SECURITE DES DONNÉES PERSONNELLES ET POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT (PSSIE)

Dassa, le 02 septembre 2022

AGENDA

1. Définitions et concepts de sécurité
2. La PSSIE: Contexte, enjeux, objectifs et champ d'application
3. Sécurité des données personnelles et PSSIE: Quelques règles de sécurité
4. Questions/Réponses

Définitions et concepts de sécurité

DÉFINITIONS ET CONCEPTS DE SÉCURITÉ

- **Données à caractère personnel**: Toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, dont les données à caractère personnel font l'objet d'un traitement.

Réf: Code du numérique

DÉFINITIONS ET CONCEPTS DE SÉCURITÉ

- **PSSIE**: Politique de sécurité des systèmes d'information de l'Etat. Document stratégique qui définit les orientations nationales en matière de sécurité des SI.

Elle constitue le socle de base des mesures techniques, organisationnelles, physiques et règlementaires à mettre en œuvre par les entités étatiques pour protéger les systèmes d'information qu'ils déploient dans leur secteur d'activité..

DÉFINITIONS ET CONCEPTS DE SÉCURITÉ

- **la confidentialité:** elle se définit comme la propriété pour un système d'information d'être accessible seulement à des utilisateurs ou autres systèmes d'information autorisés.
- **l'intégrité:** qui se définit comme étant la propriété d'un système d'information de ne permettre que les modifications autorisées.

DÉFINITIONS ET CONCEPTS DE SÉCURITÉ

- **la disponibilité** : qui se définit comme étant la propriété pour un système d'information à être accessible et utilisable à la demande par les utilisateurs autorisés.
- **la traçabilité:** qui est la propriété pour un système d'information de permettre la vérification d'une action ou d'un événement à des fins d'analyse et d'en retrouver l'auteur.

2 La PSSIE: Contexte, enjeux, objectifs et champ d’application

CONTEXTE

- Ambition de positionner le pays comme la référence en Afrique de l'Ouest en matière de plateformes de services numériques.
- Faire des TIC l'un des principaux leviers de développement socio-économique.
- Adoption de la SNSN.

ENJEUX ET OBJECTIFS

- Contribuer à la promotion des bonnes pratiques de sécurité au sein des entités de l'Etat
- Harmoniser la protection des infrastructures des systèmes d'information à l'échelle de l'Etat
- Favoriser la confiance des utilisateurs dans les systèmes d'information de l'Etat

ENJEUX ET OBJECTIFS

- Définir le cadre relationnel entre l'ANSSI et les entités de l'Etat
- Contribuer à l'économie numérique au Bénin en favorisant la consommation des services et produits de confiance numérique.

CHAMP D'APPLICATION

La PSSIE s'applique:

- à tous les systèmes d'information sans exception des administrations publiques
- à tous les établissements publics et les sociétés d'Etat
- aux utilisateurs des systèmes d'information de l'Etat
- aux personnes chargées de leur gestion et aux personnes chargées de leur sécurité

CHAMP D'APPLICATION

La PSSIE ne s'applique pas :

- aux systèmes d’information pris en compte par la Loi n° 2019-05 portant organisation du secret de la défense nationale en République du Bénin
- aux organismes privés mettant en œuvre leurs propres systèmes d’information. La PSSIE peut toutefois servir de source d’inspiration pour ces organismes qui sont libres de l’adopter ou non.

3 Sécurité des données personnelles et PSSIE: Quelques règles de sécurité

Objectif n°2 : Faire des ressources humaines, un maillon fort de la sécurité des systèmes d'information

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
RH-01	Sélection des candidats	**Règle :** Le recrutement des rôles de confiance (administrateurs bases de données, systèmes, réseau, consultants, auditeurs, ...) devra faire l'objet de vérifications sécuritaires approfondies, dans le strict respect du cadre juridique applicable au Bénin, afin de garantir la probité des postulants. **Recommandation :** L'entité peut procéder à des vérifications portant sur le casier judiciaire, les contrôles de référence, l'authenticité des diplômes et certifications professionnelles, les réseaux sociaux, ...	C
RH-02	Engagement sécurité	**Règle :** Tout personnel embauché (interne, partenaire ou tiers) destiné à manipuler un composant du système d'information, reçoit et signe une charte, opposable juridiquement, récapitulant les mesures pratiques d'utilisation du SI. Il doit signer un « accord de non-divulgation » dès son entrée en fonction. **Recommandation :** Lorsque cela est administrativement faisable, il est recommandé de faire modifier le règlement intérieur de l'organisme pour inclure les dispositions applicables en matière de sécurité du SI (PSSI spécifique, respect des textes règlementaires applicables, sanctions en cas de violation des règles de sécurité, ...).	C

Objectif n°2 : Faire des ressources humaines, un maillon fort de la sécurité des systèmes d'information

RH-03	Intégration des nouvelles recrues	**Règle :** Le circuit d'intégration des nouvelles recrues au sein de la structure d'accueil de l'entité doit prévoir une étape de formation aux outils de travail, aux procédures et pratiques de sécurité en vigueur.	N
RH-04	Sensibilisation du personnel	**Règle :** L'entité doit dispenser régulièrement et au moins deux fois l'an, au profit du personnel, des formations de sensibilisation sur les règles d'hygiène pour une sécurité numérique améliorée dont le contenu sera adapté au profil des utilisateurs (utilisateurs sédentaires, itinérants, administrateurs, fournisseurs, ...). Ces formations doivent faire l'objet d'évaluation des acquis par les utilisateurs.	C

Objectif n°3 : Identifier les actifs du système d'information de l'entité et s'assurer que les responsabilités sont définies pour la protection des actifs.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ACT-01	Inventaire des actifs SI	**Règle :** Chaque entité établit et maintient à jour un inventaire des actifs du système d'information (matériels, logiciels, réseaux, locaux informatiques...) sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire doit être certifié sur une base annuelle à minima.	C
ACT-02	Responsabilités sur les actifs	**Règle :** A chaque actif SI identifié, l'entité doit s'assurer qu'un responsable est désigné pour en assurer la sécurité.	C
ACT-03	Usage correct des actifs SI	**Règle :** L'entité doit rédiger et diffuser une charte d'utilisation des systèmes d'information à tous les utilisateurs des actifs du SI. L'entité doit s'assurer que les termes de ladite charte sont compris par les utilisateurs.	N

Objectif n°9: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs

PHY-10	Sécurité du câblage réseau	**Règle :** L'ensemble des câbles réseaux doit être correctement étiqueté, c'est-à-dire aux deux extrémités. L'entité doit documenter le plan de câblage du réseau informatique et s'assurer que le câblage réseau est à l'abri des endommagements (travaux de voierie, ...).	C
PHY-11	Maintenance du matériel	**Règle :** Pour les actifs SI vitaux, un contrat de maintenance doit être conclu avec un délai d'intervention ou de remplacement garanti, compatible avec les besoins de disponibilité et d'intégrité de ces actifs.	C
PHY-12	Sortie du matériel	**Règle :** Aucun matériel contenant des données de l'entité ne doit sortir hors de ses locaux sans autorisation préalable dûment signée par les responsables habilités. L'entité encadre cette mesure par une procédure formelle garantissant la traçabilité des sorties de matériel.	C

Objectif n°11: Fournir aux utilisateurs, des postes de travail sécurisés pour leurs activités professionnelles

PDT-05	Partage des fichiers	**Règle :** Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé. **Recommandation :** Il est recommandé de réaliser le partage de fichiers entre les utilisateurs par l'intermédiaire des espaces partagés mis à disposition par les administrateurs.	C
PDT-06	Sauvegarde des données	**Règle :** Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs. Les disques de stockage en local doivent être chiffrés avec des outils de confiance.	N
PDT-07	Réaffectation d'un poste de travail déjà utilisé	**Règle :** L'entité définit une procédure concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.	N

Objectif n°12 : Protéger l'information stockée sur des équipements nomades.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ITIN-01	Stockage des données sensibles	**Règle :** Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement agréé par l'ANSSI.	C
ITIN-02	Filtre de confidentialité	Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité.	N
ITIN-03	Pare-feu local	**Règle :** Un pare-feu local conforme aux recommandations de l'ANSSI doit être installé sur les postes nomades.	N

Objectif n°13 : Assurer l'exploitation correcte et sécurisée des SI et gérer les actions d'administration du SI.

EXP-06	Protection contre les codes malveillants	**Règle :** L'entité doit formaliser et mettre en œuvre une politique de lutte antivirale qui stipule les mesures de prévention, de détection et de réaction en cas d'infections virales. En règle générale, une solution antivirus ou Endpoint Detection and Response doit être installée sur chaque composant du SI (postes de travail, portables, serveurs, passerelles, ...). **Recommandation :** Il est recommandé l'utilisation de solutions centralisées pour la gestion antivirale.	C
EXP-07	Utilisation de la messagerie personnelle et professionnelle	Le système de messagerie professionnelle mis en place par l'entité est le seul autorisé dans le cadre des activités professionnelles. L'utilisation des courriels personnels (Gmail, Yahoo, Hotmail...) est interdite.	C

Objectif n° 14 : Intégrer la sécurité dans le cycle de vie des systèmes d'information qu'ils soient acquis ou développés par l'entité

ADM-07	Données de test	**Règle :** En règle générale, les données utilisées comme jeu d'essais pour les applications ne peuvent être des données réelles. En cas de sélection de données réelles comme données d'essai, l'entité doit définir des dispositions empêchant la divulgation de ces données et garantissant leur destruction dans les environnements de test une fois les tests achevés. **Recommandation :** Il est recommandé de procéder si techniquement faisable à l'anonymisation des données réelles dans les environnements de test.	**N**
ADM-08	Collecte et traitement des données à caractère personnel	**Règle :** Les entités doivent se référer à l'APDP dans le cadre de toute activité nécessitant la collecte et le traitement des données à caractère personnel.	**N**

Objectif n°15 : Sécuriser les informations impliquées dans les applications de e-services.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ESV-01	Sécurité des services d'application en ligne	**Règle :** Toute plateforme de e-services doit employer des méthodes d'authentification sécurisée pour réduire les risques grâce à la cryptographie à clef publique et aux signatures numériques offertes par la PKI nationale. Des services de tiers de confiance doivent être utilisés. **Recommandation:** Les systèmes d'authentification de la PKI nationale ou du Portail National des Services Publics (PNSP) peuvent être utilisés.	C
ESV-02	Filtrage applicatif	**Règle :** L'entité qui met en oeuvre une plateforme de e-services doit faire usage d'une solution tierce de filtrage applicatif.	C

Objectif n° 18 : Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
FRN-01	Accord de non-divulgation	**Règle :** Tout contrat commercial entre l'entité et un tiers doit faire l'objet d'une signature systématique d'un accord de non-divulgation lorsque des informations de l'entité sont susceptibles d'être communiquées au tiers.	C
FRN-02	Contractualisation des exigences de sécurité	**Règle :** Toute fourniture de biens et/ou services dans le domaine des SI doit être encadrée par des clauses contractuelles entre l'entité et les tiers. Le contrat signé entre l'entité et ces tiers doit refléter les exigences de sécurité à la hauteur des risques induits par la relation entre l'entité et ces tiers. Les clauses de sécurité minimales à aborder incluent : la responsabilité du tiers, la prise en compte de la PSSI spécifique, les procédures d'échanges des données, l'auditabilité, la réversibilité, la confidentialité, ...	C

Objectif n° 22 : Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CONF-01	Droits de propriété intellectuelle	**Règle :** L'entité doit se soumettre au texte du code du numérique se rapportant à la protection de la propriété intellectuelle et des droits d'auteurs. En règle générale tout logiciel (payant, gratuit et open source) utilisé par l'entité doit être accompagné d'une licence.	C
CONF-02	Données à caractère personnel	**Règle :** Les entités doivent se référer à l'APDP dans le cadre de toute activité nécessitant la collecte et le traitement des données à caractère personnel.	N
CONF-03	Mesures cryptographiques	**Règle :** L'entité doit se conformer aux dispositions du code du numérique se rapportant à la cryptologie et aux recommandations de la Commission Cryptologie.	N

Objectif n° 23 : Effectuer des contrôles et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CONF-04	Contrôles locaux	**Règle :** La conformité à la PSSIE et à la PSSI spécifique est vérifiée par des contrôles réguliers. Le RSSI de chaque entité conduit des actions locales d'évaluation de la conformité à la PSSIE et contribue à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en oeuvre.	C
CONF-05	Audits de sécurité	**Règle :** Des audits de sécurité approfondis du SI doivent être réalisés dans le cadre d'un programme de tests de sécurité. Ces audits doivent être confiés à des FSSNQ.	C

RESPONSABLE DE LA SECURITE DES SI

- Acteur majeur de la mise en œuvre de la PSSIE au sein des SI des administrations publics, établissements publics et société d'état
- Profil type défini dans le décret n°2021-550 portant adoption des règles de la Politique de de Sécurité des Systèmes d'Information de l'État (PSSIE)

RSSI # DPDP

- RSSI : décret n°2021-550 portant adoption des règles de la Politique de de Sécurité des Systèmes d'Information de l'État (PSSIE)
- DPO : Code du numérique

MERCI DE VOTRE AIMABLE ATTENTION !