ANNEXE 2

Charte individuelle relative à la Sécurité Informatique

Version 1.7.4
13/08/2009

SOMMAIRE

1. INTRODUCTION

Ce document a vocation à s'appliquer **essentiellement à** tous les salariés de C.I.T (Casino Information Technology), C chez vous, Casino Services, Casino Restauration, DCF (Distribution Casino France), Comacas, Easydis, EMC distribution, IGC Services, Mercialys, R2C (Restauration Collective Casino) Serca et Sudéco désignées ci-après par l'acronyme « CA-SI-NO », **et plus généralement à** tous les Utilisateurs[1] du Système d'Information.

La protection des personnes, des biens et des informations est un enjeu permanent pour assurer la croissance et la pérennité du groupe Casino. Elle contribue au renforcement de sa position sur le marché et préserve son image de marque, la satisfaction de ses clients et de ses collaborateurs.

La sécurité dans l'entreprise est un objectif qui doit être partagé par tous.
Chaque intervenant chez CA-SI-NO doit y contribuer à son niveau et mettre en application un certain nombre de règles de bon usage et de recommandations édictées par le service informatique garant de la pérennité des Systèmes d'Information.
La Charte a pour objectifs :

- de définir les obligations et les responsabilités des Utilisateurs afin d'instaurer un usage correct et approprié des moyens informatiques[2]
- de rappeler les procédures de contrôle mises en œuvre au sein de CA-SI-NO, dans le respect des droits fondamentaux des personnes dans l'entreprise

Le non respect des règles définies dans la présente charte est susceptible d'entraîner des sanctions disciplinaires.

2. DEFINITIONS

Toutes les définitions sont données en note de bas de page.

3. REGLES GENERALES DE BON USAGE

Les moyens informatiques sont mis à la disposition de l'Utilisateur dans une finalité professionnelle et leur utilisation doit rester conforme aux besoins du service et aux intérêts de l'entreprise.

Chaque utilisateur est tenu pour responsable de toute utilisation des moyens informatiques mis à sa disposition. Toute opération effectuée à partir de ses mots de passe ou codes confidentiels personnels sera réputée, a priori, être de son fait. Dans le même temps il est interdit d'utiliser le compte (ou matricule) d'un autre utilisateur sans son autorisation.
Un usage à des fins privées de ces moyens est toléré dans des limites raisonnables et sous réserve des conditions énumérées dans le cadre des règles spécifiques ci-après.

1 **Utilisateur(s)** désigne les salariés de CA-SI-NO, ainsi que toute personne utilisatrice du Système d'Information du groupe Casino. Cela concerne tous les statuts qui lient une personne physique ou morale au groupe Casino (sous-traitants, stagiaires, intérimaires, autres intervenants externes, gérants mandataires non salariés…) et ce quelle que soit leur localisation géographique.
2 **Moyens informatiques** désigne indifféremment les « ressources informatiques », « systèmes informatiques » et tous moyens matériels et logiciels, englobant à la fois les serveurs, stations de travails, micro-ordinateurs, cartes à puce et tous les moyens techniques et de télécommunications des services administratifs et techniques, des laboratoires et des salles communes, ainsi que les logiciels et matériels affectés au fonctionnement du réseau.

3.1 Protection du patrimoine informationnel[3] de l'entreprise

L'utilisateur s'engage à :

- respecter les règles de gestion relatives à la classification et la protection des informations et documents* *[Voir le tableau synthétique de ces règles en annexe 1 du présent document];
- ne pas diffuser d'informations sensibles sur les lignes ou réseaux non sécurisés tels que le fax et le téléphone en externe, la messagerie électronique ou Internet ; en ce qui concerne la messagerie, les moyens de protection, décrits dans l'annexe 1 et relatifs à chaque niveau de classification, doivent être utilisés et plus particulièrement lorsque les informations transitent par des réseaux publics;
- s'assurer que ses données sont régulièrement sauvegardées
- ne pas effectuer des opérations qui pourraient nuire, de manière directe ou indirecte, à l'intégrité, la disponibilité et la confidentialité des moyens informatiques et des informations dont l'entreprise est propriétaire.

3.2 Utilisation appropriée des moyens informatiques

Sous réserve des nécessités liées à sa mission professionnelle, l'Utilisateur s'engage à ne jamais quitter son poste de travail en laissant une session réseau ouverte et accessible, laquelle doit être au minimum protégée par un écran de veille avec mot de passe.
Il se garde strictement d'interrompre le fonctionnement normal du réseau ou des systèmes connectés au réseau (manipulations anormales, introduction de virus, ...).

Chaque Utilisateur doit en outre :

- respecter les règles relatives à l'identification et l'authentification, notamment :
    - se garder strictement de masquer ou tenter de masquer sa véritable identité ;
    - se garder strictement d'accéder au compte d'un autre utilisateur sans l'autorisation de celui-ci ;
    - respecter les règles de création et de gestion des mots de passe définies par la Direction de la Sécurité des SI (disponibles sur INTRANET), et notamment :
        - choisir des mots de passe ou codes secrets sûrs,
        - lorsqu'elle est proposée par l'application, ne pas répondre à la sollicitation de mémorisation du mot de passe;
        - ne pas communiquer ses mots de passe ou codes secrets à un tiers, sous réserve des nécessités liées à la continuité du service, telles que définies par chaque responsable de service ;
        - respecter la limite de ses droits d'accès et/ou des droits étendus que confère son rôle (administrateur[4] par exemple) ;
- respecter les consignes propres à chaque application ;
- user raisonnablement de toutes les ressources propres et partagées (espace disque dur, bande passante[5] sur le réseau…) ;

3 Le **patrimoine informationnel**, ou patrimoine immatériel, représente l'ensemble du patrimoine, au sens juridique, constitué par les informations et connaissances détenues par une organisation, entreprise, administration, ou collectivité locale.
4 **Administrateur** désigne la personne chargée de gérer un système informatique (réseau, serveur, base de données, etc.) et qui est responsable à la fois de sa sécurité, de son fonctionnement, de son exploitation et de son évolution.
5 La **bande passante** indique un débit d'informations. On mesure généralement cette bande passante en octets (byte en anglais) par seconde ou en bit par seconde (bit/s ou bps).

- se conformer aux prescriptions d'utilisation définies par l'auteur et/ou le fournisseur d'un logiciel ;
- éviter les stockages redondants et inutiles ;
- se garder strictement d'installer des matériels ou logiciels autres que ceux validés par C.I.T (Casino Information Technology), et sauf l'autorisation préalable et formelle du responsable hiérarchique ;
- se garder strictement de :
    - modifier ou détruire des informations appartenant à d'autres utilisateurs et ceci sans leur autorisation ;
    - effectuer des installations de logiciels ou de matériels non autorisées
    - d'établir une double connexion sur le réseau du groupe Casino et un réseau externe;
    - changer la configuration du logiciel anti-virus installé sur son ordinateur professionnel par le service informatique ;
    - modifier la configuration des postes et autres moyens mis à sa disposition (messagerie, réseau, Internet,…) sur des paramètres ayant trait à la sécurité du poste de travail et son environnement ;
    - s'interdire toute action illicite ou malveillante, telle que :
        - utiliser des outils mettant sciemment en cause l'intégrité des systèmes ;
        - utiliser des outils espions de type balayage (« scan ») ou repérage (« sniff ») ou tout autre moyen de surveillance et d'écoute du trafic réseau ;
        - contourner ou tenter de contourner des moyens ou procédures de sécurité.

- dans le cadre du chiffrement (cryptage) de données, utiliser les outils et clés de chiffrement fournis par la Direction de la Sécurité des SI de l'entreprise ; ainsi dans le cadre d'échange avec l'extérieur, l'Utilisateur veillera à chiffrer[6] également au moyen de la clé qui lui a été fournie par l'entreprise.

Même si les technologies numériques le permettent, chaque utilisateur se garde strictement d'effectuer des enregistrements vidéo ou phoniques à l'insu d'autres utilisateurs.

3.3 Respect des réglementations

Chaque Utilisateur se garde strictement de faire toute utilisation des ressources (informations ou moyens informatiques) mises à sa disposition :

- qui violerait les législations et réglementations en vigueur (tels que des actes de contrefaçon de logiciels ou l'absence de déclaration à la CNIL de fichiers nominatifs)
- ou bien
- qui violerait sciemment certains engagements contractuels du groupe Casino et/ou des politiques de sécurité d'autres entreprises;
- ou bien
- qui serait incompatible avec le développement et les intérêts du groupe Casino.

6 **Chiffrer ou crypter** désigne l'action de rendre des données incompréhensibles à toute personne ne détenant pas la convention de décryptage associée.

Chaque Utilisateur se garde strictement :

- d'installer un logiciel sur un système sans s'être assuré préalablement que les droits de licence le permettent ;
- de faire des copies de logiciels commerciaux pour quel qu'usage que ce soit, excepté une copie de sauvegarde.
- de télécharger et d'utiliser un outil de chiffrement (cryptage) et/ou de signature qui ne serait pas formellement validé par la Direction de la Sécurité des SI;
- d'enfreindre les droits propriété intellectuelle et/ou industrielle détenus par des tiers ;
- de commettre des infractions de nature à engager sa responsabilité et/ou celle de du groupe Casino, notamment en portant atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, par exemple par l'intermédiaire de messages, textes ou images provocants. A cet égard, il est précisé que la diffusion ou rediffusion, tant en interne que vers l'extérieur, de messages et/ou images à caractère sexuel, raciste ou discriminatoire sera considérée comme constitutive d'une faute.

4. REGLES SPECIFIQUES PAR APPLICATION

4.1 Services Internet (WEB, FTP,…)

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle.
Une consultation ponctuelle et dans des limites raisonnables du web, pour un motif personnel, de sites Internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation de l'entreprise ainsi que les conditions d'accès professionnel au réseau, est tolérée.

- La modification de configuration du logiciel de navigation (comme Internet Explorer) est interdite. Tout besoin de déroger à cette règle est soumis à autorisation.

- Toute publication en rapport avec l'activité sociale et commerciale du groupe Casino et en son nom, par voie de presse, vidéo, podcast, forum de discussion externe ou tout autre moyen technologique rendant l'information publique n'est autorisée que pour les personnes ayant mandat de la Direction de la communication du groupe Casino.

4.2 Messagerie électronique

Un usage raisonnable de la messagerie électronique professionnelle pour envoyer ou recevoir, dans le cadre des nécessités de la vie courante et familiale, des messages à caractère personnel est toléré, à condition que cette utilisation ponctuelle n'affecte pas le trafic normal des messages professionnels et qu'elle ne nuise pas à l'accomplissement des activités professionnelles ; de plus, concernant l'utilisation à des fins extra professionnelles de la messagerie, l'Utilisateur se conforme à la procédure décrite au paragraphe 5.2.1 destinée à garantir la protection du secret de ses correspondances à caractère personnel ;

L'Utilisateur s'engage à respecter les règles d'usage suivantes :

- les règles de gestion relatives à la classification et la protection des informations et documents, telles que visées au paragraphe 3.1. A cet égard, l'Utilisateur apporte une attention particulière à la sensibilité et la nature des informations qu'il transmet par courrier électronique via le réseau Internet et s'engage à utiliser les outils mis à sa disposition par C.I.T (ex. logiciel de cryptage des données, PKI[7] interne, …) afin de garantir la protection des informations qu'il transmet ;

- les recommandations techniques définies par l'administrateur de la messagerie. En outre, il s'interdit de chiffrer (crypter) les messages sortant signalés comme « PRIVÉ ou privé ou PRIVE ou prive ou PRIVATE ou private ou personnel ou PERSONNEL» conformément à la procédure de l'article 5.2.1, tant dans leur contenu qu'en ce qui concerne les fichiers (image, texte, …) qui y sont attachés.

4.3 Intranet (Web interne)

Chaque Utilisateur est responsable des publications et de leur contenu sur l'Intranet du groupe Casino. Ces publications sont en lien direct avec l'activité professionnelle, leur contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne met pas en cause les intérêts et la réputation du Groupe Casino. De plus, il est rappelé à l'Utilisateur que ces publications doivent respecter la procédure interne de protection et de classification des informations telle que visée au paragraphe 3.1.

4.4 Utilisateurs nomades

Outre les règles déjà énoncées aux paragraphes précédents, les Utilisateurs nomades appliquent les recommandations d'usage suivantes :

- Les connexions nomades ne sont autorisées qu'à partir de matériels fournis par C.I.T ; à titre dérogatoire, les connexions à la messagerie ou au réseau du groupe Casino en utilisant des services offert par C.I.T (OWA[8], portail VPN SSL[9]) sont autorisées à partir d'autres matériels ;
- Ne pas enregistrer les mots de passe pour les accès distants sur le PC portable ou sous quelque forme que ce soit (étiquette, PDA[10], …) ;
- Chiffrer (crypter) toutes les informations classifiées « Confidentiel » enregistrées en local sur le disque ;
- En cas de perte ou de vol de son PC portable, l'Utilisateur avertit immédiatement le 'HelpDesk (SVP)' des Utilisateurs, ainsi que son responsable hiérarchique et son assistante ;
- Lors de ses déplacements en train, en avion, par tout transport et en tout lieu public, l'Utilisateur prend les précautions suivantes :
    - garder sous son contrôle exclusif et permanent les matériels et documents qu'il transporte ;

7 **IGC ou PKI** une Infrastructure de Gestion de Clefs (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.
8 Outlook Web Access (**OWA**) est une interface Webmail permettant aux utilisateurs du groupe Casino d'accéder à leur messagerie via un navigateur Internet,
9 Le **VPN SSL** offre des services sécurisés de partage de fichier et d'accès à l'Intranet du groupe Casino au travers d'un navigateur Internet
10 Un assistant personnel ou ordinateur de poche est un appareil numérique portable, souvent appelé par son sigle anglais **PDA** pour Personal Digital Assistant.

- se garder d'avoir des discussions pouvant être écoutées par les personnes qui l'entourent et nuire aux intérêts du groupe Casino.
- signaler toute anomalie ou incident de sécurité qui se sont déroulés au cours de ses déplacements ou travail à domicile.

5. PROCEDURES DE CONTROLE DE L'ACTIVITE DES UTILISATEURS

Dans l'exercice de son droit légitime à contrôler l'activité des Utilisateurs au sein de l'entreprise, CA-SI-NO s'engage à ne mettre en place aucun moyen de contrôle qui serait à l'insu des Utilisateurs ou bien contraire au respect de leurs droits fondamentaux à la vie privée, à la liberté d'opinion et à la liberté d'expression, droits intangibles qui s'exercent en tous temps et tous lieux.
En cas d'urgence, suivant un principe de précaution l'employeur pourra effectuer une opération en informant l'utilisateur a posteriori.

Afin de garantir aux Utilisateurs le respect de cet engagement qui serait requis par la législation, CA-SI-NO a défini des procédures détaillées pour la mise en œuvre des contrôles qui s'opèrent au sein de l'entreprise.

Ce chapitre définit par conséquent pour chaque groupe d'application

- les données qui sont contrôlées,
- la finalité des contrôles et la durée de conservation des données enregistrées (5.1),
- les procédures applicables en fonction du caractère plus ou moins intrusif des contrôles (5.2).

5.1 Traces et contrôles

CA-SI-NO souhaite au préalable attirer l'attention de chaque Utilisateur sur le fait que les outils informatiques génèrent aujourd'hui automatiquement des traces, sans que celles-ci aient été spécifiquement conçues pour permettre d'exercer une surveillance. Toutefois, certaines de ces données sont effectivement utilisées à des fins de contrôle de l'activité des Utilisateurs sur le réseau de l'entreprise. La description des données ainsi exploitées est détaillée ci-après par groupe d'applications.

D'une manière générale, l'Utilisateur admet que toute connexion aux réseaux internes de l'entreprise l'identifie et qu'elle est une acceptation de l'enregistrement automatique de traces de son activité.

5.1.1 Internet (Web)

La sécurisation des accès Internet est réalisée par la mise en place de pare-feu (firewall) et de serveurs proxy[11] qui enregistrent et filtrent les accès entrant et sortant.

En outre, il est rappelé à l'Utilisateur que certaines traces de ses connexions sont enregistrées automatiquement sur son disque dur, notamment dans le volet « Historique » de son navigateur et dans la mémoire cache de l'ordinateur (souvent appelée « Temporary Internet Files » ou « cache » dans l'arborescence du disque C:\).

11 **Proxy** désigne une machine « passerelle » permettant d'accéder à Internet. Un proxy gère des connexions multiples par un point de sortie unique. Une politique de filtrage est implémentée sur le proxy pour contrôler l'usage de l'internet

Le cas échéant, CA-SI-NO se réserve le droit d'investiguer ces données sous réserve du respect des procédures décrites à la section 5.2 du présent document.

Au-delà du blocage automatique des données ou fichiers comportant un virus ou un autre programme logique malveillant, un filtre, basé sur une liste de sites non autorisés ou « liste noire » (remise à jour périodiquement), est également mis en place et enregistre les tentatives de connexion sur ces sites. Cette « politique de filtrage » vise notamment les sites ayant un contenu pornographique ou obscène, les sites se rapportant au terrorisme et à toute action fondée sur la menace ou la terreur, les sites dont le contenu est une provocation à la haine raciale et aux théories négationnistes ou qui sont discriminants. D'une manière générale, le filtrage des URL[12] peut être mis en place pour tous les sites n'ayant aucun lien avec les missions professionnelles des Utilisateurs (ex. : les sites relatifs aux jeux et aux paris). La politique de filtrage est rendue publique sur l'INTRANET du groupe Casino.

Les données enregistrées dans le cadre de l'utilisation des accès Internet sont :

- adresse IP[13] de la machine connectée
- identifiant de l'Utilisateur
- date et heure des connexions
- identification des sites visités (nom et adresse IP)
- catégorie du site (la catégorie est prédéfinie et affectée par le filtre)
- type des données demandées (page HTML, image, etc.)
- statut de la connexion : autorisé/refusé
- taille des données expédiées ou reçues

Les données ainsi enregistrées pourront être conservées pendant une (1) année et ce en référence à la Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

Le contrôle des données susvisées a pour objectif :

- la prévention de la mise en péril des systèmes notamment par l'importation de virus,
- la prévention de l'encombrement du réseau,
- le contrôle du respect des règles définies par la présente Charte (ex.: usage personnel dans des limites raisonnables),
- l'optimisation de la bande passante

Les statistiques et les contrôles effectués à partir de ces données peuvent, indirectement et *a posteriori*, être ventilées par Utilisateur. Dans ce cas, ces opérations sont réalisées conformément à la procédure d'autorisation décrite au paragraphe 5.2.3 :

- soit à des fins uniquement de maintenance et de bonne administration
- soit à des fins de contrôle.

12 **Adresse URL** (Uniform Resource Locator) désigne l'adresse Internet exploitée par les navigateurs (Internet Explorer par exemple) et qui permet de localiser n'importe quel document sur n'importe quel ordinateur relié au Web (World Wide Web).
13 **Adresse IP** (Internet Protocol) désigne un numéro unique (normalement compris sur quatre octets séparés par un point. Par exemple : 87.34.53.12) et permettant d'identifier une machine sur un réseau TCP/IP (TCP est le protocole de transport de l'information pour assurer une communication de bout en bout). Cette adresse standardisée est indispensable pour le dialogue des machines entre elles et leur reconnaissance mutuelle sur le réseau Internet ou local.

5.1.2 Messagerie électronique

Le contrôle de l'utilisation de la messagerie porte sur les données suivantes :

- les flux entrant et sortant,
- la désignation de l'expéditeur,
- la désignation du destinataire,
- la date et l'heure du message,
- le sujet du message,
- le contenu du message (lorsqu'il n'est pas signalé ou archivé comme « PRIVÉ ou privé ou PRIVE ou prive ou PRIVATE ou private ou personnel ou PERSONNEL» ou « SOCIAL ou social ou SOCIALE ou sociale», conformément à la règle énoncée au paragraphe 5.2.1.),
- les messages bloqués par le serveur de mail (ex. : porteur d'un virus ou spam),
- la taille des messages.

Par ailleurs les traces ainsi conservées sont utilisées à des fins de maintenance pour les opérations suivantes :

- la sauvegarde des messages, mais uniquement à des fins de restauration,
- le suivi de route (cheminement) des courriers et l'optimisation des performances,
- l'entretien du système et la détection préventive de virus,
- la prévention de l'encombrement du serveur de messagerie.

Ces données sont conservées au maximum pendant 6 mois. Elles peuvent être contrôlées seulement par l'administrateur, son supérieur hiérarchique, le Directeur RH de la filiale ou la Direction de la Sécurité des SI.

L'accès au contenu des messages d'un Utilisateur donné à des fins de contrôle et d'investigation est exceptionnel : il ne peut intervenir qu'au cas par cas sur demande de la Direction de la sécurité des SI et dans le respect strict de la procédure décrite aux paragraphes 5.2.1 et 5.2.3.

5.1.3 Applications et réseaux internes

Des fichiers de journalisation des connexions permettent d'identifier et d'enregistrer toutes les connexions ou tentatives de connexion aux différentes applications, bases de données et domaines du réseau du groupe Casino. Les données qui peuvent être ainsi enregistrées sont les suivantes :

- date et heure des connexions
- certains éléments de la configuration des postes Utilisateur (système d'exploitation, type de navigateur par exemple)
- activité courante des serveurs et des segments réseau
- activité sur les fichiers (accès, lecture, modification, suppression)
- activité sur les serveurs d'impression,
- activité sur les annuaires : espace disque utilisé, statut du compte et du mot de passe, dernière connexion, nombre de fichiers ouverts, …
- échecs de connexion
- tentatives de violation de droits d'accès
- changement des fonctions de sécurité

Cette liste n'est en aucun cas exhaustive et augmente au fil des évolutions de toute nouvelle fonction proposée par les logiciels de maintenance et de surveillance de l'activité des systèmes d'information.

La vocation première de ces fichiers de journalisation n'est pas le contrôle des utilisateurs proprement dit, mais a essentiellement pour objectif de garantir :

- la maintenance et la bonne utilisation des systèmes,
- l'optimisation des ressources,
- la sécurité du système et la prévention des attaques ou des mauvais fonctionnements.

Ces fichiers de journalisation sont conservés selon les besoins entre 1 semaine et 1 an. Ils sont réservés à l'usage des administrateurs des applications et systèmes et, de leur responsable hiérarchique, lesquels font suivre, le cas échéant, des rapports d'incident (tels que visés au paragraphe 5.2.2) auprès de la Direction de la Sécurité des SI.

5.1.4 Téléphonie

Les données enregistrées dans le cadre de l'autocommutateur téléphonique (PABX) sont les suivantes :

- numéro appelant extérieur complet
- numéro appelé extérieur complet
- identification de l'appelant
- la durée de la communication,
- le nombre de communications par jour et par mois.

Le même type de données est enregistré dans le cadre du contrôle de la téléphonie mobile (flotte GSM). Le format correspond aux informations classique d'une facture détaillée opérateur.

Nota bene :

- Lorsque ces données figurent sur des documents diffusés en interne, les quatre (4) derniers chiffres des numéros sont masqués dans un souci de confidentialité.
- Aucun matériel d'écoute et d'interception des correspondances n'est mis en œuvre sur le réseau de communication de CA-SI-NO. Ainsi aucune surveillance et aucun enregistrement des conversations n'est possible ni autorisé.

Le contrôle de ces données et l'analyse des facturations Télécoms a pour unique objectif la maîtrise et le suivi des coûts d'exploitation. Ces données sont conservées pour une durée maximale de un (1) an et sont contrôlées par l'équipe d'exploitation du service maintenance et/ou la direction financière.

Les utilisations à titre privé manifestement abusives sont signalées le cas échéant au responsable hiérarchique de l'Utilisateur en cause.

5.2 Procédures applicables

Il sera présumé qu'un message envoyé ou reçu ainsi que tout fichier, répertoire ou archive créés depuis le poste de travail ou tout moyen mis à la disposition de l'Utilisateur par l'entreprise revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire ou du dossier où il pourrait avoir été archivé par son destinataire du caractère et de la nature privée (voir § 5.2.1) ou sociale (voir § 5.2.2) du message ou du fichier ou répertoire ou archive en cause, lesquels sont dès lors protégés par le principe du respect de la vie privée et du secret des correspondances.

5.2.1 Principe préalable concernant l'usage des moyens informatiques à des fins privées

Afin de favoriser un marquage commun par tous les Utilisateurs, et facilement reconnaissable par les administrateurs réseaux et systèmes, les messages électroniques ainsi que tout document et archives associées et tout fichier, répertoire ou archive auquel l'Utilisateur souhaite conférer une nature et un caractère personnel, devront être identifiés sous l'intitulé ci-après : « Privé ou privé ou PRIVE ou prive ou PRIVATE ou private ou personnel ou PERSONNEL».

L'ensemble de ces messages (contenu et données attachées) ou fichiers, répertoires ou archives signalés comme « PRIVÉ ou privé ou PRIVE ou prive ou PRIVATE ou private ou personnel ou PERSONNEL» ne devront à aucun moment avoir été chiffrés (cryptés) par l'Utilisateur qui en est le propriétaire.

Un contrôle des données désignées comme «PRIVÉ ou privé ou PRIVE ou prive ou PRIVATE ou private ou personnel ou PERSONNEL» pourra avoir lieu pour répondre à des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau ou de l'espace disque. Ce contrôle peut conduire à la mise en place d'outils de mesure de la fréquence ou de la taille des messages, fichiers, répertoires et archives créés, transmis ou archivés, ainsi que tout contrôle d'ordre statistique permettant d'évaluer la sensibilité ou la dangerosité de ces données pour l'entreprise et son réseau informatique (ex. : analyse sémantique et par mot-clé mise en œuvre par des agents logiciel). En tout état de cause, CA-SI-NO s'interdira d'accéder à leur contenu sauf l'autorisation préalable de l'Utilisateur et la présence d'un représentant du personnel garantissant le respect des droits de l'Utilisateur.

5.2.2 Principe préalable concernant l'usage des moyens informatiques à des fins privées

Afin de favoriser un marquage commun par tous les Utilisateurs, et facilement reconnaissable par les administrateurs réseaux et systèmes, les messages électroniques ainsi que tout document et archives associées et tout fichier, répertoire ou archive et ayant pour émetteur, destinataire ou propriétaire un ou plusieurs:

- membres du service médical de l'entreprise devront être identifiés sous l'intitulé ci-après « prive », « privé », « PRIVE », « PRIVÉ », « private», «PRIVATE», «personnel», «PERSONNEL»
- représentants du personnel devront être identifiés sous l'intitulé ci-après : « SOCIAL ou social ou SOCIALE ou sociale ».

Un contrôle des données désignées comme « SOCIAL ou social ou SOCIALE ou sociale » pourra avoir lieu pour répondre à des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau ou de l'espace disque. Ce contrôle peut conduire à la mise en place d'outils de mesure de la fréquence ou de la taille des messages, fichiers, répertoires et archives créés, transmis ou archivés, ainsi que tout contrôle d'ordre statistique permettant d'évaluer la sensibilité ou la dangerosité de ces données pour l'entreprise et son réseau informatique (ex. : analyse sémantique et par mot-clé mise en œuvre par des agents logiciel). En tout état de cause, CA-SI-NO s'interdira d'accéder à leur contenu sauf l'autorisation préalable de l'Utilisateur et la

présence d'un représentant d'une des catégories listées ci-dessus en fonction de la nature de la correspondance et ce pour garantir le respect des droits de l'Utilisateur.

5.2.3 Rapport d'incidents

D'une manière générale, CA-SI-NO rappelle que la sécurité est l'affaire de tous et qu'il appartient à chaque Utilisateur qui constate des comportements contraires aux règles de bon sens en matière de sécurité ou à l'une des obligations énoncées dans la présente Charte d'en signaler les faits au responsable de la sécurité.

En particulier, les Utilisateurs sont tenus d'informer immédiatement les administrateurs :

- de toute violation, tentative de violation ou toute violation suspectée de son compte ou d'un système informatique ;
- de tout virus qu'il aura détecté, de tout changement de configuration, et de toute anomalie dans le fonctionnement de ses matériels ou applications informatiques ;
- de tout problème (mauvaise gestion des protections, faille système, logiciel suspect,...) pouvant nuire au bon niveau de sécurité.

De plus, que ce soit à l'occasion de l'accomplissement des missions professionnelles des équipes techniques de maintenance et d'exploitation, de contrôles par sondage (aléatoires) ou d'audits de sécurité internes ou externes, tout constat du non-respect des règles définies dans la présente Charte ou de la commission d'actes manifestement illicites pourra faire l'objet d'un rapport d'incident (information la Direction de la Sécurité des SI).

5.2.4 Traitement des suites

i. Les rapports d'incident (voir paragraphe précédent) pourront le cas échéant être suivis d'une mise en garde de l'Utilisateur et, en fonction de la gravité des faits, d'un signalement auprès du responsable de la Sécurité et, le cas échéant, des responsables ressources humaines et hiérarchique de l'Utilisateur mis en cause.
Les rapports d'incident constituent le faisceau d'indices de la violation répétée des règles de la Charte susceptible de justifier une investigation ciblée plus approfondie telle que visée au paragraphe ci-après :

ii. Lorsqu'un faisceau d'indices suffisamment large ou que la gravité des faits qui semblent pouvoir être reprochés à un Utilisateur le justifie, la décision de mener une investigation ciblée et plus approfondie sur les sessions de travail et les données ou fichiers se rapportant ou appartenant à cet Utilisateur est soumise aux conditions suivantes :

- cette décision est obligatoirement validée par la Direction des Ressources Humaines de la filiale, et le responsable de la sécurité ;
- l'Utilisateur visé est informé préalablement, à moins que l'urgence ne justifie une intervention immédiate (dans ce cas, le degré d'urgence est motivé);
- les opérations de contrôle sont menées en présence de l'Utilisateur accompagné s'il le souhaite d'un représentant du personnel de son choix (en cas d'absence de l'Utilisateur, les opérations de contrôle sont menées en présence d'un représentant du personnel pouvant témoigner, de façon impartiale et objective, du respect des droits de l'Utilisateur et de la finalité recherchée ;
- un procès-verbal des opérations de contrôle est établi et contresigné par l'Utilisateur ou le représentant du personnel.

iii. Si à l'issue de l'investigation précitée, il s'avère que les incidents relèvent bien de la responsabilité de l'utilisateur, son supérieur hiérarchique en accord avec la Direction des Ressources Humaines, se réserve le droit de prendre des mesures disciplinaires à son encontre.

6. ROLE ET RESPONSABILITE DES ADMINISTRATEURS

Les administrateurs, qui ont pour rôle de veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes, sont conduits par leur fonction même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à Internet, fichiers de journalisation, etc.), y compris toutes celles qui sont enregistrées sur le disque dur du poste de travail.

Dans le cadre de ces missions, ils peuvent être amenés à :

- utiliser des logiciels habituellement réservés et utilisables uniquement par des administrateurs. Ces logiciels devront, dans les meilleurs délais, être déclarés à la Direction de la Sécurité.
- utiliser des logiciels de télémaintenance qui permettent de détecter et de réparer les pannes à distance ou à prendre le contrôle, à distance, du poste de travail de l'Utilisateur avec l'accord de ce dernier ;
- procéder à l'une des opérations suivantes :
    - interruption prolongée de service moyennant l'information préalable des Utilisateurs ;
    - interruption de toute tâche utilisateur dans le cas où une utilisation excessive des ressources nuit au bon fonctionnement du système (avec ou sans préavis, selon l'urgence du problème) ;
    - mise sur un support externe ou compression des fichiers excessivement volumineux ou sans lien direct avec l'activité professionnelle (avec ou sans préavis) en cas de dégradation de service,
    - interruption des sessions de travail trop longtemps inactives.
- établir des rapports d'incident, signalant notamment tout événement mettant en cause la qualité et la sécurité des ressources informatiques ainsi que toute manifestation contraire au respect des règles de la présente Charte, conformément au paragraphe 5.2.2.

Tenus au secret professionnel, les administrateurs de réseaux et systèmes ne peuvent être contraints de divulguer des informations de nature personnelle qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des Utilisateurs et qu'elles ne mettent pas en cause ni le bon fonctionnement technique des applications, ni la sécurité, ni l'intérêt ou la responsabilité de l'entreprise.

7. PROTECTION DES DONNEES PERSONNELLES

En fonction de la législation en vigueur CA-SI-NO procède à la déclaration ou la demande d'autorisation préalable pour la mise en œuvre des fichiers, bases de données et autres traitements informatisés contenant des informations dites nominatives ou personnelles – c'est-à-dire des informations qui permettent l'identification, directe ou indirecte, des Utilisateurs.

Ces déclarations sont effectuées à l'initiative et sous la responsabilité des personnes ou services destinataires de ces fichiers, bases de données ou traitements.

Le responsable désigné du fichier ou de la base de données concernée a la charge d'informer les Utilisateurs de la nature des données traitées, de la finalité et de la durée du traitement, ainsi que de leur droit d'accès et des modalités d'exercice de ce droit.

Afin de simplifier les procédures internes ou externes notamment vis-à-vis de la CNIL (Commission Nationale Informatique et Libertés), CA-SI-NO a nommé un C.I.L (Correspondant Informatique et Libertés) (cf. annexe2)
La fonction de correspondant répond à un double objectif. Elle emporte un allègement considérable des formalités. Sa désignation permet en effet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants.
Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisations et continuent à faire l'objet de formalités. Le Correspondant Informatique et Libertés (C.I.L) apporte une aide précieuse au responsable du traitement. Il a un rôle de conseil et suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion de données à caractère personnel.
Il propose les solutions permettant de concilier protection des libertés individuelles et intérêt légitime des professionnels.

8. RESPONSABILITE ET SANCTIONS

Le non respect ou la violation des règles et obligations de la présente Charte engage la responsabilité de l'Utilisateur et constituera une faute susceptible de sanctions disciplinaires conformément à l'application des dispositions du règlement intérieur applicable.

De plus, la responsabilité personnelle de l'Utilisateur pourra être recherchée :

- en cas de dommages causés à un tiers ou à CA-SI-NO ou au groupe Casino et ;
- pour les infractions pénales qu'il commet au sein de l'entreprise ou au moyen des ressources mises à sa disposition.

De plus, lorsque l'Utilisateur en cause est un intervenant externe ou tout agent d'un prestataire ou d'un sous-traitant, le non-respect de la Charte par l'Utilisateur fait l'objet d'une expulsion des locaux du groupe Casino de ce dernier. Le service Achats est également informé. Des sanctions à l'encontre des commettants, lorsqu'elles sont prévues par le contrat passé entre CA-SI-NO et ce commettant, peuvent être mise en œuvre à la discrétion de CA-SI-NO.

9. DIVERS

L'ensemble des stipulations de la présente Charte remplace et annule tous les engagements, acceptations, ententes et accords préalablement convenus ou souscrits entre CA-SI-NO et les Utilisateurs relativement au contenu des dispositions auxquelles cette Charte s'applique ou qu'elle prévoit.

Dans l'hypothèse où l'une des dispositions de la Charte devait être considérée comme nulle du fait d'une décision des tribunaux, la validité de la Charte dans son ensemble n'est pas remise en cause et les autres dispositions continuent de s'appliquer.

CA-SI-NO se réserve le droit de modifier à tout moment l'une quelconque des dispositions de la présente Charte en respectant les procédures légales en vigueur sauf si cela concerne des changements mineurs se traduisant par de simples ajustements rédactionnels ou de forme.

ANNEXE 1

RESUME DES REGLES DE GESTION RELATIVES A LA CLASSIFICATION ET LA PROTECTION DES INFORMATIONS

	RESTREINT / USAGE INTERNE SEULEMENT	***CONFIDENTIEL***	***SECRET***
Risque en cas de divulgation	*– Pouvant causer un certain impact pour CA-SI-NO, un de ses sites ou de ses partenaires, la divulgation est inappropriée ou prématurée.*	*– Pouvant causer des dommages graves à CA-SI-NO, un de ses sites ou de ses partenaires*	*– Pouvant mettre en péril CA-SI-NO, un de ses sites ou de ses partenaires*
Marquage	*– En évidence sur chaque page (ou sur le support).*	*– En évidence sur chaque page et en rouge sur la première (ou sur le support)*	*– En évidence et en rouge sur chaque page (ou sur le support)*
Protection des zones et des réseaux	*– Zone à accès protégé* *– Réseaux à accès protégés*	*– Zone fermée à accès contrôlable* *– Réseaux contrôlables seulement*	*– Zone fermée à accès contrôlé* *– Aucune connexion réseau*
Copies et diffusion	*– Groupe de personnes autorisées identifié sur chaque copie* *– Pas de liste de diffusion requise* *– Copies libres en cas de besoin seulement*	*– Liste de diffusion initiale sur chaque copie* *– Liste complète conservée par l'émetteur* *– Numéro de page / total, sur chaque page* *– Copies additionnelles avec autorisation explicite de l'émetteur*	*– Nom du destinataire sur chaque copie* *– Pas de liste de diffusion sur les copies ; liste complète gardée par l'émetteur* *– Numéro de page / total, sur chaque page* *– Copies additionnelles interdites*
Transport	*– Simple enveloppe sans marque externe* *– par courrier de confiance* *– Fax et E-mail interne CA-SI-NO en clair* *– Fax et E-mail cryptés pour réseaux externes.*	*– Double enveloppe sans marque externe, enveloppe interne marquée "Confidentiel"* *– par transporteur de confiance* *– accusé de réception* *– Fax et E-mail cryptés seulement*	*– Double enveloppe sans marque externe, enveloppe interne marquée "Secret"* *– en main propre ou tiers de confiance* *– accusé de réception* *– aucune transmission électronique*
Stockage	*– Zone et moyens à accès protégé*	*– Coffre sécurisé contrôlé*	*– Coffre sécurisé contrôlé*
Destruction	*– Broyeur ou tout autre moyen de destruction homologué par C.I.T.*	*– Broyeur ou tout autre moyen de destruction homologué par C.I.T.* *– Destruction tracée par l'émetteur*	*– Broyeur ou tout autre moyen de destruction homologué par C.I.T.* *– Destruction par l'émetteur*

ANNEXE 2

DISPOSITIONS SPECIFIQUES RELATIVES AU DEPLOIEMENT

1. – Dispositif de protection par caméra vidéo

Il est rappelé aux utilisateurs que le droit d'accès aux enregistrements vidéo est de droit et qu'il peut être exercé auprès du Service de la Sécurité dans la limite de la durée de conservation des enregistrements fixée à 8 jours.

Par ailleurs, le Service Sécurité des Sites du groupe Casino pour la France atteste par la présente Charte que l'emplacement des caméras vidéo mises en œuvre pour la protection des personnes et des biens sur les Sites du groupe Casino, n'est pas dissimulé.

2. – Informations relatives à la législation en matière de protection des données personnelles (« Informatique et Libertés »)

L'autorité administrative compétente en matière de contrôle du respect de la législation sur la protection des données personnelles est la Commission Nationale Informatique et Libertés, couramment désignée sous l'acronyme 'CNIL'.

2.1 – Les déclarations à la CNIL

Il appartient à chaque responsable de service de s'assurer de la conformité des fichiers nominatifs* mis en œuvre dans le cadre de son service à la législation en matière de protection des données personnelles.
(*) Par fichier nominatif, il faut entendre tout fichier ou traitement informatisé de données permettant d'identifier, directement ou indirectement, une personne donnée.
En particulier, ils sont tenus responsables du correct accomplissement des formalités préalables de déclaration à la CNIL des traitements concernés.
L'encadrement sera informé des dispositions légales en vigueur et assisté par le C.I.L (Correspondant Informatique et Libertés) nommé par CA-SI-NO.

Pour en savoir plus sur ces formalités et déterminer vos obligations légales en la matière, les responsables de service sont invités à contacter le service juridique ou le CIL de CA-SI-NO.

2.2. – L'information sur les droits des personnes objet des fichiers automatisés de données personnelles

Les salariés et autres intervenants du groupe Casino sont invités à adresser leurs demandes d'information

- soit auprès du C.I.L (Correspondant Informatique et Libertés)
- soit auprès du responsable du traitement des données personnelles concernées

Type de document : Procédure		
	Origine de la contribution : GTE 06 Espace RH	Pays concerné(s) : France Branche(s) / Activité(s) / Service(s) concerné(s) : Géant, Proximité, Supermarchés

Titre du document :
REGLEMENT INTERIEUR DU 01/11/2009 DISTRIBUTION CASINO FRANCE (Procédure Pays)

Mots-clés / Objectifs du document :
REGLEMENT INTERIEUR DCF 2009

Remarques :

Nom du fichier attaché :
ANNEXE_2_RI_DCF_2009.pdf
Ce fichier est attaché au document :
REGLEMENT INTERIEUR DU 01/11/2009 DISTRIBUTION CASINO FRANCE

Valideur	Certificateur
CROZIER FRANCOISE (020911)	SZYDLAK AGNES (015116)

Date d'application	Date de publication	Version publiée
02/11/2009	02/11/2009	V0