POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ASPP

Versão 1.0 – 11/11/2025

OBJETIVO DA POLÍTICA

Esta política estabelece regras simples para proteger as informações da Associação dos Servidores Públicos do Paraná (ASPP). Seu objetivo é garantir a confidencialidade, integridade e disponibilidade dos dados da associação, assegurando seu uso adequado e reduzindo riscos à segurança da informação. Em resumo, busca preservar a confiança nas informações da ASPP, evitar danos ou perdas e orientar boas práticas de segurança no trabalho diário.

A QUEM SE APLICA

Esta política se aplica a todos os colaboradores da ASPP, independentemente do cargo ou função. Isso inclui funcionários, servidores, estagiários, terceirizados, prestadores de serviço e quaisquer outras pessoas que tenham acesso a informações da associação. Todos devem conhecer e seguir estas diretrizes no desempenho de suas atividades.

Princípios Gerais de Segurança da Informação

A segurança da informação na ASPP baseia-se em três princípios fundamentais:

- CONFIDENCIALIDADE: garantir que a informação só seja acessada por quem deve ter acesso a ela. Isso significa proteger dados confidenciais (por exemplo, dados pessoais de associados ou documentos sigilosos) para que pessoas não autorizadas não os vejam.
- INTEGRIDADE: assegurar que a informação não seja alterada de forma indevida. Ou seja, os dados devem se manter corretos e confiáveis desde a criação até o uso, evitando modificações acidentais ou maliciosas.
- DISPONIBILIDADE: garantir que a informação esteja disponível sempre que necessária para as pessoas autorizadas. Isso implica ter sistemas e dados acessíveis no momento certo (por exemplo, evitar que um sistema fique fora do ar sem necessidade).
- AUTENTICIDADE: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Esses princípios servem para proteger tudo o que sustenta as atividades da ASPP, desde documentos em papel até sistemas digitais.

DIRETRIZES PRÁTICAS DE PROTEÇÃO NO DIA A DIA

No cotidiano de trabalho, todos os membros da ASPP devem adotar práticas simples de segurança. Aqui estão algumas orientações claras e exemplos práticos:

- SENHAS SEGURAS: Use senhas fortes e únicas para cada sistema (misture letras maiúsculas e minúsculas, números e símbolos). Nunca compartilhe sua senha com ninguém e não reutilize a mesma senha em vários serviços. Por exemplo, não use senhas óbvias como "123456" ou datas de aniversário, e não conte sua senha a colegas ou familiares.
- CUIDADO COM E-MAILS E LINKS SUSPEITOS: Esteja atento a tentativas de fraude (phishing). Não abra anexos nem clique em links de e-mails ou mensagens suspeitas – por exemplo, desconfie de e-mails dizendo que você ganhou prêmios ou pedindo dados pessoais. Em caso de dúvida, confirme com o remetente por outro canal antes de clicar.
- WI-FI E REDES SEGURAS: **Evite conexões Wi-Fi públicas não seguras para acessar** sistemas ou informações da ASPP. Redes abertas (como de cafeterias ou aeroportos) podem expor dados. Se for necessário usar uma rede pública, não acesse informações confidenciais sem uma proteção extra (como VPN) e prefira usar a rede 4G/5G do celular, se possível.
- DISPOSITIVOS PESSOAIS: Se você utiliza dispositivos pessoais (como seu smartphone ou notebook) para trabalho, siga os mesmos cuidados de segurança. Mantenha esses aparelhos protegidos com senha/PIN ou biometria e antivírus atualizado. Não deixe informações da ASPP salvas em dispositivos pessoais sem proteção. Lembre-se de que o colaborador é responsável pela segurança das informações da ASPP acessadas através de seu dispositivo pessoal – por exemplo, não permita que terceiros usem seu notebook de trabalho e mantenha-o sempre atualizado e bloqueado.
- CONFIDENCIALIDADE E SIGILO: Mantenha sigilo sobre as informações da ASPP. Não divulgue dados internos, documentos ou informações pessoais de associados sem autorização prévia. Isso vale para conversas fora do trabalho, redes sociais e aplicativos de mensagem – evite comentar assuntos confidenciais em locais inadequados. Compartilhe informações apenas com quem tem autorização e necessidade de conhecê-las.
- MESA LIMPA E TELA BLOQUEADA: Adote a prática de mesa limpa no ambiente de trabalho. Guarde documentos confidenciais em local seguro (por exemplo, em gavetas trancadas) quando não estiverem em uso, e bloqueie a tela do computador sempre que se afastar do seu posto. Por simples que pareça, isso evita que pessoas não autorizadas vejam dados sensíveis na sua mesa ou computador. Mesmo pausas rápidas (como para

um café) exigem que você nunca deixe o computador desbloqueado sem supervisão.

Seguindo essas diretrizes no dia a dia, cada colaborador contribui para um ambiente mais seguro e reduz muito as chances de incidentes de segurança.

RESPONSABILIDADES DOS COLABORADORES

A segurança da informação é responsabilidade de todos os membros da ASPP. Em termos práticos, espera-se que cada colaborador:

- CONHEÇA E CUMPRA A POLÍTICA: Todos devem ler, entender e seguir as orientações desta Política de Segurança da Informação. A proteção dos dados da associação depende da participação de cada um, independente do cargo ou departamento.
- PROTEJA AS INFORMAÇÕES SOB SUA GUARDA: Use as diretrizes de segurança ao manusear informações da ASPP, mantendo sigilo e cuidado. Isso inclui proteger senhas, dispositivos e documentos conforme citado acima, evitando qualquer uso indevido ou divulgação não autorizada.
- REPORTE PROBLEMAS DE SEGURANÇA: Caso identifique alguma violação ou incidente de segurança (por exemplo, suspeita de vazamento de informação, perda de dispositivo com dados, ou qualquer descumprimento desta política), comunique imediatamente a equipe responsável (TI ou segurança da informação). Agir rápido pode evitar danos maiores. Não tenha receio de reportar mesmo que seja um erro seu – é melhor notificar e resolver, do que ocultar um incidente.
- COLABORE COM A CULTURA DE SEGURANÇA: Participe de treinamentos e iniciativas de conscientização oferecidos pela ASPP. Ajude colegas menos familiarizados com tecnologia, compartilhe boas práticas e, em caso de dúvidas, procure orientação (ninguém espera que você saiba tudo, mas sim que busque ajuda quando necessário).

Em suma, cada colaborador deve incorporar a segurança como parte de suas tarefas. Todos são responsáveis pela segurança da informação, e juntos mantemos a ASPP protegida.

CONSEQUÊNCIAS DO DESCUMPRIMENTO

O não cumprimento desta política de segurança é algo sério. Violações das regras aqui estabelecidas poderão resultar em medidas disciplinares conforme as normas internas da ASPP, que podem incluir advertências verbais ou escritas, suspensão e, em casos graves ou reincidência, até desligamento do colaborador. Além disso, situações de infração grave (como vazamento intencional de dados ou uso indevido de informações confidenciais) podem acarretar sanções legais, civis e criminais, de acordo com a legislação vigente – por exemplo, penalidades previstas na Lei Geral de Proteção de Dados (LGPD) se dados pessoais forem expostos indevidamente.

É importante destacar que essas consequências visam proteger tanto a associação quanto seus membros e o público que atendemos. Ao seguir a política, evitamos problemas para todos. Em caso de dúvidas sobre o que é permitido ou não, sempre busque orientação em vez de arriscar violar uma regra.

DÚVIDAS E CANAL DE APOIO

A ASPP mantém canais abertos para esclarecimento de dúvidas e apoio aos colaboradores em relação à segurança da informação. Se após ler esta política você tiver dúvidas ou precisar de ajuda para seguir alguma orientação, não hesite em procurar o Departamento de TI ou o responsável pela Segurança da Informação na ASPP. Você pode entrar em contato pelo canal de comunicação através do link: ***(HTTPS://APP.BREVENLAW.COM/MANAGEMENT/HOLDER/REQUEST/PT/B003FE54-D480-42F9-A0C9-099E81A52F23)*** para obter suporte.

Lembre-se: a segurança da informação é uma construção coletiva. Perguntar e buscar ajuda faz parte do processo de conscientização. Estamos todos no mesmo time, trabalhando para proteger os dados e a confiança de todos os associados. Em caso de qualquer incidente ou suspeita, informe imediatamente pelos canais de suporte fornecidos.

ESTA É UMA VERSÃO INICIAL E SIMPLIFICADA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ASPP, ELABORADA PARA CONSCIENTIZAÇÃO GERAL. ELA NÃO ABRANGE TODOS OS DETALHES TÉCNICOS, MAS FOCA NAS PRÁTICAS ESSENCIAIS DO DIA A DIA. TODOS OS COLABORADORES DEVEM SEGUIR ESTAS DIRETRIZES E TAMBÉM FICAR ATENTOS A FUTURAS ATUALIZAÇÕES OU TREINAMENTOS COMPLEMENTARES SOBRE O TEMA.