Política de Segurança da Informação

pay4fun
PAY FOR FUN

SUMÁRIO

1. Objetivo

Esta Política de Segurança da Informação ("Política") da **PAY4FUN** tem por objetivo de orientar e estabelecer os conceitos e diretrizes baseada nas melhores práticas, visando proteger as informações da organização, dos clientes e do público em geral e com a finalidade de prevenção de danos.

A **PAY4FUN** mantém um adequado programa de Segurança da Informação para administrar os riscos e proteger dados confidenciais, a marca e sua reputação, mitigando prejuízos financeiros, reconhecendo, desta forma, sua obrigatoriedade em proteger certas informações, de modo a:

- Preservar a confidencialidade, disponibilidade, integridade, sigilo e autenticidade das suas informações;
- Orientar quanto ao uso adequado de seus ativos, proteger as atividades fim e a gestão da **PAY4FUN**;
- Estabelecer medidas técnicas e administrativas capazes de proteger as informações, inclusive dados pessoais, contra acessos não autorizados e de situações acidentais ou ilícitas envolvendo a destruição, perda, alteração, comunicação ou vazamento de informação; e
- Nortear a definição de procedimentos específicos de controles e processos para a gestão dos riscos de segurança da informação.

2. Público-Alvo

Esta Política aplica-se a todo e qualquer usuário ("colaborador") com acesso a informações da **PAY4FUN**, independentemente de seu vínculo com a **PAY4FUN**, seja ele administrador, funcionário, estagiário, temporário, terceiro ou qualquer representante e/ou parceiros de negócios. Também se aplica a todos ativos de informação, seja por meio de sistemas, servidores, computadores, bases de dados, componentes de redes, laptops, PDA, tablet ou quaisquer outros dispositivos de armazenamento, processamento ou tráfego de informações.

Em razão da sensibilidade da informação trafegada na **PAY4FUN**, esta poderá, nos limites da lei aplicável e conforme necessário, monitorar, gravar e registrar os ambientes, sistemas, serviços, computadores e redes da **PAY4FUN** para garantir a disponibilidade e a segurança das informações utilizadas.

É obrigação de cada Colaborador manter-se atualizado em relação a esta Política, bem como as políticas, procedimentos e normas a ela subordinados.

Todos os colaboradores devem obrigatoriamente cumprir as disposições expressas nesta política, independentemente de seu cargo, função, área de atuação ou localidade na qual exerça suas atividades vinculadas à **PAY4FUN**. O não cumprimento das disposições ora previstas sujeitará o colaborador infrator às sanções dispostas no item 9.

3. Vínculos e Documentações Complementares

- **Código de Ética e Conduta;**
- **Estatuto Social da PAY4FUN;**
- **Política de *Compliance***;
- **Políticas e procedimento subordinados:**
  - ✓ Política de Gestão de Ativos
  - ✓ Política de Controle de Acesso

- ✓ Política de Gestão de Mudanças
- ✓ Procedimento de Gestão de Mudanças
- ✓ Procedimento de Gestão de Incidentes
- ✓ Política de Gestão de Vulnerabilidades
- ✓ Política *Antimalware*
- ✓ Política de Gestão de Logs de Evento
- ✓ Política de Segurança de Rede
- ✓ Política de *Backup*
- ✓ Política de Resiliência Operacional
- ✓ Política de Contratação de Serviços de Computação em Nuvem

4. Definições

- **Antivírus**: software utilizado para mitigar a ameaça de malwares, vírus, trojans e demais classificações de aplicativos ofensivos, oferecendo uma prevenção quando a sua instalação e/ou execução em Sistemas Operacionais.

- **Ativo de Informação**: qualquer patrimônio da **PAY4FUN** composto por dados, informações geradas e manipuladas durante a execução dos sistemas e processos da **PAY4FUN**.

- **Ativo de Processamento**: qualquer patrimônio da **PAY4FUN** composto por elementos de hardware e software necessários para a execução dos sistemas e processos da **PAY4FUN**.

- **BACEN:** Banco Central do Brasil.

- ***Backup***: cópia fiel de dados e/ou programas de um sistema a partir de um determinado ponto ou data, definido através de uma configuração e programação de execução.

- **Colaboradores:** sócios, diretores, administradores, empregados, prestadores de serviços, parceiros e/ou quaisquer outros similares.

- **Controle de Acesso** - restrições ao acesso às informações, sistemas ou infraestrutura, definidas pelos *Information Owner* ou *Systems Owner*, supervisionadas pela unidade de suporte à segurança.

- **Criptografia** - é a ciência matemática que envolve o uso de algoritmos matemáticos para transformar um texto normal em um texto ilegível, e vice-versa.

- **Datacenter**: área restrita destinada ao armazenamento ordenado de servidores de computadores e equipamentos de comunicação.

- **Data *Owner***: Proprietário da informação.

- **Data *Steward*** – Administrador ou suplente do proprietário da informação.

- **Direito de Acesso** - privilégio associado a um cargo, pessoa ou processo para ter acesso a um determinado ativo.

- **Ferramentas** - conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação.

- **Firewall** - dispositivo utilizado com o objetivo de filtrar as conexões de entrada/saída de uma rede de dados baseados em uma configuração específica.
-
- **Incidente de Segurança**: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que seja uma ameaça a qualquer ativo da **PAY4FUN**.

- **Informações Protegidas:** Todo e qualquer dado ou informação que o Colaborador desenvolva ou venha a ter acesso em virtude do seu vínculo com a **PAY4FUN** ou do desempenho de suas atividades contratadas pela **PAY4FUN**.

- **Legalidade**: propriedade que garante que a informação se encontra em concordância com as legislações vigentes e aplicáveis à **PAY4FUN**.

- **Menor Privilégio**: princípio que garante apenas o acesso necessário para o desenvolvimento de uma atividade em um *software*/aplicativo e/ou Sistema operacional.

- **Não repúdio**: propriedade da informação, em que o autor não pode negar a responsabilidade para ele atribuída. Consegue-se estabelecer a característica de não repúdio com a combinação de confidencialidade e integridade da informação.

- ***Need-to-know***: conceito utilizado quando dado uma necessidade para a execução das atividades diárias de trabalho e desempenho de responsabilidade do colaborador.

- **OWASP** (*Open Web Application Security Project*): referente às Boas Práticas de segurança para desenvolvimento de aplicações *web*.

- **Perfil de acesso** - Conjunto de permissões definidas em um sistema ou aplicativo focado nas necessidades de um determinado posto de trabalho ou cargo seguindo as necessidades do negócio.

- **Perímetro de segurança**: Áreas onde existem a exposição de dados e informações sensíveis. Ex.: Datacenter, Sala de Telecom e rede, Diretoria etc.

- **SPAM**: e-mail recebido sem o consentimento do destinatário, sendo geralmente propagandas indesejadas ou anúncio de ofertas.

- **Senha Forte**: Conjunto de caracteres recomendados que, quando da verificação da identicidade de um usuário, gera maior segurança e proteção contra *hackers*, *softwares* maliciosos.

5. Princípios

A segurança da informação é caracterizada pela preservação dos seguintes princípios:

I. Confidencialidade: garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário.

II. Disponibilidade: garante que a informação esteja disponível para as pessoas autorizadas sempre que necessário.

III. Integridade: garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

IV. Autenticidade: garante que a propriedade da informação não foi alvo de alterações indevidas ao longo de um processo estabelecido.

6. Diretrizes

Os princípios estabelecidos nesta Política têm relacionamento direto ou indireto com aspectos de segurança da informação, controle e gestão dessas informações utilizadas e/ou geradas pela **PAY4FUN** em seu desempenho corporativo.

Esses princípios devem ser desdobrados em diretrizes e instruções através de diferentes normativos visando a sua correta aplicação, execução, controle e monitoramento.

As diretrizes devem expressar estratégias, valores e o nível de comprometimento que a **PAY4FUN** estabelece em relação à segurança da informação corporativa, bem como as respectivas instruções devem orientar o quadro de funcionários quanto ao cumprimento de atividades e rotinas relacionadas ao tema.

Todo os esforços de segurança da informação devem ser projetados, implantados e mantidos buscando suportar os requisitos de negócio da **PAY4FUN**, observando práticas de análise de risco e procurando um alinhamento a esta política.

6.1. Privacidade e Proteção de Dados

Esta Política aplica-se aos dados, incluindo Dados Pessoais, que podem ser coletados sobre os clientes e os Colaboradores, por exemplo. É vedado, sem a prévia autorização da **PAY4FUN**, o uso destes dados para finalidades diversas das que lastrearam a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados, nos termos desta Política.

A **PAY4FUN** usa provedores de serviços externos. Se os dados que estão sendo tratados são Dados Pessoais, devem ser firmados acordos contratuais apropriados e medidas organizacionais devem ser implementadas de acordo com a legislação aplicável para assegurar a proteção dos dados.

O Colaborador deve atuar para que todos os Dados Pessoais a que tiver acesso não sejam divulgados ou compartilhados sem autorização expressa da **PAY4FUN**, bem como não sejam transmitidos ou acessados por terceiros não autorizados. O Colaborador deve adotar as melhores práticas de segurança da informação durante todo o ciclo de vida dos dados dentro da **PAY4FUN**.

6.2. Monitoramento e Auditoria do Ambiente

Todo ambiente físico e digital da **PAY4FUN** é ou poderá ser monitorado a qualquer momento, respeitados os limites previstos na legislação vigente, incluindo o acesso, uso ou tráfego de informações em tal ambiente por qualquer meio (por exemplo, e-mail) com o objetivo de apurar o cumprimento das

normas de segurança e proteção de dados da **PAY4FUN**. Sendo assim, os dispositivos da **PAY4FUN** não devem ser utilizados para fins pessoais.

Os colaboradores devem estar cientes de que a **PAY4FUN** poderá:

a) Monitorar todos os servidores, redes, conexões de internet, *softwares*, equipamentos e dispositivos corporativos, móveis ou não, conectados à rede corporativa; e

b) Realizar inspeções físicas nos equipamentos e nas estações de trabalho do Colaborador, periodicamente ou sob fundada suspeita de infração às normas internas da **PAY4FUN**.

O Colaborador também está ciente de que o monitoramento poderá identificá-lo e apresentar dados sobre o seu uso da infraestrutura técnica da **PAY4FUN** e do material e conteúdo manipulado pelo Colaborador, sendo certo que todas as informações coletadas no curso do monitoramento são guardadas nos backups da **PAY4FUN** para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela **PAY4FUN** ou pela legislação em vigor. Caso solicitado pelos órgãos competentes, essas informações poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto.

O Colaborador entende que o monitoramento é realizado para resguardar a segurança não só dos sistemas da **PAY4FUN** e das Informações Protegidas, como também do próprio Colaborador. Os dados e as informações monitoradas somente poderão ser acessadas pelos departamentos competentes e para finalidades legítimas, como a apuração de denúncias e condução de investigações no ambiente laboral. Todo e qualquer tratamento de dados para estes fins será fundamentado no relatório de auditoria ou em outro instrumento apropriado para tanto, e cumprirá as normas específicas sobre privacidade e proteção de Dados Pessoais descritas mais detalhadamente na Política de Privacidade para Colaboradores.

6.3. Diretrizes Específicas

6.3.1. Gestão de Identidades e Acessos

A **PAY4FUN** define como obrigatório que todo usuário com acesso aos sistemas de informação possua uma identificação única, de uso pessoal e intransferível. Como parte de suas responsabilidades, os usuários devem ser responsáveis por proteger suas informações de autenticação e devem seguir as práticas da **PAY4FUN** no uso de informações confidenciais. Portanto, a **PAY4FUN** deve informar aos usuários como criar, manter e usar senhas com segurança.

A **PAY4FUN** realiza a gestão do ciclo de vida dos acessos dos colaboradores e terceiros, garantindo que haja a concessão, manutenção e revogação dos acessos, incluindo um processo de revisão periódico a fim de garantir que não sejam permitidos acessos indevidos às informações.

Acessos privilegiados (administradores de infraestrutura, banco de dados e outros) devem ser monitorados e controlados por meio de mecanismos de segurança que permitam o acesso seguro e auditável.

O acesso à informação e aos sistemas de propriedade da **PAY4FUN** ou sob sua custódia baseia-se no conceito de que o usuário deve ter um nível de acesso à informação suficiente e necessária para executar suas tarefas e não mais do que isto, baseando-se no conceito de *Need-to-know*.

A **PAY4FUN** reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, por meio das áreas competentes, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de segurança da informação da **PAY4FUN**.

6.3.2. Acesso remoto e Teletrabalho

O acesso remoto à rede corporativa é previamente autorizado para atividades de suporte e monitoria de serviços críticos, desde que realizados pelas áreas responsáveis por estas tarefas, bem como para coordenadores, gerentes e diretoria, através de perfis pré-estabelecidos. Os demais acessos devem ser avaliados pela Segurança da Informação;

É proibido o acesso remoto para colaboradores que tenham o ponto controlado, as exceções devem ser aprovadas pela Diretoria de Recursos Humanos mediante solicitação do diretor da área usuária.

Todas as conexões não locais, que permitam acesso a informações ou sistemas de forma remota ao ambiente da **PAY4FUN**, devem utilizar os métodos disponibilizados pela área de infraestrutura de TI e Segurança da Informação para a viabilização do acesso remoto.

Fica vedada a utilização de qualquer dispositivo de propriedade individual ou privada. Qualquer exceção requer aprovação pelo departamento infraestrutura de TI e Segurança da Informação

Para mitigar o risco derivado de dispositivos móveis e teletrabalho, a **PAY4FUN** deve definir as regras a serem aplicadas para sistemas móveis e a prática de teletrabalho acessando os ativos de informação.

6.3.3. Uso de Senhas

A senha é considerada de uso confidencial, pessoal e intransferível, e possui requisitos mínimos de segurança de acordo com o seu grau de criticidade. O Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas nesta Política, mas também as penalidades civis, criminais e trabalhistas, respondendo, inclusive, por todo e qualquer dano que causar à **PAY4FUN**. Os sistemas, redes e aplicativos de informação devem ser protegidos pelo uso de senhas fortes para garantir que as informações não sejam divulgadas, modificadas, excluídas ou tornadas indisponíveis incorretamente.

A identidade de um usuário deve ser verificada, exigindo várias informações exclusivas do usuário antes da redefinição de uma senha. As credenciais do usuário (por exemplo, ID do usuário e senha) devem ser comunicadas separadamente.

A elaboração e uso de senhas para acesso à rede ou aos sistemas deve ser realizada conforme as seguintes diretrizes:

a) Criação de senhas diferentes para cada finalidade;

b) Criação de senhas com no mínimo 08 (oito) caracteres, alfanuméricos, com caracteres especiais (@ # $ %) e variação de maiúsculo e minúsculo; A senha não deve ser baseada em informações pessoais, como próprio nome ou sobrenome nome de familiares, data de nascimento e não deve ser constituída de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras;

c) Se possível, deverá ser realizada a autenticação de dois fatores (2FA) para acesso a serviços críticos, exigindo que o usuário forneça dois meios de identificação antes de conseguir se autenticar;

d) Não devem ser digitadas em computadores e dispositivos móveis de terceiros; e

e) Não devem ser anotadas ou armazenadas em meios físicos e digitais (ex.: e-mail, planilhas, bloco de notas, arquivos na rede, *post-its*, embaixo do teclado ou do monitor etc.).

Em caso de suspeita de descoberta ou furto, roubo, perda ou invasão (hackeamento) de equipamento, solicitar alteração e/ou bloqueio imediato.

6.3.4. Concessão de acesso privilegiado

Todos os ativos ou grupos de ativos da **PAY4FUN** devem ser identificados e classificados pela área de infraestrutura de TI e Segurança da Informação quanto ao nível de confidencialidade da informação a fim possibilitar a criação, uso, monitoramento e gestão de acessos privilegiados. Apenas os usuários que forem habilitados serão autorizados a executar tarefas que usuários comuns não possuem permissões para realizar.

A concessão e uso de acesso a usuários privilegiados deve ser realizada conforme as seguintes diretrizes:

a) Os usuários privilegiados deverão usar sua conta de administrador exclusivamente vinculada ao indivíduo que está usando a conta;

b) Essa conta deve ser distintamente diferente da conta de uso geral do usuário ("Não privilegiada");

c) Contas privilegiadas não devem ser associadas a nomes de computadores, nomes de departamentos, cargos ou qualquer outra informação semelhante que possa revelar a natureza privilegiada da conta;

d) Contas privilegiadas devem ser usadas apenas quando necessário e devem ser desconectadas imediatamente após o uso;

e) Um inventário de contas privilegiadas deve ser estabelecido, mantido, revisado e aprovado periodicamente pela área de tecnologia;

f) Devem ser estabelecidos registros e monitoramentos auditáveis para emitir um alerta de múltiplas tentativas malsucedidas em efetuar login em uma conta administrativa; e

g) Toda conta privilegiada deve ser aprovada pelo diretor de tecnologia.

6.3.5. Ambiente e Recursos de Trabalho

O Colaborador é responsável pelo uso que fizer dos documentos e informações. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de segurança da informação.

6.3.6. Estações de trabalho

A responsabilidade pela integridade do equipamento é exclusiva do colaborador. Em caso de furto, roubo, extravio, invasão (hackeamento) ou dano o colaborador deve comunicar imediatamente a equipe de Suporte Local que tomará as devidas providências.

As estações de trabalho são recursos da **PAY4FUN** e devem ser utilizadas de acordo com as diretrizes descritas no Código de Conduta Ética.

Informações da **PAY4FUN**, clientes, colaboradores, fornecedores e parceiros devem ser armazenados em servidores corporativos onde existam processos consolidados e direcionados à sua integridade, disponibilidade e confidencialidade. Informações salvas no disco local são de responsabilidade do colaborador e em caso de perda total ou parcial e/ou necessidade de *backup* não será suportada pela área de TI.

Todo equipamento conectado na rede corporativa deve ter suas configurações padronizadas conformes as boas práticas de segurança (*hardening*), o que inclui:

a) Ter o sistema de antivírus padrão da companhia instalado e atualizado (equipamentos com *Windows*).

b) Todas as atualizações (*patch*) críticas de segurança aplicados em até 30 dias após a sua divulgação pelo fornecedor, ou período inferior se assim determinado pelo time de tecnologia.

c) Todos os serviços não utilizados devem ser removidos ou desabilitados.

d) Verificação periódica de aderência ao *hardening*.

6.3.7. Mesa limpa

Todas as mesas de trabalho devem ficar limpas. Documentos e Informações Protegidas devem estar seguros de forma a impedir os riscos de acesso não autorizado, perda e/ou danos às informações fora do período de trabalho.

Mídias de armazenamento eletrônico classificadas como Informações Protegidas devem ser armazenadas em compartimentos trancados quando o colaborador não estiver no escritório.

As gavetas das mesas devem ser trancadas e as chaves guardadas de forma segura quando os seus ocupantes não estiverem presentes.

Documentos que forem imprimidos devem ser imediatamente retirados das impressoras.

Após a utilização de salas de reuniões, quadros negros (lousas) devem estar limpos e sem quaisquer informações. Quaisquer folhas utilizadas em reuniões, sejam em *flipchart* ou fora deles que possam conter Informações confidenciais devem ser descartadas e/ou guardadas de forma adequada.

Ao descartar documentos com Informações protegidas, triturá-los com máquina fragmentadora ou manualmente.

6.3.8. Acesso à Internet

O serviço de Internet Corporativa da **PAY4FUN** é concedido de forma restrita e exclusivamente como ferramenta de trabalho de pesquisa e tratamento de assuntos relacionados às funções do usuário da **PAY4FUN**

A **PAY4FUN** visa ao desenvolvimento de um comportamento ético e profissional no uso da internet. Para garantir a utilização racional desses recursos, bem como a segurança dos dados e *softwares*, a **PAY4FUN** se reserva o direito de utilizar ferramentas para verificar o conteúdo dos e-mails corporativos e monitorar o uso da internet e da rede corporativa.

O uso do serviço de Internet não é autorizado para:

a) Acesso a Sites Web com conteúdo abusivo, ameaçador, obsceno, racista, pornográfico ou de qualquer outra forma censurável.

b) Fins comerciais ou ganhos pessoais, divergentes da finalidade da ferramenta ou da função do usuário.

c) Uso de aplicações ponto-a-ponto (*peer-to-peer*) para distribuição de arquivos.

d) Qualquer outro aplicativo que possa configurar ameaça à segurança e inviolabilidade do ambiente de informações.

e) *Download* ou *upload* de qualquer material que, sem a devida licença, viole leis de direitos autorais.

6.3.9. E-mail

O serviço de correio eletrônico será disponibilizado para todos os usuários da Rede Corporativa de acordo com a sua necessidade de trabalho para cumprimento de suas atividades. Todos os endereços e contas de correio são de propriedade da **PAY4FUN**, incluindo respectivos conteúdos, fazendo parte de sua propriedade intelectual.

Os endereços de e-mail fornecidos pela **PAY4FUN** aos Colaboradores são individuais e destinados exclusivamente para fins corporativos e relacionados às atividades do Colaborador dentro da **PAY4FUN**. As mensagens de e-mail sempre deverão incluir assinatura com o formato padrão da **PAY4FUN** e seguir as regras definidas neste item.

Todos os serviços de correios eletrônicos corporativos não são privativos e são monitorados, acarretando bloqueio do serviço sem prévio aviso nos casos de violação. O acesso ao conteúdo das caixas postais é um direito restrito, porém não exclusivo do usuário. A **PAY4FUN** reserva-se o direito de acesso a estas caixas postais através das Áreas de Segurança da Informação e Jurídico.

O correio eletrônico corporativo é um serviço disponibilizado como ferramenta de trabalho para comunicação interna e externa de assuntos estritamente relacionados ao negócio da **PAY4FUN** sendo proibida a utilização para:

a) Envio de mensagens com conteúdo abusivo, ameaçador, obsceno ou de qualquer outra forma censurável, que infrinja direitos de propriedade intelectual, sigilo da **PAY4FUN** ou de Terceiros;

b) Envio de mensagens de conteúdo não profissional como: piadas, correntes ou qualquer outro assunto correlato ao desempenho profissional das atividades;

c) Divulgação de informações e campanhas de caráter assistencial e/ou humanitário;

d) Tráfego de anexos de extensões não autorizadas pela área de Segurança da Informação (ex. *.exe; *.tif; *.scr; entre outros);

O conteúdo manipulado através do E-mail corporativo da **PAY4FUN**, que seja contrário às regras aqui estabelecidas, poderá acarretar ao usuário o bloqueio de sua utilização, bem como sanções previstas em Lei, no contrato de trabalho e no item 16 desta Política.

6.3.10. Proteção contra *malware*

Todas as estações de trabalho, servidores e ativos que sejam compatíveis com uma solução de antivírus e que estejam conectadas na rede corporativa ou façam uso de informações da **PAY4FUN** devem ser protegidos com a solução de antivírus determinada pela área de Segurança da Informação.

A área de Segurança da Informação é responsável pela implantação, manutenção e atualização dos programas de antivírus nas estações e servidores da **PAY4FUN**.

Não é permitido ao usuário remover, desabilitar, alterar as configurações ou instalar outro programa de antivírus em computadores pertencentes a **PAY4FUN,** sendo tal conduta passível de sanções e medidas disciplinares.

6.4. Gestão de Ativos

6.4.1. Segurança em Manuseio de Mídias

A utilização de mídias removíveis que podem gravar como pen drive e gravador de CD ou DVD, é limitada aos Administradores, Gestores e profissionais autorizados pela Diretoria de Tecnologia.

6.4.2. Informações Protegidas

As Informações Protegidas serão consideradas informações de exclusiva propriedade da **PAY4FUN**, salvo disposição diversa. Em relação a tais informações, é expressamente proibida a sua reprodução, divulgação, publicação, transmissão, cessão ou facilitação de acesso a quaisquer terceiros, direta ou indiretamente, total ou parcialmente, salvo se autorizado por esta Política ou, previamente e por escrito, pelos representantes legais da **PAY4FUN**.

A qualquer tempo, caso seja solicitado pela **PAY4FUN**, ou em caso de término da relação do Colaborador com a **PAY4FUN**, independentemente da causa, o Colaborador restituirá à **PAY4FUN** todas as cópias, bancos de dados, reproduções ou adaptações que porventura tiver realizado. O Colaborador reconhece, ainda, que as obrigações e proibições previstas neste item permanecerão válidas durante toda a existência do vínculo do Colaborador com a **PAY4FUN** e mesmo após o término de tal vínculo, independentemente do motivo.

Qualquer Informação Protegida cuja divulgação seja exigida por Lei, ordem judicial, determinação de autoridades administrativas competentes ou acordos celebrados pela **PAY4FUN** com terceiros somente poderá ser divulgada após análise e validação da área Jurídica da **PAY4FUN**.

6.4.3. Classificação da Informação

Todas as Informações Protegidas da **PAY4FUN** devem ser classificadas de acordo com as categorias abaixo especificadas:

i. **Pública:** informações de caráter informativo, profissional ou que, em função da legislação vigente, são divulgadas a todo o público interno e externo, ou informação oficialmente liberada pela **PAY4FUN** para o público geral. A divulgação deste tipo de informação não tem potencial de causar problemas à **PAY4FUN**, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade, mediante a avaliação da Assessoria de Comunicação ou Unidade equivalente.

ii. **Interna:** informações pertencentes ou custodiadas pela **PAY4FUN**, que podem ser acessadas por todos os usuários, mediante autorização do respectivo proprietário.

iii. **Confidencial:** informação sigilosa que não deve ser divulgada. Seu uso é restrito a um determinado número de pessoas para desempenharem as suas atividades vinculadas à **PAY4FUN**, mediante autorização do respectivo proprietário. A sua divulgação não autorizada pode causar prejuízos para a **PAY4FUN** (tais como perda de clientes, danos financeiros, depreciação da imagem etc.), propiciando vantagens aos seus concorrentes e clientes, bem como revelando estratégias e resultados de negócios.

iv. **Secreta:** informação sigilosa, com acesso controlado e liberado apenas às pessoas nomeadas para tanto, que contém matérias de ordem vital para a **PAY4FUN** ou seus clientes, cuja divulgação, inexatidão e indisponibilidade (total ou parcial) podem causar danos reputacionais ou patrimoniais graves à **PAY4FUN**. Devem ser consideradas Informações Secretas as informações de saúde (p. ex., exames médicos de Colaboradores), os procedimentos de segurança, outras informações de notável criticidade para os negócios da **PAY4FUN** e outras informações protegidas por legislação específica.

6.4.4. Recomendações para classificação:

a) A classificação da informação deve ser realizada com base nas exigências de negócio da **PAY4FUN**, considerando as implicações que seu nível de criticidade trará para o negócio;

b) A classificação da informação deve ser feita para determinar as medidas de proteção necessárias, visando agilizar o processo de tratamento da informação e otimizar os custos com a sua proteção;

c) A classificação deve ser exercida quando a informação é gerada ou adquirida. Na hipótese de o proprietário (Data *Owner*) não ser o gerador da informação, este deve designar um substituto (Data *Steward*) e instruí-lo previamente sobre como classificá-la. Na ausência do proprietário da informação, o seu superior hierárquico será o responsável pela classificação;

d) O proprietário pode solicitar apoio técnico à equipe de Segurança da Informação caso existam dificuldades ou dúvidas acerca da classificação a ser dada a uma informação. Nestes casos, a informação deve ser considerada inicialmente como sendo, no mínimo, uma Informação Confidencial;

e) A informação deve receber tratamento adequado à sua classificação durante todo o seu ciclo de vida;

f) A inexistência de classificação explícita não exime o proprietário, os custodiantes e os usuários das suas responsabilidades quanto a avaliar o nível de sensibilidade da informação;

g) Um conjunto de ativos assume automaticamente a classificação mais restrita atribuída a um dos ativos que compõem o conjunto;

h) É expressamente proibida aos usuários a utilização, repasse e/ou divulgação indevida de toda e qualquer informação de propriedade da **PAY4FUN**.

i) Toda divulgação de informação deve ser autorizada. As informações a serem divulgadas interna ou externamente, devem ser cuidadosamente avaliadas quanto à importância e aos

possíveis impactos negativos nos negócios da **PAY4FUN**, especialmente as que tenham como destinatário o público externo;

j) Terceiros devem ser orientados e supervisionados quanto aos aspectos da segurança da informação. O contratante deve garantir que o compromisso de sigilo seja parte integrante do contrato; e

k) Informações impressas classificados como Internas ou Confidenciais não devem ser descartadas em lixo comum. Documentos impressos ou em mídia eletrônica, que contenham informação com esses níveis de classificação, devem ser destruídos antes de serem descartados, de forma que torne impossível a sua recuperação.

6.5. Segurança na operação e Padrões de configuração

6.5.1. Aplicação de *Hardening*

Todos os sistemas operacionais, sistemas de informação, aplicativos e ativos de rede devem ser implantados seguindo os padrões de configurações de segurança definidos pela área de Segurança da Informação.

Os padrões de configuração devem ser implementados pelo time de tecnologia e/ou seus respectivos provedores e administradores do ambiente tecnológico e liberados para ambiente produtivo pelo time de segurança da informação.

6.5.2. Desenvolvimento Seguro de *Software*

A **PAY4FUN** possuí como boa prática de arquitetura das aplicações à segregação em camadas de apresentação, aplicação e banco de dados com o objetivo de proporcionar a padronização de desenvolvimento e implantação de soluções.

Para proteger as aplicações web da **PAY4FUN** e para mitigar os riscos de apropriação das vulnerabilidades, devem ser adotadas as boas práticas de desenvolvimento seguro como, por exemplo, *OWASP*.

Todos os projetos devem envolver as áreas de Tecnologia para garantir a aderência dos recursos envolvidos em relação aos padrões tecnológicos e mitigar riscos de infringir os direitos de propriedade intelectual. Devem também envolver a área de Segurança da Informação para que todos os projetos tenham claramente definidos os requisitos de Segurança e sejam devidamente aplicados em todo o ciclo de vida do projeto.

Exceções a estas regras devem ser negociadas e aprovadas pela área de Segurança da Informação da **PAY4FUN**.

6.5.3. Segurança de rede e perímetro

A **PAY4FUN** mantém uma estrutura de segurança para a rede corporativa com o objetivo de garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações mediante a adoção dos seguintes mecanismos e controles:

a) Prevenção e detecção de intrusão;

b) Prevenção contra vazamento de informações; e

c) Segregação de ambientes.

As redes devem ser segregadas, minimamente distintas para Banco de Dados, Aplicações, Desenvolvimento, DMZ e área *Shared*. Somente usuários autenticados devem poder acessar os serviços de rede.

O acesso remoto deve ser feito somente através de métodos padrão autorizados pelo time de Segurança.

6.5.4. Gestão de mudanças

A **PAY4FUN** segue um processo rígido de Gerenciamento de Mudanças para garantir a integridade, performance e disponibilidade do ambiente produtivo.

O ambiente tecnológico prevê minimamente a segregação em: Desenvolvimento, Homologação, Pré-produção e Produção.

Informações sensíveis não são utilizadas nos ambientes de desenvolvimento e homologação. Em caso de necessidade, estes dados são tratados para que não contenham informações reais de clientes ou parceiros e aprovados pela área de segurança da informação.

6.5.5. Criptografia

O uso efetivo e adequado de um sistema de criptografia deve ser estabelecido com o intuito de assegurar a confidencialidade, autenticidade e integridade das informações.

Todos os sistemas, controles, ferramentas, técnicas ou soluções de criptografia devem ser aprovados pela área de Segurança da Informação. A área de tecnologia deve executar revisões de criptografia e gerenciamento de chaves periodicamente, ou mediante alterações significativas de tecnologias.

Os proprietários do sistema são responsáveis por estabelecer e manter uma descrição documentada da arquitetura criptográfica, incluindo:

a) Detalhes de algoritmos, protocolos e chaves, incluindo a força das chaves e a data de validade;

b) Descrição do uso da chave para cada chave criptográfica; e

c) Inventário de qualquer HSM (Hardware Security Modules) e outros dispositivos criptográficos seguros usados para gerenciamento de chaves.

Todas as Informações Protegidas da **PAY4FUN** devem ser classificadas de acordo com as categorias abaixo especificadas:

6.6. Teste de Segurança

A **PAY4FUN** realiza testes de penetração (*Pentests*) periódicos com o objetivo de garantir e fortalecer a segurança no ambiente corporativo e aplicacional da **PAY4FUN** com o fim de:

a) Validar a atual infraestrutura e aplicação em relação a segurança cibernética;

b) Identificar possíveis vulnerabilidades no ambiente operacional;

c) Definir planos de ação a fim de corrigir de forma preventiva e fortalecer a segurança na operação.

6.7. Gestão de Incidentes de Segurança

Caso o Colaborador tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta Política ou coloque em risco a segurança das informações da **PAY4FUN**, ele deverá imediatamente comunicar a equipe e Diretoria para o gerenciamento dos incidentes de Segurança Cibernética, que irá apurar as causas e os efeitos do incidente ocorrido, para então tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente às autoridades competentes, de modo a:

a) Garantir a gestão das vulnerabilidades a fim de reduzir a exposição aos riscos mitigando a ocorrência de incidentes.

b) Gestão dos incidentes reais, garantindo o registro que contenha a ação de contenção, notificação, a análise da causa raiz, a gestão do plano de ação (definição, planejamento, execução, teste/ validação, monitoramento e controle) e coleta de evidências.

c) Todos os Colaboradores devem reportar imediatamente quaisquer incidentes que violem a segurança e/ou os termos desta política, para que estes possam ser classificados, analisados, monitorados, comunicados e devidamente tratados conforme seu nível de criticidade, formalizando uma denúncia para a Área de Segurança da Informação.

d) Na ocorrência de incidente envolvendo dados pessoais, a área de Segurança da Informação deverá acionar, por sua vez, o responsável pelos dados, para que este tome todas as providências e procedimentos previstos no Plano de Resposta a Incidentes de Segurança da Informação da **PAY4FUN**.

e) A área responsável emitirá relatório dos registros dos incidentes para apresentação e formalização junto a Diretoria ou Conselho de administração, para que seja registrado em ata.

6.8. *Cloud Computing*

Toda empresa contratada para a prestação do serviço de *Cloud Computing* deve disponibilizar a modalidade *Private Cloud* (nuvem Privada), a fim de que possa assegurar a administração de itens como gerenciamento de redes, configurações do provedor, tecnologias de autenticação e autorização e criptografia dos dados transmitidos e armazenados possa ser realizada e/ou definida pela **PAY4FUN**.

A avaliação dos fornecedores por parte da **PAY4FUN** leva em consideração:

a) Garantir a segregação dos dados da contratante e oferecer total apoio em casos de investigação solicitado pela contratante, com prazos de retorno definidos em ANS.

b) A avaliação da capacidade em assegurar o cumprimento da legislação e regulamentação em vigor.

c) Se a região onde o fornecedor irá disponibilizar os serviços possui convênio para troca de informações com o Banco Central e as Autoridades Supervisoras, assegurando que não haverá restrição ou impedimento para o acesso aos dados e informações tanto pela **PAY4FUN** como para os órgãos reguladores.

d) Possuir capacidade de manter operação dos serviços contratados em caso de crise operacional (Continuidade).

Deve haver no contrato itens que garantam:

a) Integridade, confidencialidade, disponibilidade, autenticidade e não-repudio das informações manipuladas, informando sobre a adoção das medidas de segurança tomadas.

b) Plano de contingência dos dados (incluindo recuperação de dados e administração de incidentes).

c) Definição de ANS (Acordos de Nível de Serviço) e ANO (Acordo de Nível Operacional).

d) Gestão dos acessos conforme política de gestão de acesso **PAY4FUN**, visando a proteção dos dados e das informações dos clientes.

e) A forma como o prestador realiza a segregação dos dados e ambiente do serviço prestado.

f) Registro dos logs de acessos e logs de transações do sistema.

g) Informação das zonas, regiões e países onde o serviço poderá ser prestado.

h) Acesso aos dados da **PAY4FUN** a serem processados ou armazenados pelo prestador de serviço.

i) Acesso da **PAY4FUN** aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados.

j) Provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados.

k) Controles que mitiguem eventuais vulnerabilidades de novas versões de sistemas/ aplicativos na web.

l) Garantia de transferência dos dados ao novo prestador em caso de extinção do contrato.

m) Garantia de exclusão dos dados e caso de extinção do contrato.

n) Informação sobre a terceirização de algum serviço contratado.

o) Permissão de acesso do Banco Central aos contratos e acordos firmados para a prestação de serviços, aos dados, as copias de segurança bem como aos códigos de acesso aos dados e informações.

p) Prever a notificação prévia sobre a intenção de a empresa contratada interromper a prestação dos serviços com pelo menos 30 (trinta) dias de antecedência, com possibilidade de prorrogação de mais 30 (trinta) dias.

6.8.1. Segurança Física

A **PAY4FUN** define como obrigatório que todos os colaboradores, estagiários e prestadores de serviço devem possuir e usar de forma visível crachá de identificação.

6.8.2. Áreas Seguras

Os perímetros de segurança e controles físicos para cada perímetro devem ser definidos e usados para proteger áreas que contenham informações sensíveis ou críticas ou recursos de processamento de informações para evitar riscos de acesso físico não autorizado, danos e interferência nas instalações de processamento de informações e informações da organização.

Ameaças externas e ambientais devem ser consideradas como parte da análise de risco para definir os controles físicos que devem ser aplicados.

6.8.3 Equipamentos

Equipamentos de instalações de processamento devem ser protegidos por um conjunto formal de controles físicos para reduzir os riscos de ameaças e perigos ambientais e oportunidades de acesso não autorizado, causando perda, dano, roubo ou comprometimento de ativos e interrupção das operações da organização.

6.9. Gestão da Continuidade de Negócios

A **PAY4FUN** mantém um Plano de Continuidade de Negócios documentado, testado e revisado de forma periódica, a fim de garantir a operação e continuidade dos seus processos críticos.

Este programa segue os seguintes requisitos mínimos:

a) Definição da criticidade dos processos de negócio da **PAY4FUN** através da identificação dos impactos causados pela interrupção das atividades (*Business Impact Analysis*).

b) Definição da estratégia de recuperação a ser utilizada caso ocorra um incidente.

c) Gerenciamento de Crise para incidentes adversos que interrompam um processo crítico.

d) Planejamento da continuidade e da recuperação das operações e sistemas após uma interrupção.

e) Estabelecimento de procedimentos de retorno à normalidade, quando aplicável.

f) Incorporar a gestão da continuidade de negócio ao desenvolvimento de novos produtos e serviços críticos e ao processo de gerência de mudanças para produtos e serviços existentes.

g) Aumentar o poder de recuperação da organização contra o rompimento ou interrupção de sua habilidade de fornecer seus produtos e serviços.

h) Prover a organização de uma metodologia para a elaboração de planos de continuidade de negócios que possibilite o restabelecimento da sua habilidade de fornecer seus produtos e serviços críticos.

i) Fixar normas e padrões de continuidade, compondo assim, um programa completo e consistente para a organização, devendo ser aceito e seguido inclusive pelas empresas prestadoras de serviço.

6.10. Segurança para Recursos Humanos

Um programa de conscientização, avaliação, educação e treinamento com o objetivo de disseminar a cultura de segurança da informação na **PAY4FUN**, é essencial para garantir os objetivos desta Política.

Todos os Colaboradores e Terceiros contratados da **PAY4FUN** devem concluir o treinamento em Segurança da Informação e participarem do programa de educação contínua.

Treinamentos adicionais, incluindo treinamentos especializados em segurança, devem ser fornecidos conforme necessário a função e atribuições específicas de cada Colaborador.

Esta Política, juntamente com outras normas e padrões internos de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos Colaboradores, conjuntamente pelas áreas de Recursos Humanos e Governança em Segurança da Informação.

6.11. Gestão de Terceiros, Parceiros e Fornecedores

Em todos os contratos de prestação de serviços que envolvam o processamento, a manipulação, o acesso ou a visualização de dados protegidos da **PAY4FUN** devem ser adicionadas as cláusulas de segurança de informação, conforme seja definido pela área de Segurança de Informação, dependendo do tipo e condições do serviço prestado.

As empresas prestadoras de serviços (entidade patronal do colaborador) devem assegurar que os colaboradores externos que acessam as dependências físicas da **PAY4FUN**, a rede corporativa e/ou os sistemas de informação da organização conheçam e respeitem as normas de segurança da **PAY4FUN.**

Todas as empresas contratadas devem possuir uma permissão de segurança para a prestação de serviço que é renovada periodicamente conforme a duração do contrato.

6.12. Relatório Anual e Documentação BACEN

Em atendimento à Resolução nº 4.893 do BACEN, anualmente a **PAY4FUN** deverá emitir um relatório sobre a implementação do plano de ação de respostas a incidentes, com data base de 31 de dezembro do ano anterior ao relatório, contendo:

a) A efetividade da implementação das ações a serem desenvolvidas pela **PAY4FUN** para adequar suas estruturas aos princípios e às diretrizes desta Política;

b) O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

c) Os incidentes relevantes ocorridos no período; e

d) Resultado dos testes de continuidade de negócios.

Ainda, devem ficar à disposição do BACEN pelo prazo de 05 (cinco) anos:

a) A presente Política, em sua versão mais atualizada;

b) Ata da Reunião do Conselho de Administração que aprovou a Política;

c) Documento relativo ao plano de ação e de resposta a incidentes aprovado pelo Conselho ou Diretoria;

d) Documentação sobre os procedimentos adotados em casos de contratação de serviços relevantes de processamento e armazenamento em nuvem;

e) Documentação que comprove a adoção dos requisitos relativos à contratação de serviços relevantes de processamento e armazenamento em nuvem prestados no exterior;

f) Contratos de prestação de serviços relevantes de processamento e armazenamento em nuvem;

g) Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade das diretrizes contidas nesta Política.

7. Conscientização e Treinamento

A **PAY4FUN** mantém um programa de conscientização periódico para o público-alvo dessa Política, realizado através de comunicações recorrentes, em linha com o Programa de *Compliance* da empresa.

8. Violações e Comunicação ao Canal de Denúncia

É responsabilidade de todos os colaboradores comunicarem quaisquer violações ou suspeitas de violações aos preceitos apresentados nesta Política.

As comunicações de violações e suspeitas de violação, identificadas ou anônimas, podem ser realizadas através dos seguintes meios:

a) Site: https://forms.office.com/r/dvkA45uFU5
b) E-mail: canaldeetica@p4f.com

A **PAY4FUN** não permite ou tolera qualquer tipo de retaliação contra qualquer pessoa que apresente uma denúncia de boa-fé ou queixa de violação desta Política ou da legislação e normas vigentes.

A **PAY4FUN**, encoraja e respalda, ilimitadamente, o oferecimento de denúncia sobre qualquer ato ou omissão que possa configurar transgressão ao Código de Ética e Conduta ou a Legislação e normas em vigor, comprometendo-se a apurar punir e/ou informar às autoridades competentes, no maior rigor possível, quaisquer desvios que forem informados.

Á denúncia sobre a prática de atos ou omissões que, no juízo e melhor conhecimento do denunciante, possam constituir infração ao Código de Ética e Conduta ou a legislação e normas em vigor, deverá ser feita preferencialmente por meio do Canal de Denúncias, sem exclusão de qualquer meio ou canal disponível ao denunciante ante a impossibilidade de acessar o referido canal.

Todas as pessoas indicadas no item 2 da presente Política devem, sempre que tiverem indícios ou conhecimento da prática de ato ou omissão lesivos a legislação em vigor, registrar denúncia no Canal de Denúncias ou formalizar da melhor maneira possível, toda e qualquer suspeita ou evidência da prática vedada por essa Política, pela legislação e normas.

Tais denúncias podem ser recebidas de forma anônima pelo canal de denúncias e serão tratadas de forma absolutamente sigilosa. A administração do recebimento de denúncias e a apuração dos registros, são inicialmente geridos internamente na **PAY4FUN**, sem prejuízo da notificação e colaboração com demais autoridades competentes, conforme necessário.

É desejável que todas as denúncias registradas no Canal de Denúncias, sejam instruídas com os nomes e/ou informações pessoais, se houver, de todas as pessoas que teriam supostamente participado do ato lesivo, que contribuam para a apuração e responsabilização dos envolvidos no ato ou omissão.

Em caso de dúvidas se eventual fato constitui ou não constitui ato lesivo, o destinatário desta Política pode formular consulta ou denúncia ao Canal de Denúncias, conforme o caso, para avaliação e esclarecimentos.

9. Gestão de Consequências

A **PAY4FUN**, buscará, sempre que possível e dentro da melhor diligência, individualizar e particularizar as condutas que possam ser enquadradas como descumprimento das normas previstas nesta Política, informando e colaborando com as autoridades competentes para a completa apuração e responsabilização dos indivíduos que praticarem.

As responsabilidades dos destinatários desta Política também serão apuradas, e caso confirmadas, estes responderão pessoalmente pelos crimes cometidos, nos termos da Lei, bem como pela eventual reparação de dados sofridos pela **PAY4FUN**, em decorrência da prática de tais atos.

Serão responsabilizados os destinatários desta Política que tiverem praticado o ato lesivo e aqueles que tiverem conhecimento de sua prática, mas que tenham se omitido.

Sem prejuízo, das penalidades legais indicadas acima e aquelas que decorrem do contrato de trabalho e/ou prestação de serviços, também o colaborador ou membro dos destinatários desta Política responderá pelos prejuízos eventualmente causados à **PAY4FUN**, e/ou a terceiros, inclusive à Administração Pública.

Cabe ressaltar que todas as penalidades legais se aplicam também a Diretoria Executiva e aos membros do Conselho de Administração da **PAY4FUN**. Serão implementadas tempestivamente as ações de remediação para mitigar os riscos reativamente, evitando novas infrações. Adicionalmente, são estabelecidos procedimentos que asseguram a pronta interrupção de irregularidades e infrações nos processos, através dos processos descritos nesta Política.

10. Divulgação

Será dado conhecimento da versão atualizada da Política a todos os colaboradores com periodicidade estabelecida conforme Política de Elaboração e Publicação de Documentos Institucionais, podendo também ser revista quando necessária.

11. Responsabilidades

- **Administradores e Colaboradores:** observar e zelar pelo cumprimento da presente Política, e quando assim se fizer necessário, acionar a área de *Compliance* para consulta sobre situações que envolvam conflito com está política ou mediante a ocorrência de situações nelas descritas.
- **Diretoria de Governança, Riscos e *Compliance***: cumprir as diretrizes estabelecidas nesta Política, mantê-la atualizada para garantir que quaisquer alterações no direcionamento da **PAY4FUN** sejam incorporadas à mesma e esclarecer dúvidas relativas ao seu conteúdo e à sua aplicação, bem como promover a realização de treinamentos e comunicações contínuas.
- **Conselho de Administração e Diretoria Executiva:** apoiar e assegurar a disseminação de uma cultura de integridade e ética.

12. Exceções

As exceções a esta Política devem ser analisadas e aprovadas pela Diretoria Executiva e pelo Conselho de Administração.

13. Vigência

A vigência dessa Política ocorrerá a partir da data de aprovação e publicação, conforme o controle de histórico de versões.

Pay4Fun Instituição de Pagamento S.A.

Diretoria de Tecnologia e Segurança da Informação