Version : 1.3

RFC 2350 – CERT-HCL

C1 – Public

TLP:CLEAR

Tableau de révision

Version - Date - Synthèse
[Historique synthèse]

Table des matières

1 A propos de ce document

Ce document contient une description du CERT des Hospices Civils de Lyon (« CERT-HCL ») conformément à la RFC 23501. Il fournit des informations essentielles sur le CERT-HCL, détaillant ses responsabilités et les services fournis.

1.1 Date de dernière mise à jour

- V1.0 : 12/2025

- V1.1 : 2/2026 – correction de typo

- V1.2 : 4/2026 – corrections diverses

- V1.3 : 5/2026 – suppression d'une phrase du chapitre 6

1.2 Liste de diffusion des notifications

Aucune liste de diffusion n'est disponible pour les mises à jour de ce document.

1.3 Lieu de distribution de ce document

La version actuelle la plus récente de ce document est disponible sur le site web du CERT-HCL à l'adresse : https://www.chu-lyon.fr/cert

1.4 Authenticité de ce document

Ce document a été signé avec la clé PGP du CERT-HCL.

La signature et notre clé PGP publique (ID et empreinte) sont disponibles sur notre site web au lien suivant : https://www.chu-lyon.fr/publickey.txt et www.chu-lyon.fr/rfc2350.sig

1.5 Identification du document

Titre : "CERT-HCL_RFC2350_FR"

Version : 1.2

Date du document : 21 avril 2026

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

2 Information sur le CERT-HCL

2.1 Nom de l'entité

Nom complet : CERT-HCL

2.2 Adresse

CERT-HCL
Hospices Civils de Lyon
Direction des Services Numériques
61 boulevard Pinel
69500 BRON, France

2.3 Zone de temps

CET/CEST : Paris (GMT+01:00, et GMT+02:00 heure d'été)

2.4 Numéro de téléphone

Le CERT-HCL ne communique pas de numéro de téléphone public.
Les bénéficiaires du CERT-HCL ont accès à un numéro d'urgence.

2.5 Numéro de fax

Sans objet

2.6 Adresse électronique

Si vous avez besoin de signaler au CERT-HCL un incident de cybersécurité ou un acte de cyber malveillance lié aux Hospices Civils de Lyon ou au GHT Val Rhône Centre, veuillez le joindre à l'adresse suivante : cybersecurity@chu-lyon.fr

2.7 Autre moyen de contact

Sans objet

2.8 Clé publique et information sur le chiffrement

Le CERT-HCL a une clé PGP : https://www.chu-lyon.fr/publickey.txt

2.9 Security.txt

Les informations ci-dessus (mail, clé PGP…) ainsi que des informations complémentaires sont disponibles sur la page security.txt du CERT HCL, disponible à l'adresse suivante : https://www.chu-lyon.fr/.well-known/security.txt et https://www.chu-lyon.fr/security.txt.

2.10 Membres de l'équipe

La liste des membres de l'équipe n'est pas publiée. Elle est constituée d'experts en sécurité des systèmes d'information avec des compétences en analyse des vulnérabilités, analyse SOC et analyse forensique. L'identité de l'un des membres du CERT-HCL peut être communiquée au cas par cas selon la règle du besoin d'en connaitre.

2.11 Autres informations

Sans objet

2.12 Point de contact

Il est demandé de contacter le CERT-HCL par mail.

Les heures ouvrées sont les suivantes : du lundi au vendredi, de 9 h à 17 h (CEST).

3 Charte

3.1 Ordre de mission

Le CERT-HCL est le Computer Emergency Response Team (CERT) interne des Hospices Civils de Lyon. Sa mission principale est d'assurer la réponse aux incidents de sécurité informatique pour l'ensemble des établissements des Hospices Civils de Lyon (hôpital public). Il assure également un support et une expertise auprès des établissements du GHT Val Rhône Centre [1] sur le même domaine.

Les missions du CERT-HCL couvrent également la prévention, la détection et la reprise :

- Aide à prévenir les incidents de sécurité en mettant en place les mesures de protection nécessaires ;
- Détecte les vulnérabilités sur les réseaux et les systèmes ;
- Partage des informations sur les menaces cyber avec les membres du GHT et avec d'autres hôpitaux en France et en Europe ;
- Relaie et transfère des informations pertinentes depuis et vers le CERT SANTE et l'EH-ISAC[2].

3.2 Bénéficiaire

L'ensemble des sites des Hospices Civils de Lyon bénéficie des services du CERT-HCL. L'ensemble des établissements du GHT Val Rhône Santé peuvent également bénéficier des services du CERT-HCL.

3.3 Parrainage et affiliation

Le CERT-HCL entretient des contacts privilégiés avec son CERT Sectoriel (CERT Santé) et possède également un canal d'échange avec l'EH-ISAC. Il est également en mesure de contacter le CERT-FR.

3.4 Autorité

Le CERT-HCL réalise ses activités sous l'autorité du Directeur des Services Numériques des HCL.

[1] Groupement hospitalier de territoire permettant la mise en commun de stratégies et d'activités entre établissements proches.
Le GHT Val Rhône Centre regroupe : CH de Beaurepaire, CH de Condrieu, CH de Givors, CH du Mont-d'Or, CHI de Neuville-Fontaines, CH du Pilat Rhodanien, CH de Sainte-Foy-lès-Lyon, CH de Vienne, CH Le Vinatier, Hospices Civils de Lyon.

[2] European Health Information Sharing & Analyses Center : Collectif d'organisations européennes dans le domaine de la santé ayant pour but d'améliorer la cybersécurité et la résilience dans ce secteur pour l'Union Européenne.

4 Politiques

4.1 Types d'incidents et niveau d'intervention

Le CERT-HCL est habilité à traiter tous types de cyberattaques susceptibles de porter atteinte à la sécurité du système d'information des HCL. Selon le type d'incident de sécurité, le CERT-HCL mettra en œuvre ses services, notamment la réponse aux incidents et l'analyse forensique numérique.

Il peut intervenir, sur demande, en support sur les incidents informatiques du GHT Val Rhône Centre.

Le niveau de soutien apporté par le CERT-HCL variera en fonction de la gravité de l'incident ou du problème de sécurité, de son impact potentiel ou évalué et des ressources disponibles du CERT-HCL au moment de l'incident.

Le CERT-HCL peut aussi bénéficier d'un appui technique du CERT Santé et du CERT-FR.

4.2 Coopération, interaction et divulgation d'informations

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord de la partie nommée. Les informations fournies restent confidentielles et ne sont communiquées qu'au CERT Santé et CERT-FR en cas de déclaration d'incident.

4.3 Communication et authentification

La méthode de communication privilégiée est l'e-mail. Pour l'échange d'informations sensibles et la communication authentifiée, CERT-HCL utilise PGP pour chiffrer et/ou signer les messages. Il est fortement recommandé que toute communication sensible adressée à CERT-HCL soit chiffrée avec notre clé PGP publique, comme indiqué dans la Section 2.8.

5 Services

5.1 Activités Réactives - Réponse aux incidents

Le CERT-HCL réalise les services suivants dans le cadre de la réponse aux incidents de sécurité informatique :

- Détection des incidents ou réception de leur signalement ;
- Diagnostic, analyse technique, corrélation et triage des incidents ;
- Assistance à résolution et contrôle des remédiations ;
- Coordination avec les autres entités hors du périmètre d'action.

Le service de réponse aux incidents est disponible de 9h à 17h les jours ouvrés. Un service minimum est assuré sous astreinte en dehors de ces plages.

Le traitement et la déclaration des incidents est de la responsabilité des structures de santé. Le CERT-HCL intervient, sur demande, en support pour le traitement des incidents sur les établissements du GHT.

5.2 Activités proactives

5.2.1 Alertes et CyberThreat Intelligence

Le CERT-HCL réalise une veille sur les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires.

Il notifie ses bénéficiaires le cas échéant.

5.2.2 Conseil en sécurité informatique

Le CERT-HCL fournit à ses bénéficiaires des conseils en architecture sécurisée.

6 Formulaire de notification d'incident

Les incidents sont remontés automatiquement au CERT-HCL via les outils de gestion des incidents du SOC HCL.

La déclaration des incidents est de la responsabilité des structures de santé (HCL et établissements de GHT) et se fait via le portail de signalement des évènements sanitaires indésirables dans la section « Professionnel de santé » : https://signalement.social-sante.gouv.fr

7 Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CERT HCL ne peut être tenu responsable des erreurs ou omissions, ou des dommages résultant de l'utilisation des informations fournies.