ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

RÉPUBLIQUE DE CÔTE D'IVOIRE
Union – Discipline – Travail

CI-CERT
RFC 2350

TLP: CLEAR

Agence Nationale de la sécurité des Systèmes d'Information

INFORMATIONS GENERALES			
Titre	CI-CERT_RFC2350_FR		
Date de création	22/05/2025	Statut	
Version	1.1	Diffusion	**Sans restriction**
Authentification	Ce document a été signé avec la clé PGP officielle du CI-CERT.		
Description	Ce document contient une description du CI-CERT conformément à la norme RFC 2350. Il fournit des informations de base sur le CI-CERT, ses canaux de communication, les rôles et responsabilités.		

REGLES DE MARQUAGE ET DIFFUSION DES DOCUMENTS (TLP 2.0)

TLP: RED = Diffusion exclusive.

Les documents avec ce marquage sont diffusés exclusivement et strictement aux seuls bénéficiaires individuellement identifiés, sans aucune autre divulgation. Les destinataires ne peuvent donc pas partager les documents ou informations marquées **TLP : RED** avec qui que ce soit d'autre.

TLP: AMBER = Diffusion restreinte.

Les documents avec ce marquage sont diffusés seulement à l'organisation et à ses parties prenantes (partenaires, fournisseurs, etc.) en tenant compte du besoin de savoir. Les destinataires ne peuvent partager les documents ou informations marquées **TLP : AMBER** qu'avec les membres de leur propre organisation et parties prenantes, mais seulement selon le besoin de savoir.

TLP: AMBER+STRICT = Diffusion strictement restreinte.

Les documents avec ce marquage sont diffusés seulement au sein de l'organisation en tenant compte du besoin de savoir. Les destinataires ne peuvent partager les documents ou informations marquées **TLP : AMBER+STRICT** seulement qu'avec les membres de leur propre organisation.

TLP: GREEN = Diffusion limitée.

Les documents avec ce marquage sont diffusés seulement au sein de communautés d'intérêts, lorsque l'information est utile pour y accroître la sensibilisation. Les bénéficiaires peuvent partager les documents et informations marquées **TLP: GREEN** seulement avec leurs pairs et les organisations partenaires au sein de leur communauté, mais pas par des canaux accessibles au public.

TLP: CLEAR = Diffusion sans restriction.

Les documents avec ce marquage peuvent être diffusés sans restriction, sous réserve du respect des règles de copyright. Les bénéficiaires peuvent partager les documents et informations avec ce marquage sans restriction.

1. INFORMATIONS DE CONTACTS

Statut	TLP	Version
Validé	RED : Diffusion restreinte	1.0

1.1. Nom de l'équipe

Nom complet :

Côte d'Ivoire – Computer Emergency Response Team

Sigle :

CI-CERT

1.2. Adresse géographique

Côte d'Ivoire, Abidjan – Rue des Hortensias, quartier ambassade Cocody

1.3. Fuseau horaire

UTC +00H00

1.4. Numéro de téléphone

Secrétariat Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : +225 27 22 48 97 63

1.5. Courriels

Pour les déclarations d'incidents : cert.incidents@anssi.gouv.ci

Pour toutes autres demandes : cert@anssi.gouv.ci

1.6. Clé publique et informations de chiffrement

Nous utilisons PGP pour les échanges opérationnels tels que les notifications, les signalements d'incidents et le partage d'informations avec nos homologues, partenaires et parties prenantes.

- ID Utilisateur : CI-CERT Incidents « cert.incidents@anssi.gouv.ci »
- ID de la clé : 0x13AF2F47
- Emprunte numérique : 2B98 33E1 E04E 6682 ED3A 1563 9297 0859 13AF 2F47
- La clé PGP est disponible à l'adresse suivante : https://keys.openpgp.org

1.7. Membres de l'équipe

L'équipe du CI-CERT est composée d'experts en sécurité informatique. La liste de ses membres n'est pas publique. Leur identité peut être communiquée au cas par cas, conformément au principe du strict besoin d'en connaître.

Autres informations

1.8. CI-CERT est membre de :

- FIRST (FIRST4, the Forum of Incident Response and Security Teams),
- AFRICA-CERT,
- OIC-CERT (Organization of Islamic Countries – Computer Emergency Response Team).

1.9. Points de contact

Le CI-CERT privilégie la réception des déclarations d'incidents par courriel à l'adresse suivante : cert.incidents@anssi.gouv.ci. Merci d'utiliser notre clé PGP pour garantir l'intégrité et la confidentialité des échanges. En cas d'urgence, veuillez ajouter [**URGENT**] dans l'objet du message.

2. CHARTE

2.1. Déclaration de mission

Aux termes de l'article 2 du Décret n° 2020-128 du 29 janvier 2020 portant création, organisation et fonctionnement du centre de veille et de réponse aux incidents de sécurité informatique dénommé CI-CERT, les missions du CI-CERT sont les suivantes :

- Assurer la coordination d'une réponse rapide et efficiente en cas d'incident de sécurité informatique ;
- Assurer la veille technologique et le monitoring de sécurité des réseaux et systèmes d'information ;
- Assurer la sécurité des systèmes d'information des infrastructures critiques d'information ;
- Collecter et traiter les incidents survenant sur les réseaux et systèmes d'information ;
- Assurer la fonction de point focal de la Côte d'Ivoire pour les cas de cybercriminalité ;
- Fournir les moyens techniques nécessaires pour l'échange efficace d'informations en situation de crise;
- Développer des outils et moyens de sensibilisation des usagers d'Internet, afin de développer la culture nationale de la cybersécurité ;
- Développer des programmes de formation de haut niveau en matière de sécurité des systèmes d'informations ;
- Assurer le développement de la coopération nationale et internationale en matière de cybersécurité.

2.2. Parties prenantes / Champs d'action

- Gouvernement et ses démembrements (ministères, institutions d'Etat)
- Administration publique (Agences, établissements publics, etc.)
- Entreprises et organisations établies en Côte d'Ivoire
- Universités, centres de recherches et écoles
- Particuliers

2.3. Tutelle /affiliation

CI-CERT est le centre national de veille et de réponse aux incidents de sécurité informatique, placé sous la direction de l'Agence nationale de la sécurité des Systèmes d'Information.

2.4. Autorité

Ministère de la transition numérique et de la digitalisation

Ministère de l'intérieur et de la sécurité

ANSSI/CI-CERT

3. POLITIQUES

3.1. Type d'incidents et niveaux d'assistance

Le CI-CERT est le point de focal national pour les incidents de sécurité informatique en Côte d'Ivoire.

Tous les incidents de cybersécurité sont traités avec la même diligence, sauf dans les cas spécifiques évalués au niveau CRITIQUE ou d'extrême URGENCE. Par ailleurs, les incidents affectant les infrastructures critiques nationales seront traités en priorité par le CI-CERT.

3.2. Coopération, interaction et partage d'informations

La coopération avec les autres CERT, CSIRT, Organisation professionnelles, Centres de recherches et entreprises est un piller essentiel de l'action du CI-CERT. Toutes les formes de coopération et de partage d'informations et de bons procédés susceptibles de contribuer au renforcement de la cybersécurité sur le plan régional et international, sont privilégiées sans restriction.

3.3. Sécurité des communications et protection des données à caractère personnel

Le CI-CERT met en œuvre toutes les mesures de sécurité, afin de protéger les informations créées, reçues, stockées ou transmises sur ses systèmes d'information, conformément à ses politiques spécifiques, au normes et standards de l'industrie et à la législation en vigueur en Côte d'Ivoire.

4. SERVICES OFFERTS

Le CI-CERT offre trois types de services :

4.1. Services proactifs

- Analyse de vulnérabilités
- Tests de pénétration
- Partage de renseignements de cybersécurité
- Sensibilisation

4.2. Services réactifs

- Réponses aux incidents
- Investigation numérique légale
- Analyse des codes et fichiers malveillants

4.3. Management de la sécurité de l'information

- Conseils pour le développement de stratégies et plans de cybersécurité
- Développement de programme de sensibilisation
- Renforcement des capacités

5. Déclaration d'incidents

Le CI-CERT a développé une plateforme de déclaration des incidents, signalement des vulnérabilités et des cybercrimes accessibles via sur son site internet. Cependant, les déclarations peuvent être faites directement par courriel à l'adresse cert.incidents@anssi;gouv.ci

6. Mentions légales

Statut	TLP	Version
Validé	RED : Diffusion restreinte	1.0

Notre équipe prend toutes les précautions nécessaires afin de fournir des informations, alertes et conseils aussi précis et à jour que possible. Toutefois, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ainsi que le CI-CERT, ne sauraient être tenus responsables des dommages résultant d'erreurs, d'omissions, d'inexactitudes ou de l'usage des informations diffusées.