

Termos de uso da plataforma Vyntra

SHA-256: aad629b9d19adaae62046cd93afe3be188dda974f1b81b6bfc079a53dee4748f

APRESENTAÇÃO

A Vyntra é uma iniciativa de pesquisadores independentes de segurança. Por meio do portal, desenvolvedores e times podem cadastrar um produto, delimitar o que pode ser testado, receber uma proposta e acompanhar uma análise de segurança. A Vyntra é o nome da iniciativa e do portal; a pessoa física ou jurídica responsável por cada pentest é identificada no termo específico apresentado antes do pagamento.

1. DEFINIÇÕES

Para estes termos, “Portal” é a plataforma Vyntra; “Usuário” é a pessoa que mantém uma conta; “Cliente” é a pessoa ou organização que solicita o pentest; “Responsável” é quem assume a execução e é identificado no termo específico; “Produto” ou “Ativo” é o sistema, aplicação, infraestrutura, código ou outro recurso indicado pelo Cliente; “Escopo” reúne os ativos autorizados, limites e regras do teste; “Proposta” registra preço, forma de pagamento, previsão e demais condições; e “Relatórios” são as entregas técnicas disponibilizadas durante ou ao final do trabalho.

2. FINALIDADE DO PORTAL

O Portal organiza o cadastro, a revisão, a autorização, o pagamento, o acompanhamento e as entregas de análises de segurança. Criar uma conta ou salvar um rascunho não gera cobrança, reserva de agenda nem autorização para iniciar testes.

3. CADASTRO E ACEITE

O Usuário deve ter capacidade para aceitar estes termos e, quando agir por outra pessoa ou organização, autorização para representá-la. As informações fornecidas devem ser verdadeiras, completas e atualizadas. O aceite eletrônico fica vinculado à conta autenticada, à versão e ao hash do documento, à data e à hora do registro.

4. CONTA E CREDENCIAIS

A conta é pessoal. O Usuário deve proteger sua senha e os demais meios de autenticação, não compartilhar o acesso com pessoas não autorizadas e comunicar prontamente qualquer suspeita de uso indevido. Ações realizadas por uma conta autenticada podem ser consideradas válidas até que um comprometimento seja comunicado e verificado.

5. USO PERMITIDO

O Portal deve ser usado apenas para cadastrar e acompanhar produtos que possam ser legitimamente submetidos a uma análise de segurança. É proibido acessar dados de terceiros, contornar controles de acesso, interferir no funcionamento do Portal, enviar conteúdo ilícito ou usar a plataforma para preparar ou apoiar ataques não autorizados.

6. PRODUTOS, ESCOPO E AUTORIZAÇÃO

O Cliente somente pode cadastrar ativos próprios ou para os quais possua autorização suficiente do titular. O envio do pentest não autoriza testes imediatos. A autorização específica é registrada em documento próprio, depois da revisão do escopo e antes do pagamento, e a execução somente começa após a confirmação do pagamento exigido e o início efetivo indicado no Portal.

7. PROPOSTA E PAGAMENTOS

O preço, as etapas de pagamento, a previsão de início e o prazo estimado são informados na proposta de cada pentest. O pagamento remunera uma análise técnica concreta e sua documentação, dentro do escopo aprovado; não corresponde à compra de uma quantidade garantida de vulnerabilidades. Cartão e Pix podem ser processados por provedores externos identificados na tela de pagamento.

8. CANCELAMENTO E REEMBOLSO

Antes da entrega do relatório final, o Cliente pode solicitar o cancelamento do pentest e pedir reembolso pelos canais informados no Portal. O pedido será tratado diretamente e de boa-fé, considerando o estágio da análise, o trabalho já realizado, eventuais entregas técnicas disponibilizadas e os custos do meio de pagamento. Quando o cancelamento for confirmado, os testes são interrompidos e a autorização correspondente é encerrada.

Se o Responsável não puder realizar ou concluir a parte contratada e não houver reagendamento ou alternativa aceita pelo Cliente, será devolvido o valor correspondente ao que não tiver sido executado. Direitos obrigatórios previstos na legislação aplicável, inclusive condições de reembolso mais favoráveis, permanecem preservados.

9. RESPONSABILIDADES DO CLIENTE

O Cliente deve fornecer contexto e acessos necessários, definir claramente os limites do teste, informar restrições e ações proibidas, manter meios adequados de recuperação do ambiente e responder às solicitações que impeçam a continuidade. Também é responsável por avaliar e aplicar as correções que considerar adequadas.

10. RESPONSABILIDADES DO RESPONSÁVEL E DOS PESQUISADORES

A análise será conduzida com cuidado técnico, dentro da autorização registrada e das restrições do escopo. Os pesquisadores podem utilizar ferramentas manuais e automatizadas quando apropriado, limitarão o acesso ao necessário para validar os achados e comunicarão impedimentos ou vulnerabilidades relevantes durante o trabalho.

11. RELATÓRIOS E PROPRIEDADE INTELECTUAL

Os relatórios entregues podem ser usados pelo Cliente para compreender e corrigir os riscos do próprio produto. Métodos, ferramentas, modelos, código e materiais preexistentes continuam pertencendo aos seus respectivos titulares. O relatório não representa certificação, garantia permanente de segurança ou autorização para atribuir aos pesquisadores qualquer aprovação além do conteúdo documentado.

12. CONFIDENCIALIDADE

Informações do produto, credenciais, evidências e achados serão usados apenas para executar, proteger e administrar o pentest, ressalvadas obrigações legais. O Cliente deve evitar o envio de dados pessoais ou segredos que não sejam necessários. Comunicações e documentos do trabalho não serão divulgados publicamente sem autorização, salvo quando a divulgação for exigida por lei.

13. LIMITES TÉCNICOS

Uma análise de segurança representa os ativos, acessos, período e condições avaliados. Ela pode reduzir riscos e revelar vulnerabilidades, mas não garante que toda falha possível será encontrada nem substitui desenvolvimento seguro, monitoramento, resposta a incidentes ou novas avaliações após mudanças no produto.

14. DADOS PESSOAIS E EXCLUSÃO DA CONTA

São tratados os dados necessários para autenticação, contato, execução, cobrança, segurança e administração do Portal. O titular pode solicitar correção ou exclusão pelo próprio Portal ou por contact@vyntra.sh. Dados sem necessidade de conservação serão eliminados ou anonimizados; registros contratuais, financeiros, de segurança ou necessários ao exercício de direitos podem ser preservados pelo prazo aplicável.

15. DISPONIBILIDADE E SEGURANÇA DO PORTAL

São adotadas medidas razoáveis para proteger o Portal e manter sua disponibilidade, mas podem ocorrer interrupções para manutenção, correção de falhas ou eventos fora de controle razoável. Incidentes ou dificuldades de acesso devem ser comunicados a contact@vyntra.sh.

16. COMUNICAÇÕES

O Portal, o e-mail da conta e os canais de contato informados pelo Cliente podem ser usados para mensagens relacionadas ao pentest. O Cliente deve manter esses dados atualizados. Para dúvidas, cancelamento ou dificuldades, o canal geral é contact@vyntra.sh; um canal por telefone ou WhatsApp poderá ser informado no Portal quando estiver disponível.

17. ALTERAÇÕES E ENCERRAMENTO

Alterações materiais destes termos geram uma nova versão e podem exigir novo aceite antes do uso de funções protegidas. O acesso pode ser suspenso em caso de uso ilícito, risco de segurança, fraude ou violação relevante, sem impedir o acesso a direitos e documentos que devam permanecer disponíveis.

18. DISPOSIÇÕES FINAIS

Estes termos, o termo específico de autorização, a proposta, o escopo versionado e as regras de engajamento formam o registro da relação aplicável a cada pentest. Se alguma disposição não puder ser aplicada, as demais permanecem válidas. A tolerância com uma situação pontual não altera estes termos. A legislação brasileira é aplicável, preservado o foro assegurado por normas obrigatórias.

Ao marcar a opção de aceite e prosseguir, o Usuário declara que leu, compreendeu e concorda com estes termos.