

Declaração de Segurança da Informação

Na SkillOnNet, a segurança da informação é um componente fundamental da nossa estrutura de governação e é crítica para manter a confiança dos nossos jogadores, parceiros e partes interessadas. Como empresa de jogos que lida com dados sensíveis dos jogadores e transações financeiras, a organização está empenhada em proteger a confidencialidade, integridade e disponibilidade de todos os ativos de informação.

Um Sistema de Gestão de Segurança da Informação (SGSI) é estabelecido, implementado e mantido para apoiar os objetivos empresariais através de uma abordagem baseada em riscos. A gestão de riscos está integrada na cultura organizacional, incluindo a identificação, avaliação e mitigação de riscos, suportada por um registo de riscos mantido e revisto regularmente. Os controlos estão alinhados com a norma ISO/IEC 27001 para garantir um quadro de segurança consistente e eficaz.

Os principais compromissos de segurança da informação incluem:

- Proteção de dados pessoais e sensíveis através de controlos de acesso robustos, arquitetura de sistema segura, encriptação e monitorização contínua.
- Integração da segurança nas operações, incluindo práticas seguras de ciclo de vida de desenvolvimento, endurecimento de sistemas e capacidades proativas de deteção e prevenção de ameaças.
- Processamento seguro de depósitos, levantamentos e transações financeiras utilizando encriptação, mecanismos de deteção de fraudes e conformidade com normas de segurança financeira.
- Manutenção da integridade do software de jogos, bases de dados e infraestrutura de backend através de avaliações de segurança regulares e gestão eficaz de patches.
- Conformidade com os requisitos legais, regulamentares e contratuais aplicáveis, incluindo obrigações de proteção de dados, regulamentos de Prevenção da Lavagem de Dinheiro (PLD) e requisitos de licenciamento das autoridades de jogos.
- Garantia de resiliência operacional através de Planos de Continuidade de Negócios (PCN) e estratégias de Recuperação de Desastres (RD) para manter a disponibilidade do serviço e proteger os dados dos jogadores.
- Definição clara de papéis e responsabilidades para a segurança da informação, apoiada pelo compromisso da liderança, recursos adequados e conformidade por parte dos colaboradores e terceiros.
- Promoção de uma forte cultura de consciência de segurança, responsabilidade e vigilância contínua em toda a organização.
- Implementação de processos eficazes de gestão de incidentes para detetar, responder e recuperar de eventos de segurança da informação.
- Monitorização, revisão e melhoria contínua do SGSI para responder a ameaças em evolução, mudanças tecnológicas e necessidades empresariais.

A gestão da SkillOnNet apoia plenamente esta política e está comprometida com a sua implementação e eficácia contínua.