



Politique de divulgation coordonnée des vulnérabilités

Version: 28 août 2026

Explication

Soucieux d'améliorer continuellement la performance et la sécurité de ses réseaux et systèmes d'information, Civadis a mis en place une politique de Divulgateur Coordonnée des Vulnérabilités (CVD) afin d'offrir un canal clair, sécurisé et encadré pour le signalement des vulnérabilités affectant nos services et infrastructures. Ce cadre donne la possibilité aux participants de rechercher, avec de bonnes intentions, de potentielles vulnérabilités dans les systèmes, les équipements et les produits de Civadis et de nous transmettre toute information découverte sur une vulnérabilité. En renforçant la transparence et la traçabilité, la CVD favorise la confiance de nos clients et partenaires, soutient nos obligations réglementaires (p. ex. RGPD, NIS2), nourrit notre démarche d'amélioration continue et offre aux chercheurs animés de bonnes intentions, un point de contact pour mettre en œuvre la loi belge de 2023.

Dans le cas où cette politique serait contraire à la législation en vigueur, cette dernière prévaudrait. Civadis s'engage à mettre tout en œuvre pour éviter une telle discordance.

Obligations mutuelles des deux parties

Proportionnalité

Les participants acceptent de se conformer strictement au principe de proportionnalité dans toutes leurs activités, notamment : ne pas porter atteinte à la disponibilité des services fournis par le système et ne pas faire usage des vulnérabilités au-delà de ce qui est strictement nécessaire pour démontrer la faille de sécurité. Leurs approches doivent rester proportionnées : si le problème de sécurité a été démontré à petite échelle, aucune action supplémentaire ne doit être engagée.

Restrictions de participation

Le chercheur ne doit pas faire partie de Civadis (interne ou externe) ni de Keyes, afin d'éviter toute confusion avec les procédures internes des lanceurs d'alerte.

Périmètre

Le périmètre de ce document reprend les domaines suivants ainsi que leurs sous-domaines :

*.go2digital.be

*.go2jobs.be

*.civadis.be

*.civacloud.be

*.e-guichet.be

*.loth-info.be

*.adehis.be

Action non autorisée

Les participants ne sont pas autorisés à effectuer les actions suivantes :

- Copier ou altérer les données du système IT ou supprimer les données de ce système.
- Modifier les paramètres du système d'information
- Installer des malwares, virus, vers, cheval de Troie, etc. ou tout autre logiciel ou matériel, malveillant ou non
- Effectuer des attaques DDOS ou autres attaques nuisant à la disponibilité du système d'information
- Utiliser des techniques d'ingénierie sociale, par exemple le phishing
- Voler des mots de passe ou se livrer à des attaques de type « brute force »
- Utiliser des appareils dans le but d'intercepter, stocker et prendre connaissances de communications électroniques qui ne sont pas accessible au public.
- Se procurer délibérément, conserver, communiquer ou distribuer du contenu non public ou d'autres données des systèmes d'information. Cette interdiction concerne les données personnelles, et inclut également toute autre information confidentielle telle que les secrets d'affaire, les secrets de tiers, etc

Si le participant souhaite utiliser l'assistance d'un tiers pour effectuer ses recherches, le participant doit s'assurer que le tiers est dument informé de cette politique et qu'il accepte, en offrant son assistance, d'en suivre les termes.

Confidentialité

Le participant doit s'abstenir strictement de partager ou de divulguer toute information collectée avec des tiers sans notre consentement préalable et explicite.

Une attention toute particulière sera portée aux données personnelles obtenue involontairement dans le cadre des travaux de recherche. Ces recherches seront alors qualifiées de traitement au sens du RGPD, et doivent être menées comme telles.

Exécution de bonne foi

Notre organisation s'engage à appliquer cette politique de bonne foi et à ne pas engager de poursuites judiciaires, civiles ou pénales, contre un participant qui respecte ses conditions.

Le participant doit être exempt de toute intention frauduleuse, intention de nuire, d'utiliser ou de causer des dommages au système visité ou à ses données. Cela s'applique également aux systèmes de tiers situés en Belgique ou à l'étranger.

En cas de doute concernant l'une des conditions de notre politique, le participant doit d'abord consulter notre point de contact risk@civadis.be et obtenir son consentement écrit avant d'agir.

Récompense

Civadis, à sa discrétion, peut attribuer une prime en nature, de valeur limitée, en fonction de la valeur de la vulnérabilité trouvée.

Civadis peut, à sa discrétion, proposer au participant de l'ajouter à un « hall of fame » sur son site web.

Communication des découvertes

Validation

Lorsqu'un participant prend connaissance d'informations relatives à une vulnérabilité potentielle, il doit, dans la mesure du possible, effectuer des vérifications préalables afin de confirmer l'existence de la vulnérabilité et d'identifier les risques éventuels.

Notification

Le participant s'engage à communiquer, dès que possible, les informations techniques relatives aux vulnérabilités potentielles à l'adresse risk@civadis.be. La communication aura lieu de préférence en Français, en Néerlandais ou en Anglais. Toute autre langue est permise mais le délai de réponse pourra être allongé.

La clé PGP disponible sur le site vous permettra de sécuriser le contenu de la communication.

Civadis s'engage à envoyer au participant, dans les 5 jours ouvrables, un accusé de réception, sa référence interne ainsi que les prochaines étapes de la procédure.

Dans le cadre où le participant ne recevrait pas de réponse, il est autorisé, en conformité avec la loi, de prévenir le régulateur après un délai de 90 jours.

Le participant recevra également un mail le prévenant lorsque la vulnérabilité sera résolue.

Communication

Les parties s'engagent à mettre tous les moyens en oeuvre pour garantir une communication continue, sécurisée et efficace. Les informations fournies par le participant peuvent être très utiles pour identifier et corriger la vulnérabilité.

En l'absence de réaction de l'une des parties dans un délai de 90 jours, chaque partie peut notifier le Centre pour la Cybersécurité de Belgique (CCB) (incident@ccb.belgium.be).

Annonce publique potentielle

Civadis décidera, en coordination avec le participant, des modalités de la divulgation publique éventuelle de l'existence de la vulnérabilité. Cette divulgation publique doit intervenir le plus tôt possible, conjointement avec le déploiement d'une solution et la diffusion d'un avis de sécurité aux utilisateurs.

Civadis s'engage également à recueillir les retours des utilisateurs concernant le déploiement de la solution et à prendre les mesures correctives nécessaires pour résoudre tout problème lié à la solution, y compris la compatibilité avec d'autres produits ou services.

Loi applicable

La loi belge est applicable à tout litige découlant de l'application de la présente politique.

Le CCB (incident@ccb.belgium.be) peut agir en tant qu'intermédiaire afin de tenter de concilier notre organisation et le participant en cas de problèmes liés à l'application de cette politique.

Durée d'application

Les règles de la politique sont applicables à partir du 28/08/2026 jusqu'à leur modification ou suppression par notre organisation. Ces modifications ou suppressions seront publiées sur le site web de notre organisation et s'appliqueront automatiquement après un délai de 30 jours suivant leur publication.

Annexe I : Formulaire de signalement des vulnérabilités

Veuillez fournir suffisamment d'informations pour nous permettre de reproduire le problème et de le résoudre le plus rapidement possible.

Nous vous demandons de fournir au minimum les informations pertinentes suivantes :

Nom :	
Prénom :	
Adresse/Pays :	
Email :	
Numéro de téléphone :	
Description de la vulnérabilité :	
Type de vulnérabilité :	
Détails de configuration :	
Opérations effectuées (logs) :	
Outils utilisés :	
Dates et heures de tests :	
Adresse IP ou URL des systèmes concernés :	
En cas de traitement de données personnelles :	Types de données personnelles traitées / accédées : Catégories des données (employé, client, etc) : Est-ce qu'il y a eu transfert de données dans un pays en dehors de l'europe ou de la zone économique européenne : Si oui -> indiquer le pays concerné ET retourner l'annexe 2 complétée et signée.
Autres informations utiles :	
Pièces jointes (screenshots) :	

Annexe II – Transfert de données personnelles par le participant vers un pays situé en dehors de l'Union européenne ou de l'Espace économique européen.

À compléter si nécessaire : Annexe I de la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données personnelles vers des pays tiers conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil.