LE BEAU VALLON
Soins spécialisés en santé mentale

Le Beau Vallon

Politique de divulgation coordonnée de vulnérabilités

Table des matières

Autorité et révision 2
Contrôle et révision des documents 2
Gestion des versions 2
1. Objectifs et périmètre 3
2. Règles de comportement 3
2.1 Confidentialité 3
2.2 Actes prohibès pour l'auteur du signalement 3
2.3 Mise en œuvre de bonne foi 4
3. Obligation spécifiques liées aux données personnelles (RGPD) 4
4. Signalement d'une faille de sécurité 4
4.1 Contenu requis pour un signalement 4
4.2 Canal de signalement 4
5. Délais procéduraux 4
5.1 Accusé de réception 5
5.2 Suivi du traitement 5
5.3 Délai de correction 5
5.4 Divulgation publique 5

Contrôle et révision des documents

Vérification des documents	
Auteur	**Julien Hautecourt**
Propriétaire	**Pierre-Yves Delrez**
Date de création	**18/05/2026**
Dernière révision par	**Jean-Philippe Rottiers**
Date de la dernière révision	**12/10/2026**

Gestion des versions

Version	Date d'approbation	Approuvé par	Description du changement
0.1	/	/	Brouillon
0.2	19/08/2026	/	Revue par le service informatique
0.3	07/10/2026	/	Révision suite aux remarques du Comité de Direction
1.0	12/10/2026	Comité de direction	Révision par le comité de direction

1. Objectifs et périmètre

Dans l'objectif de garantir la sécurité des systèmes d'information du Beau Vallon celui-ci met en place une politique de divulgation coordonnée des vulnérabilités. Elle s'adresse à toute personne agissant de bonne foi qui découvre une vulnérabilité, nommée « auteur du signalement », dans nos systèmes d'information, qu'elle l'ait cherchée ou non, et lui offre un cadre légal et sécurisé pour nous en informer.

Cette politique concerne tous les systèmes exposés sur internet.

Tout système informatique appartenant à des tiers prestataires, sous-traitants, fournisseurs ou partenaires, est explicitement exclu du périmètre de cette politique, sauf mention contraire expresse. Ces tiers ne sont pas liés par le contenu de la présente politique et pourraient entreprendre des actions judiciaires indépendantes en raison du comportement de l'auteur du signalement à leur égard.

Cette politique ne s'applique à aucun autre système non mentionné précédemment.

2. Règles de comportement

En cas de doute concernant les conditions de la présente politique, l'auteur du signalement est invité à contacter Le Beau Vallon » (voir 4.2) avant d'entreprendre toute action susceptible de sortir du cadre défini.

2.1 CONFIDENTIALITE

Le partage de la vulnérabilité, trouvé par l'auteur du signalement, avec des tiers est strictement interdit sans un accord écrit et préalable du Beau Vallon. De même il est interdit de communiquer ou diffuser à des tiers des données informatiques quel que soit leur format ainsi que des données de communication ou à caractère personnel.

2.2 ACTES PROHIBES POUR L'AUTEUR DU SIGNALEMENT

L'auteur du signalement s'engage à respecter en toutes circonstances le principe de proportionnalité : il ne doit pas exploiter une vulnérabilité au-delà de ce qui est strictement nécessaire pour en démontrer l'existence.

Les actions suivantes sont explicitement proscrites :

- Les attaques par :
  - Déni de service (Distributed Denial of Service, ou DDoS)
  - Force brute
  - Ingénierie sociale (phishing, usurpation d'identité, manipulation de personnel, etc.)
- Le vol, le test ou la compromission de mots de passe
- La modification de paramètres du système
- L'installation de n'importe quel type de malware (virus, ransomware, cheval de Troie, vers, etc.
- Le maintien d'un accès persistant au système au-delà de ce qui est strictement nécessaire à la démonstration de la vulnérabilité
- L'interception, l'enregistrement ou la prise de connaissance intentionnels de communications non accessibles au public
- L'installation de tout matériel permettant l'interception, la prise de connaissance ou l'enregistrement de communications non accessibles au public
- La copie, l'altération, la suppression ou l'exfiltration de données présentes dans le système d'informations, y compris les données à caractère personnel
- La conservation de données collectées lors de la recherche au-delà de ce qui est strictement nécessaire à la démonstration de la vulnérabilité

- Toute action susceptible de perturber la continuité des soins ou le fonctionnement des systèmes critiques du Beau Vallon

2.3 MISE EN ŒUVRE DE BONNE FOI

Le Beau Vallon s'engage à traiter chaque signalement avec sérieux et en toute confidentialité. Dans la mesure où l'auteur du signalement respecte scrupuleusement l'ensemble des conditions définies dans la présente politique, Le Beau Vallon s'engage à ne pas engager de poursuites civiles ou pénales à son encontre.

Cette protection ne s'applique pas dans les cas suivants :

- Tout acte commis avec une intention frauduleuse ou dans le but de nuire
- Toute action visant à exploiter, endommager ou compromettre les systèmes d'information du Beau Vallon au-delà de la démonstration de la vulnérabilité
- Tout manquement aux règles définies dans cette politique
- Toute action portant atteinte aux données à caractère personnel des patients, du personnel ou tiers.

3. Obligation spécifiques liées aux données personnelles (RGPD)

Le traitement de données à caractère personnel recouvre un ensemble large d'opération, il comprend le stockage, la modification, la consultation, la recherche, l'utilisation ou la transmission de toutes information se rapportant à une personne physique identifié ou identifiable. Le caractère « identifiable » de la personne ne dépend pas de la volonté de celui qui traite les données, mais de la simple possibilité d'identifier cette personne directement ou indirectement, à partir de ces données, par exemple : une adresse e-mail, un numéro d'identification, un identifiant en ligne, une adresse IP ou encore des données de localisation).

La présente politique n'a pas vocation à engendrer un traitement intentionnel de donnée personnelle. Toutefois, dans le cadre de ses recherches, l'auteur du signalement peut être amené à accéder fortuitement à de telle données. Dans ce cas, il est tenu de limiter strictement cet accès à ce qui est nécessaire à la démonstration de la vulnérabilité, de ne pas les conserver au de-delà de cette finalité et d'informer immédiatement le Data Protection Officer (DPO) à l'adresse suivante : dpo@beauvallon.be

4. Signalement d'une faille de sécurité

4.1 CONTENU REQUIS POUR UN SIGNALEMENT

Il est nécessaire de communiquer suffisamment d'information concernant la vulnérabilité pour pouvoir la reproduire et résoudre celle-ci dans les meilleurs délais. Par exemple : le type de vulnérabilité, le détail de la configuration, les mesures prises, les outils utilisés, les données de test, les preuves, l'adresse IP ou l'URL du système concerné, des captures d'écran, etc.
De plus, il demandé de transmettre au minimum votre nom (ou pseudonyme) et votre adresse e-mail. L'objectif est que Le Beau Vallon puisse contacter l'auteur du signalement en cas de besoin d'informations complémentaires.

4.2 CANAL DE SIGNALEMENT

Le signalement d'une faille de sécurité doit être transmis à l'adresse e-mail suivante : Vulnerability.Disclosure@beauvallon.be

5. Délais procéduraux

Afin de garantir un traitement efficace et transparent des signalements, Le Beau Vallon s'engage à respecter les délais suivants à compter de la réception d'un signalement valide.

5.1 ACCUSE DE RECEPTION

Le Beau Vallon adresse un accusé de réception à l'auteur du signalement dans un délai de 5 jours ouvrables suivant la réception du signalement. Cet accusé confirme la bonne prise en compte de la déclaration et attribue un identifiant unique au dossier, permettant à l'auteur du signalement de suivre l'avancement du traitement.

5.2 SUIVI DU TRAITEMENT

L'auteur du signalement est tenu informé de l'avancement du traitement de son signalement à chaque étape significative du processus. Le Beau Vallon s'engage à communiquer à l'auteur du signalement , dans un délai de 15 jour ouvrable, une première évaluation de la vulnérabilité signalée, précisant notamment sa criticité estimée et les premières mesures envisagées.

5.3 DELAI DE CORRECTION

Le Beau Vallon s'engage à corriger la vulnérabilité dans un délai cible de 90 jours à compter de la confirmation de son existence. Ce délai peut être adapté en fonction des éléments suivants :

- La complexité technique de la vulnérabilité
- Le nombre de systèmes affectés
- La criticité de la vulnérabilité et son impact potentiel sur la continuité des soins
- La nécessité de coordonner la correction avec des tiers (fournisseurs, prestataires)

Dans le cas où ce délai ne peut être respecté, Le Beau Vallon en informe l'auteur du signalement dans les meilleurs délais en lui communiquant un nouveau calendrier estimatif.

5.4 DIVULGATION PUBLIQUE

Aucune divulgation publique de la vulnérabilité ne peut intervenir avant que celle-ci ait été corrigée, sauf accord mutuel entre Le Beau Vallon et l'auteur du signalement. La date et les modalités de toute divulgation publique sont définies conjointement. La description de la vulnérabilité et sa correction sont publiées simultanément.