REPUBLIQUE DU BENIN

FORMULAIRE DE FORMALITES PREALABLES

A LA MISE EN OEUVRE DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL
(Article 407 et 409 de la loi n° 2017-20 portant code du numérique en République du Bénin)

ANNEXE 3 : INTERCONNEXION

		Enoncez les fichiers ou traitements distincts mis en relation	
		Fichier ou traitement 1 :	Références APDP du traitement à interconnecter :
			Finalité
		Fichier 2 ou traitement 2 :	Références APDP du traitement à interconnecter :
			Finalité
		Fichier ou traitement 3 :	Références APDP du traitement à interconnecter :
			Finalité
		Modalités de mise en oeuvre de l'interconnexion	
		☐ API. ☐ Services web. ☐ Autres : ……	
		Quelle est la nature ou la portée de l'automatisation créée dans le cadre de l'interconnexion	
		☐ Fusion ☐ Transfert d'informations ☐ Assemblage ☐ Consultation de bases de données par internet	
		Services nécessitant une interconnexion à Internet :	
		☐ Navigation web. ☐ Récupération de sources depuis des sites de confiance ☐Résolution de noms DNS. ☐Hébergement web ☐ les services d'infrastructures de l'entité exposés sur Internet (ex : passerelle VPN IPsec ou TLS pour les accès nomades, passerelle VPN IPsec pour des tunnels site à site) ; ☐ les services collaboratifs de l'entité exposés sur Internet (ex : messagerie, téléphonie, visioconférence, portail Extranet) ;	
		Précisez les données concernées par l'interconnexion	
		L'interconnexion est-elle prévue par un texte réglementaire ou légal ?	
		☐ Non ☐ Oui (Enoncez le texte)……	
		Précisez les raisons pour lesquelles l'interconnexion est nécessaire :	

		Précisez la durée de l'interconnexion
		Risques identifiés
		☐ Exfiltration de données vers internet ☐ Intrusion ☐ Usurpation d'identité ☐ Accès à des sites interdits ☐ Facteur humain
		Architecture et fonction de sécurité
		☐ Mise en place d'une DMZ. ☐ Présence de Pare-feux ☐ Filtrage périmétrique ☐ Mise en oeuvre d'une rupture protocolaire des flux. ☐ Authentification sans exposition d'annuaire. ☐ Cloisonnement de zones ☐ Journalisation ☐ Interception TLS. ☐ Poste de rebond pour la navigation web ☐ Autres : ……

Je déclare sur l'honneur que les renseignements fournis sont exacts.		
Nom et Prénom	Fonction	Date

CHECK LIST MESURE DE SECURITE INTERCONNEXION A INTERNET

1. Déterminer l'ensemble des services nécessitant l'interconnexion à Internet
2. Déployer un pare-feu maîtrisé entre la DMZ et le routeur d'accès Internet
3. Déployer un pare-feu maîtrisé entre le SI de l'entité et la DMZ
4. Rendre incontournable la passerelle Internet sécurisée
5. Déployer si nécessaire des pare-feux intermédiaires dans la passerelle Internet sécurisée
6. Cloisonner les flux au sein de chaînes de traitement homogène
7. Respecter une cinématique sécurisée des flux
8. Procéder à une rupture protocolaire des flux
9. Procéder à une analyse des flux en fonction de l'analyse de risque
10. Ne pas exposer d'annuaire du SI de l'entité aux ressources de la passerelle Internet sécurisée
11. Évaluer les risques de mutualisation par virtualisation
12. Déployer une passerelle Internet sécurisée à base d'équipements physiques dédiés par zone
13. Déployer une passerelle Internet en acceptant la mutualisation de certains équipements de commutation
14. Proscrire toute mutualisation des pare-feux interne et externe
15. Homogénéiser les passerelles Internet sécurisées dans le cas d'une architecture multi-zones
16. Utiliser une offre qualifiée par l'ANSSI pour les fonctions relais externalisées
17. Évaluer rigoureusement les risques d'une offre non qualifiée par l'ANSSI pour les fonctions relais externalisées
18. Administrer de manière sécurisée la passerelle Internet sécurisée
19. Garantir la disponibilité attendue grâce à la résilience des accès opérateurs
20. Mettre en œuvre des contre-mesures aux attaques en déni de service
21. Utiliser un routage statique au sein de la passerelle Internet sécurisée
22. Ignorer les paquets refusés par la politique des pare-feux externes
23. Masquer l'architecture interne vis-à-vis d'Internet
24. Mettre en place un serveur mandataire pour l'accès aux contenus Web
25. Authentifier tous les accès aux contenus Web
26. Prévoir des restrictions pour les accès non authentifiables
27. Étudier la mise en place d'une interception TLS maîtrisée
28. Centraliser et sécuriser les journaux liés aux accès Web
29. Déployer des postes de rebond pour la navigation Web
30. Maîtriser le déploiement et l'exploitation du ou des navigateurs Web
31. Configurer le serveur mandataire en mode explicite
32. Empêcher le contournement du serveur mandataire
33. Appliquer une politique de configuration locale du serveur mandataire