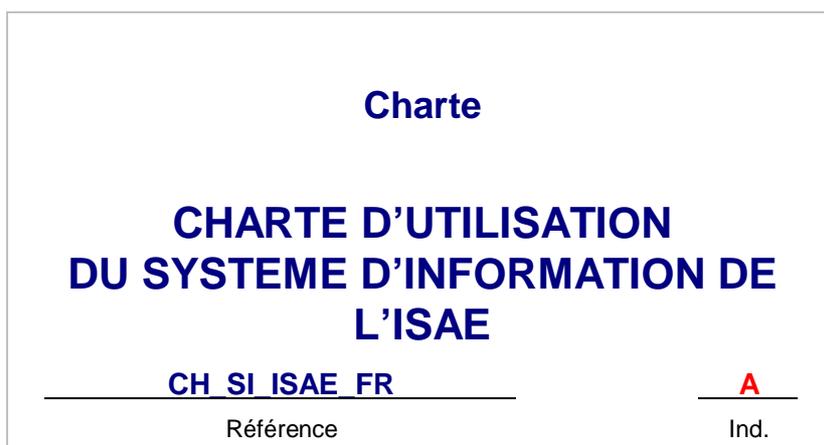


| Indice | Date     | Statut | Evolutions  |
|--------|----------|--------|---|
| A2     | 26/02/09 | Eb     | Validation en CTPC du 26/02/09                            |
| A      | 21/04/09 | Bpa    | Version approuvée en Conseil d'administration du 01/04/09 |



**Résumé d'auteur :**

La charte d'utilisation du système d'information définit les règles d'utilisation de l'ensemble des dispositifs informatiques de l'ISAE. A cette fin, il précise les structures, les principes de fonctionnement et certaines règles particulières à l'Institut. L'utilisateur du système d'information doit s'engager formellement à les respecter.

**Original :** Papier

**Source informatique :** Oui  Non  **Nom du fichier :** CH\_SI\_ISAE\_fr\_a.doc

**Classification :** Aucune

|       | Rédacteur/pilote        | Vérificateur            | Approbateur             |
|-------|-------------------------|-------------------------|-------------------------|
| Nom   | Laurent Dairaine        | Emmanuel Lochin         | Olivier Fourure         |
| Sigle | SI                      | OSSI                    | DG                      |
| Date  | <b>Visé le 22/04/09</b> | <b>Visé le 09/06/09</b> | <b>Visé le 09/06/09</b> |
| Visa  |                         |                         |                         |

### REDACTEURS ET CONTRIBUTEURS

| Date       | Rédacteur   | Contributeur  | Type de contribution   |
|------------|---|---|--|
| 2008.08.11 | Eric Barbry,<br>Cabinet, d'avocats<br>Alain Bensoussan. | Eric Barbry   | Rédaction de la version initiale, Prise en compte des spécifications ISAE. |
| 2008.08.28 | Eric Barbry,<br>Cabinet, d'avocats<br>Alain Bensoussan. | L. Dairaine (RSI),<br>E. Lochin (OSSI),<br>T. Parisot | Relecture et commentaires  |
| 2008.08.30 | Eric Barbry,<br>Cabinet, d'avocats<br>Alain Bensoussan. | C. Dussart (AJ)                                       | Relecture et commentaires  |
| 2008.09.04 | Eric Barbry,<br>Cabinet, d'avocats<br>Alain Bensoussan. | T. Parisot (SI)                                       | Relecture et commentaires  |
| 2008.09.24 | Eric Barbry,<br>Cabinet, d'avocats<br>Alain Bensoussan. | L. De Tchaguine,<br>CODIR                             | Relecture et commentaires  |

## TABLE DES MATIERES

|     |   |    |
|-----|---|----|
| 1.  | DOMAINE D'APPLICATION DE LA CHARTE                  | 4  |
| 2.  | DEFINITIONS   | 4  |
| 3.  | MISE A DISPOSITION DES SYSTEMES D'INFORMATION       | 5  |
| 4.  | REGLES D'USAGE DES SYSTEMES D'INFORMATION           | 5  |
| 5.  | CONDITIONS D'UTILISATION DES SYSTEMES D'INFORMATION | 7  |
| 6.  | IDENTIFIANT UTILISATEUR                             | 8  |
| 7.  | MOBILITE  | 9  |
| 8.  | GESTION DES ABSENCES ET DES DEPARTS                 | 9  |
| 9.  | SECRETS ET CONFIDENTIALITE                          | 10 |
| 10. | SERVICES WEB 2.0                                    | 10 |
| 11. | CONTROLE DES SYSTEMES D'INFORMATION                 | 10 |
| 12. | PUBLICATION DE PAGES WEB                            | 11 |
| 13. | VIGILANCE DE L'UTILISATEUR                          | 12 |
| 14. | MAINTENANCE   | 12 |
| 15. | CONVENTION DE PREUVE                                | 13 |
| 16. | GESTION DES DONNEES A CARACTERE PERSONNEL           | 13 |
| 17. | INFORMATION ET SANCTIONS                            | 13 |

## PREAMBULE

1. Conformément au point a) de l'article I.5.1 de la 2<sup>ème</sup> Partie du Règlement Intérieur de l'ISAE, la présente charte a pour objet de fixer les règles et principes relatifs à l'utilisation des systèmes d'information de l'Institut Supérieur de l'Aéronautique et de l'Espace (« ISAE »).
2. L'utilisation des systèmes d'information suppose le respect des règles destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance, ainsi que le respect des dispositions légales et réglementaires applicables. La présente charte est rédigée dans l'intérêt de chaque utilisateur et manifeste la volonté de l'ISAE d'assurer un développement harmonieux et sécurisé de l'utilisation des systèmes d'information.
3. Elle a pour objectif de formaliser les règles de déontologie et de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition par l'ISAE des systèmes d'information. Elle a également pour objectif d'harmoniser et d'optimiser l'utilisation des systèmes d'information.
4. La présente charte participe à « la culture de la sécurité » qui constitue une exigence essentielle de l'ISAE et illustre le comportement responsable que chaque utilisateur doit avoir.
5. La présente charte tient compte notamment des recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL), du « Forum des droits sur l'Internet », des meilleures pratiques du domaine, ainsi que de la jurisprudence. Elle tient également compte de la charte déontologique Renater<sup>1</sup>, et de la charte de bon usage de l'informatique et du réseau Renater.

## 1. DOMAINE D'APPLICATION DE LA CHARTE

6. La présente charte s'applique à tous les utilisateurs, c'est-à-dire à toutes les personnes qui sont autorisées à accéder ou à utiliser les systèmes d'information de l'ISAE et ce, quel que soit leur statut.
7. La présente charte, qui est applicable par principe à l'ensemble des utilisateurs sans distinction, peut être complétée le cas échéant de documents spécifiques pour certaines catégories d'utilisateurs.
8. Pour les utilisateurs extérieurs, les dispositions de la présente charte sont des règles impératives qui pourront le cas échéant être complétées par les dispositions contractuelles conclues entre l'ISAE et l'employeur des utilisateurs extérieurs et par les éventuelles règles de sécurité propres aux dits employeurs.

## 2. DEFINITIONS

9. Au sens de la présente charte, les termes ci-dessous ont la signification suivante :
  - « systèmes d'information » : ensemble des moyens informatiques et de communications électroniques regroupant notamment les matériels informatiques, les supports de stockage de toute nature, leurs périphériques et logiciels, les moyens ou solutions d'identification électronique, l'accès internet et/ou intranet, la messagerie électronique, la téléphonie fixe ou mobile, le fax, le minitel, les agendas et assistants personnels électroniques qu'il s'agisse de matériel fixe ou nomade, les réseaux

---

<sup>1</sup> Renater, Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche, opérateur Internet de l'ISAE

physiques d'accès (filaire, wifi ou autres), les données informatiques hébergées, sans que cette liste ne soit exhaustive.

- « utilisateur » : toutes les personnes astreintes au Règlement Intérieur de l'ISAE et pouvant accéder au, ou utiliser les systèmes d'information.
- « personnel habilité » : personnel désigné par l'ISAE dont la liste est formalisée par une note de service, donnant lieu à une note de service et disposant du droit d'installer, de configurer et de paramétrer tout ou partie des systèmes d'information mis à la disposition de l'utilisateur.

### 3. MISE A DISPOSITION DES SYSTEMES D'INFORMATION

10. L'ensemble des systèmes d'information mis à la disposition des utilisateurs sont et demeurent la propriété de l'ISAE.
11. Les systèmes d'information mis à la disposition de l'utilisateur sont exclusivement installés, configurés et paramétrés par le personnel habilité de l'ISAE.
12. L'utilisateur s'interdit de modifier les systèmes d'information mis à sa disposition notamment par l'ajout de logiciels ou de matériels, et ce pour quelle que raison que ce soit. Si des logiciels ou des matériels lui semblent nécessaires pour l'exercice de sa mission, il en fait part au service des systèmes d'information. Certains utilisateurs peuvent bénéficier de la part du service du système d'information d'un droit d'administration. Ces utilisateurs s'engagent alors à respecter l'ensemble des obligations afférentes et le cas échéant à signer la « charte des droits d'administration ».
13. Pour des raisons de sécurité ou de confidentialité, certaines configurations peuvent être verrouillées, c'est-à-dire interdites, restreintes ou bloquées par l'ISAE.
14. Les conditions d'utilisation des systèmes d'information sont définies par l'ISAE, qui se réserve notamment le droit de restreindre ou filtrer ou verrouiller les accès et usages (poste de travail, accès internet, ...). L'ISAE peut interrompre, modifier ou supprimer tout ou partie des équipements et des services pour quelle que raison que ce soit, de manière temporaire ou définitive.
15. L'ISAE s'efforcera, autant que faire se peut de prévenir les utilisateurs dans des délais raisonnables, notamment en cas de maintenance.

### 4. REGLES D'USAGE DES SYSTEMES D'INFORMATION

16. L'utilisateur est seul responsable du bon usage des systèmes d'information et s'engage à les utiliser dans le respect des lois et règlements, de la présente charte ainsi que des règles propres à son statut. Un site Web<sup>2</sup> décrivant l'usage et la disponibilité des systèmes d'information est maintenu à jour par le service des systèmes d'information.
17. La mise à disposition de contenus par voie électronique comporte des risques inhérents à la technologie employée. Ces risques peuvent être causés par :
  - un mauvais contrôle de l'information qui, une fois mise à disposition sur un réseau, peut être détournée de sa finalité ;
  - la récupération par téléchargement de contenus privatifs (logiciels ou œuvres protégées...) ou la consultation de sites à contenus illicites et contraires aux bonnes mœurs ou à l'ordre public.
18. Il est notamment interdit, sans que cette liste soit limitative de :
  - envoyer des messages à caractère injurieux, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de porter atteinte à la vie privée des personnes ou à leur

---

<sup>2</sup> <http://si.isae.fr>

- dignité, relatif à la race, l'origine nationale, les mœurs, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap ;
- consulter, copier ou télécharger le contenu de fichiers, messages ou sites à caractère pornographique, pédophile, négationniste, extrémiste ou contraire aux bonnes mœurs ou à l'ordre public et plus généralement se référant à des comportements dégradants ;
  - commettre toute action susceptible de mettre en cause la sécurité matérielle ou juridique de l'ISAE, de porter atteinte à sa réputation ou de constituer pour elle une gêne quelconque ;
  - de porter atteinte aux systèmes d'information de l'ISAE ou de toutes autres organisations ;
  - diffuser l'adresse e-mail créée au sein de l'ISAE sur des sites Internet sans rapport avec l'activité exercée au sein de l'ISAE ;
  - commettre toute action impliquant :
    - toute forme de dénigrement et tout propos de nature diffamatoire à l'égard de l'ISAE ;
    - le harcèlement sexuel et/ou moral ;
    - et plus généralement toute action illégale, contraire à la présente charte applicable à l'ISAE et toute action susceptible d'entraîner la responsabilité civile et/ou pénale de l'ISAE ;
    - tout mode de chiffrement non conforme aux procédures internes de l'ISAE, sauf dérogation expresse du service des systèmes d'information;
  - de dissimuler son identité par utilisation de pseudonymes sur internet ;
  - d'utiliser ou de tenter d'utiliser l'identité (identifiant) d'un autre utilisateur de l'ISAE ;
  - d'accéder ou de tenter d'accéder à des parties des systèmes d'information pour lesquelles l'autorisation ne lui a pas été accordée ;
  - de modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;
19. L'utilisation des systèmes d'information de l'ISAE implique le respect des droits de propriété intellectuelle de l'ISAE, de ses partenaires et de tout tiers titulaire de tels droits.
20. Toutes les données issues de l'ISAE, mises en ligne sur un site (interne ou externe), sous forme de carnets d'adresses, annuaires, photographies, logiciels, articles de presse, œuvres protégées ou toutes autres données de toutes natures, devront faire l'objet d'une autorisation préalable de :
- l'ISAE ;
  - des auteurs pour les contenus protégés par le droit d'auteur ;
  - des personnes photographiées, le cas échéant.
21. L'utilisateur s'engage à :
- utiliser les logiciels, progiciels, applications, dans les conditions de la licence souscrite par l'ISAE et uniquement dans ces conditions ;
  - ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels l'ISAE ne posséderait pas un droit d'usage ;
  - ne pas diffuser de textes, d'images, de photographies, d'œuvres musicales, audiovisuelles ou toute création copiée sur le réseau Internet ;
  - ne pas copier et remettre à des tiers des créations appartenant à l'ISAE ou à des tiers sans s'assurer de l'autorisation du titulaire des droits qui s'y rapporte ;
  - de manière générale, ne pas reproduire ou utiliser les progiciels, bases de données, page web ou autre création de l'ISAE ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;

22. Dans l'hypothèse où l'utilisateur recevrait régulièrement ou non un ou plusieurs message(s) non sollicité(s), ou message(s) tel(s) que listé(s) au point n°18 paragraphes 1 et 2, ou plus généralement un ou plusieurs message(s) manifestement illicite(s), il en prévient immédiatement le service des systèmes d'information afin que ce dernier puisse prendre les mesures nécessaires en fonction des obligations légales, de ses possibilités techniques et de ses contraintes économiques.
23. L'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents et les détruire en cas de réception fortuite.
24. Les utilisateurs sont également informés de la nécessité de respecter les dispositions légales en matière de traitement automatisé ou manuel de données à caractère personnel. Toute constitution de fichiers ou de bases de données comprenant des données à caractère personnel doit faire l'objet de formalités préalables auprès de la Commission Nationale Informatique et Libertés, sauf dérogations légales ou réglementaires. En conséquence, de tels fichiers ou bases de données doivent faire l'objet, avant leur mise en oeuvre, d'une autorisation de l'ISAE. L'utilisateur doit respecter les finalités des traitements de données à caractère personnel objet des formalités préalables susvisées.
25. L'utilisateur s'interdit toute utilisation malveillante destinée à perturber ou porter atteinte aux systèmes d'information mis à sa disposition.
26. L'utilisateur s'engage à utiliser de manière loyale les systèmes d'information en évitant de créer ou de générer des données ayant pour effet la saturation du réseau ou encore épuiser les ressources des systèmes d'information. Toute utilisation particulière des systèmes d'information pouvant entraîner une baisse notable des performances globales de ce système doit être précédée d'une autorisation préalable du service des systèmes d'information.
27. S'il existe des documents ou formats types (télécopie type, courrier électronique type, etc.), ceux-ci doivent impérativement être utilisés par les utilisateurs de l'ISAE car ils comportent des mentions obligatoires ou protectrices des intérêts de l'ISAE. Les agents de l'ISAE devront notamment apposer la signature qui leur est proposée par l'ISAE, à la fin des courriers électroniques dont ils sont les auteurs.
28. De même toutes les règles de marquage et d'identification des documents doivent nécessairement être appliquées sur les documents électroniques.

## 5. CONDITIONS D'UTILISATION DES SYSTEMES D'INFORMATION

29. Les systèmes d'information sont utilisés dans le strict respect des activités propres à l'ISAE, à savoir des activités d'enseignement, de formation, scientifiques, culturelles et professionnelles et de recherche, ou de support à ces activités. L'utilisateur s'engage à respecter les principes de laïcité, de neutralité politique, religieuse, économique et idéologique caractérisant les établissements du service public de l'enseignement supérieur
30. A ce titre, est interdite toute utilisation des systèmes d'information à des fins lucratives (autrement que liées à l'activité directe de l'ISAE), ou à des fins ludiques.
31. L'utilisateur ne peut, en aucun cas, donner accès à un tiers, à titre commercial ou non, rémunéré ou non, aux systèmes d'information mis à sa disposition par l'ISAE.
32. L'utilisation des systèmes d'information de l'ISAE, sous quelle que forme que ce soit, en ce compris les échanges de courriers électroniques, l'usage des répertoires ou de fichiers informatiques et les connexions à internet est présumée ne pas relever de l'intimité de la

vie privée. De ce fait, l'ISAE peut en prendre connaissance ou consulter ces différents éléments, même en l'absence de l'utilisateur.

33. L'utilisation des systèmes d'information à des fins privées est tolérée. Pour ce faire, les répertoires, fichiers ou correspondances émises ou reçues devront être clairement identifiés comme « privés ». Dans cette circonstance, l'utilisateur pourra créer un répertoire informatique intitulé « privé ». De même les courriers électroniques émis ou reçus devront comporter dans l'objet du message la mention « privé » et être conservé le cas échéant dans un répertoire « privé » du système de gestion des courriels.
34. Une telle utilisation doit demeurer résiduelle et raisonnable, tant dans la fréquence que dans la durée. L'ISAE se réserve le droit de limiter ou de suspendre cette tolérance en cas d'abus.
35. L'utilisation des systèmes d'information à des fins privées ne doit pas avoir pour effet de nuire à la qualité des travaux de l'utilisateur, ni au temps qui est consacré à ceux-ci.
36. En tout état de cause, un tel usage ne doit pas perturber le bon fonctionnement des systèmes d'information et demeure sous la seule responsabilité de l'utilisateur qui dégage l'ISAE de toute responsabilité.
37. L'ISAE s'interdit d'accéder ou de prendre connaissance des courriers électroniques identifiés comme « privé » ou des fichiers inclus dans le répertoire « privé » de l'utilisateur sauf pour des raisons d'urgence ou de sécurité. Dans ces conditions et autant que faire ce peut, l'utilisateur sera invité à être présent lors de ces opérations.
38. Les courriers électroniques ou répertoires identifiés comme « privé » ou des fichiers inclus dans le répertoire « privé » ne sont pas par principe, sauvegardés ou archivés au sein des systèmes d'information de l'ISAE sauf en cas d'urgence ou de sécurité ou sur demande des autorités compétentes, il convient donc à chaque utilisateur de réaliser les sauvegardes de ses données privées s'il le souhaite.

## 6. IDENTIFIANT UTILISATEUR

39. Chaque utilisateur est doté d'un identifiant (ou plusieurs) d'accès confidentiel aux systèmes d'information, nomades ou non, qui sont mis à sa disposition.
40. Cet identifiant d'accès se matérialise par :
  - un code utilisateur ;
  - un mot de passe ;
  - ou n'importe quelle autre solution mise en œuvre par l'ISAE.
41. L'efficacité d'un mot de passe dépend du nombre de caractères alphanumériques, de son originalité. Il doit être modifié selon une fréquence déterminée par l'ISAE.
42. Cet identifiant est personnel et ne doit pas faire l'objet de la moindre divulgation, même intra-service.
43. Si l'utilisateur a des raisons de penser que son identifiant est ou peut être exploité par un tiers, il doit en avertir immédiatement le service des systèmes d'information qui prendra les mesures nécessaires.
44. Chaque utilisateur s'interdit d'user, par quel que moyen que ce soit, du droit d'accès d'un autre utilisateur. Notamment, l'utilisateur s'interdit d'utiliser l'identifiant d'un autre utilisateur, dans le cas où il en aurait eu connaissance ou accès.
45. L'utilisateur s'interdit de supprimer, masquer ou modifier sa véritable identité ou son identifiant.

46. Il est interdit à un utilisateur d'user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.
47. Sauf défaut avéré des systèmes d'information ou de ses dispositifs de sécurité et sauf à avoir engagé préalablement une demande de suppression ou de suspension, tout usage des systèmes d'information est réputé avoir été réalisé par le porteur de l'identifiant d'accès.
48. Il en assume alors les conséquences juridiques et financières, sauf à ce qu'il soit en mesure de prouver le contraire.
49. Toute personne qui est amenée à envoyer un courrier électronique au nom d'un autre utilisateur, et à la demande expresse de ce dernier, est tenu de s'assurer que le destinataire aura parfaitement conscience que le message lui a été adressé « pour ordre de ».

## 7. MOBILITE

50. Les moyens informatiques et de communication électronique dits « nomades » sont mis à la disposition de l'utilisateur contre récépissé. On entend par « nomade » tous les moyens techniques (ordinateur portable, téléphone mobile, les agendas et assistants personnels électroniques, ...) et éléments accessoires (disquette, cd rom, clé USB, équipement réseaux, équipement sans fil, ...) qui peuvent être utilisés hors les murs de l'ISAE. Lorsque ces matériels sont utilisés hors les murs de l'ISAE, l'utilisateur en assure la garde et la responsabilité. Il assiste l'ISAE ou procède lui-même selon les cas à toutes les démarches (déclaration d'assurance, dépôt de plainte, ...) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.
51. L'utilisation de moyens informatiques et de communications électroniques nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcé, car ces moyens ne bénéficient plus de tous les dispositifs de sécurité spécifiques à l'utilisation dans l'enceinte de l'établissement.
52. L'utilisation de tels moyens est conditionnée par le respect des consignes de sécurité spécifiques liées à ce type d'usage, données par le service des systèmes d'information.
53. L'utilisateur doit notamment veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens et éléments accessoires, les utiliser ou accéder à leurs contenus.
54. En cas d'incident avéré mais aussi en cas de doute, il doit immédiatement en aviser sa hiérarchie.
55. Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser les moyens techniques d'authentification qui lui seront remis et aucun autre. L'autorisation d'accès à distance ne doit en aucun cas être cédée à un tiers. En terme de sécurité et de confidentialité, l'utilisateur est soumis aux mêmes obligations que celles visées pour la gestion des identifiants et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées. Il devra aviser, sans délai, les services compétents de la perte ou du vol des moyens d'authentification à distance.

## 8. GESTION DES ABSENCES ET DES DEPARTS

56. Chaque utilisateur doit veiller à ce que la continuité du service soit assurée conformément aux modalités d'organisation de l'ISAE.
57. Il n'est pas prévu de recourir à l'utilisation d'automatisme de gestion des messageries électroniques, ni de procédure spécifique en cas d'absence de lecture des messages au-delà d'un certain délai.

58. Lors de son départ définitif de l'ISAE pour quelle que raison que ce soit (notamment fin de scolarité, démission, cessation des fonctions, fin de mission pour un prestataire extérieur,...), l'utilisateur doit restituer l'ensemble des éléments qui auront pu lui être remis.
59. Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder 3 mois, le compte messagerie de l'utilisateur est supprimé le jour de son départ.
60. Sauf procédure judiciaire, pour les étudiants et les élèves, le compte messagerie ainsi que le compte utilisateur et l'ensemble des répertoires sont supprimés à la fin de leur scolarité, à charge pour eux de procéder à une copie de sauvegarde s'ils le jugent nécessaire.
61. Ses identifiants sont également désactivés. Si l'utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage à le restituer.
62. Le répertoire « privé » doit être supprimé par l'utilisateur au plus tard la veille de son départ de l'ISAE.
63. Il devra en être de même des courriers électroniques « privé ».
64. A défaut, et sauf procédure judiciaire ou enquête administrative, ce répertoire est automatiquement supprimé le lendemain du départ de l'utilisateur de l'ISAE, sans être consulté et sans qu'aucune copie ne soit réalisée.

## 9. SECRETS ET CONFIDENTIALITE

65. Les règles correspondant à la gestion des secrets spécifiques faisant l'objet d'une organisation particulière s'appliquent à ces informations lorsqu'elles sont mises en œuvre au sein des systèmes d'information et ce, nonobstant l'application de la présente charte.
66. Les règles concernant les informations et les supports classifiés au titre du secret défense s'appliquent indépendamment de la présente charte.

## 10. SERVICES WEB 2.0

67. La mise en place des services web 2.0 (on qualifie de Web 2.0 les interfaces permettant aux internautes d'interagir à la fois avec le contenu des pages mais aussi entre eux, il s'agit en particulier de services tels que les groupes de discussion par courrier électronique, forums de discussion, wiki, blogs, chat etc.). ne peut se faire que sur accord de l'ISAE.
68. L'ouverture d'un forum interne à l'ISAE, d'un thème de « News Group » ou d'une communauté par un utilisateur s'effectue sur autorisation préalable de l'ISAE.
69. Ces services peuvent faire l'objet d'un contrôle par un modérateur désigné à cet effet.
70. Les messages circulant sur ces services ne sont pas nécessairement sauvegardés. Il appartient donc à chaque utilisateur de sauvegarder les messages qui lui sont utiles.
71. L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est réservée à un usage strictement professionnel.
72. En outre, l'utilisateur doit systématiquement vérifier lors de l'inscription qu'il existe une procédure de désabonnement.

## 11. CONTROLE DES SYSTEMES D'INFORMATION

73. L'ISAE est soumis à une obligation générale de sécurité en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données et de la loi du 6 janvier 1978 dite « Informatique et libertés », modifiée le 6 août 2004.

74. En cas de risque pour la sécurité des systèmes d'information ou pour des raisons liées à la continuité du service, le personnel habilité se réserve le droit de « prendre la main » sur n'importe quel élément du système d'information et « *bypasser* » un code utilisateur en utilisant un code administrateur. L'utilisateur concerné par cette opération en sera informé.
75. Les systèmes d'information peuvent donner lieu à surveillance et contrôle à des fins statistiques de traçabilité, d'optimisation, de sécurité ou de détection des abus.
76. L'ISAE peut diligenter toutes opérations techniques de contrôle permettant de vérifier le respect des dispositions de la présente charte ou des règles légales, soit de sa propre initiative, soit dans le cadre de procédures judiciaires ou d'enquêtes administratives.
77. Dans le cadre de ces opérations de contrôle, l'ISAE peut notamment être amené à accéder à l'ensemble des informations relatives à l'utilisateur, y compris :
  - o sa session de travail ;
  - o tout message figurant sur sa messagerie ;
  - o les données enregistrées sur le disque dur du poste de travail.
78. Lors de ces accès, les personnes habilitées réalisant ces accès sont tenues de respecter la confidentialité des informations auxquelles elles accèdent.
79. L'usage des services Internet peut faire l'objet d'un contrôle a posteriori. Ce contrôle peut porter sur le temps de connexion par poste ou sur les sites consultés par une technique appropriée, notamment par la technique dite de « re-jeu ».
80. En cas de perturbation, signalée notamment par l'apparition d'alertes suite à tentatives d'infection des systèmes à l'aide de virus informatiques, l'ISAE est habilitée à mener toutes les investigations qu'il jugera utiles aux fins d'éradiquer les dits virus. Pour des raisons de sécurité, l'ISAE pourra également détruire tout message émis ou reçu qui contiendrait un virus ou un fichier auto-extractible ou exécutable.
81. Tout logiciel installé illicitement ou tout fichier suspect sera supprimé dès le constat de leur présence sur le poste de travail, les conséquences de cette suppression étant supportées par le seul utilisateur.
82. L'utilisateur en sera informé.
83. L'utilisateur est informé que par application de la charte déontologique Renater, le Gip Renater peut procéder à des contrôles de la bonne utilisation du réseau Renater, conformément à l'annexe 3 de ladite charte, et qu'en cas de manquement à ladite charte, le Gip Renater se réserve le droit de suspendre l'accès au réseau Renater. Le Gip Renater peut ainsi avoir accès, notamment auprès des opérateurs concernés aux informations d'administration de réseau (tels que des données de volumétrie, d'incident, etc.). Ces données sont considérées par le Gip Renater comme confidentielles, et seuls des bilans de synthèse globaux peuvent être rendus publics.

## 12. PUBLICATION DE PAGES WEB

84. L'ISAE accepte d'héberger différents services de publication sur Internet permettant la diffusion d'information dans différents contextes (telles que des pages personnalisées, des pages de projets, des pages d'associations, etc.), à condition que :
  - o ces pages s'inscrivent dans le cadre des activités de l'ISAE, correspondant à des activités d'enseignement, de formation, scientifiques, culturelles et professionnelles et de recherche ;
  - o ces pages respectent une identité graphique acceptée par l'ISAE ;
  - o ces pages aient reçu l'autorisation préalable de diffusion par l'ISAE.

- les liens hypertextes renvoyant à des sites internet extérieurs à l'ISAE sont possibles à condition que :
    - les contenus des dits sites internet extérieurs s'inscrivent dans le cadre des activités de l'ISAE, correspondant à des activités d'enseignement, de formation, scientifiques, culturelles et professionnelles et de recherche ;
    - l'insertion d'un tel lien hypertexte ait préalablement fait l'objet d'une autorisation de la part du propriétaire du dit site internet.
85. L'utilisateur demeure seul et unique responsable des contenus des pages ainsi publiées.
86. L'ISAE se réserve le droit de supprimer, sans préavis, tout contenu signalé comme susceptible d'être illicite.

### 13. VIGILANCE DE L'UTILISATEUR

87. L'utilisateur s'engage à user des systèmes d'information de façon loyale et à être vigilant en signalant toute anomalie ou intrusion.
88. L'utilisateur s'engage à exercer une vigilance particulière dans le contrôle des contenus échangés et à prendre toutes les précautions nécessaires en cas de reproduction ou de rediffusion d'œuvres ou de données susceptibles de bénéficier d'une protection.
89. Il est rappelé à l'utilisateur que des échanges électroniques peuvent constituer des preuves et former un contrat. L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il envoie ou qu'il échange et ne doit en aucun cas engager l'ISAE sans autorisation préalable de sa direction.
90. L'utilisateur est tenu d'informer sans délai le service du système d'information de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les systèmes d'information.
91. L'utilisateur est tenu de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au sein des systèmes d'information.
92. Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le système d'information de l'ISAE, c'est-à-dire :
- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ;
  - ne pas répondre à des messages reçus de l'extérieur qu'il n'a pas sollicité
  - détruire les messages du type « chaîne de solidarité » ;
  - ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la sécurité informatique.
93. L'utilisateur doit utiliser les systèmes d'information dans le respect des procédures et méthodologies qui lui sont adressées (livrets des procédures, livrets des préconisations, manuels utilisateurs, note de service,...) et s'engage à user exclusivement des services d'accès sécurisés mis à sa disposition.
94. En cas de fraude informatique ou dans toute autre hypothèse où l'utilisateur serait invité à prendre des mesures d'urgence ou de sécurité spécifique, celui-ci s'engage à les appliquer sans le moindre délai.

### 14. MAINTENANCE

95. L'ISAE peut diligenter toutes opérations techniques que la mise à disposition des systèmes d'information implique nécessairement, qu'il s'agisse des opérations de maintenance technique, de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

96. Ces opérations de maintenance peuvent nécessiter l'intervention d'une personne habilitée sur site ou sous la forme d'une prise de main à distance.
97. L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité des systèmes d'informations.
98. Dans le cadre de ces interventions, la personne habilitée peut être amenée à prendre connaissance de messages émis ou reçus par l'utilisateur et à examiner en détail le journal de ses connexions.
99. La personne habilitée fera en sorte de ne pas accéder au répertoire intitulé « privé » et aux messages d'objet « privé », en dehors de la présence de l'utilisateur. Dans le cas contraire, l'utilisateur en sera informé.
100. Cependant elle peut y être contrainte pour des raisons de sécurité ou pour des raisons techniques (surcharge du système, lutte anti virus, lutte anti-spam,...) et ce malgré l'opposition de l'utilisateur.
101. Si à l'occasion de ses opérations de maintenance ou de contrôle, une personne habilitée identifie une utilisation anormale et/ou un contenu illicite ou préjudiciable, elle rappellera à l'intéressé les éléments de la présente charte.

## 15. CONVENTION DE PREUVE

102. Il est entendu que constituent des preuves l'ensemble des éléments techniques, logs et traces relatifs à l'utilisation des systèmes d'information de l'ISAE et que celles-ci sont opposables à l'utilisateur. Constituent également des preuves les documents sous forme électronique échangés entre l'ISAE et l'utilisateur, en ce compris les échanges de courriers électroniques.

## 16. GESTION DES DONNEES A CARACTERE PERSONNEL

103. L'ISAE s'engage à ce que les données concernant les utilisateurs soient collectées et traitées conformément aux exigences de la loi « Informatique et Libertés ».
104. Les traitements opérés dans le cadre de la présente charte ont pour finalités :
- le suivi et la maintenance des systèmes d'information ;
  - la gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et réseaux ;
  - la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux ;
  - la gestion de la messagerie électronique attribuée par l'ISAE ;
  - le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation et de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;
  - la sécurité des systèmes d'information ;
  - le respect de la présente charte.
105. Conformément à la loi « Informatique et Libertés », les utilisateurs sont informés qu'ils disposent d'un droit d'accès, de rectification et d'opposition, pour motif légitime, relatif à l'ensemble des informations à caractère personnel les concernant, qui s'exerce auprès du service des systèmes d'information.

## 17. INFORMATION ET SANCTIONS

106. Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner pour l'utilisateur la suppression immédiate du droit d'utilisation des systèmes

d'information qui sont mis à sa disposition et, le cas échéant, des sanctions disciplinaires et/ou des poursuites judiciaires.

107. La présente charte est disponible en anglais. Seule la version française de la charte fait foi.

Nonobstant lesdites sanctions, l'utilisateur est avisé que par application de l'article 40 du Code de procédure pénale, tout fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.



## ENGAGEMENT PERSONNEL DE L'UTILISATEUR DU SYSTEME D'INFORMATION DE L'ISAE

Je, soussigné ..... en qualité de<sup>3</sup> ....., déclare avoir pris connaissance des dispositions de la charte d'utilisation du système d'information de l'ISAE, et m'engage à les respecter. Dans le cas contraire, je ne pourrais pas m'opposer à la suppression de mon compte d'utilisateur du système d'information de l'ISAE.

A.....  
le.....

Signature :

<sup>3</sup> Précisez Elèves (indiquez la formation SUPAERO ou ENSICA), étudiant (indiquez la formation), personnel ISAE, extérieur, etc.