SOCIETE GENERALE

Direction Organisation et Système d'Information
(DOSI)

C1 RESTREINT

Date 17/11/2023

CHARTE D'UTILISATION DU SYSTÈME D'INFORMATION

DESTINATAIRES
L'ensemble du personnel travaillant pour SOCIETE GENERALE COTE D'IVOIRE : salariés, consultants, prestataires de services, intérimaires, stagiaires
RÉSUMÉ
Le présent document décrit les exigences de sécurité auxquelles doivent se conformer l'ensemble des utilisateurs du Système d'Informations de la SOCIETE GENERALE COTE D'IVOIRE.
RENSEIGNEMENT

AFS CISO
RSSI AFS
Contact : afs.ciso@socgen.com

Hind KAROUF
RSSI SG COTE D'IVOIRE
Contact: hind.karouf@socgen.com

Walter KOUADIO et Fabrice KOUASSI
CRSSI SGCI
RISQUE_SECURITE_SI@bhfm-ci.fr.socgen.com

VALIDITE	**CLASSEMENT**
Date d'effet : dd/mm/2023 Diffusion : tous les collaborateurs SG COTE D'IVOIRE	C1- RESTREINT

Table des matières

I. Préambule ... 3
1. Objet du document ... 3
2. Contexte et enjeux ... 3
3. Objectifs de la charte ... 3
4. Périmètre d'application de la charte utilisateurs ... 3
5. Communication de la charte utilisateurs ... 4
II. Sécurité de l'information ... 4
1. Conditions d'accès au SI ... 4
2. Protection des informations ... 4
III. Sécurité du poste de travail ... 5
1. Généralités ... 5
2. Règles de sécurité du poste de travail ... 6
3. Règles d'usage du partage « réseau » et fichiers personnels ... 6
4. Utilisation des supports de stockage ... 7
5. Intervenants extérieurs ... 7
IV. Sécurité de la messagerie ... 7
1. Règles à respecter pour garantir la sécurité de la messagerie ... 7
2. Contrôle de l'usage ... 9
V. Accès aux réseaux extérieurs ... 9
1. Utilisation de l'accès Internet mis à disposition par SGCI ... 9
2. Utilisation d'internet à des fins personnelles ... 10
VI. Cas particulier des responsables hiérarchiques ... 10
VII. Cas particulier des administrateurs informatiques ... 11
VIII. Signalement des incidents ... 12
1. Détection d'un incident de sécurité ... 12
2. Contact ... 12
3. Actions à mener en cas d'incident ... 12
IX. Respect des lois en vigueur ... 13
X. Traçabilité, contrôles et sanctions ... 13
1. Traçabilité ... 13
2. Contrôles effectués sur l'utilisation du SI ... 14
3. Sanctions ... 15

I. Préambule

1. Objet du document

Ce document vise à présenter les droits et les devoirs propres à tout utilisateur du Système d'Information de la *SOCIETE GENERALE COTE D'IVOIRE*

Important

Une partie spécifique détaille les droits et devoirs propres aux administrateurs du Système d'Information, qui sont également concernés par la présente charte.

2. Contexte et enjeux

Le système d'information (SI) est l'ensemble des ressources (matérielles, logicielles, humaines, etc.) qui permettent de collecter, de stocker, de traiter et de diffuser des informations au sein d'une organisation. Il vise à soutenir les processus opérationnels, la prise de décision et la gestion au sein de cette organisation.

La sécurité et la disponibilité de ces moyens dépendent de l'usage qui en est fait par chacun.

Un 1er niveau de protection est assuré par de multiples dispositifs (antivirus, anti-spam, coupe-feu, droits d'accès aux ressources informatiques, procédures, etc.), répartis en couches successives sur tous ses éléments, suivant le principe de « la défense en profondeur ».

Toutefois, ces dispositifs n'assurent pas une protection totale, et le facteur humain est un élément essentiel de la sécurité du SI, qu'il convient d'encadrer par le présent texte.

Important

Une Politique de Sécurité du système de l'Information (PSSI) a été définie. Elle institue des principes et des règles de sécurisation des Systèmes d'Information, et précise les règles et responsabilités de la filiale, SGABS et de tous les acteurs du SI. La présente charte s'inscrit dans le cadre de ces principes, et vient en complément de la Politique de Sécurité du système de l'Information.

3. Objectifs de la charte

Cette charte a pour objectif de :

- Préciser les règles et précautions que se doit de respecter tout utilisateur du SI de la *SGCI*, quel que soit son niveau hiérarchique.
- Souligner la responsabilité de l'utilisateur quant à l'usage qu'il en fait, au regard du patrimoine collectif.

Cette charte ne prétend pas à l'exhaustivité et n'est pas le mode d'emploi ou un référentiel technique de tous les éléments du SI. Les informations plus approfondies peuvent être trouvées dans des documents spécifiques à chaque élément du SI.

4. Périmètre d'application de la charte utilisateurs

La charte utilisateurs de la *SGCI* s'applique à tout utilisateur du SI de la *SGCI*

Un **utilisateur** est toute personne ayant accès au SI :

- Les collaborateurs de la SGCI, quelle que soit leur localisation (locaux de la SGCI ou en connexion distante)
- Les tiers intervenants : prestataires, sous-traitants, stagiaires, vacataires, etc.

5. Communication de la charte utilisateurs

La charte doit être communiquée à tous les utilisateurs. Sa mise à jour doit faire l'objet d'une communication.

II. Sécurité de l'information

1. Conditions d'accès au SI

L'accès au SI par l'utilisateur s'effectue par une identification et une authentification :

- Soit via un dispositif d'authentification normale (un identifiant associé à un authentifiant)
- Soit via un dispositif d'authentification forte (calculette, carte image,…).

L'utilisateur doit assurer la protection des moyens d'accès qui lui sont affectés : compte, mots de passe, certificats sur carte à puce, dispositif d'authentification forte,…

Règles d'utilisation du mot de passe

L'utilisateur doit :

- Choisir des mots de passe sûrs : 12 caractères minimum, cumulant au moins une majuscule, une minuscule, un chiffre et un caractère spécial (!-{[|@...).
- Changer ses mots de passe régulièrement, au minimum tous 90 jours.
- Les garder secrets et s'obliger à les mémoriser, il s'interdit de noter ses mots de passe sur papier ou dans un fichier non protégé.

Il ne doit jamais :

- Communiquer ses mots de passe à un tiers, ses collègues, son correspondant informatique.
- Demander les mots de passe à un tiers, y compris à ses collaborateurs.
- Prêter ou emprunter des moyens d'authentification.
- Utiliser un mot de passe d'administration en dehors des SI de la SGCI

2. Protection des informations

L'utilisateur doit adopter un niveau de protection en rapport avec :

- Le niveau de classification de l'information (C0, C1, C2, C3) tel que défini dans la Politique de classification des données de SGCI.

  Les documents à diffusion restreinte (C2) ne peuvent être adressés en messagerie interne ou externe (Internet) qu'en pièces jointes chiffrées par un logiciel agréé, l'échange des clés de chiffrement s'effectuant par un autre moyen de communication ou au travers d'un mail séparé. Les logiciels disponibles à SGCI sont 7-Zip, Secureshare et SecureHub.

Règles de protection de l'information

L'utilisateur :

- Veille à ne pas mettre à la disposition de personnes non autorisées un accès aux systèmes d'information et à ne pas utiliser ou essayer d'utiliser des droits d'accès autres que les siens, en particulier l'accès physique au bureau.
- Ne doit pas tenter de lire, modifier, copier ou détruire des données ou documents autres que ceux qui lui appartiennent en propre ou pour lesquels il dispose du droit correspondant : lecture, modification ou suppression.
- Utilise les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection physique des équipements mobiles (ordinateur portable, périphériques USB, etc.).
- Doit demander à son supérieur hiérarchique le droit de conserver des données lorsqu'il quitte ses fonctions. Cela doit être formalisé dans un document signé par le supérieur hiérarchique et mentionnant précisément les documents en question sans qu'une ambiguïté puisse subsister. À défaut, il est strictement interdit de conserver des données professionnelles lors d'une mutation ou une fin de fonction (y compris à des fins professionnelles ultérieures).

III. Sécurité du poste de travail

1. Généralités

Un poste de travail désigne l'ensemble des moyens techniques mis à la disposition d'un utilisateur, lui permettant d'accomplir sa mission. (*Rentrent dans la cadre de cette définition : écrans, claviers, imprimantes, télécopieurs, tablettes, Smartphones, etc.)*

Règles générales d'utilisation du poste de travail

L'utilisateur :

- Est responsable de l'usage qu'il fait des ressources informatiques mises à sa disposition.
- Ne doit connecter au SI de la SGCI que les équipements professionnels mis à sa disposition par *SGCI* (postes de travail fixe ou portables, tablettes, smartphones, périphériques USB, disque dur…)
- Ne doit jamais modifier lui-même la configuration de son poste de travail et de ses autres équipements. Ceci ne peut être réalisé que par la cellule informatique.
- Ne doit réaliser aucune copie de logiciels.
- Est tenu de restituer son matériel en cas de départ de la SGCI
- Ne doit pas désactiver le logiciel anti-virus de son poste de travail ni faire obstacle aux mises à jour régulières (correctifs de sécurité et autres).
- S'interdit d'installer de nouveaux logiciels (en particulier, les logiciels de jeux, « barres d'outils », logiciels Peer-to-Peer), en provenance d'Internet, des supports amovibles récupérés dans les revues informatiques.
- Ne pas connecter des périphériques USB.

- Veillera à respecter les mesures de précaution nécessaires lorsqu'il quitte son poste de travail
- L'utilisateur est tenu de verrouiller sa session avant de quitter son poste en composant les touches (Windows+L ou Ctrl+Alt+Suppr).
- Déconnexion systématique de l'application utilisée lors d'une absence
- Extinction systématique du poste de travail en fin de journée, sauf en cas de sollicitation expresse de l'équipe informatique (mise à jour logicielle, …)
- Doit ranger sous clef les cartes à puce, calculette,…
- Doit fermer les bureaux.
- L'utilisation de logiciels non fournis par la **SGCI** est interdite sauf dérogation du service informatique et du RSSI.

L'utilisateur est responsable de l'utilisation du SI réalisée via ses droits d'accès et la protection des équipements mis à sa disposition.

2. Règles de sécurité du poste de travail

Règles spécifiques aux postes nomades

L'utilisateur :

- Ne doit pas connecter son ordinateur portable professionnel sur d'autres réseaux que celui de la SGCI (notamment sur Internet, à domicile ou via point d'accès Wifi), sauf en cas de situations exceptionnelles (connexion à domicile via VPN, plan de continuité d'activité, ou déplacement…)
- Doit utiliser exclusivement les dispositifs d'accès distant fournis par *SGCI* lorsqu'il se connecte depuis Internet
- Doit veiller tout particulièrement à signaler au SUPPORT INFORMATIQUE (help.desk-sgci@socgen.com) dans les meilleurs délais toute perte, dégradation ou vol du matériel amovible mis à sa disposition : portables, carte 3G, dispositif d'authentification forte, Etc.

3. Règles d'usage du partage « réseau » et fichiers personnels

Les fichiers créés par l'utilisateur grâce aux outils informatiques mis à sa disposition sont présumés, sauf si l'utilisateur les identifie comme personnels, avoir un caractère professionnel, de sorte que *SGCI* peut y accéder hors de la présence de l'utilisateur.

Ainsi, Il appartient à l'utilisateur d'identifier les documents qui lui sont personnels, en les stockant dans un répertoire intitulé « privé ». Il sera le seul à avoir accès à ce dossier et celui-ci sera détruit à son départ.

Règles spécifiques à l'utilisation du partage « réseau »

- Il est interdit d'y stocker des fichiers personnels.
- Il est recommandé de privilégier systématiquement le stockage des fichiers à caractère professionnel sur les répertoires partagés, la sauvegarde y étant automatique et quotidienne.

4. Utilisation des supports de stockage

L'usage de tout type de support de stockage (clés USB, smartphone, PC, serveurs, disques externe…) est interdit, sauf dérogation formelle de la part du RSSI.

5. Intervenants extérieurs

Règles spécifiques à l'appel et à l'accueil d'intervenants extérieurs

- Les intervenants extérieurs sont tenus de respecter la présente charte (l'employeur du tiers étant responsable des actes de ses salariés), qui doit être incluse dans le contrat avec le prestataire.
- La connexion temporaire d'ordinateurs d'intervenants extérieurs est interdite, sauf mention explicite du contraire dans un contrat avec autorisation de la sécurité du système d'information (ex. audits, tests d'intrusion) signé entre ***SGCI*** et le prestataire.

IV. Sécurité de la messagerie

1. Règles à respecter pour garantir la sécurité de la messagerie

Règles d'utilisation de la messagerie

L'utilisateur :

- Est responsable des messages émis avec son adresse de messagerie.
- Veille à ce que le message émis ne porte pas atteinte à la personnalité, à la vie privée ou à l'activité professionnelle d'aucune personne, qu'elle soit collaborateur de la SGCI ou extérieure.
- Ne stocke ni ne diffuse de messages ou de documents de contenu diffamatoire, discriminatoire (raciste, sexiste…), pornographique ou incitant à la violence ou la haine raciale, qui sont interdits et réprimés par la loi.
- S'abstient de faire suivre des messages « canulars » : fausses alertes aux virus ; fausses chaînes de solidarité ; fausses promesses etc. Dans le doute il sollicite sa cellule informatique.
- Ne doit pas utiliser à des fins professionnelles les services de sites web spécialisés dans la messagerie (messagerie de type Web mail), ces sites n'apportent aucune garantie de confidentialité.
- Veille à la protection des informations diffusées par messagerie. Une information confidentielle doit être chiffrée lors de son échange.
- Doit utiliser avec discernement les listes de diffusion personnelles ou collectives et éviter l'envoi de copies à un nombre injustifié de destinataires.

Règles de vigilance sur la messagerie cas du PHISHING

Le phishing ou l'hameçonnage est un cybercrime qui consiste à utiliser de faux mails, sites Web et messages textes incitant la victime à révéler des informations personnelles et corporatives confidentielles : données de carte de crédit, numéro de téléphone, adresse postale, informations sur l'entreprise, etc. Ces informations sont ensuite utilisées par les criminels pour effectuer un vol d'identité et commettre une fraude.

Pour reconnaître un phishing, soyez attentif aux signes suivants :

1. **Lien suspect** : Vérifiez l'URL du site. Les liens de phishing peuvent ressembler à des sites légitimes mais avec des fautes d'orthographe ou des domaines similaires.

2. **Demandes d'informations sensibles** : Les courriels ou messages demandant des informations confidentielles, tels que des mots de passe ou des numéros de carte bancaire, sont souvent des tentatives de phishing.

3. **Mauvaise grammaire et orthographe** : Les communications de phishing ont souvent des erreurs linguistiques. Soyez attentif aux fautes de grammaire et d'orthographe.

4. **Pression pour agir rapidement** : Les messages de phishing créent souvent un sentiment d'urgence pour inciter à agir sans réfléchir.

5. **Absence de personnalisation** : Les messages de phishing génériques ne s'adressent pas directement à vous. Soyez sceptique si le message semble trop général.

Que faire en face d'un message suspect ?

1. **Ne pas cliquer** : Évitez de cliquer sur des liens ou de télécharger des pièces jointes provenant de sources suspectes.

2. **Ne partagez pas d'informations** : Ne fournissez jamais d'informations personnelles ou sensibles en réponse à des e-mails ou des messages douteux.

3. **Vérifiez l'expéditeur** : Assurez-vous que l'expéditeur est légitime en examinant l'adresse e-mail. Méfiez-vous des adresses qui semblent inhabituelles ou contiennent des erreurs.

4. **Signalez le phishing** : Signalez tout mail considéré comme suspect via le bouton Outlook "Message suspect" ou en envoyant le message en pièce jointe à l'équipe **CRSSI** « ***RISQUE_SECURITE_SI@bhfm-ci.fr.socgen.com*** »

5. **Supprimez le message** : Supprimez le message suspect de votre boîte de réception avoir l'avoir signalé pour éviter de cliquer accidentellement sur des liens.

6. **Changez vos mots de passe** : Si vous avez accidentellement fourni des informations sensibles, changez immédiatement vos mots de passe concernés.

7. **Surveillez vos comptes** : Gardez un œil sur vos comptes en ligne pour détecter toute activité suspecte. Signalez tout problème à l'équipe CRSSI.

2. Contrôle de l'usage

Les messages dont la taille dépasse la limite autorisée sont supprimés au niveau des serveurs de messagerie. De même, les pièces jointes aux extensions dangereuses (.exe, .dll etc.) sont supprimées automatiquement.

Dans les deux cas, un message d'information concernant la suppression et la non-rémission est envoyé à l'émetteur.

V. Accès aux réseaux extérieurs

L'accès à Internet est doté d'un mécanisme de filtrage d'adresses qui interdit les sites ou catégories de sites prohibés (sites à contenu raciste, pédophile,...). L'utilisateur doit, néanmoins, rester vigilant et s'interdire d'accéder à des sites illégaux.

1. Utilisation de l'accès Internet mis à disposition par SGCI

Règles d'usage de l'Internet

L'utilisateur :

- S'interdit de Visualiser, télécharger, transmettre ou conserver des contenus à caractère pornographique, pédophile, raciste, xénophobe, diffamatoire, portant atteinte au respect de la personne humaine et à sa dignité, incitant à la commission d'un délit ou d'un crime, contraires à l'ordre public ou aux bonnes mœurs, attentatoires à l'image de marque interne ou externe de la banque
- S'interdit toute intervention sur Internet (blog par exemple) en faisant état de son appartenance à *SGCI*, sauf accord écrit de sa hiérarchie.
- Ne doit pas faire usage de services et logiciels de messagerie instantanée et de téléphonie par Internet.
- Réserve la consultation de contenu vidéo et audio en temps réel (streaming) à un usage professionnel.
- Ne doit pas installer sur le réseau de la SGCI un quelconque moyen d'accès à un autre réseau, et en particulier à Internet (ADSL, Wifi, etc.).
- Ne doit pas contourner ou de tenter de contourner les dispositifs de protection et de contrôle (« proxy » pirate, « tunneling », prise de main à distance etc.).
- Ne doit accéder au réseau Internet, lorsqu'il est dans les locaux de la SGCI, qu'à partir de la connexion du réseau de la SGCI
- Ne doit pas transmettre ou publier des informations de classe différente de C0 (publiques) à propos de SGCI, de ses filiales ou plus généralement sur des entités du Groupe, de ses clients ou partenaires, ou de son personnel (sauf si autorisé par la hiérarchie et protégé par des moyens adéquats validés).

2. Utilisation d'internet à des fins personnelles

L'accès à internet est réservé à des fins strictement professionnelles. Cependant, un usage personnel au sein des locaux de la SGCI est toléré, dans le respect des règles mentionnées dans la présente charte et le suivi des recommandations suivantes.

SGCI s'autorise d'effectuer des contrôles sur l'usage d'Internet et de tracer certaines informations (*exemples : nom du site, pages consultées, date & heure de connexion),* nominativement, et les journaux sont conservés pendant une durée maximale définie par la réglementation en vigueur.

Règles d'utilisation d'internet à des fins personnelles au sein des locaux *de la SGCI*

L'utilisateur :

- Privilégie l'utilisation d'Internet à des fins personnelles pendant les heures de pause (*pauses déjeuner par exemple*) de sorte à ne pas perturber le trafic réseau professionnel de la SGCI.
- S'interdit de télécharger des fichiers volumineux
- S'interdit le téléchargement de programmes et d'utilitaires non autorisés sauf pour les personnes explicitement habilitées par le RSSI
- Veille au respect du droit d'auteur en s'interdisant de télécharger des films, musiques, images et logiciels soumis à un droit de licence.

VI. Cas particulier des responsables hiérarchiques

Les responsables hiérarchiques sont soumis, en tant qu'utilisateurs du Système d'Information, aux règles décrites ci-avant.

Par ailleurs, du fait de leur responsabilité hiérarchique, ils sont également tenus de respecter les exigences suivantes :

Règles à destination des responsables hiérarchiques

- Dans les cas d'infraction constatée ou suspectée à l'encontre des lois et règlements, procéder à la mise en place de mesures conservatoires préservant les preuves éventuelles (mise au coffre du serveur attaqué, du poste de travail de l'utilisateur en infraction, etc.) en l'attente du résultat de l'enquête administrative.
- Veiller à fournir aux processus métiers un niveau de sécurité adapté aux enjeux, en relation avec les services informatiques

VII. Cas particulier des administrateurs informatiques

Les administrateurs informatiques *de la SGCI* sont soumis, en tant qu'utilisateurs du système d'Information, aux règles décrites ci-avant.
Cependant, ces acteurs bénéficiant de privilèges élevés sur les ressources informatiques *de la SGCI*, ils sont tenus de respecter les exigences suivantes :

Règles à destination des administrateurs informatiques

Ils sont tenus à un strict devoir de confidentialité et de discrétion :

- Les informations confidentielles et/ou personnelles (traces informatiques, fichiers, contenus de bases de données, en-têtes de messages électroniques, etc.) auxquelles ils ont accès ne peuvent être utilisées qu'à des fins de diagnostic ou d'administration des systèmes, dans le strict respect de la règlementation en vigueur
- Ils ne doivent pas accéder ou tenter d'accéder à des informations personnelles telles que le contenu de messages électroniques ne leur étant pas destinés ou des fichiers et répertoires manifestement et/ou explicitement personnels, sauf actions ponctuelles, en présence de l'utilisateur concerné et avec son autorisation expresse
- Ils n'autorisent personne à accéder à ces informations, sauf cas particuliers prévus par la Loi ou habilitations formelles et légitimes préalablement déclarées (délégation d'agenda, etc.)
- Ils ne doivent pas chercher à obtenir des informations confidentielles en dehors des besoins liés à leurs missions
- Ils ne doivent pas se connecter à une ressource sans l'autorisation expresse de la personne à qui elle est attribuée, notamment dans le cas d'une prise de main à distance sur un poste de travail, ou d'absence prolongée de la personne concernée

Ils sont vigilants à ne jamais :

- Abuser de leurs pouvoirs et de leurs privilèges sur les ressources informatiques. L'exercice malveillant des prérogatives d'un administrateur peut être constitutif d'une infraction pénale.
- Communiquer à des tiers non habilités des informations sur les systèmes qu'ils administrent
- Ne jamais autoriser la connexion temporaire d'ordinateurs d'intervenants extérieurs, sauf en situation de force majeure et sous la validation du Responsable de la Sécurité des Systèmes d'Information de la DSI *de la SGCI*

Ils jouent de plus un rôle central dans la gestion des incidents de sécurité :

- Ils escaladent systématiquement tout incident sécurité ou tout élément permettant de suspecter un incident de sécurité

Il est de plus rappelé qu'ils sont chargés :

- De la gestion technique des droits des utilisateurs de leur périmètre, et veillent en particulier à la suppression des droits et comptes des utilisateurs ayant quitté *SGCI*,
- De veiller à bien supprimer tout fichier des disques durs et clés USB mis au rebut (par les outils de formatage et de suppression définitive de fichiers),
- De l'application dans les meilleurs délais des divers correctifs diffusés
- De l'impérative tenue à jour de l'antivirus des serveurs et ordinateurs personnels de leur parc.

VIII. Signalement des incidents

1. Détection d'un incident de sécurité

Les situations suivantes peuvent être qualifiées d'incident de sécurité :

- En cas de comportement anormal (au sens disponibilité, intégrité, confidentialité) du poste de travail, des applications ou des données utilisées ou en constatant, par exemple, la suppression ou la modification de fichiers.
- Une machine opère des actions non commandées, le système s'arrête et redémarre tout seul, des messages non sollicités qui s'affichent seuls.
- En cas de constatation de comportements ou évènements « suspects » : messagerie, vol ou perte de données, compromission de données personnelles ou confidentielles.
- Antivirus inhibé : le logiciel antivirus ne répond plus, ou est désactivé.
- Correspondants mécontents : l'utilisateur a reçu un courriel en provenance d'un ou plusieurs correspondants, qui prétendent que ses courriels sont infectés.
- En cas d'usurpation d'identité par mail.

En cas d'incident, l'utilisateur est tenu de le signaler le plus rapidement possible au Correspondant Risque et Sécurité local « RISQUE_SECURITE_SI@bhfm-ci.fr.socgen.com» . Tout retard peut entraîner des conséquences graves et croissantes avec le temps.

2. Contact

Procédure à suivre en cas d'incident

- L'utilisateur doit prévenir le plus rapidement possible le Correspondant Risque et Sécurité local « ***RISQUE_SECURITE_SI@bhfm-ci.fr.socgen.com***»
- Le Correspondant Risque et Sécurité local transmettra cette information au CERT SG, le RSSI et la DSI

3. Actions à mener en cas d'incident

L'utilisateur, sur le plan technique, ne doit mener aucune action corrective ou d'investigation.

La cellule informatique, en cas d'incident avéré, met tout en œuvre, en coopération avec Correspondant Risque et Sécurité local, le RSSI et le CERT SG, pour permettre une résolution rapide de l'incident :

- Isolement des serveurs ou postes de travail ou segment réseau concernés : il convient de déconnecter la machine suspecte (PC ou serveur) du réseau en débranchant le câble réseau. L'isolation sera fonction de l'étendu de l'incident.
- Il convient de ne pas éteindre ou redémarrer la machine pour permettre la recherche d'indices et de traces.

IX. Respect des lois en vigueur

Tout utilisateur doit respecter les lois en vigueur relatives à l'utilisation des technologies de l'information et de la communication.

Les lois ou réglementations incluent notamment des mesures interdisant :

- L'atteinte à la vie privée (sujets relatifs entre autres aux opinions politiques, philosophiques ou religieuses, aux origines ethniques, à la vie sexuelle ou à la santé des personnes)
- Les actes de violence écrite ou verbale ou contraires aux règles d'éthique du Groupe Société Générale ou aux bonnes mœurs, notamment :
  - La diffamation et l'injure
  - L'incitation aux crimes et délits et l'incitation au suicide, à la discrimination, à la haine (notamment raciale), ou à la violence
  - Le révisionnisme et l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité
  - La compromission de mineurs ou leur exposition à des messages à caractère violent, ou pornographique ou pédopornographique
  - L'incitation à la consommation de substances interdites
- La fraude informatique, incluant des actes tels que :
  - L'accès ou le maintien frauduleux dans un Système d'Information
  - La falsification, la modification, la suppression et l'introduction d'informations avec l'intention de nuire
  - La modification, la suppression et l'introduction de traitements dans un système dans le but d'en fausser le comportement
- La violation du secret d'affaires (divulgation d'informations confidentielles, d'informations commercialement sensibles…)
- Les actes allant à l'encontre des règles protégeant les droits de propriété intellectuelle, notamment :
  - La contrefaçon de marque et les copies de logiciels commerciaux pour quelque usage que ce soit
  - Le non-respect des droits d'auteurs
- Le non-respect de la réglementation relative aux fichiers comportant des données à caractère personnel

X. Traçabilité, contrôles et sanctions

1. Traçabilité

Dans le respect des principes de transparence et de proportionnalité, l'attention des utilisateurs est attirée sur le fait que les dispositifs de sécurité informatique (pare-feu, systèmes de contrôle des accès…) mis en place par *SGCI* enregistrent les traces d'activités des systèmes.

L'utilisateur est donc informé que les messages émis ou reçus sont conservés, de même que les traces suivantes :

- Liste des ressources auxquelles l'utilisateur a eu accès sur Internet avec les paramètres techniques de connexion (avec notamment l'identifiant de compte de l'utilisateur, date et heure, volume des données transmises…)
- Date et heure des authentifications des utilisateurs sur les systèmes d'accès aux moyens de communication électronique

- Liste des paramètres techniques nécessaires à la gestion des services de messagerie électronique (identification du compte de l'utilisateur, coordonnées du destinataire, date et heure, volume, format et nature des pièces jointes,…)

Les traces et messages pourront être conservés pendant une durée maximale conforme aux dispositions légales ou réglementaires locales.

Une exploitation statistique des enregistrements est réalisée, sous forme anonyme, pour des motifs opérationnels. Elle consiste, notamment, à établir des statistiques relatives aux connexions et contacts réalisés.

Important

SGCI peut procéder à des audits à caractère nominatif sur les enregistrements informatiques, à la suite d'un dysfonctionnement, d'une alerte de sécurité ou d'une présomption d'une utilisation non conforme des moyens de communication, sous réserve du respect du secret de la correspondance privée.

En ce cas, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront la SGCI sur l'éventuelle réalisation d'un fait fautif et sur l'identité de son auteur.

Pour les traitements et données permettant de remonter à une information nominative, *SGCI* procédera en préalable aux déclarations nécessaires auprès des autorités compétentes, et à l'information des instances représentatives des personnels.

2. Contrôles effectués sur l'utilisation du SI

SGCI a mise ne place des outils d'analyse et de contrôle sur l'utilisation des ressources matérielles et logicielles ainsi que les échanges, quel que soit leur objet ou leur nature.

Ces contrôles sont réalisés :

- Dans l'objectif de garantir le bon fonctionnement technique et la sécurité des systèmes d'information, et de préserver les intérêts *de la SGCI*
- Dans le respect de la législation applicable, notamment les lois sur la protection des données personnelles ;
- Exclusivement sous la responsabilité des administrateurs des systèmes d'information qui garderont confidentielles les informations qu'ils pourraient être amenés à connaître à cette occasion.

On peut citer comme exemple de contrôle : contrôle de la qualité des mots de passe, surveillance de mails envoyés avec ou sans pièce jointe à l'extérieur, bloquer l'accès à certains sites, top 10 des sites internet consultés…

Par ailleurs, par mesure technique ou administrative, l'accès aux moyens de communication électronique pourra être suspendu, restreint ou supprimé, individuellement ou collectivement quand cela est nécessaire, notamment pour le maintien de la bonne marche ou de l'intégrité du système d'information de la SGCI

3. Sanctions

Important

Le non-respect des règles d'utilisation et des mesures de sécurité figurant dans la présente Charte est susceptible de justifier la suspension immédiate de l'utilisation du Système d'Information, et/ou l'engagement de poursuites disciplinaires adaptées à la gravité des agissements constatés s'agissant d'un utilisateur salarié de la SGCI, réserve étant faite de tous autres droits et actions à l'encontre de l'utilisateur que peuvent engager les tiers ou *SGCI* elle-même.
En outre, certains comportements sont susceptibles de faire l'objet de poursuites pénales.
Concernant les personnels liés par un contrat de prestation avec *SGCI*, et utilisant les ressources du Système d'Information mises à leur disposition par *SGCI* : la constatation d'une infraction à la présente Charte peut avoir une incidence sur ledit contrat.

Charte Utilisateur

Je soussigné(e)

Nom :

Prénom :

Fonction :

Direction de rattachement :

Type et Durée du contrat (si nécessaire) :

Certifie avoir pris connaissance de la Charte utilisateur pour le bon usage des ressources informatiques et du réseau de la *Société Générale Côte d'Ivoire* et m'engage à m'y conformer strictement.

Fait à……, le …….

Signature

(Signature à faire précéder de la mention manuscrite "Lu et approuvé").