Urgence Cyber région Sud

RÉGION SUD PROVENCE ALPES CÔTE D'AZUR

Soutenu par RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité

RFC 2350

Contrôle du document				
	Prénom Nom	Fonction	Date	Signature
Rédaction	Florian Putaud	CP IDE	27/08/2020	
Validation	Pascal Ausseur	DG	06/10/2020	

Historique des révisions			
Version	Date	Auteur	Nature
V0.1	27/08/2020	FP	Création
V1.0	05/10/2020	TJ	Revu
V1.1	07/08/2023	TM	Revu
V1.2	02/10/2023	AH	Revu
V1.3	20/02/2025	DH	Révision – Ajout des services additionnels

Table des matières

1. À propos du présent document

1.1 Version du document

Ceci est la version 1.3, publiée le 20 février 2025.

1.2 Liste de distribution pour notifications

Les mises à jour sont notifiées par mail à l'ensemble des adhérents de l'association.

1.3 Publication du document

La dernière version du présent document est disponible à l'adresse suivante :

https://www.urgencecyber-regionsud.fr/a-propos/

1.4 Authenticité du document

Ce document a été signé avec la clé PGP d'Urgence Cyber région Sud.

La clé publique PGP, l'identification et l'empreinte digitale sont disponibles sur le site Web d'Urgence Cyber région Sud à l'adresse suivante : https://www.urgencecyber-regionsud.fr/a-propos/

Expiration : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure

2. Information de contact

2.1 Nom du centre

Le nom officiel du centre est « Urgence Cyber – CSIRT région Sud »

Il est souvent nommé par son nom usuel « Urgence Cyber région Sud » ou encore par son acronyme « UCRS ».

2.2 Adresse

Urgence Cyber – CSIRT Région Sud
Maison du numérique et de l'innovation
Place George Pompidou
83000 Toulon

2.3 Fuseau horaire

Le fuseau horaire de travail du centre est l'heure normale d'Europe centrale en hiver (UTC+1) et l'heure d'été d'Europe centrale en période estivale (UTC+2).

2.4 Numéro de téléphone

Numéro d'information : 04 23 36 09 30
Numéro d'urgence : 0 805 036 083

2.5 Numéro de FAX

Non disponible.

2.6 Autre canal de communication

Non disponible.

2.7 Adresse de courrier électronique

L'adresse de courrier électronique d'Urgence Cyber région Sud est :
contact@urgencecyber-regionsud.fr

2.8 Clé publique et informations de chiffrement

Le centre possède une clé publique PGP :

- ID utilisateur : Urgence Cyber région Sud <contact@urgencecyber-regionsud.fr>
- ID clé : 0x7365A4BD
- SHA256 : *B221453565F05A77550753BA2C24BE9676028F4A776CCD4A8A94F679CF5D52A2*

La clé publique est disponible sur le site du centre à l'adresse :
https://www.urgencecyber-regionsud.fr/a-propos/

2.9 Composition de l'équipe

L'équipe est constituée de spécialistes et analystes en cybersécurité.
Aucune information nominative relative aux membres du CSIRT n'est diffusée dans ce document.

2.10 Horaires de fonctionnement

Le CSIRT est joignable du lundi au vendredi de 09h00 à 18h00.
En dehors de ces horaires, les appels sont redirigés vers le standard du CERT-FR.

2.11 Points de contact

Vous pouvez contacter le CSIRT Urgence cyber :

- Par téléphone au 0805 036 083
- Par courriel à l'adresse contact@urgencecyber-regionsud.fr
- Par le formulaire de contact présent sur le site web

3. Charte

3.1 Missions

Urgence Cyber Région Sud a pour mission principale de proposer aux acteurs de taille intermédiaire présents sur le territoire régional un service d'assistance face aux incidents de cybersécurité, adapté à leurs besoins sous la forme d'un service d'intérêt général. A minima, il assure :

- Le soutien et l'accompagnement dans la réponse à incident de premier niveau ;
- Le suivi dans la gestion technique et stratégique de l'incident ;
- Le référencement des prestataires régionaux spécialisés en réponse à incident ;
- Une veille des menaces numériques et la diffusion d'alertes sur le territoire ;
- Le relai et transfert des informations pertinentes vers le CERT-FR ;
- La consolidation de l'incidentologie régionale et partage du résultat avec le CERT-FR.

3.2 Bénéficiaires

Peuvent bénéficier du service d'accompagnement d'urgence en cas d'incident de cybersécurité, toutes structures de type Très Petites Entreprises (TPE), Petites et Moyennes Entreprises (PME), Entreprises de Taille Intermédiaires (ETI), collectivités territoriales et associations localisées dans un des départements de la région Provence-Alpes-Côtes d'Azur.

3.3 Affiliations

Urgence Cyber région Sud est un centre de réponse aux incidents cyber public. Il est affilié à la région Provence-Alpes-Côte d'Azur. Il maintient des relations avec les CSIRT régionaux et le CERT-FR de l'ANSSI.

3.4 Autorité

Urgence Cyber région Sud est placé sous l'autorité du directoire de l'association éponyme. Il dispose du soutien de la région Sud et de l'ANSSI.

4. Politiques

4.1 Types d'incidents et niveau de support

Urgence Cyber région Sud est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler l'un de ses bénéficiaires.

A minima, il assure :

- Le recueil, la qualification et le suivi de l'incident ;
- Le soutien et l'accompagnement dans la réponse à incident de premier niveau ;
- Le suivi et l'accompagnement dans la gestion technique et stratégique de l'incident ;
- L'information aux victimes sur les poursuites juridictionnelles à engager et orientations vers les professionnels qualifiés ;
- La mise en relation avec des prestataires régionaux pour la mise en œuvre de la réponse à incident de second niveau au besoin ;

4.2 Coopération, échanges et confidentialité de l'information

Aucune donnée personnelle ou sensible ne sera transmise ou exploitée sans l'accord préalable du bénéficiaire. En cas de judiciarisation, Urgence cyber accompagne le bénéficiaire mais n'a pas pour mission de transmettre directement des informations aux forces de l'ordre. Urgence Cyber s'engage à protéger la confidentialité des données et à orienter les victimes vers les autorités compétentes en cas de besoin.

Chaque traitement d'incident fera l'objet d'un compte-rendu anonymisé qui sera transmis au CERT-FR à des fins de retours d'expériences et de statistiques. Urgence cyber peut enfin être amené à communiquer des informations techniques anonymisées aux autres CSIRTs régionaux ou sectoriels, également à des fins statistiques ou de consolidation.

La diffusion d'information sera traitée en accord avec le protocole TLP défini par FIRST (https://www.first.org/tlp).

4.3 Communication

Le téléphone et le courriel sont les principaux moyens de communication utilisés par le CSIRT pour la transmission de données de faible sensibilité. Les informations non sensibles peuvent être échangées par courriels conventionnels. Cependant, Urgence cyber préconise l'utilisation du chiffrement PGP pour l'échange d'informations sensibles ou confidentielles

Urgence Cyber région Sud respecte le protocole de partage d'informations (TLP) comme décrit à l'adresse www.first.org/tlp/

5. Prestations de services additionnels

Dans le cadre de son fonctionnement associatif, Urgence cyber propose à ses adhérents des services additionnels payants, orientés sur la prévention et l'anticipation des menaces numériques. L'adhésion au CSIRT se présente sous la forme d'un abonnement annuel et donne accès aux services suivants :

Le diagnostic de maturité cyber	Evaluation du niveau de préparation grâce à un diagnostic sur mesure qui identifie les forces et les vulnérabilités en cybersécurité
L'accompagnement stratégique	Définition des objectifs adaptés à vos besoins réels et accompagnement dans la mise en place d'une gouvernance efficace
La formule veille standard	Veille informationnelle : actualités quotidiennes ou hebdomadaires
	Veille technique : un bulletin de sécurité quotidien ou hebdomadaire (concernant les vulnérabilités annoncées dans l'un des périmètres de veille prédéfinis)
Les évènements	Pour rester à la pointe des bonnes pratiques, gagner en compétences et rencontrer les professionnels du territoire avec des événements dédiés à la cybersécurité.

Dans ce cadre, les informations suivantes vous seront demandées :

- La nomination d'un correspondant au sein de la structure ;
- La réponse à un questionnaire d'identification des composants du Système d'Information de la structure.

6. Déclaration d'incident

En cas d'urgence, Urgence cyber encourage fortement l'emploi du numéro d'urgence (0805 036 083).

Il est également possible d'utiliser le formulaire de déclaration d'incident disponible sur le site web de l'association. Ce formulaire est conçu pour recueillir toutes les informations nécessaires à la prise en charge de l'incident.

7. Avertissements

Bien que les informations transmises dans le document aient été vérifiées, Urgence Cyber région Sud refuse toute responsabilité en cas d'erreur ou d'omission ou pour tout préjudice résultant d'information contenues dans ce document.

Si vous constatez une erreur dans ce document merci de nous le signaler par mail. Nous tâcherons de rectifier les informations au plus vite.