**NOTE POUR UNE GOUVERNANCE**

**DE LA MISE EN OEUVRE DE LA CYBER SECURITE**

**DANS LE GROUPE SNPC**

**CONTENU**

1. **Contexte Organisationnel**
2. **Stratégie de Gestion des Risques**
3. **Rôles, Responsabilités et Pouvoirs**
4. **Politique**
5. **Surveillance**
6. **Gestion des Risques de la Chaîne d'Approvisionnement en Cybersécurité**
7. **Contexte Organisationnel**

La Société Nationale des Pétroles du Congo (SNPC) est un acteur majeur et incontournable du secteur pétrolier congolais. Elle est un établissement public à caractère industriel et commercial doté de la personnalité morale et de l’autonomie financière. La SNPC est l’outil technique de l’Etat, dépositaire de la banque de données de l’industrie pétrolière du Congo. Son capital est de 81.334.654.844 FCFA.

Constituée en Groupe, la Société Nationale des Pétroles du Congo est active sur toute la chaîne de l'industrie pétrolière au travers de six filiales proactives dans les filières pétrolières Amont et Aval : SONAREP, ILOGS, SFP, SNPC TRADING, CORAF, SNPC D. La SNPC possède également une Fondation d'entreprise, la FONDATION SNPC.

La vision de la Direction Générale est définie à travers le document stratégique performance 2025 qui se décline en quatre piliers distincts, à savoir :

1. Pilier 1 : Augmentation des revenus
2. Pilier 2 : Maîtrise des coûts
3. Pilier 3 : Contribution à l’action gouvernementale
4. Pilier 4 : Gouvernance et maîtrise des activités

Pour réaliser les objectifs fixés pour ces différents piliers les systèmes d’information de la SNPC et de ses filiales sont amenés à travers les DSI à y apporter une contribution en favorisant une transition numérique par le déploiement d’infrastructure, matérielle et logiciels encadrés par des normes, mesures, exigences et contrôles qui concourent à la protection contre les cyberattaques internes ou externes.

1. **Stratégie de Gestion des Risques**

Pour garantir la protection contre les cyberattaques internes ou externes il convient d’identifier tous les risques encourus susceptibles de mettre en cause la Confidentialité, la Disponibilité et l’Intégrité des données.

1. **Rôles, Responsabilités et Pouvoirs**

Le processus de définition des rôles et des responsabilités est un élément crucial dans la mise en place d’un système de défense solide contre les cybermenaces.

1. **Le Conseil d’Administration**

Fixera des orientations et des objectifs de haut niveau

1. **Le Directeur Général**

Assurera la tactique, le financement et le management des ressources. Il marquera son engagement et son approbation du programme de cybersécurité.

1. **Les Ressource Humaines**

Intégrera les considérations de gestion des risques de cybersécurité dans les processus de ressources humaines (par exemple, sélection du personnel, intégration, départ).

Considérez les connaissances en cybersécurité comme un facteur positif dans les décisions d’embauche et de formation.

Définir et faire respecter les obligations du personnel afin qu'il soit informé, respecte et fasse respecter les politiques de sécurité liées à ses fonctions.

1. **Les Directeurs des Systèmes d’Information**

Dirigera la mise en œuvre du programme de cybersécurité

1. **Le Responsable de la Sécurité des Systèmes d’Information**

Veillera au succès de la mise en œuvre et de la gestion opérationnelle des pratiques en matière de cybersécurité

1. **Les Utilisateurs**

Rapportent les accidents de cybersécurité dont ils sont victimes et s’approprient les recommandations et exigences de sécurité définis.

1. **Politique**

La SNPC devra restreindre l'accès aux données confidentielles et sensibles pour éviter qu'elles ne soient perdues ou compromises, de façon à ne pas nuire à nos clients, à ne pas encourir de sanctions pour non-conformité et à ne pas nuire à notre réputation.

Les politiques, processus et procédures de gestion des risques de cybersécurité seront établis en tenant compte d’un certain nombre de priorités parmi lesquelles :

1. La protection des données sensibles contre l'exposition à des parties non autorisées.
2. La garantir que les données n'ont pas été modifiées pendant qu'elles sont stockées ou en transit.
3. La Fourniture d’un accès continu aux données et aux systèmes aux utilisateurs légitimes.
4. L’élaboration et la validation d’une charte informatique pour l’ensemble du groupe
5. L’adoption des règles et exigences communes d’authentification
6. Systématiser la mise en place de pare-feu à travers les réseaux locaux
7. Maintenir le niveau d’expertise des techniciens en matière de cybersécurité par les sessions de formation
8. **Surveillance**

Les risques ne sont pas statiques. Les évènements, la valeur des biens, les menaces, les vulnérabilités, la vraisemblance et les conséquences peuvent changer brutalement sans aucune indication préalable. Il convient de procéder à une surveillance constante afin de détecter ces changements. Cette surveillance peut être assurée par des services externes qui fournissent des informations relatives à de nouvelles menaces ou vulnérabilités. Il convient que les organismes assurent la surveillance des facteurs pertinents.

Par ailleurs il convient aussi d’une part d’examiner les indicateurs de performance clés (KPI) pour garantir que les politiques et procédures à ‘échelle de l’organisation atteignent les objectifs, d’autre part d’examiner les indicateurs de risque clés (KRI), pour identifier les risques auxquels l’organisation est confrontée, y compris leur probabilité et leur impact potentiels.

1. **Gestion des Risques de la Chaîne d'Approvisionnement en Cybersécurité**

Les exigences visant à répondre aux risques de cybersécurité dans les chaînes d’approvisionnement devront être établies, hiérarchisées et intégrées dans les contrats et autres types d’accords avec les fournisseurs et autres tiers concernés, afin de conduire à :

1. Analyser en permanence le paysage de l'entreprise à la recherche de nouveaux partenaires et fournisseurs capables de fournir des capacités complémentaires et de soutenir la réalisation de la stratégie I&T, de la feuille de route et des objectifs de l'entreprise.
2. Établir et maintenir des critères relatifs au type, à l'importance et à la criticité des fournisseurs et des contrats avec les fournisseurs, permettant de se concentrer sur les fournisseurs préférés et importants.
3. Identifiez, enregistrez et catégorisez les fournisseurs et les contrats existants selon des critères définis pour maintenir un registre détaillé des fournisseurs préférés qui doivent être gérés avec soin.
4. Évaluer et comparer périodiquement les performances des fournisseurs existants et alternatifs pour identifier les opportunités ou un besoin impérieux de reconsidérer les contrats des fournisseurs actuels.