Proteção de Dados dos Clientes da Accenture

Este documento descreve as medidas técnicas e organizacionais, controles internos e rotinas de segurança da informação que a Accenture mantém para proteger os dados fornecidos por ou em nome de nossos clientes em conexão com um contrato de serviço ao cliente ("**Dados do Cliente**"). Essas medidas destinam-se a proteger os Dados do Cliente nos ambientes da Accenture (por exemplo, sistemas, redes, instalações) contra acesso, divulgação, alteração, perda ou destruição acidental, não autorizada ou ilegal. Na medida em que os Dados do Cliente incluam dados pessoais, a implementação e conformidade com essas medidas e quaisquer medidas de segurança adicionais estabelecidas no contrato de cliente aplicável são projetadas para fornecer um nível adequado de segurança em relação ao processamento dos dados pessoais. A Accenture reserva-se o direito de atualizar essas medidas de segurança a qualquer momento, sem aviso prévio, desde que tais revisões não reduzam ou degradem materialmente a proteção fornecida para os Dados do Cliente.

1. **Organização de Segurança da Informação**
    a) **Responsabilidade pela segurança.** A Accenture nomeará um ou mais representantes de segurança responsáveis pela coordenação e monitoramento das regras e procedimentos de segurança.
    b) **Funções e responsabilidades de segurança.** O pessoal da Accenture com acesso aos Dados do Cliente estará sujeito a obrigações de confidencialidade.
    c) **Programa de gerenciamento de risco.** A Accenture terá um programa de gestão de risco em vigor para identificar, avaliar e tomar as ações apropriadas com relação aos riscos relacionados ao processamento dos Dados do Cliente em conexão com o [Contrato / SOW] aplicável entre as Partes.
2. **Gestão de ativos**
    a) **Inventário de ativos.** A Accenture manterá um inventário completo de ativos de sua infraestrutura, rede, aplicativos e ambientes em nuvem. A Accenture também manterá um inventário de todas as suas mídias nas quais os Dados do Cliente são armazenados. O acesso aos inventários de tais mídias será restrito ao pessoal das Partes com autorização por escrito para tal acesso.
    b) **Tratamento de dados.** Accenture irá

        i. Classificar os Dados do Cliente para ajudar a identificá-los e permitir que o acesso a eles seja adequadamente restrito.
        ii. Limitar a impressão dos Dados do Cliente de seus sistemas ao mínimo necessário para realizar os serviços e manter procedimentos para o descarte de materiais impressos que contenham Dados do Cliente.
        iii. Exigir que seu pessoal obtenha a autorização apropriada antes de armazenar os Dados do Cliente fora dos locais e sistemas aprovados contratualmente, acessar remotamente os Dados do Cliente ou processar Dados do Cliente fora das instalações das Partes.

3. **Segurança de Recursos Humanos**
    a) **Treinamento de segurança.** Accenture irá

        i. Informar seu pessoal sobre os procedimentos de segurança relevantes e suas respectivas funções.
        ii. Informar o seu pessoal sobre as possíveis consequências da violação das regras e procedimentos de segurança.
        iii. Utilizar apenas dados anônimos no treinamento.

4. **Segurança Física e Ambiental**

a) **Acesso físico às instalações.** A Accenture só permitirá que indivíduos autorizados acessem suas instalações onde os sistemas de informação que processam Dados do Cliente estão localizados.
b) **Acesso físico aos componentes.** A Accenture manterá registros da mídia de entrada e saída contendo Dados do Cliente, incluindo o tipo de mídia, o remetente / destinatário autorizado, data e hora, o número de mídia e os tipos de Dados do Cliente contidos em tais mídias.

c) **Descarte de componentes.** A Accenture usará processos padrão da indústria (por exemplo, ISO 27001, CIS Sans 20 e/ou NIST Cyber-Security Framework, conforme aplicável) para excluir os Dados do Cliente quando eles não forem mais necessários.

5. **Gestão de comunicações e operações**
   a) **Política operacional.** A Accenture manterá documentos de segurança que descrevem suas medidas de segurança e os procedimentos e responsabilidades relevantes de seu pessoal que tem acesso aos Dados do Cliente.
   b) **Gerenciamento de dispositivos móveis (MDM) / Gerenciamento de aplicativos móveis (MAM).** A Accenture manterá uma política para seus dispositivos móveis que:

      i. Imponha a criptografia do dispositivo.
      ii. Proíbe o uso de aplicativos na lista negra.
      iii. Proíbe a inscrição de dispositivos móveis que tenham sido "jail broken".

   c) **Procedimentos de recuperação de dados.** Accenture irá

      i Possuir procedimentos específicos de recuperação de dados com relação aos seus sistemas, desenvolvidos para permitir a recuperação dos Dados do Cliente mantidos em seus sistemas.
      ii Revisar seus procedimentos de recuperação de dados pelo menos uma vez por ano.
      iii Registrar os esforços de restauração de dados em relação aos seus sistemas, incluindo a pessoa responsável, a descrição dos dados restaurados e, quando aplicável, a pessoa responsável e quais dados (se houver) tiveram que ser inseridos manualmente no processo de recuperação de dados.

   d) **Software malicioso.** A Accenture terá controles antimalware para ajudar a evitar que softwares mal-intencionados obtenham acesso não autorizado aos Dados do cliente, incluindo softwares mal-intencionados originados de redes públicas.
   e) **Dados que saiam do ambiente da Accenture.** Accenture irá

      i Criptografar os Dados do Cliente que ela transmitir em redes públicas.
      ii Proteger os Dados do Cliente na mídia que sai de suas instalações (por exemplo, por meio de criptografia).
      iii Implementar ferramentas automatizadas onde for viável para reduzir os riscos de e-mail, cartas e / ou faxes mal direcionados a partir de seus sistemas.

   f) **Registro de eventos.**
      i Para seus sistemas contendo Dados do Cliente, a Accenture registrará eventos de forma consistente com suas políticas ou padrões declarados.
6. **Controle de acesso**
   a) **Política de acesso.** A Accenture manterá um registro dos privilégios de segurança dos indivíduos que têm acesso aos Dados do Cliente por meio de seus sistemas.
   b) **Autorização de acesso.** Accenture irá
      i Manter e atualizar um registro do pessoal autorizado a acessar os Dados do Cliente por meio de seus sistemas.
      ii Quando for responsável pelo provisionamento de acesso, fornecer imediatamente as credenciais de autenticação.
      iii Desativar as credenciais de autenticação quando essas credenciais não tiverem sido usadas por um período de tempo (esse período de não uso não deve exceder 90 dias).
      iv Desativar as credenciais de autenticação após a notificação de que o acesso não é mais necessário (por exemplo, demissão de funcionário, reatribuição de projeto, etc.) dentro de dois dias úteis.

v Identificar o pessoal que pode conceder, alterar ou cancelar o acesso autorizado aos dados e recursos.

vi Certificar-se de que, onde mais de um indivíduo tiver acesso aos seus sistemas contendo Dados do Cliente, os indivíduos tenham identificadores / logins exclusivos (ou seja, nenhum id compartilhado).

c) **Menor privilégio.** Accenture irá

i Permitir que seu pessoal de suporte técnico tenha acesso aos Dados do Cliente apenas quando necessário

ii Manter controles que permitam o acesso de emergência aos sistemas de produção por meio de *firefighter* ids, ids temporários ou ids gerenciados por uma solução de gerenciamento de acesso privilegiado (PAM).

iii Restringir o acesso aos Dados do Cliente em seus sistemas apenas aos indivíduos que precisam de tal acesso para desempenhar suas funções.

iv Limitar o acesso aos Dados do Cliente em seus sistemas apenas aos dados minimamente necessários para executar os serviços.

v Reforçar a segregação de funções entre seus ambientes de forma que nenhuma pessoa individual tenha acesso para realizar tarefas que criam um conflito de interesse de segurança (por exemplo, desenvolvedor / revisor, desenvolvedor / testador).

d) **Integridade e confidencialidade.** A Accenture instruirá seu pessoal a desabilitar as sessões administrativas ao sair das instalações ou quando os computadores forem deixados sem supervisão.

e) **Autenticação.** Accenture irá

i Utilizar as práticas padrão da indústria (por exemplo, ISO 27001, CIS Sans 20 e/ou NIST Cyber-Security Framework, conforme aplicável) para identificar e autenticar usuários que tentam acessar seus sistemas de informação.

ii Quando os mecanismos de autenticação são baseados em senhas, exigir que as senhas sejam renovadas regularmente.

iii Quando os mecanismos de autenticação são baseados em senhas, exigir que a senha contenha pelo menos oito caracteres e três dos quatro tipos de caracteres a seguir: numérico (0-9), minúsculo (az), maiúsculo (AZ), especial (por exemplo, !, *, &, etc.).

iv Certificar-se de que identificadores desativados ou expirados não sejam concedidos a outros indivíduos.

v Monitorar as tentativas repetidas de obter acesso aos seus sistemas de informação usando uma senha inválida.

vi Manter procedimentos padrão da indústria (por exemplo, ISO 27001, CIS Sans 20 e/ou NIST Cyber-Security Framework, conforme aplicável) para desativar senhas que foram corrompidas ou divulgadas inadvertidamente.

vii Utilizar as práticas de proteção de senha padrão da indústria (por exemplo, ISO 27001, CIS Sans 20 e/ou NIST Cyber-Security Framework, conforme aplicável), incluindo práticas destinadas a manter a confidencialidade e integridade das senhas quando são atribuídas e distribuídas, bem como durante o armazenamento.

f) **Autenticação multifatorial.** A Accenture implementará a autenticação multifator para acesso interno e acesso remoto por rede privada virtual (VPN) a seus sistemas.

7. Teste de penetração e verificação de vulnerabilidade de sistemas Accenture.

a) Pelo menos anualmente, a Accenture realizará avaliações de penetração e vulnerabilidade nos ambientes de TI da Accenture de acordo com as políticas de segurança interna e práticas padrão da Accenture.

b) A Accenture concorda em compartilhar com o Cliente informações resumidas relacionadas a tais testes conduzidos pela Accenture, na medida aplicável aos Serviços.

c) Para maior clareza, no que se refere a tais testes de penetração e vulnerabilidade, o Cliente não terá direito a (i) dados ou informações de outros clientes ou clientes da Accenture; (ii) testar ambientes de TI de terceiros, exceto na medida em que a

Accenture tenha o direito de permitir tais testes; (iii) qualquer acesso ou teste de infraestrutura ou ambientes de serviço compartilhado, ou (iv) qualquer outra Informação Confidencial da Accenture que não seja diretamente relevante para tais testes e Serviços.

d) Para quaisquer sistemas de TI da Accenture que sejam fisicamente dedicados ao Cliente, as Partes podem concordar em separado, planos de teste escritos e tais testes não excederão dois testes por ano.

8. **Projeto e gerenciamento de redes e aplicativos.** Accenture irá
   a) Possuir controles para evitar que indivíduos obtenham acesso não autorizado aos Dados do Cliente em seus sistemas.
   b) Utilizar a prevenção contra perda de dados baseada em e-mail para monitorar ou restringir a movimentação de dados sensíveis.
   c) Utilizar a filtragem da web baseada em rede para impedir o acesso a sites não autorizados.
   d) Utilizar firefighter IDs ou IDs de usuário temporários para acesso de produção.
   e) Utilizar detecção e / ou prevenção de intrusão de rede em seus sistemas.
   f) Utilizar padrões de codificação seguros.
   g) Procurar e corrigir vulnerabilidades OWASP em seus sistemas.
   h) Na medida do tecnicamente possível, espera-se que as Partes trabalhem juntas para limitar a capacidade do pessoal da Accenture de acessar ambientes não pertencentes ao Cliente e não pertencentes à Accenture a partir dos sistemas do Cliente.
   i) Manter os padrões de configuração de segurança de servidor, rede, infraestrutura, aplicativos e nuvem atualizados.
   j) Realizar uma varredura em seus ambientes para garantir que as vulnerabilidades de configuração identificadas foram corrigidas.

9. **Gerenciamento de Patch**

a) A Accenture terá um procedimento de gerenciamento de patch que implanta patches de segurança para seus sistemas utilizados para processar Dados do Cliente, que inclua:

   i Tempo definido permitido para implementação de patches (não superior a 90 dias para patches altos ou médios conforme definido pela respectiva norma da Parte); e
   ii Processo estabelecido para lidar com patches de emergência ou críticos assim que possível.

10. **Estações de Trabalho**

a) A Accenture implementará controles para todas as estações de trabalho fornecidas que são usadas em conexão com a entrega / recebimento do serviço, incorporando o seguinte:

   i Agente de software que gerencia a conformidade geral da estação de trabalho e relata no mínimo uma vez por semana para um servidor central
   ii Disco rígido criptografado
   iii Processo de patching para que as estações de trabalho sejam corrigidas dentro do cronograma de patching documentado
   iv Capacidade de impedir a instalação de software na lista negra
   v Antivírus com varredura mínima semanal
   vi Firewalls instalados

11. **Gerenciamento de violação de segurança da informação**

a) **Processo de resposta a violação de segurança.** A Accenture manterá um registro de suas próprias violações de segurança em seus sistemas com uma descrição da violação, o período de tempo, as consequências da violação, o nome do denunciante e a quem a violação foi relatada e o processo de recuperação de dados.
b) **Monitoramento de serviço.** O pessoal de segurança da Accenture analisará seus próprios registros como parte do processo de resposta a violações de segurança para propor esforços de remediação, se necessário.

12. **Gestão de Continuidade de Negócios**

a) A Accenture terá processos e programas alinhados à ISO 22301 para permitir a recuperação de eventos que afetam sua capacidade de desempenho de acordo com o Contrato.