Charte de l'
« InterCERT-FR »

Table des matières

1. Introduction

Le groupe « **InterCERT-FR** » réunit de façon régulière sous la coordination d'un comité de pilotage, un ensemble d'organismes ayant des activités d'IRT (Incident Response Team) sur le territoire français.

Ce groupe est une association de fait et il est convenu que l'appartenance à ce dernier ne doit pas être mise en avant à des fins commerciales ou de promotion.

Ce document définit le fonctionnement du groupe, et les règles que chaque participant au groupe s'engage à respecter. Ces règles sont adoptées à l'unanimité et pourront évoluer dans le temps. Le présent document sera mis à jour en conséquence.

2. Membres du groupe

2.1. Critères d'adhésion

Le groupe rassemble des équipes (ci-après appelées **Membres**) de type CSIRT (Computer Security Incident Response Team), dont les activités concernent au moins le territoire français, mais peuvent s'étendre au-delà. Ces activités doivent comprendre *à minima* la détection ou la réaction aux incidents de sécurité. Ces équipes peuvent être rattachées à une **Organisation** (entreprise, administration, institution, association, etc.).

Le groupe fait la distinction entre les CSIRT internes, dont le périmètre concerne leur Organisation ou une partie de celle-ci, et les CSIRT externes, qui proposent leurs services à des clients.

Dans le cas où une Organisation dispose de plusieurs CSIRT internes, seule l'une d'entre elles pourra devenir Membre du collège des CSIRT internes du groupe sauf exception. Il en va de même dans le collège des CSIRT externes.

2.2. Représentation du Membre au sein du groupe

Chaque Membre du groupe est représenté par une personne physique (ci-après appelée **Représentant Membre)** ainsi que d'un délégué (ci-après appelé **Représentant Membre délégué)**. Ce binôme est responsable, vis-à-vis du groupe « InterCERT-FR », du suivi par son Organisation des règles du code de conduite.

Le Représentant Membre doit nécessairement être employé par l'Organisation dont il fait partie. Cette dernière condition ne concerne pas le Représentant Membre délégué.

Le Représentant Membre détient le droit de vote du membre (cf. §6).

2.3. Participation aux travaux du groupe

En plus du Représentant Membre et du Représentant Membre délégué, les personnes appartenant à l'équipe CSIRT du Membre peuvent participer aux travaux (et en particulier aux réunions) du groupe « InterCERT-FR » dans la limite des places disponibles. Cette extension de participation concerne exclusivement des personnes ayant des activités de détection ou de réaction aux incidents de sécurité. Les stagiaires ne peuvent pas participer aux travaux du groupe pour des raisons de confidentialité.

Les autres personnes (mêmes si elles appartiennent à la même Organisation que le Membre) ne peuvent pas participer, sauf si elles y ont été invitées ponctuellement par le groupe « InterCERT-FR ». Cette précision est importante en particulier par rapport aux règles de confidentialité appliquées au sein du groupe (cf. § 7.4).

3. Autorité et Responsabilité

3.1. Responsabilité des membres

Chaque Membre représente et intervient au nom de son Organisation. Il doit s'assurer de sa capacité et légitimité à représenter son organisation auprès du groupe. Il est responsable vis-à-vis du groupe des actes des membres de son équipe. Il doit en particulier :

- Sensibiliser son équipe aux règles définies par le code de bonne conduite ;
- S'assurer que le code de bonne conduite est respecté par l'ensemble de son équipe.

3.2. Gouvernance du groupe

3.2.1. Comité de Pilotage de l'InterCERT-FR

La gouvernance et l'animation du groupe sont assurées par le Comité de Pilotage de l'InterCERT-FR. Celui-ci est composé de 5 membres répartis comme suit :

- Le CERT-FR est membre du Comité de Pilotage ;
- Deux (2) Membres sont élus au sein du collège des "CSIRTs internes" ;
- Deux (2) Membres sont élus au sein du collège des "CSIRTs externes".

Le mandat d'un Membre élu au Comité de Pilotage est de deux ans. Un Membre élu ne peut exercer plus de 2 mandats consécutifs.

Tout Membre élu du Comité de Pilotage est libre de quitter le Comité de Pilotage et sans préavis. Le Responsable Membre doit le manifester formellement au groupe.

3.2.2. Election du Comité de Pilotage

1 – Deux Membres sont à élire pour chacun des deux collèges, "CSIRTs internes" et "CSIRTs externes".

2 – Chaque Membre de l'InterCERT-FR peut voter pour les candidats de son collège. A noter que le CERT-FR ne prend pas part au vote pour cette élection.

3 – Les Membres candidats peuvent établir tous les contacts qu'ils souhaitent avec les Membres de leur collège durant la phase de campagne, et peuvent notamment diffuser une profession de foi. Toute profession de foi doit être diffusée à tous les Membres quel que soit leur collège.

4 – Chaque Membre dispose de deux (2) voix qu'il exprime dans un unique bulletin de vote. Il ne vote que pour les Membres candidats du collège auquel il appartient. Chaque Membre peut utiliser zéro, une ou deux voix, ou ne pas participer au vote. En cas d'envoi d'un second bulletin de vote, ce dernier ne sera pas pris en compte.

5 – Un Membre ne peut pas utiliser ses deux voix pour le même Membre candidat. A noter qu'un Membre candidat ne peut donc voter pour lui-même qu'à hauteur d'une seule voix.

6 – Toute voix pour un Membre n'étant pas candidat dans le collège concerné sera comptabilisée comme "nulle".

7 – Pour être pris en compte, les votes devront être transmis selon les consignes données préalablement au vote.

8 – En cas de l'expression d'une voix non valide, la voix concernée sera considérée comme "nulle". Cette nullité ne s'appliquera qu'à la voix concernée et non au bulletin de vote dans son ensemble.

9 – Les votes resteront secrets : ils ne seront donc pas communiqués aux Membres élus du Comité de Pilotage à l'issue du vote.

10 – Durant la phase de vote, le CERT-FR transmettra à intervalles réguliers le nombre d'entités ayant voté, ainsi que le nombre de voix exprimées. De plus, un email individuel de rappel sera envoyé à chaque équipe n'ayant pas encore voté.

11 – A chaque réception de vote, le CERT-FR transmettra un accusé de réception afin que l'entité votante sache que son vote a bien été comptabilisé. Cet accusé de réception ne signifiera en revanche pas que le vote et son contenu sont valides.

12 – Le calendrier de la campagne et du vote sera communiqué par écrit préalablement. Il précisera en particulier, la date de fin de campagne, les dates durant lesquelles le vote sera ouvert et la date de proclamation des résultats.

13 – Il sera interdit aux candidats de communiquer explicitement sur leur candidature ou d'en faire mention dans quelque contexte que ce soit après la date de fin de période de campagne.
Si une équipe souhaite communiquer avec une équipe candidate au-delà de cette date, il est fortement recommandé qu'une demande explicite de contact soit transmise sous la forme d'un email signé par PGP.
Cette recommandation s'applique à toute forme de communication, échange par messagerie (email, instantanée, etc.…), échange téléphonique, rencontre physique, ...
Afin d'éviter toute erreur d'interprétation, il est fortement recommandé que l'équipe candidate vérifie bien la légitimité de la demande ainsi que la signature PGP du demandeur avant toute réponse, et conserve la trace de la demande.

14 – La légitimité des votes et le respect des règles du présent document seront vérifiés et validés par le CERT-FR.

15 – En cas de contestation ou de litige, le CERT-FR sera seul habilité à trancher, compte-tenu de sa neutralité dans le processus électoral.

16 – le CERT-FR (ou son Représentant en charge de dépouiller les votes et de les contrôler), s'engage à respecter la confidentialité des votes.

4. Principe de participation

Les Membres du groupe **« InterCERT-FR** » se réunissent de façon régulière *a minima* une fois par an en plénière.

Une place par Membre est réservée pour la participation aux réunions. L'accueil de personnes supplémentaires se fait dans la limite des capacités d'accueil.

La participation des Membres à chaque réunion est fortement encouragée, car elle est indispensable pour atteindre les objectifs d'échanges que le groupe s'est fixés.

A défaut de pouvoir être présent un Représentant Membre peut se faire remplacer par une personne de son équipe, sous réserve que cette dernière ne soit ni un prestataire, ni une personne extérieure à l'organisation représentée, ni un tiers (partenaires, etc.), ni un stagiaire.

Le cas échéant, le Représentant Membre doit signifier formellement au Comité de Pilotage de l'InterCERT-FR son absence et la personne de son équipe qui le représentera. Cette personne sera de facto porteuse du droit de vote du Membre (cf. § 7).

5. Admission / Exclusion

5.1. Conditions d'admission d'un nouveau Membre

Pour qu'un nouveau Membre soit admis au sein du groupe **« InterCERT-FR** » il faut :

- Qu'il ait des activités de détection ou de réponse aux incidents de sécurité localisées sur le territoire national ;
- Qu'il adhère sans réserve aux dispositions décrites dans la présente charte ;
- Qu'il suive la procédure d'admission décrite ci-dessous.

5.2. Procédure d'admission d'un nouveau Membre

La procédure d'admission d'un nouveau Membre dans le groupe « **InterCERT-FR** » est la suivante :

- Le candidat doit être coopté par un Membre du groupe. Ce Membre est appelé « le sponsor ». Le sponsor s'engage à ne pas avoir de relations commerciales et à ne pas faire partie de la même Organisation que le candidat en date de la cooptation. Le nombre maximal de nouveaux Membres qu'un sponsor peut coopter est fixé à 1 par an.
- Le sponsor doit préalablement s'assurer que les activités du candidat sont conformes à la définition donnée au § 5.1, et que ce dernier est un acteur de confiance.
- Le candidat doit ensuite fournir la RFC 2350 dûment renseignée au sponsor ainsi que la présente charte InterCERT-FR datée, paraphée et signée, que le sponsor lui aura préalablement transmise. La charte étant un document engageant, elle doit être signée par le responsable de l'équipe CSIRT.
- Le sponsor doit compléter la fiche de cooptation[1] qu'il transmet par la suite en même temps que la RFC 2350 et la charte signée par le responsable de l'équipe CSIRT du candidat au comité de pilotage par email.
- Le comité de pilotage accuse réception de la nouvelle candidature dans un délai maximum de 2 semaines et valide les éléments fournis dans un délai maximum de deux mois ; cette validation peut faire l'objet d'une visite optionnelle sur site par le comité de pilotage ou par un membre qu'il aura désigné. La recevabilité de la candidature est prononcée à l'issue de ce délai.
- Les candidatures recevables feront l'objet d'une audition devant le comité de pilotage visant à présenter les activités et les motivations du nouveau Membre à rejoindre le Groupe.
- Le comité de pilotage propose un avis au Groupe, accompagné de la RFC 2350 transmise par le sponsor ; sans objection sous quinzaine, la candidature du nouveau Membre est retenue pour une période probatoire d'une année. Toute objection à l'entrée d'un nouveau Membre devra être argumentée par email auprès du comité de Pilotage qui décidera de la recevabilité de l'objection et de la suite à donner à la demande de candidature.
- Le nouveau Membre sera notifié de la décision le concernant dans un délai maximum d'un mois après son audition.

Si un membre du Comité de Pilotage est sponsor du candidat, il ne peut se prononcer sur la recevabilité de la candidature, il ne participe pas aux délibérations suite à la présentation ainsi qu'à la rédaction de l'avis à destination des Membres du groupe.

Lors de son admission dans le groupe « **InterCERT-FR** », le nouveau Membre acquiert le statut de membre temporaire pour une durée d'un an.

[1] https://www.cert.ssi.gouv.fr/uploads/Fiche_de_cooptation_InterCERT-FR.pdf

Le nouveau Membre s'engage à :

- Se présenter au Groupe durant la première réunion plénière à laquelle il assiste ;
- Participer à un minimum de la moitié des réunions téléphoniques du groupe pendant cette première année d'affiliation temporaire ;
- Participer à toutes les réunions plénières du groupe qui seront organisées sur cette période ;
- Compléter, dans un délai de six mois à compter de son admission, l'auto-évaluation "CSIRT Maturity"[2] proposée par l'ENISA et en communiquer les résultats au comité de pilotage ;
- Informer le comité de pilotage de toute incapacité à participer à une réunion du Groupe avant celle-ci ;
- Respecter les dispositions prévues pour le partage d'information (TLP) et de leurs surcharges éventuelles.

Le non-respect de ces engagements peut aboutir à la radiation du nouveau Membre, sur décision du comité de pilotage.

Le nouveau Membre est vivement encouragé à :

- Proposer, sur une base biannuelle, des thématiques à présenter lors de réunions téléphoniques ou plénières ;
- Contribuer aux groupes de travail actifs au moment de son adhésion au groupe ;
- Utiliser les outils de partage adoptés par le Groupe pour les échanges d'informations.

Un membre temporaire ne peut coopter un candidat.

5.3. Exclusion d'un Membre

Le non-respect manifeste des règles du code de conduite par un Membre est une raison légitime pour que l'exclusion de ce Membre soit discutée au sein du groupe.

Un Membre peut être exclu du groupe s'il y a accord de la majorité absolue des autres Membres du groupe, selon le principe de vote décrit au paragraphe § 7.

Le processus type d'exclusion est le suivant :

- Discussions préalables, au sein du comité de pilotage à propos de l'exclusion potentielle d'un des membres. Ces discussions se font hors la présence du membre dont l'exclusion est envisagée ;
- Si le processus d'exclusion se poursuit, le membre dont l'exclusion est envisagée est informé de la procédure en cours, et il a la possibilité de donner son point de vue au Comité de pilotage à propos des griefs qui lui sont reprochés ;
- Le vote est organisé selon les modalités définies au paragraphe § 6, et son résultat annoncé.

Il est important de noter qu'en cas d'exclusion, le Membre est tenu à l'obligation de confidentialité (cf. § 7.4) sans limitation de temps.

Chaque Membre du Groupe a la possibilité de signaler au comité de pilotage tout manquement à la présente Charte ou agissement contraire à l'éthique.

Le comité de pilotage s'engage à accuser réception de ces signalements dans un délai maximum de 7 jours. Il procède ensuite à l'instruction d'une décision dans un délai maximum de 3 mois. Cette décision

[2] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

sera soumise au vote de l'ensemble des membres du Groupe (à l'exception du membre dont l'exclusion est envisagée). Ce vote pourra se tenir en plénière ou par correspondance. Si cette seconde méthode est utilisée, un délai de deux semaines sera accordé aux Membres pour procéder au vote avant décision.

Dans le cas où le signalement concerne un membre du comité de pilotage de l'InterCERT-FR, ce dernier pourra être suspendu temporairement de ses fonctions au sein du comité de pilotage.

5.4. Départ volontaire

Tout Membre est libre de quitter le groupe et sans préavis. Le Responsable Membre doit le manifester formellement au groupe.

Il est important de noter qu'en cas de départ volontaire, le Membre est tenu à l'obligation de confidentialité (cf. § 7.4) sans limitation de temps.

6. Vote

Le principe du vote à **la majorité absolue** (s'entendant comme majorité des suffrages exprimés) est retenu pour la prise de décision au sein du groupe selon les modalités suivantes :

- Exclusion d'un Membre : **à la majorité absolue** (et à l'exception du Membre concerné)
- Modifications des règles de fonctionnement du groupe : **à la majorité absolue**

Le mode de vote et les modalités de dépouillement associées (main levée, bulletin secret, etc.) seront décidés préalablement à chaque vote. Le comité de pilotage de l'InterCERT-FR est responsable du bon déroulement du vote.

Chaque Membre, à travers son Représentant (ou son délégué) est doté d'une seule et unique voix.

En cas d'absence du Représentant Membre, cette voix peut être déléguée à une personne de l'équipe du Membre (cf. §4).

En cas d'absence du Membre, et pour faire partie des votants, cette voix doit formellement avoir été donnée à un autre (et un seul) Membre du groupe. La délégation de vote doit être signifiée au comité de pilotage au plus tard une semaine avant la date du vote.

7. Code de conduite

L'ensemble des Membres du groupe s'engage à respecter le code de conduite décrit ci-dessous.

7.1. Aider à la détection et à la résolution des incidents de sécurité informatique

L'objectif premier du groupe est de renforcer au niveau français la capacité de chaque Membre à détecter et à traiter les incidents de sécurité impactant sa communauté. L'échange d'expérience et le partage d'informations pertinentes sont les deux principales missions concourant à la réalisation de cet objectif.

7.2. Agir avec déontologie et dans le respect des lois

Le respect des lois et de la déontologie constitue une des valeurs fondamentales promues au sein du groupe que les Membres s'engagent à appliquer.

La déontologie de l'InterCERT-FR repose sur le partage gracieux d'informations et d'expérience entre les Membres afin d'améliorer leur capacité à sécuriser les Systèmes d'Information de leurs parties prenantes, et d'une façon générale, de l'ensemble des usagers d'Internet.

Toute activité d'un Membre contraire à cette déontologie est donc proscrite et peut donner lieu à la proposition de l'exclusion du Membre.

7.3. Participer activement et loyalement aux activités du groupe

Pour que le principe du partage d'expérience au sein du groupe soit équitable il est important que chaque Membre participant contribue à ce partage. A ce titre il s'engage donc à prendre une part active dans la vie du groupe et à ne pas se contenter d'un rôle d'observateur.

7.4. Respecter la confidentialité des échanges au sein du groupe

La confidentialité des informations échangées au sein du groupe « **InterCERT-FR** » repose en particulier sur l'utilisation du protocole TLP (Traffic Light Protocol) en version 1.0 tel que défini par le FIRST (https://first.org/tlp/). L'application des réglementations et lois en vigueur est prépondérante sur l'application du TLP.

Ce protocole définit la confidentialité attendue par l'émetteur quant aux informations échangées, à l'aide d'un marquage spécifique apposé par ce dernier. En l'absence d'un marquage TLP explicite, toute information échangée au sein du groupe « **InterCERT-FR** » est considérée marquée TLP:AMBER.

Le marquage TLP s'écrit en lettres capitales sous la forme "TLP:COULEUR" et doit être idéalement spécifié :

- Par courriel : dans le sujet et le corps du message, avant l'information concernée ;
- Dans les documents : dans les en-têtes et pieds de page, d'une taille minimale de 12 points.

Les seules valeurs possibles pour le marquage sont les suivantes, celles-ci ne doivent pas être traduites en français (par exemple ne pas utiliser TLP:ROUGE) :

TLP: RED = Ne pas divulguer, information restreinte uniquement aux récipiendaires.

Les émetteurs peuvent utiliser TLP:RED lorsque l'information ne doit pas être partagée à d'autres parties que les récipiendaires, et dont la divulgation ou le mauvais usage implique des risques pour la vie privée, la réputation ou les opérations si elle est partagée en dehors des récipiendaires. Les récipiendaires ne peuvent pas partager les informations TLP:RED avec des parties en dehors de l'échange, de la réunion ou de la conversation spécifique dans laquelle elles ont été divulguées à l'origine. Dans le cadre d'une réunion, par exemple, les informations TLP:RED sont limitées aux personnes présentes à la réunion. Dans la plupart des cas, TLP:RED doit être échangé verbalement ou en personne.

TLP: AMBER = divulgation limitée, information limitée aux organisations et aux parties prenantes des participants sur la base du besoin d'en connaître.

Les émetteurs peuvent utiliser TLP:AMBER lorsque l'information requiert un partage pour son usage, mais dont la divulgation ou le mauvais usage implique des risques pour la vie privée, la réputation ou les opérations si elle est partagée en dehors des organisations impliquées. Les récipiendaires ne peuvent partager les informations TLP:AMBER qu'avec les membres de leur propre organisation et les clients qui doivent connaître l'information pour se protéger ou prévenir de dommages. *Les émetteurs sont libres de spécifier des limites supplémentaires au partage : celles-ci doivent être respectées par les récipiendaires.*

TLP: GREEN = divulgation limitée, information restreinte à la communauté.

Les émetteurs peuvent utiliser TLP:GREEN lorsque l'information est utile pour la sensibilisation de toutes les organisations participantes ainsi que des pairs dans la communauté ou le secteur en général. Les récipiendaires peuvent partager des informations TLP:GREEN avec des pairs et des organisations partenaires dans leur secteur ou leur communauté, mais pas via des canaux accessibles au public. L'information dans cette catégorie peut circuler largement dans une communauté particulière. Les informations TLP: GREEN ne peuvent pas être diffusées en dehors de la communauté.

TLP: WHITE = La divulgation de l'information n'est pas limitée.

Les émetteurs peuvent utiliser TLP:WHITE lorsque les informations comportent un risque prévisible ou inexistant d'utilisation abusive, conformément aux règles et procédures applicables à la publication publique. Sous réserve des règles de droit d'auteur standard, les informations TLP:WHITE peuvent être distribuées sans restriction.

D'une façon générale, les Membres du groupe « **InterCERT-FR** » mettent en œuvre les moyens appropriés pour la protection et la conservation des informations échangées au sein du groupe.

Nom : **Prénom :**

Fonction :

Date :

Signature :

Fin du document