REPUBLIQUE DE COTE D'IVOIRE

Union-Discipline-Travail

CODE GÉNÉRAL DES RSSI OUEST AFRIQUE

TOURE ISSIAKA

Président - Fondateur
de Cloudcom

VERSION SYNTHÉTIQUE

Préambule

Ce dit document intitule´« Code GÉNÉRAL DES RSSI – OUEST AFRIQUE », a pour objectif d'éduquer les professionnels du numérique ainsi que tout individu du secteur des TICs, sur les différents niveaux de sécurité des ressources de cet écosystème, leurs spécifications dans les RFC et les divers standards et normes conseillables.

Cette première édition est le début d'une série d'édition triennale qui prendra en compte les éventuelles mises à jour tant sur les comportements humains que sur l'aspect informatique regroupant matériels et applications

Les recommandations sont façonnées pour chaque strate de l'entreprise administrée dans un tableau organisés selon 3 principes que sont les objets inspecter, des recommandations suivies des normes qui s'y rattachent, L'ensemble est subdivisé en 4 chapitres à savoir :

-La Corporate ;

-l'Individu lambda ;

-le Hardware ;

-Le Software ;

Toute reproduction, même partielle ou toute vente de ce document, par quelque procède´que ce soit, sans autorisation préalable de Monsieur TOURE ISSIAKA, constitueraient une contrefaçon ou une usurpation, une attente au patrimoine moral et financier de l’auteur désigné.

Table des abréviations

COBIT : Control Objectives for Information and Related Technology

HIPAA : Health Insurance Portabilité and Accountability Act

IEC : International Electrotechnical Commission

ISO : International Organization for Standardization

NIST : National Institute of Standards and Technology

PCI DSS : Payment Card Industry Data Security Standard

RFC : Request For Comments

RGPD : Règlement Général sur la Protection des Données

RSSI : Responsable de la Sécurité des Systèmes d'Information

TRPM : Third Party Risk Management

SOMMAIRE

Troisième point : Stockage des données

Quatrième point : Archivage des données

Cinquième point : Applications/Frameworks

CODE GÉNÉRAL DES RSSI – OUEST AFRIQUE

CHAPITRE 1
LA CORPORATE

Premier point : Référencement site web (officiel)

Objets inspecter	Recommandations	Normes
Protocole	-HTTPS : Certificat SSL	La Norme ISO/IEC 27005, RGPD, rfc7540
Format url	-URL Rewriting : Échapper certains caractères	La Norme ISO/IEC 27005, La Norme ISO/IEC 27002 , rfc1738
SEO	-Publicités -Repost	La Norme ISO/IEC 27005, La Norme ISO/IEC 27002

Deuxième point : Réseaux sociaux(officiel)

Objets inspecter	Recommandations	Normes
Community Manager	-Informations exactes(Noms, Adresse, Contacts, Logo)	RGPD, La Norme ISO/IEC 27002

Doublon	-Compte Certifié	RGPD, La Norme ISO/IEC 27002

Troisième point : Actualités(Fake news)

Objets inspecter	Recommandations	Normes
Informations	-Sourcer -Signaler	La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003
Commentaires	-Sourcer -Signaler	La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003

Quatrième point : Système d'information

Objets inspecter	Recommandations	Normes
Humains	-Accès unique sécurisé -Listing de Bonnes pratiques	Le référentiel CobiT , ISO/IEC 38500, ISO 27000, TRPM,

		NIST
Matériels	-Espaces adéquats -Articles d'origine -Maintenance	Le référentiel CobiT , ISO/IEC 38500, ISO 27000
Applications	-Pentesting	Le référentiel CobiT , ISO/IEC 38500, ISO 27000, TRPM, NIST

CHAPITRE 2
L'INDIVIDU LAMBDA

Premier point : Réseaux sociaux(officiel)

Objets inspecter	Recommandations	Normes
La photo	-Portrait : uniquement l'individu	RGPD, La Norme ISO/IEC 27002
Paramétrages	-Visibilité des informations -Interactions	RGPD, La Norme ISO/IEC 27002

Deuxième point : Données personnels

Objets inspecter	Recommandations	Normes
Numéro de téléphone	-Renseigner sur les sites de confiance	La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003 , NIST
Adresses		La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003 , NIST
Données Sanitaires		La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003, HIPAA,

		NIST
Carte de Crédit		La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003 , NIST
Mot de passe	-Caractères spéciaux - Différent pour chaque compte -Backup -Enregistrer sur les sites de confiance	La Norme ISO/IEC 27002 , RGPD, rfc2898, NIST

Troisième point : Le navigateur

Objets inspecter	Recommandations	Normes
Paramétrages	-Certificats -Cookies -Mise en cache -Javascript -Pare-feu -Téléchargement -Upgrade	La Norme ISO/IEC 27002 , La Norme ISO/IEC 27004, La Norme ISO/IEC 27005, rfc6265, rfc5280, rfc2979, TRPM, NIST

Extension	-Paramètres -Upgrade	La Norme ISO/IEC 27002 , La Norme ISO/IEC 27003 , TRPM, NIST

Deuxième point : Double authentification

Objets inspecter	Recommandations	Normes
TOTP	-Device : Toujours connecté et en notre possession	La Norme ISO/IEC 27002 , rfc6238, TRPM, NIST
HOTP	-Réponse de question : Orthographe complexe	La Norme ISO/IEC 27002 , RGPD, rfc4226, TRPM, NIST

Troisième point : Anti spam

Objets inspecter	Recommandations	Normes
Publicités électroniques	-Ne pas cliquer sur des liens	La Norme ISO/IEC 27002 , RGPD
Messages suspects du Centre de service client	-Ne pas Répondre	La Norme ISO/IEC 27002 , RGPD

CHAPITRE 3
LE HARDWARE

Premier point : Local des équipements

Objets inspecter	Recommandations	Normes
Conditions de Température et de Pression	-Chambre Froide aéré	ISO 9000, ISO 14000, La Norme ISO/IEC 27004
Protection des circuits électriques	-Stabilisateur -Transformateur -Groupe électrogène	ISO 9000, ISO 14000, La Norme ISO/IEC 27004

Deuxième point : Prises et câbles

Objets inspecter	Recommandations	Normes
Articles d'origine	-Fournisseurs agréés	ISO 9000, ISO 14000, La Norme ISO/IEC 27004
Maintenance	-Équipes agrées	ISO 9000, ISO 14000, La Norme ISO/IEC 27004

Troisième point : Serveurs

Objets inspecter	Recommandations	Normes
Articles d'origine	-Fournisseurs agréés	ISO 9000, ISO 14000, La Norme ISO/IEC 27004
Maintenance	-Équipes agrées	ISO 9000, ISO 14000, La Norme ISO/IEC 27004

CHAPITRE 4
LE SOFTWARE

Premier point : Saisies des données

Objets inspecter	Recommandations	Normes
Href	-Protocole HTTPS -Limites des types de requêtes	PCI DSS , RGPD, La Norme ISO/IEC 27002 , rfc7540, NIST
Format	-Fonction Cryptographique	PCI DSS , RGPD, La Norme ISO/IEC 27002 , rfc3174, rfc6931, rfc8017, rfc1321 , rfc2104, HIPAA, NIST
Filtres	-Caractères spéciaux -Images -Requêtes	PCI DSS , RGPD, La Norme ISO/IEC 27002 , NIST

Deuxième point : Transmissions des données

Objets inspecter	Recommandations	Normes
Données à caractères personnels	-Protocole HTTPS -Limites des types de requêtes - Fonction Cryptographique -Token	La Norme ISO/IEC 27003, ISO 27001, PCI DSS, RGPD, rfc8693, rfc6749, rfc7540, HIPAA, TRPM, NIST
Données de connexion	-Protocole HTTPS -Limites des types de requêtes - Fonction Cryptographique -Token -Hmac	La Norme ISO/IEC 27003, ISO 27001, PCI DSS, RGPD, rfc8693, rfc6749, rfc7540, TRPM, NIST

Données à caractères commerciales	-Protocole HTTPS -Paramétrages Cookies -Fonction Cryptographique	La Norme ISO/IEC 27003, ISO 27001, PCI DSS, RGPD, rfc7540, TRPM, NIST

Troisième point : Stockage des données

Objets inspecter	Recommandations	Normes
Base de données	-La Bande passante -Les Permissions -Les configurations	La Norme ISO/IEC 27003, La Norme ISO/IEC 27005, PCI DSS, RGPD, rfc793, rfc5246, rfc6101, rfc4253, HIPAA, TRPM, NIST
Maintenance	-Programmée aux horaires de faibles affluences	La Norme ISO/IEC 27004,

		La Norme ISO/IEC 27003, Le référentiel CobiT , NIST
Backup de la Base de données	-Sauvegarde programmée : Chaque mois -Fichier encrypté	La Norme ISO/IEC 27005, NIST

Quatrième point : Archivage des données

Objets inspecter	Recommandations	Normes
Base de données	-La Bande passante -Les Permissions -Les configurations	La Norme ISO/IEC 27003, La Norme ISO/IEC 27005, PCI DSS, RGPD, HIPAA, TRPM, NIST
Maintenance	-Programmée aux horaires de faibles affluences	La Norme ISO/IEC 27004, La Norme ISO/IEC 27003, Le référentiel CobiT , NIST
Backup de la Base de données	-Sauvegarde programmée : Chaque mois -Fichier encrypté	La Norme ISO/IEC 27005, NIST

Cinquième point : Applications/Frameworks

Objets inspecter	Recommandations	Normes
Scan des fichiers	-Firewall à jour -Programmée chaque trimestre	La Norme ISO/IEC 27004, La Norme ISO/IEC 27003, Le référentiel CobiT , NIST
Upgrade des modules	-Versions les plus stables	La Norme ISO/IEC 27004, La Norme ISO/IEC 27003, Le référentiel CobiT , NIST
Cache	-Vider quotidiennement	La Norme ISO/IEC 27005, La Norme ISO/IEC 27002, NIST
Backup de l'architecture	-Sauvegarde programmée : Chaque trimestre -Fichier encrypté	La Norme ISO/IEC 27005, NIST
Pentest	-Frontend -Middle Party -Backend	Le référentiel CobiT, ISO/IEC 38500, ISO 27000, TRPM, NIST

TOURE ISSIAKA
Président – Fondateur de Cloudcom
tissiaka@outlook.fr

Abidjan – CÔTE D'IVOIRE
Version Synthétique – 2024