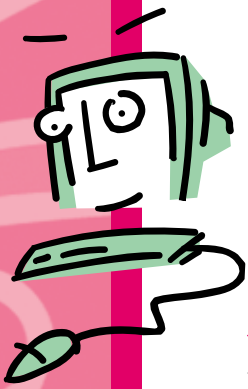
Memento de l'Utilisateur

des Moyens Informatiques du Commissariat à l'Énergie Atomique

cea

L'ATOME, DE LA RECHERCHE À L'INDUSTRIE



Champ d'application

Le présent mémento s'adresse aux utilisateurs des moyens informatiques du Commissariat à l'Energie Atomique.

Il explicite les règles d'utilisation de ceux-ci définies par la Note d'Instruction Générale n°469 : Utilisation des moyens informatiques du CEA.

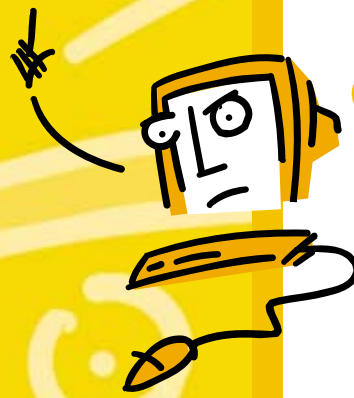
Moyens informatiques concernés

Il s'agit de tous les moyens informatiques faisant partie des systèmes d'information du CEA (moyens locaux et ressources auxquels il est possible d'accéder à distance à partir du réseau administré sous la responsabilité des unités du CEA), et qui sont destinés à élaborer, traiter, stocker, échanger ou détruire les informations.

Ces informations concernent tous les domaines d'activité du CEA : scientifique, technique, administratif, gestion, bureautique, etc..

Utilisateurs concernés

Les dispositions de la NIG sont applicables à toute personne ayant accès aux moyens informatiques ci-dessus définis, quel que soit son statut : salarié du CEA, personnel intérimaire, stagiaire de courte ou de longue durée, thésard, chercheur d'un laboratoire associé, personnel d'une entreprise extérieure et salarié de filiale dans les conditions définies par voie de convention, et de façon générale, toute autre personne autorisée à utiliser ces moyens informatiques.



Organisation et responsabilités générales

La sécurité des systèmes d'information relève, d'une part de l'autorité qualifiée, et d'autre part de l'autorité hiérarchique.

Le Directeur Central de la Sécurité, en qualité d'autorité qualifiée, est responsable de la sécurité des systèmes d'information du CEA. A ce titre, il définit la politique de sécurité de ces systèmes, en fixe les objectifs et en assure le contrôle.

Les directeurs fonctionnels, de pôle et de centre, ainsi que les chefs de département, en qualité d'autorités hiérarchiques, sont responsables de la définition des objectifs de sécurité de leur système d'information, ainsi que de l'application des mesures appropriées. Pour cela, ils se font assister par l'Agent de Sécurité des Systèmes d'Information (ASSI) et par le Correspondant de l'Agent Central de la Sécurité (CACS).

La définition et la mise en œuvre des moyens techniques et organisationnels permettant de garantir la sécurité des systèmes d'information sont réalisées par la Direction des Technologies de l'Information, après validation par la Direction Centrale de la Sécurité.

Règles d'utilisation et de sécurité

L'utilisation de systèmes et de moyens informatiques du CEA s'effectue dans le cadre des missions confiées à l'unité détentrice de ces moyens, et selon les besoins de celle-ci. La mise à disposition d'un équipement ou d'une ressource informatique (service, messagerie électronique, accès distant, espace disque, imprimante, ...) à un utilisateur se fait sous la responsabilité de l'unité, selon les procédures réglementaires et les modalités précisées par celle-ci.
L'utilisation de ces moyens cesse lorsque la mission est terminée ou lorsque le besoin disparaît. Les moyens matériels sont alors restitués à l'unité concernée ; ils doivent faire l'objet d'un suivi physique et, le cas échéant, de la procédure de réforme telle que définie dans le Code de gestion des biens du CEA.

- **Droit d'accès**
- **Responsabilité**
- **Mot de passe**

L'utilisateur doit contribuer à la sécurité générale du CEA, notamment en respectant les règles et recommandations qui lui sont prescrites.

Le droit d'utilisation est délivré par le chef d'unité ; il est strictement personnel et n'est en aucun cas transmissible, même temporairement, à des collègues ou à des tiers.

Le droit d'utilisation se matérialise par un droit d'accès précisément défini soit à un poste de travail individuel ou partagé (micro-ordinateur, station de travail, ...) soit à des ressources réseaux (comptes utilisateurs sur des machines distantes, ...), voire les deux.

L'utilisation d'un équipement informatique ou d'un compte est placée sous l'entière responsabilité de celui qui l'utilise, dans le cadre de ses droits d'accès. Il lui appartient en conséquence de maintenir la protection matérielle et logicielle des ressources qui lui sont confiées. L'accès à la machine doit être protégé au minimum par un mot de passe. Les supports d'information amovibles (logiciels ou données) de toute nature doivent être gérés et placés en lieu sûr, en fonction de la sensibilité des informations qu'ils renferment et conformément à la réglementation en vigueur.

Les mots de passe donnant accès à des équipements informatiques ou à des comptes doivent être choisis avec un soin tout particulier. Ils doivent être constitués d'au moins 8 caractères comportant un mélange de majuscules, minuscules, chiffres et caractères spéciaux. Ils doivent être changés périodiquement et ne jamais être communiqués à autrui, ni laissés accessibles à proximité du poste de travail.

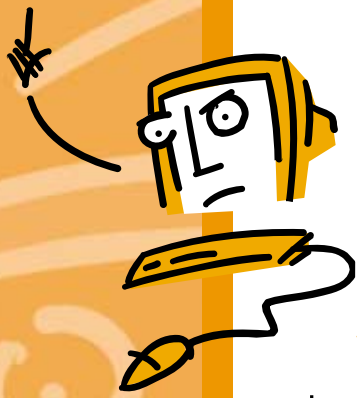
L'utilisateur qui, pour les besoins du service, partage des ressources dont il est propriétaire (fichiers, exécutables, répertoires ...), **doit limiter les droits d'accès donnés aux tiers concernés au strict minimum nécessaire**. Ces derniers sont responsables des traitements informatiques qu'ils effectuent sur ces ressources comme indiqué ci-après.

L'utilisateur se déconnecte en quittant son poste de travail, afin de ne pas laisser d'informations accessibles.

Les anomalies ou tout problème rencontré (vol d'équipements ou d'accessoires, tentative d'intrusion, suspicion de virus, ...) **doivent être signalés dans les plus brefs délais** au gestionnaire ou à l'administrateur des moyens informatiques, au chef d'unité ainsi qu'à l'Agent de Sécurité des Systèmes d'Information (ASSI), avec qui une solution appropriée sera validée.

Dans ces circonstances, l'ASSI, peut être amené à intervenir dans l'ordinateur de l'utilisateur, ce dernier étant tenu informé, au préalable et sauf impossibilité, des opérations effectuées.

L'utilisateur doit signaler au gestionnaire ou administrateur du système toute évolution dans ses besoins, notamment les ressources dont il n'a plus l'usage dans le cadre de ses fonctions, ou à l'occasion de son départ de l'unité détentrice.



Principes d'utilisation

- Droit d'usage
- Fichiers nominatifs
- Messages électroniques
- Services Internet
- Virus

Respect de la confidentialité

On entend par confidentialité le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.

Les fichiers des utilisateurs sont réservés à leur usage propre (même s'ils comportent certaines possibilités d'utilisation par des tiers).

En conséquence, il est interdit de s'approprier ou de tenter de s'approprier les droits d'usage ainsi que l'accès aux comptes d'autrui par quelque moyen que ce soit, notamment captation d'un mot de passe ou usurpation d'identité. Cette interdiction est également valable pour l'usage de la messagerie électronique. L'accès à un poste de travail appartenant à un autre utilisateur n'est autorisé qu'après l'accord de ce dernier. Cette utilisation ne pourra en aucun cas être faite sous l'identité de l'utilisateur ayant donné l'accès.

Il est rappelé qu'est pénalement sanctionné le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système infor-

matique, même s'il en est résulté aucune suppression ou modification des données, ni aucune altération du fonctionnement du système.

Si l'activité exercée par l'utilisateur nécessite la constitution ou la modification de fichiers contenant des informations nominatives, la Commission Nationale de l'Informatique et des Libertés (CNIL) doit au préalable être saisie sous forme d'une demande d'avis, ou d'une déclaration simplifiée pour les traitements les plus courants. Elle doit également être saisie d'une déclaration en cas de suppression de ces fichiers. La seule entité au CEA habilitée à effectuer ces formalités auprès de la CNIL est la Direction Juridique et des relations Commerciales (DJC). Le guide " Informatique et libertés " diffusé par la DJC rappelle les dispositions applicables, les modalités de création et de traitement des fichiers informatiques, ainsi que les droits que détiennent les personnes concernées par ces fichiers.

Il est rappelé que la confidentialité n'est pas assurée par la messagerie électronique. En conséquence, cette dernière ne doit pas être utilisée sans sécurisation appropriée pour les échanges d'informations ou de documents à caractère confidentiel ou sensible, même à titre de projets.

Chaque utilisateur qui diffuse ou transfère des messages échangés par courrier électronique, même partiels, est entièrement responsable du respect de la confidentialité qui y est attachée.

Préservation de la disponibilité et de l'intégrité

On entend par disponibilité l'aptitude du système d'information à remplir une fonction répondant à l'objectif attendu, dans des conditions définies d'horaires, de délais et de performances.

L'utilisation des moyens informatiques d'une unité, en dehors du domaine d'activité de celle-ci, notamment l'ouverture de services personnels, au même titre que toute activité rémunératrice ou ludique, **est interdite.**
Cette interdiction est également valable pour l'usage des services Internet et de la messagerie électronique, qui doivent être limités aux besoins professionnels, et qui en particulier ne sont pas destinés à échanger, au sein de l'organisme, des informations de nature politique, sociale, confessionnelle ou syndicale en dehors du cadre de l'exercice du droit syndical tel que défini dans les accords collectifs du CEA.
Un usage personnel raisonnable de ces moyens est admissible dans la mesure où l'activité

professionnelle ne s'en trouve aucunement affectée.

L'envoi de messages " en chaînes " à des listes de personnes ou à des individus ainsi que l'envoi de messages pouvant provoquer la saturation des réseaux ou détériorer le travail d'autrui sont strictement interdits.

On entend par intégrité la garantie que le système et l'information ne sont modifiés que par une action volontaire et légitime ; lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire la garantie de son origine et de sa destination.

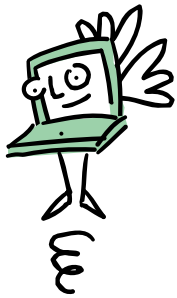
La propagation volontaire des virus, le développement et l'utilisation des logiciels permettant de contourner les dispositifs de sécurité mis en place dans les systèmes, ainsi que le détournement des outils d'exploitation des systèmes à des fins de piratage constituent des fautes susceptibles de sanctions professionnelles ou pénales.

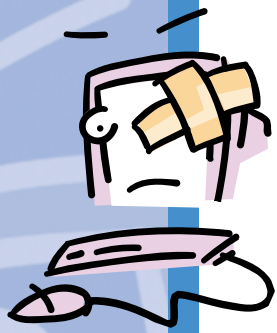
Il est rappelé que sont pénalement sanctionnés :
- le fait d'entraver ou de fausser le fonctionnement d'un système informatique ;
- le fait d'introduire frauduleusement des données dans un système informatique ou de modifier frauduleusement les données qu'il contient.

Les utilisateurs doivent être conscients que les échanges par messagerie électronique ne sont pas anonymes et, en particulier, qu'ils sont faits avec une adresse indiquant l'appartenance de l'utilisateur au CEA. Les prises de position doivent être conformes aux intérêts du CEA.

L'accès à des ressources communes doit se faire avec un souci constant d'utilisation non abusive et de partage équitable. En particulier, l'utilisateur doit veiller à occuper aussi peu d'espace disque que possible, à libérer les logiciels avec "licence à jetons" lorsqu'il ne les utilise plus et à ne pas monopoliser les postes dédiés.

Toute modification matérielle d'un poste de travail ou d'un équipement de réseau ne doit être effectuée qu'après accord écrit du gestionnaire ou administrateur du système concerné et par du personnel qualifié dûment habilité.





Protection du patrimoine

- Diffusion de l'information
- Chiffrement
- Usage des logiciels et des informations
- Connexion aux réseaux

Il est rappelé que les informations relevant de la classification de défense ne doivent pas être traitées sur des machines connectées à des réseaux non agrées, notamment les réseaux informatiques interconnectés du CEA civil.

La divulgation des informations traitées peut compromettre le patrimoine du CEA. En conséquence, l'utilisateur s'engage à ne pas mettre d'informations à disposition d'autrui sans s'être assuré au préalable qu'il est autorisé à le faire.

Il doit s'assurer que les moyens de protection sont adaptés au niveau de sensibilité de l'information et que la diffusion est bien limitée aux destinataires prévus et autorisés.
L'utilisateur ne doit pas répondre aux sollicitations externes visant à obtenir des renseignements qui lui seraient demandés (moyens informatiques, contacts humains, annuaires, ...) sous quelque forme que ce soit (démarchage téléphonique, courrier électronique, formulaires, enquêtes, ...).
Il est rappelé que l'utilisation du chiffrement à des fins de confiden-

tialité, ne peut se faire qu'après accord de la Direction Centrale de la Sécurité et conformément à la réglementation en vigueur.

L'utilisateur ne doit pas chercher à obtenir, ni à exploiter, des informations ou des logiciels dont il n 'a pas l'usage dans le cadre de sa mission ou pour lesquels il n'aurait pas les droits d'utilisation. En particulier, il est interdit d'utiliser et même d'installer sur un poste de travail des logiciels protégés (pour lesquels il faut acquérir une licence) qui proviendraient de copies illicites ou d'actes de piratage, y compris à titre provisoire ou pour les essayer.

Chaque utilisateur s'engage à ne pas introduire de risques potentiels pour la sécurité des réseaux du CEA.
Il doit respecter la réglementation interne d'accès à ces réseaux. En particulier, tout nouvel accès spécial (RTC, RNIS, TRANSPAC, ...) doit être déclaré et soumis à l'autorisation de la Direction des Technologies de l'Information du CEA. Les solutions faisant appel à des dispositifs d'accès aux réseaux publics doivent impérativement utiliser des procédures permettant l'identification de l'appelant (rappel automatique, connexions à des serveurs de sécurité, ...). Quand il doit être fait usage d'accès par réseau téléphonique à des machines connectées aux réseaux informatiques du CEA, seule l'utilisation des moyens d'accès centralisés gérés par la Direction des Technologies de l'Information est autorisée.

La circulaire DCS n°15 du 18/10/95 réglemente les services informationnels accessibles depuis l'extérieur du CEA. La circulaire DCS n°16 du 10/05/99 réglemente les services d'information à accès informatique restreint. Ces deux types de services ne peuvent être mis en place qu'après accord de la Direction Centrale de la Sécurité et de la Direction des Technologies de l'Information.

Utilisation de l'Internet

On entend par Internet la mise à disposition, par des serveurs distants extérieurs au CEA, de moyens d'échanges et d'informations.

- **Respect des règles d'Internet "Netiquette"**

L'utilisation de l'Internet doit se faire conformément aux principes d'utilisation définis précédemment, et dans le respect de la législation en vigueur. Lorsqu'il accède à un site extérieur au CEA, l'utilisateur doit s'imposer de respecter la politique de sécurité et les règles locales du site hôte. Il ne sera pas procédé, à partir d'un équipement du CEA, à une connexion sur des sites qui contiennent des informations susceptibles de faire l'objet de poursuites pénales.

Il est interdit de diffuser des informations confidentielles comme ci-avant définies, ainsi que d'altérer volontairement le bon fonctionnement des serveurs auxquels il est possible d'accéder.

Informations utiles

Administrateur ou Gestionnaire de systèmes

Tel : _____

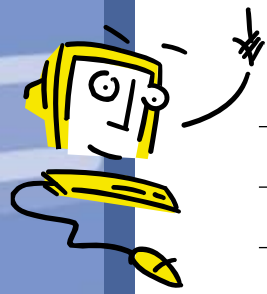
E-mail : _____

Agent de Sécurité des Systèmes d'Information (ASSI)

Tel : _____

E-mail : _____

Pour plus d'informations sur la sécurité des systèmes d'information, consultez le site http://www-ssi.cea.fr/



Notes

DIRECTION CENTRALE DE LA SÉCURITÉ
SERVICE DE PROTECTION DES ACTIVITÉS CLASSÉES ET DES INFORMATIONS
CEA/FAR - ROUTE DU PANORAMA - BP6 - 92265 FONTENAY-AUX-ROSES CEDEX
TEL : 01 46 54 97 35 - FAX : 01 46 54 97 37

Parution septembre 2001

Création graphique Angel'Art : 01 48 05 48 04