'un projet autrement que par son nom de code ou en termes génériques ;

- veiller à utiliser tous les moyens de prévention de vol (câble antivol, coffres d'hôtels) et de protection d'informations disponibles (chiffrement, écrans polarisés) et ne pas laisser ses affaires professionnelles sans surveillance, afin de réduire la probabilité d'un vol de matériel ou d'information et d'en limiter les conséquences ;

- lors d'un voyage en avion, de systématiquement conserver son ordinateur portable, son terminal téléphonique, ainsi que l'ensemble des supports de stockage transportés en tant que bagages à main et de ne jamais les faire voyager en soute ;

- ne jamais laisser sans surveillance les matériels informatiques dans un lieu public (compartiment bagage d'un train, salon d'attente d'aéroport, banquette arrière ou coffre d'un véhicule dont le contenu est visible de l'extérieur) ;

- alerter la Direction du système d'information dans les plus brefs délais de tout évènement suspect (déplacement d'ordinateur portable ou d'objets personnels dans la chambre d'hôtel, fouille et saisie temporaire d'ordinateurs au contrôle des douanes, intérêt manifeste et questionnement sur Ubifrance de la part de voyageurs tiers, etc.) ;

- alerter la Direction du système d'information en cas de perte ou de vol de matériel à support@ubifrance.fr en précisant dans l'objet « Vol de matériel ».

78. L'utilisateur du système d'information d'Ubifrance est averti du fait que les formalités douanières de certains pays étrangers (USA et Chine notamment) permettent, en toute

légalité, aux agents assermentés de ces pays, de procéder à une saisie temporaire des matériels informatiques afin d'en examiner le contenu et d'en établir une copie intégrale.

79. L'utilisateur doit se soumettre à ces formalités sans réserve.

80. Toutefois, afin de limiter les conséquences potentielles pour Ubifrance, il est expressément recommandé aux utilisateurs de réduire au strict nécessaire la quantité d'informations confidentielles, secrètes, sensibles ou stratégiques présentes sur ces matériels lors de tels déplacements.

81. Dans certains cas, il sera préférable d'utiliser un support de stockage amovible chiffré (clé USB ou carte mémoire) pour stocker de telles informations lors d'un déplacement, en utilisant qu'un seul support de stockage.

10 OUTILS COLLABORATIFS ET PLATES-FORMES DE COMMUNICATION COLLECTIVES

82. La mise en place des outils collaboratifs et plateformes de communication collectives ne peut se faire que sur autorisation écrite et préalable de l'autorité hiérarchique.

83. L'ouverture d'un forum professionnel se fera dans le respect de règles édictées dans le cadre de la charte d'utilisation du système d'information.

84. Les forums auxquels participe l'utilisateur devront exclusivement être dédiés à des thèmes professionnels, d'intérêt général ou à des études poursuivies par un groupe de travail dans le cadre de l'activité professionnelle de l'utilisateur.

85. Il convient, lors de la participation à un forum d'identifier clairement les contributions respectives de chacun et, à défaut, d'indiquer l'origine de chaque contribution au dialogue.

86. Aucune information sur Ubifrance ayant un caractère confidentiel ne peut y être fournie.

87. L'utilisateur n'est pas autorisé à s'exprimer au nom d'Ubifrance, sauf autorisation préalable, expresse et spéciale de la hiérarchie d'Ubifrance.

11 RECOMMANDATIONS SPECIFIQUES SUR LA MESSAGERIE ELECTRONIQUE

88. L'utilisation de la messagerie électronique a pour objet de renforcer la mutualisation de l'information et l'optimisation de la production, sans modifier la qualité de ladite production.

89. Cependant cet outil produit un certain nombre d'impacts dans l'organisation du travail que chaque utilisateur doit mesurer afin de respecter les règles internes d'organisation du travail et la qualité de la production.

90. La messagerie électronique ne doit pas permettre une violation des règles connues de chaque utilisateur en matière de correspondance non électronique.

91. Les incidences fondamentales portent sur :

- la dématérialisation du courrier,
- la modification des règles de distribution du courrier,
- l'élargissement du cercle d'interlocuteurs habituels de chaque utilisateur au sein d'Ubifrance, notamment via l'utilisation des boîtes aux lettres électroniques et des possibilités d'envoi de documents en copie.

92. Tout en respectant les règles de sécurité contenues dans la charte d'utilisation du système d'informatique et le guide juridique, les utilisateurs de la messagerie doivent respecter des procédures spécifiques liées à l'utilisation de la messagerie électronique.

11.1 Le respect des principes de circulation de l'information

93. Le respect des principes de circulation de l'information s'impose à chaque utilisateur. En effet, la diffusion d'informations, même en apparence anodine, sans impact pour Ubifrance, peut permettre par voie de recoupement des opérations d'intelligence économique et nuire en conséquence aux intérêts d'Ubifrance.

94. Ce respect est basé sur les éléments suivants :

- le respect de la voie hiérarchique,
- le respect des principes d'information,
- le respect de la réalisation de tâches conforme à la qualité de la production.

95. L'utilisation de la messagerie électronique ne doit pas avoir pour objet, pour finalité ou pour conséquence de modifier le respect de la voie hiérarchique.

96. Hormis le cas où le message électronique est précédé de la mention « PRIVÉ », chaque utilisateur est informé qu'il peut faire l'objet d'une ouverture suite à une demande adressée à la Direction des systèmes d'information.

11.2 Envoi et réception de messages électroniques

97. La sécurité des données implique que chaque utilisateur s'assure de l'exactitude de l'adresse des destinataires des messages, afin de ne les transmettre qu'aux seules personnes auxquelles ils sont destinés.

98. Chaque utilisateur doit :

- ouvrir et consulter sa messagerie électronique quotidiennement,
- s'assurer de l'exactitude de l'adresse des destinataires des messages,
- adresser les messages en copie qu'aux seules personnes concernées par lesdits messages,
- informer chaque expéditeur de message de l'erreur d'affectation du message,
- prévenir chaque expéditeur du message du caractère complet ou non du message adressé, y compris en termes de fichiers attachés,

- signaler à tout expéditeur les difficultés de lecture du message ou des fichiers attachés,
- Utiliser le module de mailing commercial mis en place par la DSI dans le SICOM.

11.3 Gestion des boîtes aux lettres

99. Les messages envoyés ne doivent pas dépasser 15 mégaoctets.

100. En cas de dépassement d'un espace de 900 mégaoctets pour une boîte aux lettres, un message informe l'utilisateur sur la nécessité de classer ou de supprimer les messages.

101. Au-delà de 1 000 mégaoctets aucun envoi de message ne peut être effectué.

11.4 Absence de reroutage externe des messages

102. En aucun cas, il ne pourra être procédé à un reroutage par défaut des messages de l'utilisateur vers une boîte aux lettres externe à Ubifrance.

11.5 Classement

103. L'utilisation de la messagerie nécessite :

- de procéder au classement quotidien des messages dans les dossiers physiques et/ou électroniques correspondant suivant la méthodologie du service,
- de procéder au classement des fichiers rattachés dans les dossiers physiques et/ou électroniques correspondant suivant la méthodologie du service.

11.6 Sécurité antivirale et fichiers attachés

104. L'utilisation de fichiers attachés, compressés ou non, aux messages électroniques transmis est rendue possible grâce à l'outil de messagerie mis à disposition de chaque utilisateur dans le cadre de la messagerie.

105. Chaque utilisateur, préalablement à la transmission desdits fichiers, doit s'assurer de l'origine du fichier, (origine interne ou externe à Ubifrance).

106. Chaque utilisateur doit, préalablement à l'envoi de fichiers, s'assurer la faisabilité d'une diffusion, tant en termes de sécurité technique (contrôle antivirus), que de la sécurité juridique (liberté quant à la communication des informations contenues dans le fichier au regard des règles du Code de la propriété intellectuelle et de la loi Informatique, fichiers et libertés, notamment).

107. Il est indispensable de disposer d'une protection antivirale sur chaque poste de travail et de désactiver les fonctions susceptibles d'exposer le système d'information aux virus.

108. Si l'utilisateur détecte un virus dans une pièce jointe, il doit cesser tout envoi sur la messagerie et prévenir les administrateurs du système d'information et ceux à qui les fichiers contaminés ont été envoyés, voir à ceux qui l'ont créé.

109. Ubifrance se réserve le droit de retenir et d'isoler et/ou de supprimer tous messages, sans que ces messages n'aient été ouverts, afin de vérifier qu'ils ne comportent pas de virus.

110. D'une manière générale, les utilisateurs sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de la Direction du système d'information.

112. les utilisateurs s'interdisent de transférer les messages de chaines, de spams. Etc. à des contacts.

11.7 Stockage et archivage des messages électroniques

111. Ubifrance détermine une politique d'archivage des messages qui sont transférés automatiquement dans une boîte d'archives.

12 RECOMMANDATIONS SPECIFIQUES A INTERNET

12.1 Sécurisation de l'accès Internet

112. L'accès à Internet n'est autorisé qu'au travers de systèmes de sécurité dénommés pare-feu et proxy.

113. Ce dispositif est indispensable pour sécuriser chaque terminal du réseau. Toutefois, il ne protège pas contre toutes les menaces. Son efficacité dépend donc, en particulier, du respect des règles de connexion, qu'il est donc impératif d'observer.

114. Le raccordement de cet ensemble à Internet exige la mise en place de mécanismes destinés à protéger de l'Internet l'intégralité du système d'information d'Ubifrance et d'en assurer la confidentialité.

115. Tout trafic autorisé provenant d'Internet ou sortant du réseau d'Ubifrance passera au travers de pare-feu et d'un proxy, afin de vérifier que la politique de sécurité est bien respectée et de vérifier ses droits d'accès.

116. En revanche, ces mécanismes ne constituent pas une parade susceptible d'empêcher la diffusion d'informations confidentielles vers l'extérieur par des utilisateurs inconséquents ou malveillants.

117. Il est en outre impératif de protéger les serveurs et postes de travail par un anti-virus à jour.

118. Un pare-feu est inefficace pour les connexions qui lui échappent, telles que des connexions via un modem.

119. Il est formellement interdit d'utiliser les ressources Internet à partir de postes connectés au réseau d'Ubifrance, autrement qu'au travers du pare-feu et du proxy.

120. Il est également interdit de se connecter avec son portable en WiFi sur le réseau invité d'UbiFrance, créant ainsi un pont réseau entre le réseau interne et ledit réseau invité.

12.2 Accès sélectif ou restreint

121. La politique d'Ubifrance d'accès à Internet figure en annexe 1 des présentes.

122. Pour des raisons de sécurité, l'accès à Internet pourrait être restreint à certains postes seulement, limité dans son étendue et ce, en raison de la difficulté à se prémunir contre l'intrusion d'un pirate qui, au moyen d'un logiciel de navigation de l'utilisateur, exécute à distance des instructions pouvant avoir pour finalité d'accéder au contenu informationnel du poste utilisé pour la connexion ou des réseaux pouvant y être raccordés.

123. L'utilisateur s'interdit d'accéder à un site dont la consultation est restreinte, même dans le cas où l'accès est techniquement possible, dès lors que cet accès ne lui est pas autorisé.

124. Il est strictement interdit d'accéder à des sites contraires aux bonnes mœurs, à l'ordre public, ou à des sites qui, par leur nature même, présentent un caractère de dangerosité comme par exemple, les sites de piratage informatique.

12.3 Navigateurs

125. Les navigateurs (outils facilitant la recherche d'informations sur Internet à partir de mots clés) et les serveurs Web (zone multimédia de l'Internet) sont très difficiles à sécuriser.

126. Les utilisateurs ne doivent utiliser que les navigateurs sélectionnés par la Direction du système d'information.

127. Il est rappelé à l'utilisateur que l'utilisation des navigateurs ainsi que tout accès à Internet laissent des traces.

12.4 Téléchargement de fichiers en provenance d'Internet

128. En cas de téléchargement sur le poste de travail d'un fichier depuis Internet, il existe un risque d'importer des programmes et des fichiers indésirables, tels que des bombes logiques, chevaux de Troie ou spywares.

129. Tout téléchargement doit donc respecter les procédures en vigueur au sein d'Ubifrance.

130. En particulier, il est interdit de télécharger les logiciels de type freeware ou shareware sans autorisation, car :

- il existe un risque non négligeable d'importer des virus ;
- ces logiciels sont soumis aux conditions d'utilisation prévues par leur auteur, par exemple, le paiement d'une redevance à partir d'un certain nombre de jours après le téléchargement.

12.5 Transfert de fichiers

131. Le transfert des fichiers est susceptible d'importer et d'exporter des programmes et des fichiers indésirables, Ubifrance dispose d'un outil propre qui est le disque virtuel.

132. Tous les autres logiciels, FTP, FTP professionnels, freeware, shareware sont proscrits.

13 CORRESPONDANT CHARTES

133. Toute demande d'un utilisateur relative à l'application ou l'interprétation du présent livret des procédures, de la charte d'utilisation du système d'information, de la charte des droits d'administration et du guide juridique de l'utilisateur doit être adressée par écrit au correspondant chartes en qualité d'interlocuteur privilégié des utilisateurs.

134. Il en va de même de toute demande de dérogation aux différents points définis au sein desdits documents.

135. Le correspondant chartes est représenté par :

- le directeur du système d'information d'Ubifrance ou à défaut le RSSI (chartesSI@ubifrance.fr)

ANNEXE 1 : POLITIQUE D'ACCES A INTERNET

L'accès à internet est limité en fonction :

- de la dangerosité du site (échange de fichiers échappant aux antivirus, site contenant habituellement des virus, site pouvant bloquer la connexion internet d'une ME),
- de la légalité du site.

Ainsi sont bloqués les sites référencés par le moteur de filtrage Fortinet (http://www.fortiguard.com/webfiltering/webfiltering.html)

- Drug Abuse
- Occult
- Hacking
- Illegal or Unethical
- Racism and Hate
- Violence
- Marijuana
- Proxy avoidance
- Phishing
- Plagiarism
- Child Abuse
- Extremist Groups
- Pornography
- Web-based Email
- Instant Messaging
- Web Chat
- Peer-to-peer File Sharing
- Personal Storage
- Internet Telephony
- Personal Relationships