**Table des matières (à mettre au début du PDF)**



---

**Modèle (à remplir par l'entreprise)**

**1) Informations légales de l'entreprise**

- **Nom légal :** _____
- **N° d'entreprise (BCE) :** _____
- **Forme juridique :** _____
- **Adresse du siège social :** _____
- **Site web officiel :** _____
- **Langue de correspondance :** FR / NL / EN

**2) Personne de contact et canaux officiels**

- **Nom / Fonction :** _____
- **E-mail :** _____
- **Téléphone :** _____
- **Canal support :** support@votre-domaine.tld

- **Call center :** ouvert de **9h à 12h**, **du lundi au vendredi** (5 j/sem.)
- **Réponse standard sous :** ____ h / ____ jours ouvrés

**3) Pièces justificatives jointes (cocher)**

- ☐ Extrait BCE / Kbis (obligatoire)
- ☐ Copie pièce d'identité du signataire (obligatoire)
- ☐ Justificatif d'adresse (facture, attestation)
- ☐ Statuts de la société (si applicable)
- ☐ Autre : _____

**4) Déclaration sur l'honneur**

Je soussigné(e) _____, **[fonction]**, déclare être habilité(e) à représenter l'entreprise et **certifie l'exactitude** des informations ci-dessus.

- **Lieu/Date :** _____
- **Signature :** _____

---

**5) Programme Bug Bounty proposé**

**5.1 Objectifs et contexte**

- **Objectif principal :** (ex. « Détecter et corriger les vulnérabilités critiques sur nos applis clients »)
- **Contexte :** (ex. « Refonte 2025, nouvelle API publique, montée en charge »)

**5.2 Périmètre**

**In scope (test autorisé) :**

- Domaines : example.com, api.example.com, app.example.com
- Applis : Web (Angular), API REST (Spring Boot), environnements **Production** et **Préprod**
- Comptes de test : fournis ci-après / sandbox

**Out of scope (interdit) :**

- Ingénierie sociale, phishing, DoS/DDoS, spam
- Attaques sur tiers (CDN, passerelles de paiement externes)
- Données de production réelles (exfiltration)

- Tests intrusifs sur systèmes internes non listés

**5.3 Règles de test (Do/Don't) & Safe Harbor**

**Do (autorisé) :** tests non destructifs, fuzzing raisonnable, scans authentifiés avec comptes de test.
**Don't (interdit) :** altération de données réelles, déni de service, ransomware, pivot réseau.
**Safe Harbor :** si vous respectez ce périmètre et signalez de bonne foi, nous ne poursuivrons pas légalement vos actions de test.

**5.4 Politique de divulgation**

- **Disclosure** : responsible disclosure uniquement. **Aucune publication** avant correctif ou accord écrit.
- **Embargo** : ____ jours après correctif (ou accord spécifique).

**5.5 Barème des récompenses (indicatif)**

| Gravité | Exemple | Montant |
|---|---|---|
| **Critique** | RCE, auth bypass total | €____ |
| **Élevée** | SQLi, XXE, IDOR massif | €____ |
| **Moyenne** | XSS stocké, CSRF avec impact | €____ |
| **Faible** | XSS réfléchi mineur, info leak | €____ |

Montants nets, payés sous ____ jours ouvrés après validation.

**5.6 Priorités & délais (SLA)**

- **Triage initial :** sous **5 jours ouvrés**
- **Demande de reproductions / logs :** sous **10 jours ouvrés**
- **Correctif** : Critique ≤ 15j, Élevée ≤ 30j, Moyenne ≤ 60j, Faible ≤ 90j

**5.7 Format attendu des rapports**

- **Titre & Gravité** (CVSS si possible)
- **Étapes de reproduction** (numérotées)
- **Impact & scénario d'abus**
- **POC** (requêtes HTTP, payloads, captures)
- **Portée exacte** (URL, endpoint, compte utilisé)

- **Mitigation / recommandations**
- **Fichier** : **PDF** unique, sans macro, reprenant toutes les sections ci-dessus.

---

**6) Conformité & données**

- **Données personnelles** : minimiser la collecte, masquer tout PII.
- **RGPD** : aucun export de données réelles ; utiliser données de test/anonymisées.

**7) Calendrier & durée**

- **Lancement : //____**
- **Durée** : ouverte / jusqu'au **//____**
- **Fenêtres de test** (si contraintes) : _____

**8) Signatures**

- **Représentant entreprise** (Nom, Fonction, Signature, Date)
- **Contact programme** (Nom, Signature, Date)

---

**Exemple de programme rempli (pour inspiration)**

**Entreprise :** ACME SA
**N° BCE :** 0123.456.789
**Siège :** Rue de l'Exemple 10, 1000 Bruxelles
**Site :** https://acme.be
**Contact :** Marie Dupont, CISO – security@acme.be – +32 2 123 45 67
**Support :** support@acme.be – **Call center 9h-12h, lun-ven**

**Objectifs**

- Renforcer la sécurité de notre **API publique** et de l'**app web clients** (Angular 19 / Spring Boot 3).
- Prévenir les fuites de données et les escalades de privilèges.

**Périmètre**

**In scope :**

- acme.be, app.acme.be, api.acme.be
- API REST v2 (auth JWT), app web (Angular)
- Comptes de test fournis :

- client_test / ********
- manager_test / ********

**Out of scope :**

- status.acme.be (hébergeur tiers)
- DDoS/DoS, brute force massifs, phishing, social engineering
- Réseaux internes et environnements non listés

**Règles & Safe Harbor**

- Tests **non destructifs**, pas de modification de données réelles.
- Vous êtes **couvert** légalement si vous restez dans le périmètre et signalez de bonne foi.
- Si vous trouvez des données sensibles par erreur : **arrêtez**, **ne téléchargez pas**, signalez immédiatement.

**Divulgation**

- Pas de publication avant correctif ou accord écrit d'ACME.
- Embargo standard : **90 jours** après correctif.

**Barème des récompenses**

- **Critique** (RCE / auth bypass total / exfiltration massive) : **€1 500 – €3 000**
- **Élevée** (SQLi, XXE, IDOR large, SSRF impactant) : **€700 – €1 500**
- **Moyenne** (XSS stocké, CSRF avec impact, Broken Access Control limité) : **€300 – €700**
- **Faible** (XSS réfléchi, infos sensibles mineures) : **€100 – €300**
  Paiement sous **15 jours ouvrés** après validation.

**SLA**

- **Accusé réception** : 72h
- **Triage** : 5 j ouvrés
- **Correctifs** : Critique ≤ 15j, Élevée ≤ 30j, Moyenne ≤ 60j, Faible ≤ 90j

**Format du rapport attendu**

- PDF unique, incluant : titre, sévérité (CVSS si possible), étapes numérotées, POC, impact, périmètre précis, recommandations, annexes (captures/logs).
- Pas de macro, pas de contenu actif.

**Calendrier**

- Démarrage : 01/12/2025 — programme **ouvert**.

**Signatures**

- **ACME SA** – Marie Dupont, CISO – Date/Signature
- **Contact Programme** – (facultatif) – Date/Signature