Política de Segurança da Informação da Alphacode

Versão - Janeiro de 2024

1. Objetivo

O objetivo desta política é estabelecer um conjunto de normas e diretrizes que garantam a proteção das informações da Alphacode contra qualquer forma de acesso, modificação, divulgação ou destruição não autorizada. Busca-se, com isso, preservar a confidencialidade, integridade e disponibilidade dos dados da empresa, dos seus clientes e parceiros.

2. Escopo

Esta política aplica-se a todos os colaboradores da Alphacode, incluindo funcionários em tempo integral e parcial, contratados, consultores, prestadores de serviço e qualquer outra pessoa que trabalhe com ou tenha acesso às informações da empresa.

3. Responsabilidades

Diretoria: Aprovar e fornecer suporte à implementação da política de segurança da informação.

Gerência de TI: Implementar, monitorar e revisar as práticas de segurança da informação.

Colaboradores: Cumprir as diretrizes estabelecidas nesta política e reportar qualquer incidente de segurança ao departamento de TI.

4. Diretrizes de Segurança

4.1. Política de Senhas

A Alphacode compromete-se com a manutenção da segurança dos dados e sistemas por meio da implementação de práticas robustas de gestão de senhas. Para garantir a segurança das informações e dos sistemas de TI, são estabelecidas as seguintes diretrizes para a criação, uso e gestão de senhas:

Criação e Uso de Senhas

Complexidade: As senhas devem ter no mínimo 8 caracteres e incluir uma combinação de letras maiúsculas, minúsculas, números e símbolos.

Unicidade: Cada senha deve ser única e não ser reutilizada em diferentes sistemas ou serviços.

Confidencialidade: As senhas são de uso pessoal e intransferível. Não devem ser compartilhadas com outros colaboradores ou terceiros.

Troca Regular de Senhas

Intervalo de Troca: As senhas devem ser trocadas obrigatoriamente a cada 90 dias. Sistemas e plataformas de TI da empresa notificarão os usuários com antecedência para a realização dessa mudança.

Troca Imediata: Se houver qualquer suspeita de comprometimento de senha, a troca deve ser feita imediatamente, e o incidente, reportado ao departamento de TI.

Autenticação de Dois Fatores (2FA)

Implementação Obrigatória: Todos os serviços e sistemas de TI acessados pelos colaboradores devem ter a autenticação de dois fatores (2FA) ativada para adicionar uma camada extra de segurança.

Tipos de 2FA: Os métodos de 2FA podem incluir combinações de algo que o usuário sabe (senha), algo que o usuário tem (um dispositivo móvel ou token) e algo que o usuário é (biometria).

Configuração e Suporte: O departamento de TI fornecerá as diretrizes para a configuração do 2FA e estará disponível para suporte aos colaboradores durante o processo de ativação e uso.

Responsabilidade dos Colaboradores

É responsabilidade de cada colaborador seguir rigorosamente esta política de senhas.

Os colaboradores devem garantir a segurança das suas senhas e dos dispositivos utilizados para a autenticação de dois fatores.

Qualquer dificuldade técnica ou suspeita de violação de segurança relacionada às senhas deve ser imediatamente comunicada ao departamento de TI.

Esta política de senhas visa proteger tanto as informações corporativas quanto as pessoais dos colaboradores, minimizando o risco de acesso não autorizado aos sistemas e dados da Alphacode.

4.2. Gestão de Dados

4.2. Gestão de Dados

A segurança e a privacidade dos dados dos usuários são prioridades máximas para a Alphacode. Para garantir a proteção adequada desses dados, a seguinte política de gestão de dados está em vigor:

Acesso a Dados Pessoais

Necessidade e Minimização: O acesso direto a dados pessoais dos usuários por colaboradores deve ser limitado estritamente àquilo que é necessário para a execução de suas funções. Deve-se sempre priorizar métodos que minimizem ou anonimizem o acesso a dados pessoais quando possível.

Autorização: Qualquer acesso a dados pessoais deve ser autorizado previamente e estar de acordo com as políticas internas de privacidade e proteção de dados. A autorização para o acesso é restrita e monitorada pelo departamento de TI e pela gestão de segurança da informação.

Registro e Auditoria: Todos os acessos a dados pessoais devem ser registrados e estar sujeitos a auditorias regulares para garantir a conformidade com esta política.

Armazenamento de Dados em Estações de Trabalho

Proibição de Armazenamento Local: É estritamente proibido manter dados pessoais dos usuários finais das aplicações armazenados nas estações de trabalho dos colaboradores. Todos os dados devem ser acessados e manipulados apenas através dos sistemas centrais seguros da empresa.

Medidas de Segurança: As estações de trabalho devem ser equipadas com medidas de segurança adequadas, incluindo, mas não se limitando a, software antivírus atualizado, firewalls e criptografia de disco, para proteger contra a exposição acidental ou maliciosa de dados.

Limpeza de Dados: Ao término de qualquer tarefa que necessite o acesso a dados pessoais, os colaboradores devem assegurar que todos os dados temporários sejam adequadamente eliminados de sua estação de trabalho, conforme as diretrizes do departamento de TI.

Treinamento e Conscientização

Educação Contínua: Todos os colaboradores receberão treinamento regular sobre as práticas de gestão de dados, incluindo como acessar, manipular e destruir dados pessoais de maneira segura e conforme as leis de proteção de dados aplicáveis.

Responsabilidade dos Colaboradores: Cada colaborador tem a responsabilidade individual de aderir a esta política de gestão de dados. A negligência ou violação das práticas estabelecidas pode resultar em ações disciplinares, incluindo, mas não se limitando a, suspensão, demissão e medidas legais.

Conclusão

A Alphacode se compromete a proteger a privacidade e a segurança dos dados dos usuários, aplicando as melhores práticas de gestão de dados e cumprindo rigorosamente todas as leis e regulamentos aplicáveis de proteção de dados.

4.3. Segurança Física

A proteção física dos ativos e recursos de informação da Alphacode é crucial para a manutenção da segurança da informação. Este compromisso se estende desde a proteção dos dados até a segurança física dos equipamentos. As seguintes diretrizes são estabelecidas para assegurar essa proteção:

Uso de Software

Softwares Permitidos: Todos os colaboradores devem garantir que apenas softwares inerentes às suas atividades de trabalho estejam instalados em suas estações de trabalho. É proibida a instalação de softwares que não estejam diretamente relacionados às necessidades operacionais ou que não tenham sido aprovados pelo departamento de TI.

Licenciamento de Software: Todo software utilizado deve ser devidamente licenciado. A pirataria de software é estritamente proibida, e o uso de softwares licenciados deve estar em conformidade com os termos de serviço e as licenças aplicáveis.

Revisão e Auditoria: O departamento de TI realizará revisões e auditorias periódicas para garantir que apenas os softwares apropriados e licenciados estejam instalados nas estações de trabalho.

Segurança Física do Equipamento

Responsabilidade Fora das Dependências da Empresa: Quando os equipamentos da empresa forem levados para fora das dependências corporativas (por exemplo, trabalho remoto), o colaborador é diretamente responsável pela segurança física destes. Deve-se tomar medidas adequadas para prevenir danos, perda ou acesso não autorizado.

Proteção do Equipamento: Recomenda-se o uso de fechaduras, senhas de acesso e outras medidas de segurança física para proteger os equipamentos. Em ambientes públicos, os colaboradores devem manter os equipamentos sob vigilância constante e nunca deixá-los desacompanhados.

Relato de Incidentes: Qualquer incidente de segurança, como perda, roubo ou dano físico ao equipamento, deve ser imediatamente reportado ao departamento de TI. Medidas rápidas podem ser necessárias para proteger as informações e minimizar potenciais impactos de segurança.

Conclusão

A segurança física dos ativos de informação da Alphacode é uma responsabilidade compartilhada. Todos os colaboradores têm o dever de adotar práticas de segurança física e digital para proteger os recursos da empresa. O não cumprimento dessas diretrizes pode levar a ações disciplinares e, em casos graves, a responsabilidade legal.

4.4. Segurança em Softwares e Aplicações

Manter sistemas e aplicações atualizados com as últimas correções de segurança.

Desenvolver e testar aplicações seguindo práticas de segurança recomendadas.

4.5. Resposta a Incidentes

Seguir o plano de resposta a incidentes de segurança da informação para lidar com violações e ameaças de forma eficaz.

5. Revisão e Atualização

Esta política será revisada anualmente ou sempre que necessário, para refletir as mudanças nas práticas de negócios, tecnologias ou legislação aplicável.

6. Aceitação e Conformidade

Todos os colaboradores da Alphacode devem ler, entender e assinar uma declaração de aceitação desta política como condição para o acesso às informações e sistemas da empresa.