ANEXO II – Requisitos de segurança do fornecedor Experian (Resumo)

Os requisitos de segurança incluídos neste documento têm como objetivo fornecer ao fornecedor em potencial um resumo das principais áreas de controle, que devem formar a base do “Programa de Segurança da Informação” do fornecedor. Este programa deve estar em vigor para proteger a Experian Information que o fornecedor recebe, processa, transfere, transmite, armazena, entrega e / ou acessa de outra forma.

DEFINIÇÕES

"Experian Information" significa arquivos de dados Experian, bancos de dados, software de aplicativos (código-fonte e código objeto), documentação de software, documentos de processo de apoio, documentação de procedimentos operacionais e procedimentos, planos de teste, casos de teste, cenários de teste, relatórios de incidentes cibernéticos, informações do consumidor informações comerciais e outros dados especificamente classificados pela Experian como confidenciais ou restritos.

“Recurso” significa todos os dispositivos do Fornecedor, incluindo, entre outros, laptops, PCs, roteadores, servidores e outros sistemas de computador que armazenam, processam, transferem, transmitem, entregam ou acessam as Informações da Experian.

PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

O Fornecedor manterá um Programa de Segurança da Informação abrangente que contém salvaguardas administrativas, técnicas e físicas apropriadas à complexidade, natureza e escopo de suas atividades, e à sensibilidade de seus ativos de informação. Tais salvaguardas incluirão os elementos estabelecidos abaixo e serão razoavelmente planejadas para:
(1) alcançar a segurança e confidencialidade da Informação Experian;
(2) proteger contra quaisquer ameaças ou riscos previstos para a segurança ou integridade da Informação Experian;
(3) proteger contra o acesso não autorizado ou o uso de informações da Experian que possam resultar em danos substanciais ou inconvenientes para a Experian, seus clientes e / ou consumidores, e
(4) fornecer garantias à Experian da eficácia contínua dos controles.

Se o Fornecedor receber, armazenar, processar ou transmitir dados do portador do cartão (CHD; especificamente, o número da conta principal) ou dados de autenticação confidenciais (SAD) *, ele deverá estar em conformidade com o PCI DSS refere-se ao processamento de dados como prestador de serviços à Experian.
* Para mais definições, consulte PCI Data Security Standard, conforme publicado em https://www.pcisecuritystandards.org/

REQUISITOS DE SEGURANÇA

1. Políticas de Segurança da Informação e Governança
O Programa de Segurança da Informação do Fornecedor será consistente com as práticas descritas em um padrão da indústria, como a ISO 27002 e o Documento de Requisitos de Segurança da Experian Suuplier, que está alinhado à política de Segurança da Informação da Experian.

2. Confidencialidade e Integridade
O fornecedor utilizará uma abordagem gerenciada de segurança para garantir que as informações da Experian sejam protegidas durante todo o ciclo de vida, desde a criação, transformação e uso, armazenamento e destruição, independentemente da mídia de armazenamento, por exemplo, fita, disco, papel, etc.

3. Administração da Informação
O fornecedor designará administradores de informações responsáveis por ativos de informação sob seu controle que armazenam, processam ou transmitem informações da Experian.

4. Proteção contra perda de dados
As soluções Data Loss Prevention (DLP) devem ser utilizadas para identificar, monitorar e proteger dados em uso (por exemplo, ações de endpoint), dados em movimento (por exemplo, ações de rede) e dados em repouso (por exemplo, armazenamento de dados) por meio de inspeção de conteúdo. estrutura de gerenciamento centralizado.

5. Gestão de Vulnerabilidades
Firewalls, roteadores, servidores, PCs e todos os outros recursos utilizados na prestação de serviços à Experian serão atualizados com patches de sistema específicos de segurança apropriados. O Fornecedor realizará testes de penetração regulares (incluindo métodos automáticos e manuais) a serem preenchidos por terceiros independentes para avaliar os Recursos.

6. Segurança Física
Haverá uma função de segurança para conceder, ajustar e revogar o acesso físico às instalações onde a Experian Information reside ou pode ser acessada. Todos os sites de fornecedores e acesso a informações residirão no local contratualmente acordado, a menos que aprovado de outra forma, por escrito, pela Experian.

7. Gerenciamento de Mudanças
Modificações e melhorias no (s) recurso (s) devem ser gerenciadas por meio de um processo controlado de gerenciamento de mudanças. Um "proprietário" designado deve ser identificado para todas as solicitações de alteração e as alterações devem ser aprovadas por um grupo de gerenciamento de mudanças.

8. Registro e Monitoramento
Os mecanismos de registro devem estar em vigor para todos os sistemas que processam, transmitem ou armazenam informações da Experian. O registro em log é necessário para identificar incidentes de segurança, estabelecer responsabilidade individual e reconstruir eventos. Os registros de auditoria serão mantidos em um estado protegido (criptografado ou bloqueado) e serão processados para serem revisados periodicamente para detectar intrusões, acesso não autorizado, atividades não intencionais, softwares mal-intencionados ou tentativas dessas ou de outras ações que possam comprometer a segurança dos sistemas. processamento de dados Experian. Eles serão retidos por um período mínimo de 90 dias.

9. Sistemas de Prevenção de Intrusão
O Fornecedor usará medidas de segurança (incluindo IPS e IDS) para proteger o (s) sistema (s) de telecomunicações do Fornecedor e qualquer sistema de computador ou dispositivo de rede que o Fornecedor utilize para fornecer serviços à Experian para reduzir o risco de infiltração, invasão ou penetração de acesso uma terceira festa.

10. Resposta ao Incidente
Processos e procedimentos serão estabelecidos para responder a violações de segurança e eventos e incidentes incomuns ou suspeitos para limitar mais danos aos ativos de informações e para permitir a identificação e a ação penal contra os infratores. O Fornecedor relatará violações ou incidentes de segurança reais ou suspeitas que afetem a Experian à Experian dentro de 24 (vinte e quatro) horas do conhecimento do Fornecedor sobre tal violação ou incidente

11. Defesa contra Malware
O fornecedor usará serviços e procedimentos de detecção e varredura de malware do computador.

12. Segregação de Deveres e Enventos
O fornecedor mantém controles projetados para fornecer a segregação adequada de funções entre o pessoal do fornecedor, incluindo o acesso a sistemas e redes. Os deveres são atribuídos de tal maneira que uma pessoa não terá obrigações conflitantes que possam resultar em comprometimento acidental ou deliberado de informações, sistemas ou processos, nem ter a oportunidade de ocultar seus erros ou irregularidades.

13. Criptografia e PKI
Todas as informações da Experian serão criptografadas de acordo com os requisitos do FIPS 140 quando armazenadas (em repouso), a menos que os controles de compensação aprovados pela Experian sejam implementados. Computadores portáteis não armazenarão informações da Experian, a menos que a Experian concorde que existe uma necessidade comercial para esse armazenamento, e se o acordo for alcançado, as informações da Experian em laptops serão criptografadas.

14. Segurança de Rede
O fornecedor fornecerá os seguintes serviços de segurança de comunicação de dados:
a) salvaguardar a confidencialidade e integridade de todos os dados transmitidos através de qualquer forma de rede de dados; e
b) implementar e manter técnicas atuais de criptografia padrão de melhores práticas atuais do setor para todos os casos em que os dados identificados como Informações Experimentais sejam transmitidos através de qualquer rede pública de dados. É necessário um mínimo de criptografia de chave de 128 bits.

15. Identificação, Autenticação e Autorização
Cada usuário de qualquer recurso terá um ID de usuário atribuído exclusivamente para permitir autenticação e responsabilidade individuais. Os recursos autenticarão cada usuário antes de conceder todos os acessos autorizados. O nível de autenticação necessário para o acesso a qualquer Recurso é proporcional à sensibilidade dos dados alojados no Recurso.

O acesso a contas com privilégios será restrito apenas às pessoas que administram o recurso; a responsabilidade individual será mantida. Todas as senhas padrão (como as de fornecedores de hardware ou software) serão alteradas imediatamente após o recebimento.

16. Senhas e Contas do Usuário
Senhas de usuários irão:
a) permanecerão confidenciais e não serão compartilhados, divulgados ou de outra forma divulgados de qualquer maneira;
b) consiste em um mínimo de oito (8) caracteres para contas de usuário padrão (dez caracteres para contas de usuários privilegiados);
c) conter pelo menos três dos seguintes
Eu. caracteres maiúsculos (de A a S)
ii. caracteres minúsculos (a até s)
iii. caracteres numéricos (0 a 9)
iv. caracteres não alfabéticos (por exemplo,!, $, #,%)
d) não conter o nome da conta ou ID da conta ou outros valores facilmente adivinhados;
e) não permitir que as treze senhas anteriores sejam reutilizadas; e
f) ser criptografado em armazenamento e transmissão

As contas de usuários irão:
a) bloqueio automático após cinco (5) tentativas incorretas consecutivas; e
b) expirar após um máximo de 90 dias corridos (30 dias se o usuário da conta privilegiada)

17. Autorização de Conexão de Acesso Remoto
Todas as conexões de acesso remoto a redes internas e / ou sistemas de computadores do Fornecedor exigirão autorização e fornecerão um meio de controle de acesso aprovado no "ponto de entrada" para os recursos de computação ou comunicação do Fornecedor por meio da autenticação multifatores. Esse acesso usará canais de acesso seguro, como uma rede privada virtual (VPN).

18. Proteger o Desenvolvimento do Sistema
As aplicações desenvolvidas pelo Fornecedor para a Experian seguirão uma metodologia que permite: (i) definir requisitos de segurança como parte da fase de definição de requisitos; (ii) usando um modelo de design que incorpore as melhores práticas em segurança; (iii) desenvolver código de forma a minimizar as vulnerabilidades de segurança (como scripts entre sites, injeção de SQL, estouro de buffer, etc.); (iv) testar o código através de avaliações estáticas e dinâmicas; e (v) implantar o aplicativo em um ambiente de produção seguro.

19. Segurança Pessoal
Todo o pessoal do Fornecedor e subcontratados, se houver, que: (a) terão acesso a uma rede Experian; (b) ter acesso ou capacidade de visualizar ou usar as informações da Experian; ou (c) estar nas instalações da Experian por mais de um dia e ter emitido um crachá de acesso (Indivíduos que recebem crachás de visitantes e são acompanhados no local por um funcionário da Experian durante toda a sua visita não se enquadre neste critério) verificação de antecedentes criminais e investigação geral de antecedentes. O Fornecedor não será obrigado a rastrear qualquer indivíduo onde seja proibido por lei.

20. Treinamento e Conscientização
O Fornecedor exigirá que todo o pessoal do Fornecedor participe de treinamentos de segurança da informação e sessões de conscientização pelo menos uma vez por ano e estabeleça prova de aprendizado para todo o pessoal. Quando o fornecedor tem acesso direto aos sistemas e / ou rede Experian, o pessoal do fornecedor pode ser mandatado para completar os programas de treinamento e conscientização da Experian.

21. Continuidade de Negócios
O Fornecedor implementará e manterá um programa de Continuidade de Negócios que inclui estratégias, planos e procedimentos documentados de recuperação, para garantir que o Fornecedor possa continuar a entregar seus produtos e serviços à Experian dentro do objetivo do tempo de recuperação contratual.

22. Direito da Experian de Auditoria
A Experian pode realizar auditorias e avaliações de riscos de segurança no local para avaliar o Programa de Segurança de Informações do Fornecedor e a conformidade com os Requisitos de Segurança da Informação da Experian.

23. Relações com Terceiros
O Fornecedor não fornecerá ou iniciará o trabalho com qualquer terceiro que tenha impacto nas Informações da Experian sem a prévia aprovação por escrito da Experian. O fornecedor não utilizará recursos offshore sem a aprovação prévia por escrito da Experian.
O Fornecedor realizará avaliações de risco de segurança de quaisquer provedores de serviços terceirizados com acesso às Informações da Experian.