

Declaração de Segurança da Informação

Na SkillOnNet, a segurança da informação é um componente fundamental do nosso quadro de governança e essencial para manter a confiança de nossos jogadores, parceiros e partes interessadas. Como uma empresa de jogos que lida com dados sensíveis de jogadores e transações financeiras, a organização está comprometida 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 de negócios por meio de uma abordagem baseada em riscos. A gestão de riscos está incorporada à cultura organizacional, incluindo a identificação, avaliação e mitigação de riscos, apoiada por um registro de riscos mantido e revisado regularmente. Os controles estão alinhados com a 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 por meio de controles de acesso robustos, arquitetura de sistemas segura, criptografia e monitoramento contínuo.
- Integração da segurança em todas as operações, incluindo práticas seguras de ciclo de vida de desenvolvimento, fortalecimento de sistemas e capacidades proativas de detecção e prevenção de ameaças.
- Processamento seguro de depósitos, saques e transações financeiras utilizando criptografia, mecanismos de detecção de fraude e conformidade com padrões de segurança financeira.
- Manutenção da integridade do software de jogos, bancos de dados e infraestrutura de backend por meio de avaliações regulares de segurança e gestão eficaz de atualizações.
- Conformidade com requisitos legais, regulatórios e contratuais aplicáveis, incluindo obrigações de proteção de dados, regulamentações de Prevenção à Lavagem de Dinheiro (PLD) e exigências de licenciamento das autoridades de jogos.
- Garantia de resiliência operacional por meio de Planos de Continuidade de Negócios (PCN) e estratégias de Recuperação de Desastres (DR) para manter a disponibilidade dos serviços 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 adesão por parte dos colaboradores e terceiros.
- Promoção de uma forte cultura de conscientização em segurança, responsabilidade e vigilância contínua em toda a organização.
- Implementação de processos eficazes de gestão de incidentes para detectar, responder e se recuperar de eventos de segurança da informação.
- Monitoramento, revisão e aprimoramento contínuo do SGSI para enfrentar ameaças em evolução, mudanças tecnológicas e necessidades do negócio.

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