

Δήλωση Ασφάλειας Πληροφοριών

Στη SkillOnNet, η ασφάλεια των πληροφοριών είναι ένα θεμελιώδες συστατικό του πλαισίου διακυβέρνησής μας και κρίσιμη για τη διατήρηση της εμπιστοσύνης των παικτών, των συνεργατών και των ενδιαφερομένων. Ως εταιρεία τυχερών παιχνιδιών που διαχειρίζεται ευαίσθητα δεδομένα παικτών και οικονομικές συναλλαγές, η οργάνωση δεσμεύεται να προστατεύει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα όλων των πληροφοριών.

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) έχει θεσπιστεί, εφαρμοστεί και συντηρείται για να υποστηρίξει τους επιχειρηματικούς στόχους μέσω προσέγγισης που βασίζεται στον κίνδυνο. Η διαχείριση του κινδύνου είναι ενσωματωμένη στην οργανωτική κουλτούρα, συμπεριλαμβανομένου του εντοπισμού, της αξιολόγησης και της μείωσης των κινδύνων, με τη στήριξη ενός ενημερωμένου και τακτικά αναθεωρούμενου μητρώου κινδύνων. Οι έλεγχοι ευθυγραμμίζονται με το ISO/IEC 27001 για να διασφαλίσουν ένα συνεπές και αποτελεσματικό πλαίσιο ασφάλειας.

Οι βασικές δεσμεύσεις ασφάλειας πληροφοριών περιλαμβάνουν:

- Προστασία προσωπικών και ευαίσθητων δεδομένων μέσω ισχυρών ελέγχων πρόσβασης, ασφαλούς αρχιτεκτονικής συστήματος, κρυπτογράφησης και συνεχούς παρακολούθησης.
- Ενσωμάτωση της ασφάλειας σε όλες τις λειτουργίες, συμπεριλαμβανομένων των πρακτικών ασφαλούς κύκλου ανάπτυξης, της ενίσχυσης των συστημάτων και των ικανοτήτων εντοπισμού και πρόληψης απειλών.
- Ασφαλής επεξεργασία καταθέσεων, αναλήψεων και οικονομικών συναλλαγών μέσω κρυπτογράφησης, μηχανισμών εντοπισμού απάτης και συμμόρφωσης με τα πρότυπα οικονομικής ασφάλειας.
- Συντήρηση της ακεραιότητας του λογισμικού τυχερών παιχνιδιών, των βάσεων δεδομένων και της υποδομής backend μέσω τακτικών εκτιμήσεων ασφάλειας και αποτελεσματικής διαχείρισης διορθώσεων.
- Συμμόρφωση με τις ισχύουσες νομικές, κανονιστικές και συμβατικές απαιτήσεις, συμπεριλαμβανομένων των υποχρεώσεων προστασίας δεδομένων, των κανονισμών για την καταπολέμηση της χρηματοδότησης της τρομοκρατίας (AML) και των απαιτήσεων αδειοδότησης αρχών τυχερών παιχνιδιών.
- Διασφάλιση της επιχειρησιακής ανθεκτικότητας μέσω Σχεδίων Επιχειρησιακής Συνέχειας (BCP) και στρατηγικών Ανάκτησης από Καταστροφές (DR) για τη διατήρηση της διαθεσιμότητας υπηρεσιών και την προστασία των δεδομένων των παικτών.
- Σαφής καθορισμός ρόλων και ευθυνών για την ασφάλεια των πληροφοριών, με τη στήριξη της δέσμευσης της ηγεσίας, επαρκών πόρων και συμμόρφωσης από τους υπαλλήλους και τρίτους.
- Προώθηση μιας ισχυρής κουλτούρας ευαισθητοποίησης για την ασφάλεια, λογοδοσίας και συνεχούς επαγρύπνησης σε όλη την οργάνωση.
- Εφαρμογή αποτελεσματικών διαδικασιών διαχείρισης περιστατικών για τον εντοπισμό, την αντίδραση και την αποκατάσταση από συμβάντα ασφάλειας πληροφοριών.
- Συνεχής παρακολούθηση, αναθεώρηση και διαρκής βελτίωση του ISMS για να αντιμετωπίζει τις εξελισσόμενες απειλές, τις τεχνολογικές αλλαγές και τις επιχειρηματικές ανάγκες.

Η διοίκηση της SkillOnNet υποστηρίζει πλήρως αυτή την πολιτική και δεσμεύεται για την εφαρμογή και τη συνεχιζόμενη αποτελεσματικότητά της.