Réglementaire Sécurité

THEME	Sécurité
PRODUIT	LYDEC

Charte de Sécurité – Prestataires

Projet :
Prestataire :

Diffusion :
- Directeur DSI
- Responsable Service Sécurité SI

Document	
Auteur	R.Nefsi
Référence	CHRT-SEC-DSI-PRST01
Edition	Version 4
Date	Septembre 2015

Validation du document		
Nom	**Date**	**Signature**
Abdennacer ECHAABI		
Rachid NEFSI		

SOMMAIRE

1 Gestion documentaire

1.1 Règles de gestion

Le présent document, destiné aux prestataires ayant à intervenir sur les Systèmes d'information de **LYDEC**, leur est remis par les directions fonctionnelles faisant appel à leurs services. Il peut être joint en annexe des contrats de prestations signés entre les directions fonctionnelles et leurs prestataires.

Les confirmations d'engagement de la société prestataire et de son personnel sont centralisées et conservées par les soins des directions fonctionnelles qui tiennent ces documents à la disposition du Responsable Sécurité de **LYDEC**.

Diffusion libre – NC [non confidentiel]		
Impression	Pas de règle spécifique.	
Diffusion	Pas de limitation.	
Reproduction	Pas de limitation.	
Stockage magnétique	Pas de règle spécifique.	
Transmission	***Télécopie ou Fax***	Pas de règle spécifique.
	Messagerie interne	Pas de règle spécifique.
	Messagerie Internet	Obligation de réserve et de discrétion.
	Courrier	Pas de règle spécifique.
Stockage (conservation)	Pas de règle spécifique.	
Archivage	Pas de règle spécifique.	

1.2 Règles de mise à jour

Le présent document doit être mise à jour en fonction :

- des facteurs d'évolution internes à **LYDEC** : changement de l'organisation, diversification de l'activité et des enjeux associés, modification des systèmes d'information.
- de l'évolution du champ d'application des missions confiées à des prestataires : externalisation de certains fonctions, signature de contrats cadre de partenariat.

Les mises à jour sont réalisées et diffusées à l'ensemble des directions fonctionnelles par le Responsable Sécurité.

Le présent document possède un numéro de Version et de Révision composé comme suit : V.R.

- V : représente le numéro de Version. Une nouvelle version correspond à une évolution majeure du document sur le fond.
- R : représente le numéro de Révision. Une nouvelle révision correspond à une modification de forme ou une évolution temporaire.

2 Préambule

2.1 Objectif et champ d'application du document

L'activité de **LYDEC** repose en partie sur les performances, la fiabilité et la sécurité de ses Systèmes d'Information.

Pour cette raison, la Direction Générale de **LYDEC**, et par délégation la Direction des Systèmes d'Information – DSI, cherche à réduire les risques, sous toutes leurs formes, pesant sur son patrimoine informationnel et ses systèmes.

Dans cette optique, un engagement de bonne conduite est demandé à chaque personne, morale ou physique, ayant à intervenir sur les systèmes de **LYDEC** ou sur les infrastructures associées, que ce soit en tant que professionnel du domaine technique concerné ou en tant que simple utilisateur.

La présente « charte de sécurité », destinée aux prestataires retenus par **LYDEC**, synthétise au sein d'un unique document les exigences de sécurité de **LYDEC** à l'égard des Systèmes d'Information, leurs conséquences sur le déroulement des missions des prestataires et l'engagement de ces derniers à respecter le code déontologique de **LYDEC** en terme de Systèmes d'Information.

2.2 Structure du document

La charte de sécurité se compose de trois parties :

- la présentation, dans ses grandes lignes, de la politique de sécurité de **LYDEC**, notamment de son organisation et de ses principes de base ;
- la déclinaison de ces principes de sécurité en règles opérationnelles, appliquées au cas de la prestation de service ;
- l'engagement de bonne conduite du prestataire et de son personnel affecté à l'exécution de la mission auprès de **LYDEC**.

2.3 Champ d'application

La présente charte de sécurité s'applique aux prestations portant sur :

- les **infrastructures** (locaux techniques et équipements) nécessaires au fonctionnement des Systèmes d'Information ;
- les **matériels** informatiques et de télécommunication ;
- les **données de configuration de ces matériels** ;
- les **données de production ou de test** ;
- les **applications** ;

que ces prestations aient pour objet :

- la **conception** ;
- la **mise en œuvre** ;
- la **maintenance** ;
- l'**exploitation**.

des éléments constituant les Systèmes d'Information de **LYDEC**.

3 Présentation de la Politique Sécurité Lydec

3.1 Objectifs généraux

Les Systèmes d'information de **LYDEC** étant au cœur de ses métiers, une politique de sécurité SI est Mise en ouvre par la direction générale et diffusée à l'ensemble des utilisateurs SI de **LYDEC**.

Le présent paragraphe reprend les points concernant les intervenants externes à **LYDEC,** qui dans le cadre de contrats de prestation, sont en relation avec les Systèmes d'Information de **LYDEC**.

3.2 Description de l'organisation en charge de la Sécurité des Systèmes d'Information

3.2.1 Le Responsable Sécurité

La sécurité des Systèmes d'Information de **LYDEC** est la préoccupation privilégiée d'une personne détachée à cet effet : le Responsable du service Sécurité SI.

Ce dernier a la charge :

- de s'assurer du respect des principes et de l'application des règles de sécurité de **LYDEC** ;
- d'assurer la diffusion et la mise à jour des principes de sécurité de **LYDEC** ;
- de centraliser les éléments opérationnels relevant de la sécurité des systèmes, depuis leur conception jusqu'à leur mise en œuvre et à la gestion des incidents de fonctionnement quotidiens ;
- d'assurer le relais, en terme de sécurité, à la fois
  - entre les équipes techniques et les utilisateurs
  - entre **LYDEC** et les intervenants extérieurs (entités du Groupe Suez, prestataires...).

A ce titre, le Responsable Service Sécurité SI est, in fine, le destinataire de toute remarque relative à la Sécurité des Systèmes d'Information de **LYDEC**.

3.2.2 Les directions fonctionnelles

Les différentes directions fonctionnelles, au cœur chacune d'une activité clé de **LYDEC**, sont les propriétaires de l'information, des systèmes dédiés à son traitement ou des infrastructures nécessaires à leur fonctionnement.

De ce fait, les directions fonctionnelles définissent des exigences spécifiques en terme de sécurité en regard des prestations contractées avec des sociétés externes.

3.3 Les principes fondamentaux de la sécurité des systèmes d'information

Afin de maintenir la fiabilité et les performances des activités de **LYDEC**, toute personne intervenant sur un des éléments des Systèmes d'Information doit porter une attention particulière :

- à la **disponibilité** des services ;
- à la **confidentialité** des informations relatives tant aux systèmes qu'aux métiers de **LYDEC**
- à **l'intégrité** des informations et des systèmes ;
- à **l'auditabilité** de ses interventions sur les systèmes.

Les règles de sécurité énoncées par **LYDEC** guident les personnes dans le respect de ces critères de sécurité, mais ne sont en rien exhaustives. Toute action sur les Systèmes d'Information doit être réalisée dans la mesure où elle ne remet pas en cause sa sécurité,

même temporairement. Toute dérogation à ce principe doit être avalisée au préalable par le Responsable du Service Sécurité SI et les directions fonctionnelles concernées par la remise en cause du niveau de sécurité requis.

4 Règles de sécurité applicables aux prestataires

4.1 Règles générales

➔ Toute intervention sur un des éléments des Systèmes d'Information doit faire l'objet d'une autorisation écrite et préalable du Responsable du Service Sécurité SI, qui valident les conditions de l'intervention et de la réalisation des tâches en collaboration avec le Responsable SI concerné.

➔ Le prestataire se doit d'appliquer un devoir de réserve à l'égard de toute information relative :

- à la nature de son intervention auprès de **LYDEC** ;
- à la l'organisation de **LYDEC** et de ses métiers ;
- à l'activité de **LYDEC** ;
- à l'organisation et au fonctionnement de ses systèmes.

➔ L'intervention ne doit, pas porter préjudice :

- ni à l'intégrité des systèmes et des informations ;
- ni à la continuité des services assurés par ces systèmes.

➔ Dans le cas où le prestataire ne saurait garantir l'une des ces exigences, il doit en aviser Lydec immédiatement et obtenir son accord préalable avant d'intervenir dans tous les cas. ce dernier est tenu :

- de pouvoir restaurer le système dans son état initial au cas où l'intervention aurait conduit à une modification préjudiciable de l'environnement de **LYDEC** ;
- de limiter l'indisponibilité du système à des délais supportables par les directions fonctionnelles de **LYDEC**, en accord avec ces dernières.

➔ Toute intervention du prestataire doit faire l'objet d'un compte-rendu circonstancié précisant :

- le périmètre de l'intervention ;
- le mode opératoire suivi ;
- les résultats de l'intervention;
- les incidents rencontrés et les anomalies détectées.

➔ La détection de toute anomalie ou incident pouvant remettre en cause la sécurité des Systèmes d'Information doit être rapportée au Responsable du Service Sécurité SI.

➔ Enfin, toute dérogation à l'un des principes fondamentaux de sécurité de **LYDEC** ou à l'une des règles décrites dans ce chapitre doit être soumise à l'autorisation préalable du Responsable du Service Sécurité SI. Cette dérogation ne soustrait en rien le prestataire à son obligation de moyens afin de limiter au maximum les risques potentiels qu'il fait encourir au système d'information dans le champ de son intervention.

4.2 Règles spécifiques au domaine de compétence du prestataire

Les règles spécifiques s'appliquant aux prestataires selon le type de prestation réalisée sont données en annexe C.

Outre ces règles associées au domaine d'expertise des prestataires, les personnels de ces derniers sont également soumis aux mêmes règles que le personnel de **LYDEC** concernant l'utilisation des Systèmes d'Information. A ce titre, **LYDEC** remet au prestataire et à son personnel une "Charte Sécurité ».

5 Engagement du prestataire

5.1 Engagement du prestataire

Le prestataire, en tant que personne morale, s'engage à respecter les principes et règles exposés dans la présente charte en signant et retournant une copie de la page présentée en annexe A.

Le prestataire devra respecter tous les aspects de la politique de sécurité en matière de protection du Système d'Information notamment les aspects de :

1. classification de l'information,
2. accès physiques aux bâtiments et aux locaux,
3. accès logiques aux systèmes informatiques,
4. échanges sous toutes ses formes (électroniques, papier, …),
5. gestion d'incidents
6. gestion de changement
7. respect des lois nationales en vigueur (propriété intellectuelle, protection de la vie privée et des données personnelles, cryptographie, …).

5.2 Engagement du personnel du prestataire

Le personnel affecté par le prestataire à la réalisation de la mission auprès de **LYDEC** signe et retourne une copie de l'engagement individuel fourni en annexe B.

Toute intervention ne pourra être réalisée sans la signature préalable des engagements du prestataire et de son personnel.

6 Annexes

6.1 Annexe A : engagement de bonne conduite du prestataire

6.2 Annexe B : engagement de bonne conduite du personnel du prestataire

6.3 Annexe C : règles de sécurité spécifiques à chaque type de prestation

Engagement de bonne conduite de la société SOCIÉTÉ

- Attendu que **LYDEC** a demandé à la société _____

  société anonyme au capital de _____Dhs,
  ayant son siège social _____,
  immatriculée au Registre du Commerce de _____,
  sous le numéro _____,
  représentée par M/Mme/Mlle _____, dûment habilité(e) aux fins des présentes,

  Une prestation de _____

  _____

  pour l'exécution de laquelle ladite société est amenée à avoir accès à des systèmes ou à des informations ou se voir remettre des informations verbales ou sous tout autre forme qui appartiennent à **LYDEC.**

- Attendu que la divulgation ou l'atteinte à l'intégrité ou à la disponibilité physique ou logique de ces systèmes ou informations est susceptible de nuire aux intérêts de **LYDEC**,

- Et après avoir pris connaissance, au travers du document intitulé « charte de sécurité », des exigences de **LYDEC** en termes de sécurité de ses Systèmes d'Information,

La société _____ reconnaît accepter expressément les termes et conditions explicitées dans la « charte de sécurité prestataire » et avoir envers **LYDEC** un devoir de réserve et une obligation de satisfaire aux exigences de cette dernière.

Le prestataire s'engage également à communiquer la « charte de sécurité prestataire » à son personnel qui sera amené, dans le cadre de la prestation, à avoir accès aux informations et Systèmes d'Information de **LYDEC**, et à faire signer par le personnel concerné l'engagement individuel joint ci-après. Le prestataire se porte garante de la bonne exécution par son personnel des obligations susnommées.

Fait à _____, le_____

Pour Le prestataire,

Nom : _____

Prénom : _____

Fonction : _____

Signature :

Engagement individuel de bonne conduite du personnel du prestataire

- La société _____ a souscrit vis-à-vis de **LYDEC** un engagement de bonne conduite relatif à la sécurité des Systèmes et informations de **LYDEC** selon les termes et conditions exposés dans le document libellé « charte de sécurité prestataire » et dont le présent formulaire constitue une annexe.

- Conformément à l'engagement ci-dessus mentionné, le prestataire doit s'assurer que ses collaborateurs engagés dans la réalisation de la prestation auprès de **LYDEC** signent un formulaire confirmant qu'ils ont été informés et souscrivent aux obligations contenues dans ladite « charte de sécurité prestataire ».

Je confirme être employé de la société **présentatrice**, et avoir lu, compris et accepté les termes de la « charte de sécurité prestataire ».

Fait à _____, le_____

Nom : _____

Prénom : _____

Fonction : _____

Signature :

REGLES DE SECURITE SPECIFIQUES AUX PRESTATIONS

DE MAINTENANCE MATERIELLE

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de maintenance des matériels informatiques (serveurs, postes de travail, imprimantes...).

Enoncé des règles

- **Confidentialité des informations**

Dans la mesure du possible, tout support contenant des informations relatives à l'activité de **LYDEC** doit être maintenu dans les locaux de **LYDEC**.

Si cette disposition ne peut être respectée, l'aval de la direction fonctionnelle concernée doit être obtenue et le prestataire engage sa responsabilité quant au maintien de la confidentialité desdites informations.

- **Intégrité des informations**

Le prestataire s'assure que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tant pour les données de production que pour les données de configuration du matériel et des logiciels.

- **Intégrité des ressources**

Le prestataire s'assure qu'un retour arrière est possible, dans des délais raisonnables, éventuellement fixés en fonction des attentes de la direction fonctionnelle concernée.

- **Continuité de service**

Le prestataire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités fonctionnelles.

- **Accès physiques**

L'accès aux locaux techniques doit se faire selon les modalités en vigueur à **LYDEC**.

Il peut notamment être exigé que le personnel du prestataire soit accompagné par un collaborateur de **LYDEC** pendant son intervention.

- **Accès logiques**

Dans le cas où un accès au système est indispensable, le prestataire se voit remettre un accès restreint et temporaire qu'il devra utiliser dans le seul cadre de la prestation en cours.

- **Auditabilité**

Les interventions du prestataire sont consignées par écrit et remises à la direction fonctionnelle à la fin de la prestation.

REGLES DE SECURITE SPECIFIQUES AUX PRESTATIONS

DE MAINTENANCE DES INFRASTRUCTURES

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de maintenance des infrastructures indispensables au bon fonctionnement des Systèmes d'Information.

Il s'agit notamment des locaux techniques, de la climatisation, de l'alimentation électrique, des câblages et gaines techniques...

Enoncé des règles

- **Intégrité des informations**

Le prestataire veillera à ce que les paramétrages des équipements dans le périmètre de sa prestation ne soient pas modifiés sans l'accord des directions opérationnelles (DSI et / ou DRS) de **LYDEC**.

- **Intégrité des ressources**

L'intervention du prestataire ne doit en aucun cas altérer l'état ni le fonctionnement des ressources de **LYDEC**, que ces dernières soient ou non dans le périmètre de sa prestation.

- **Continuité de service**

Le prestataire s'engage à ne pas porter atteinte à la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités fonctionnelles.

- **Accès physiques**

L'accès aux locaux techniques doit se faire selon les modalités en vigueur à **LYDEC**.

Il peut notamment être exigé que le personnel du prestataire soit accompagné par un collaborateur de **LYDEC** pendant son intervention.

- **Accès logiques**

Dans le cas où un accès au système est indispensable, le prestataire se voit remettre un accès restreint et temporaire qu'il devra utiliser dans le seul cadre de la prestation en cours.

- **Auditabilité**

Les interventions du prestataire sont consignées par écrit et remises à la direction fonctionnelles à la fin de la prestation.

REGLES DE SECURITE SPECIFIQUES AUX PRESTATIONS

DE MAINTENANCE DES MOYENS DE TELECOMMUNICATION

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de maintenance des équipements de communication, voix et données (autocommutateurs, brassage...).

Enoncé des règles

- **Confidentialité des informations**

Le prestataire s'engage à ne pas divulguer d'informations relatives à l'architecture ou aux paramétrages des moyens de télécommunication de **LYDEC**.

- **Intégrité des informations**

Le prestataire s'assure que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tant pour les données de production que pour les données de configuration du matériel et des logiciels.

Notamment, le personnel du prestataire veillera à ne pas altérer ou empêcher la journalisation des actions réalisées sur les équipements dans le périmètre de la prestation.

- **Intégrité des ressources**

Le prestataire s'assure qu'un retour arrière est possible, dans des délais raisonnables, éventuellement fixés en fonction des attentes de la direction fonctionnelle concernée.

- **Continuité de service**

Le prestataire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités fonctionnelles.

- **Accès physiques**

L'accès aux locaux techniques doit se faire selon les modalités en vigueur à **LYDEC**.

Il peut notamment être exigé que le personnel du prestataire soit accompagné par un collaborateur de **LYDEC** pendant son intervention.

- **Accès logiques**

Dans le cas où un accès au système est indispensable, le prestataire se voit remettre un accès restreint et temporaire qu'il devra utiliser dans le seul cadre de la prestation en cours.

Les codes d'accès seront confiés aux personnels du prestataire à titre individuel et feront l'objet d'une journalisation.

- **Auditabilité**

Les interventions du prestataire sont consignées par écrit et remises à la direction fonctionnelles à la fin de la prestation.

REGLES DE SECURITE SPECIFIQUES AUX PRESTATIONS

DE TELEMAINTENANCE

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de télémaintenance.

Enoncé des règles

- **Confidentialité des informations**

Dans le cas où les environnements de **LYDEC** ne permettraient pas de masquer les informations de production au personnel maintenant, le prestataire s'engage à ne pas accéder à ces informations, ou à ne pas les divulguer et à ne pas les télécharger si un accès à ces dernières doit être envisagé.

- **Intégrité des informations**

Le prestataire s'engage à ne pas modifier les données ni les paramétrages des équipements et logiciels en dehors du périmètre de sa prestation.

- **Intégrité des ressources**

Le prestataire s'assure qu'un retour arrière est possible, dans des délais raisonnables, éventuellement fixés en fonction des attentes de la direction fonctionnelle concernée.

- **Continuité de service**

Le prestataire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités fonctionnelles.

- **Accès logiques**

Les accès aux systèmes de **LYDEC** doivent se faire par des liaisons temporaires (commutées), avec une procédure de rappel par **LYDEC**.

Les droits octroyés sur le système de **LYDEC** sont restreints et attachés à des identifiants nominatifs.

Enfin, le personnel du prestataire peut éventuellement se voir remettre des outils d'authentification renforcée.

- **Auditabilité**

Les interventions réalisées sous les noms des identifiants attribués aux personnels du prestataire font l'objet d'une journalisation systématique de la part de **LYDEC**, qui se réserve le droit d'effectuer les contrôles nécessaires.

LYDEC se réserve également le droit d'auditer les installations du prestataire afin de vérifier que les opérations de télémaintenance sont réalisées dans un environnement correspondant aux normes de sécurité de **LYDEC**.

REGLES DE SECURITE SPECIFIQUES AUX PRESTATIONS

DE DEVELOPPEMENT ET DE MAINTENANCE APPLICATIVE

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations portant sur le développement de nouvelles applications ou sur la maintenance d'applications existantes.

Enoncé des règles

- **Confidentialité des informations**

Toute information sur le projet en cours, sur les métiers de **LYDEC** ou sur leur organisation, ainsi que les données de production auquel le prestataire peut avoir accès doivent rester confidentielles.

- **Continuité de service**

Toute application doit faire l'objet de tests documentés avant sa mise en production, autorisée par la direction fonctionnelle concernée.

- **Accès logiques**

Les accès au système d'information doivent se limiter au seul environnement de développement.

- **Auditabilité**

Toute application doit faire l'objet de documentations à l'attention des utilisateurs et des administrateurs.

REGLES DE SECURITE SPECIFIQUES AUX PRESTATIONS

D'ADMINISTRATION ET D'EXPLOITATION

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations d'administration ou d'exploitation des Systèmes d'Information de **LYDEC**.

Enoncé des règles

- **Confidentialité des informations**

Toute information sur l'architecture, la configuration et le type des Systèmes d'Information de **LYDEC**, ainsi que les données de production auquel le prestataire peut avoir accès doivent rester confidentielles.

- **Intégrité des informations**

Le prestataire s'assure que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tant pour les données de production que pour les données de configuration du matériel et des logiciels.

Notamment, le personnel du prestataire veillera à ne pas altérer ou empêcher la journalisation des actions réalisées sur les équipements dans le périmètre de la prestation.

- **Continuité de service**

Des sauvegardes de recours doivent être régulièrement réalisées et les dispositifs de secours doivent faire l'objet de tests fréquents afin d'en vérifier le caractère opérationnel.

- **Accès logiques**

La gestion des mots de passe doit faire l'objet d'une attention plus rigoureuse que pour un simple utilisateur.

L'attribution de droits d'accès à une ressource doit se faire uniquement avec l'accord de la direction fonctionnelle propriétaire du système ou des informations qu'il héberge.

- **Auditabilité**

Les interventions du prestataire doivent être journalisées, les journaux étant diffusés au Responsable du Service Sécurité SI à des fins de contrôle.

Les incidents rencontrées lors des interventions et ayant trait à la sécurité du système d'information font l'objet de fiches de relevé et d'analyse communiquées au Responsable du Service Sécurité SI.