

**Projet de règlement****Fiabilité et sécurité de l'information des systèmes de jeux d'argent et de hasard en vertu de la loi sur les jeux d'argent et de hasard****Sommaire**

Fiabilité et sécurité de l'information des systèmes de jeux d'argent et de hasard en vertu de la loi sur les jeux d'argent et de hasard.....	1
1 Cadre juridique, champ d'application et définitions.....	2
1.1 Pouvoir de prescription de l'autorité de contrôle.....	2
1.2 Législation.....	2
1.3 Champ d'action.....	2
1.4 Définitions.....	2
2 Accréditation d'un organisme d'inspection.....	3
3 Pratiques générales en matière de sécurité de l'information.....	3
4 Organisme d'inspection chargé de réaliser des tests de sécurité de l'information.....	3
4.1 Domaine de compétence.....	4
5 Renouvellement des tests de sécurité de l'information.....	5
6 Test de sécurité de l'information rejeté.....	5
7 Balayage de vulnérabilité.....	6
8 Analyses de vulnérabilité réalisées dans le cadre des tests de sécurité de l'information.....	6
9 Remédier aux vulnérabilités.....	7
10 Utilisation des certificats délivrés.....	7
11 Écarts.....	7
12 Entrée en vigueur.....	7

## 1 Cadre juridique, champ d'application et définitions

### 1.1 Pouvoir de prescription de l'autorité de contrôle

Le droit de l'autorité de contrôle d'édicter des règles contraignantes est fondé sur l'article 44, paragraphe 6, de la loi sur les jeux de hasard (xx/2025). Conformément à ce paragraphe, l'autorité de contrôle peut édicter des règlements plus détaillés sur la fiabilité des systèmes de jeu, des équipements de loterie et des méthodes de loterie utilisés dans l'exploitation des jeux de hasard, sur les exigences techniques visant à garantir le caractère aléatoire du tirage, sur la forme et le contenu plus détaillés de l'enquête et de l'approbation de l'organisme de contrôle, ainsi que sur les conditions que l'organisme de contrôle doit remplir pour être approuvé par l'autorité.

Conformément à l'article 57 de la loi sur les jeux d'argent et de hasard, l'autorité de contrôle est l'Agence de supervision finlandaise. Conformément à l'article 106 de la loi, la police nationale agit en tant qu'autorité compétente visée à l'article 57 jusqu'au 31 décembre 2026.

### 1.2 Législation

Les dispositions suivantes sont pertinentes pour l'objet du présent règlement:

- Loi sur les jeux d'argent et de hasard (xxx/2025)
- Loi sur la procédure administrative (434/2003)
- Loi sur la protection des données (1050/2018)
- Règlement général de l'UE sur la protection des données (2016/679)

### 1.3 Champ d'action

Cette disposition s'applique à une personne morale ou physique visée au chapitre 1, article 2, paragraphe 1, de la loi sur les jeux de hasard à laquelle une licence exclusive ou une licence pour des activités de jeux de hasard a été accordée en vertu de la loi sur les jeux de hasard.

La licence exclusive est régie par l'article 5 de la loi sur les jeux de hasard et la licence de jeux de hasard est régie par l'article 6.

### 1.4 Définitions

Aux fins de la présente disposition, les définitions suivantes s'appliquent. Aux fins du présent règlement, on entend par:

- *licence exclusive*: une licence accordée pour les formes d'exploitation des jeux de hasard visées à l'article 5 de la loi sur les jeux de hasard;

- *licence de jeux de hasard*: licence accordée pour les formes d'exploitation des jeux de hasard visées à l'article 6 de la loi sur les jeux de hasard;
- *transaction de jeu*: la mise mise par le joueur sur le jeu, l'option de résultat choisie par le joueur, les choix faits par le joueur qui sont pertinents pour le résultat du jeu et les résultats des marchés et tirages, ainsi que les gains et pertes enregistrés dans le système de jeu du titulaire d'une licence exclusive ou d'une licence de jeu;
- *transaction sur le compte joueur*: les écritures comptables;
- *système de jeux d'argent et de hasard*: un système d'information en ligne utilisé par ou pour le compte de l'opérateur de jeux d'argent et de hasard pour l'exploitation de jeux d'argent et de hasard.

## 2 Accréditation d'un organisme d'inspection

Le titulaire de la licence est responsable de la fiabilité de ses dispositifs de loterie et de ses systèmes de jeux d'argent et de hasard, ainsi que de la réalisation des audits effectués pour garantir cette fiabilité. L'évaluation de la fiabilité et de la sécurité est effectuée par un organisme d'inspection externe agréé. L'organisme d'inspection doit être accrédité au sens du règlement (CE) n° 765/2008 du Parlement européen et du Conseil fixant les exigences relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93.

L'accréditation peut être accordée aux organismes de contrôle par l'organisme national d'accréditation FINAS (service finlandais d'accréditation). Un organisme d'accréditation étranger peut également agir en tant qu'organisme d'accréditation s'il est membre de l'accord multilatéral de reconnaissance de l'Organisation européenne d'accréditation (EA MLA) dans le domaine de compétence pertinent. Le titulaire de la licence est tenu de s'assurer que l'opérateur externe chargé de l'audit dispose d'une accréditation valide.

## 3 Pratiques générales en matière de sécurité de l'information

Le titulaire de la licence est responsable de la sécurité de l'information, de la protection des données et d'autres caractéristiques techniques de fiabilité de ses propres systèmes de jeux d'argent et de hasard. Le titulaire de la licence doit respecter les bonnes pratiques en matière de sécurité de l'information dans le cadre de ses activités et s'efforcer de minimiser les menaces pour la sécurité de l'information, les violations de données et autres problèmes susceptibles de compromettre la fiabilité des systèmes de jeux d'argent et de hasard. Le titulaire de la licence est également tenu de surveiller les facteurs susmentionnés en dehors des inspections régulières visées dans le présent règlement, afin de garantir la fiabilité de ses systèmes.

## 4 Organisme d'inspection chargé de réaliser des tests de sécurité de l'information

Le titulaire de la licence est tenu d'effectuer tous les deux ans des tests de sécurité sur ses systèmes de jeux d'argent et de hasard. Les résultats des tests de sécurité de

l'information sont soumis à l'autorité de contrôle. Les tests de sécurité de l'information et leurs résultats ne peuvent pas dater de plus de deux ans.

Les essais de sécurité de l'information sont réalisés par un organisme d'inspection externe accrédité conformément aux normes ISO/IEC 17025, ISO/IEC 17065 ou ISO/IEC 17020, comme spécifié à la section 2 du présent règlement. Les tests de sécurité de l'information doivent accorder une attention particulière à la protection et à l'intégrité des composants du système de jeux de hasard aléatoires, à la protection des composants contenant des données à caractère personnel et à la protection des composants liés aux paiements.

L'organisme d'inspection chargé d'effectuer les tests de sécurité de l'information et son personnel doivent être compétents et aptes à effectuer ces tests. La compétence nécessaire pour effectuer des tests de sécurité de l'information peut être démontrée, entre autres, par une expérience professionnelle antérieure dans le domaine des tests de sécurité de l'information, par une formation ou par des certificats reconnus dans le secteur. Le titulaire de la licence est tenu de s'assurer que les personnes chargées des essais sont qualifiées pour effectuer des essais de sécurité de l'information et, sur demande, de démontrer leurs qualifications.

Une personne désignée sera nommée pour la mise en œuvre des tests de sécurité, qui sera responsable de leur bonne exécution. Le rapport final du test de sécurité de l'information est signé et validé par la personne désignée et soumis à l'autorité de contrôle.

Dans le cadre des tests de sécurité de l'information, au moins les composants suivants, ainsi que les vulnérabilités ou incidents connexes, doivent être testés:

- Possibilité de manipulation des composants aléatoires
- Accès à la base de données des clients
- Capacité à influencer le résultat des jeux
- Capacité à influencer les systèmes de paiement ou les opérations de paiement
- Accès non autorisé aux serveurs utilisés pour stocker les transactions relatives aux jeux d'argent et de hasard et les transactions relatives aux comptes de joueur
- Possibilité de modifier les données archivées relatives aux événements de jeux d'argent et de hasard ou aux événements de comptes de jeux d'argent et de hasard
- Modification ou destruction des registres relatifs aux systèmes de jeux d'argent

#### 4.1 Domaine de compétence

L'organisme de contrôle accrédité effectuant l'audit dispose du domaine de compétence en matière de jeux de hasard et d'argent dans son accréditation ISO/IEC. Le domaine de compétence doit couvrir les exigences fixées par la législation finlandaise sur les jeux de hasard et les règlements techniques de l'autorité de surveillance.

Jusqu'au 1er janvier 2027, l'autorité de contrôle peut accepter une accréditation qui inclut un champ de compétence évalué et accordé sur la base de réglementations techniques émises pour les systèmes de jeux d'argent et de hasard danois ou suédois.

### 5 Renouvellement des tests de sécurité de l'information

Le titulaire de la licence doit soumettre les résultats des tests de sécurité de l'information approuvés à l'autorité de surveillance. Le titulaire de la licence ne peut commencer l'exploitation de jeux d'argent et de hasard avant d'avoir passé avec succès les tests de sécurité. Le résultat du test de sécurité de l'information ne doit pas dater de plus de deux ans.

L'autorité de contrôle peut, à sa discrétion, accorder un délai supplémentaire pour la mise en œuvre des tests de sécurité, au cours duquel l'exploitation des jeux d'argent et de hasard peut se poursuivre.

### 6 Test de sécurité de l'information rejeté

L'organisme d'inspection qui effectue le test de sécurité de l'information devrait évaluer les vulnérabilités recensées lors du test de sécurité de l'information et leur importance pour la fiabilité du système de jeux d'argent et de hasard. Les vulnérabilités identifiées au cours de l'évaluation doivent être évaluées à l'aide du calculateur CVSS v3 (calculateur du système commun de notation de la vulnérabilité version 3) fourni par l'Institut national de technologie (NIST). Pour le calculateur CVSS v3, la gravité de la vulnérabilité doit être évaluée à l'aide de mesures du score de base. Si des vulnérabilités ayant une valeur CVSS calculée supérieure à 5,0 sont détectées au cours des essais de sécurité, l'essai ne peut pas être considéré comme réussi.

Si le test de sécurité de l'information du titulaire de l'autorisation n'est pas approuvé, le titulaire de l'autorisation doit immédiatement prendre des mesures pour remédier aux vulnérabilités recensées en matière de sécurité de l'information. Le titulaire de la licence doit signaler le test de sécurité de l'information rejeté à l'autorité de surveillance.

Le titulaire de la licence doit effectuer un nouveau test de sécurité dans les 90 jours suivant le rejet du test de sécurité de l'information. Il n'est pas nécessaire de procéder à de nouveaux tests de sécurité de l'information sur l'ensemble du système de jeux d'argent et de hasard; au contraire, les tests de sécurité de l'information peuvent cibler les lacunes qui ont causé le rejet. Dans le cadre du renouvellement des essais de

sécurité de l'information, l'organisme de contrôle doit s'assurer que les vulnérabilités précédemment identifiées comme motifs de rejet ont été corrigées.

La mise en œuvre des jeux de hasard ne peut pas commencer avant que des tests de sécurité approuvés et valides aient été effectués.

## 7 Balayage de vulnérabilité

Outre les tests de sécurité, les titulaires de licence sont tenus de surveiller la sécurité de leurs propres systèmes au moyen d'analyses régulières des vulnérabilités. L'objectif des analyses de vulnérabilité est de s'assurer que les systèmes de jeu utilisés par le titulaire de licence ne présentent pas de vulnérabilités externes en matière de sécurité qui pourraient être exploitées pour mener des attaques contre les systèmes de jeu.

Le titulaire de la licence est tenu d'effectuer une analyse de vulnérabilité externe une fois par an et d'en communiquer les résultats à l'autorité de contrôle. L'analyse des vulnérabilités peut être effectuée par un organisme de contrôle externe accrédité conformément aux normes ISO/IEC 17025, ISO/IEC 17065 ou ISO/IEC 17020, comme spécifié au paragraphe 2 du présent règlement.

Le titulaire de la licence est tenu de remédier aux vulnérabilités détectées lors de l'analyse des vulnérabilités au moyen de mises à jour ou d'autres mesures d'atténuation urgentes si des mises à jour correctives ne sont pas disponibles. La méthode d'évaluation décrite à l'article 6 est appliquée aux vulnérabilités de sécurité détectées lors des analyses de vulnérabilité. Si la valeur CVSS calculée de la vulnérabilité externe identifiée est supérieure à 5.0, le titulaire de la licence prend des mesures immédiates pour remédier aux vulnérabilités.

L'organisme d'inspection chargé d'effectuer l'analyse de vulnérabilité et son personnel doivent être compétents et aptes à réaliser les tests. La compétence nécessaire pour effectuer des analyses de vulnérabilité peut être démontrée par une expérience professionnelle antérieure en matière de tests de sécurité de l'information, une expérience dans l'utilisation de scanners de vulnérabilité, une formation ou des certificats industriels généralement reconnus, entre autres. Le titulaire de la licence est tenu de s'assurer que les personnes effectuant les tests sont qualifiées pour réaliser des analyses de vulnérabilité et, sur demande, de démontrer leurs qualifications.

Une personne responsable de la réalisation de l'analyse de vulnérabilité doit être désignée afin de garantir que celle-ci soit effectuée de manière appropriée. Le rapport final d'analyse de la vulnérabilité est signé et validé par la personne responsable et soumis à l'autorité de contrôle.

## 8 Analyses de vulnérabilité réalisées dans le cadre des tests de sécurité de l'information

Le titulaire de la licence peut effectuer des analyses de vulnérabilité dans le cadre de tests de sécurité informatique. Les mêmes exigences s'appliquent aux analyses de vulnérabilité effectuées dans le cadre des tests de sécurité de l'information qu'aux autres analyses de vulnérabilité.

## 9 Remédier aux vulnérabilités

Le titulaire de la licence est tenu de surveiller régulièrement la sécurité de l'information de ses propres systèmes de jeux d'argent et de hasard, même en dehors des tests de sécurité de l'information, et de remédier aux vulnérabilités qui compromettent la fiabilité lorsque des solutions ou d'autres méthodes d'atténuation deviennent disponibles.

S'il n'est pas possible de remédier rapidement aux vulnérabilités, le titulaire de la licence doit chercher à utiliser les moyens disponibles pour lutter contre ces vulnérabilités et en minimiser l'impact.

Si la valeur de base CVSS v3 de la vulnérabilité externe détectée est inférieure à 5,0, le titulaire de la licence peut, à sa discrétion, mettre en œuvre des corrections et évaluer l'urgence de leur mise en œuvre.

## 10 Utilisation des certificats délivrés

Un organisme d'inspection agréé et approuvé par l'autorité de contrôle chargée d'effectuer des tests de sécurité de l'information ou des analyses de vulnérabilité peut utiliser les certificats ou autres attestations délivrés au titulaire de la licence de logiciel de jeux d'argent dans le cadre de son inspection. Si l'organisme d'inspection utilise des certificats existants dans le cadre de l'inspection, il doit évaluer si ces certificats peuvent être considérés comme des preuves suffisamment fiables de la fiabilité et de la sécurité des informations du système de jeux d'argent du titulaire de la licence de logiciel de jeux d'argent.

## 11 Écarts

Le titulaire de la licence est tenu de signaler sans délai à l'autorité de contrôle toute violation de la sécurité de l'information ou de la protection des données qu'il détecte s'il existe des raisons de soupçonner que la fiabilité des systèmes de jeux ou des équipements de loterie utilisés par le titulaire de la licence a été compromise.

Les titulaires de licence ne sont pas tenus de signaler les incidents mineurs de sécurité ou de protection des données à l'autorité de surveillance des jeux de hasard lorsque l'efficacité estimée de l'incident est limitée par nature ou lorsque l'incident n'est pas évalué comme ayant une incidence significative sur la fiabilité des systèmes de jeux de hasard.

## 12 Entrée en vigueur

Le présent règlement entre en vigueur le X [mois] 2026.

### **Office national de police**

#### **Administration des jeux de hasard**

Konepajankatu 2, PL 50, 11101 Riihimäki

Téléphone +358 295 480 181, poliisi.fi