POLÍTICA DE
SEGURANÇA DA INFORMAÇÃO

DA

UTILITY GESTORA DE RECURSOS LTDA.

2022

ÍNDICE GERAL

1. INTRODUÇÃO

A Política de Segurança da Informação ("Política") foi criada para estabelecer os princípios, conceitos e valores que deverão pautar a segurança da informação da Utility Gestora de Recursos Ltda. ("Gestora") na sua atuação interna e com o mercado, assim como suas relações com os diversos públicos.

O seu objetivo é assegurar que as informações da organização estão sendo tratadas de forma adequada para a garantia dos critérios de Confidencialidade, Integridade e Disponibilidade, conforme abaixo definidos.

Além disso, descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

2. APLICAÇÃO

Os princípios e regras desta Política devem ser observados por todos os sócios, diretores, empregados, *trainees*, estagiários, colaboradores e prestadores de serviços que venham, de maneira direta ou indireta, trabalhar para a Gestora (conjuntamente referidos como "Colaboradores", e individual e indistintamente como "Colaborador").

3. DISPOSIÇÕES GERAIS

3.1 Disposições Iniciais

Esta Política destina-se aos Colaboradores da Gestora e deverá ser observado por todos.

A segurança da informação ("Segurança da Informação") é aqui caracterizada pela preservação dos seguintes princípios:

a) **Confidencialidade:** é a garantia de que a informação é acessível somente por pessoas com acesso autorizado;

b) **Integridade:** é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade: é a garantia de que os usuários autorizados obtenham acesso a informações e aos ativos correspondentes, sempre que necessário.

Para tornar a gestão da Segurança da Informação efetiva, a Diretoria de *Compliance*, Risco e PLDFT da Gestora coordena as ações necessárias para a implantação do modelo de gestão de Segurança da Informação e avalia periodicamente a Segurança da Informação, por meio da análise de indicadores, bem como recomenda ações corretivas e preventivas.

A gestão da Segurança da Informação compreende as seguintes atividades:

a) Identificação das necessidades específicas de Segurança da Informação e proposta de implementações necessárias;

b) Elaboração dos documentos necessários à Segurança da Informação;

c) Elaboração e manutenção dos indicadores de Segurança da Informação;

d) Elaboração dos programas de treinamento e de conscientização em Segurança da Informação; e

e) Análise dos incidentes de segurança da informação e recomendações de correções necessárias.

Compete à Diretora de *Compliance*, Risco e PLDFT da Gestora a verificação do cumprimento da Política de Segurança da Informação e recomendação das ações corretivas necessárias. Assim, a Área de *Compliance* contará com a solução de controle de navegação nas páginas da rede mundial de computadores por meio da implantação de um *software* tipo "Winconnection" que, através de *firewall* configurável, será possível ter o controle de todos os acessos realizados pelos Colaboradores e Diretores da Gestora na *web*. Ou seja, será possível (i) a realização da análise do tráfego de informações pelos Diretores e Colaboradores, (ii) o veto de acesso a determinados canais de navegação (ex.: redes sociais e sites com conteúdo impróprio) e (iii) a obtenção de relatórios periódicos da navegação realizada por tais membros ligados à Gestora, de modo a auxiliar na constatação pela Área de *Compliance* de eventuais acessos irregulares e em desacordo com a presente Política.

Esta Política deve ser revisada na ocorrência de alterações materiais nas atividades, infraestrutura ou operações da Gestora. Entretanto, uma revisão mínima deve ocorrer a cada 2 (dois) anos com o intuito de verificar a eventual necessidade de produzir uma versão atualizada, a ser aprovada pela Diretoria de *Compliance*, Risco e PLDFT da Gestora.

3.2 Diretrizes

As seguintes diretrizes integram a Política de Segurança da Informação da Gestora:

a) **A informação pertence à organização:** Toda informação gerada, adquirida ou processada pela Gestora é de sua exclusiva propriedade. Deve-se obter prévia autorização da gerência imediata para a saída de documentos em meios físicos ou eletrônicos da instituição, bem como *notebooks* ou qualquer outro equipamento eletrônico que contenha informações críticas da Gestora.

b) **Segurança orientada ao negócio:** As ações de segurança serão planejadas e aplicadas de acordo com a avaliação dos riscos para o negócio da Gestora. A disponibilidade, uso, acesso e proteção das informações e seus recursos devem ocorrer sempre de forma a preservar a continuidade e a competitividade do negócio da Gestora.

c) **Propriedade da informação:** Toda informação armazenada nas dependências da Gestora é considerada patrimônio da Gestora, sendo usada exclusivamente em seu interesse e devendo estar adequadamente protegida, em qualquer que seja o meio de armazenamento, contra violação, alteração, destruição, acesso não autorizado e divulgação indevida. Os responsáveis por seu armazenamento, guarda e manuseio responderão por sua integridade, uso ou divulgação.

d) **Classificação da informação:** Cada Colaborador terá acesso às informações necessárias ao seu trabalho, respeitando os conceitos de Confidencialidade, Integridade e Disponibilidade.

e) **Responsabilidade:** Cada Colaborador é responsável pela segurança dos ativos e das informações que estejam sob sua custódia e por todos os atos executados com sua identificação de acesso. Qualquer que seja sua forma, a identificação será pessoal, intransferível e permitirá de maneira clara e indiscutível o seu reconhecimento.

f) **Menor privilégio:** O Colaborador terá acesso somente a ativos de informação que componham o imprescindível para o total desenvolvimento do seu trabalho.

g) **Cultura de segurança:** O conteúdo desta Política e das demais normas será amplamente divulgado na Gestora.

h) **Recursos computacionais:** Os recursos computacionais disponibilizados pela Gestora devem ser utilizados apenas para o desenvolvimento de

atividades relacionadas ao negócio da Gestora, sendo vedada a sua utilização para qualquer outra finalidade.

i) **Treinamento em Segurança da Informação:** Os Colaboradores devem conhecer e respeitar a Política de Segurança da Informação da organização. Deverá ser realizado, no mínimo anualmente, um programa de educação e treinamento para garantir a disseminação das informações desta Política, bem como para assegurar o conhecimento e a compreensão das políticas e procedimentos de manutenção do sigilo e segregação de informações disponíveis em vigor, e da conscientização das consequências da não observância de referidas normas e procedimentos.

4. SEGURANÇA CIBERNÉTICA E TESTES PERIÓDICOS

As medidas de Segurança da Informação têm por finalidade minimizar as ameaças aos negócios da Gestora e às disposições desta Política, buscando, principal, mas não exclusivamente, a proteção da Confidencialidade das informações.

As instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação. Todos os equipamentos da rede deverão estar acomodados em um local reservado, de acesso restrito. As estações de trabalho serão flexíveis, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A presente Política leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora. A coordenação direta das atividades relacionadas à presente Política ficará a cargo da Diretora de *Compliance*, Risco e PLDFT da Gestora, que será a responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

4.1 Identificação de Riscos

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

a) **Dados e Informações**: as informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), incluindo informações a respeito de investidores,

clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

b) Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

c) Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e

d) Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

a) Malware: softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

b) Engenharia Social: métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e Acesso Pessoal);

c) Ataques de DDoS (*distributed denial of services*) e *Botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

d) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

4.2 Ações de Prevenção e Proteção

Após a identificação dos riscos, a Gestora adota as medidas a seguir descritas para proteger suas informações e sistemas.

I. Regra Geral de Conduta:

A Gestora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise. Deverá ser depreendida especial atenção ao acesso às Informações Confidenciais por Colaboradores nos casos de mudança de atividade dentro da Gestora ou desligamento.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores da Gestora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação.

Em caso de dúvida a Área de *Compliance* deve ser acionada previamente à revelação. Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Gestora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente. Ademais, fica terminantemente proibido que os Colaboradores discutam ou acessem remotamente Informações Confidenciais.

A obtenção de cópias de arquivos de qualquer extensão, de forma gratuita ou remunerada, em computadores da Gestora, originados em máquina remota ("*Download*") depende de autorização expressa e prévia da área responsável e deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes. Em hipótese alguma será permitida a cópia de softwares que não respeitem direitos de propriedade

intelectual, bem como aqueles que firam os bons costumes ou que promovam discriminação de qualquer tipo ou espécie.

Desta forma, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora.

A Gestora não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar *pen-drivers*, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

A Gestora disponibiliza endereço eletrônico a todos os Colaboradores, sendo tal endereço eletrônico destinado para fins corporativos ("E-mail Corporativo"). A utilização do endereço eletrônico deverá ser feita para questões relacionadas às atividades profissionais e relacionadas à finalidade da Gestora, sendo, no entanto, permitida a utilização pessoal de forma moderada.

Os E-mails Corporativos enviados ou recebidos, bem como seus respectivos anexos e os arquivos constantes nos computadores de propriedade da Gestora poderão ser monitorados pela própria Gestora.

Ante a possibilidade de acesso aos e-mails e arquivos, os Colaboradores da Gestora não devem manter nos computadores de propriedade da Gestora quaisquer dados ou informações particulares que pretendam que não venham a ser conhecidas e/ou acessadas pela Gestora. O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Gestora.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Gestora.

Não obstante, é permitida a utilização apenas do programa de conversas eletrônicas (*chats*) disponibilizado pela própria Gestora, sendo permitido o seu uso para fins pessoais de forma moderada e dentro dos princípios e regras expostos no presente Código. Toda a utilização apenas do programa de conversas eletrônicas poderá também ser monitorada pela Gestora.

A navegação pela rede mundial de computadores ("Internet") deverá ser feita observando os fins sociais da Gestora, sendo permitido o seu uso para fins pessoais de forma moderada, como por exemplo, mas não se limitando a compras de objetos de uso pessoal, passagens e reservas de hotéis.

A Gestora se reserva ao direito de bloquear sites da Internet inapropriados ou que firam a moral e os bons costumes. Toda a navegação na Internet poderá ser monitorada pela Gestora. A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

II. Acesso Escalonado do Sistema:

O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pela Diretora de *Compliance*, Risco e PLDFT da Gestora e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A Gestora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Gestora necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gestora em caso de violação

III. Senha e *Login*:

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via *webmail*, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas irão expirar a cada 6 (seis) meses, sendo obrigatória a alteração, conforme aviso fornecido pelo responsável pela área de informática.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

IV. Uso de Equipamentos e Sistemas:

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, sendo permitido o seu uso para fins pessoais de forma moderada.

O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional. Nesse sentido, as ligações pessoais interurbanas e para celulares devem durar o tempo estritamente necessário e as ligações internacionais pessoais deverão ser prontamente reembolsadas à Gestora.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar a Diretora de *Compliance*, Risco e PLDFT.

V. Acesso Remoto:

A Gestora permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, no que se refere ao acesso ao e-mail, sendo que a rede e diretório conforme requisição por estes e autorização pela Diretora de *Compliance*, Risco e PLDFT.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra *malware*/antivírus nos dispositivos remotos, (iii) relatar à Diretora de *Compliance*, Risco e PLDFT qualquer violação ou ameaça de segurança

cibernética ou outro incidente que possa afetar informações da Gestora e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

VI. Controle de Acesso:

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos Diretores da Gestora.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, sendo permitido o seu uso para fins pessoais de forma moderada, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

VII. *Firewall*, *Software*, Varreduras e *Backup*:

A Gestora utiliza um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. A Diretora de *Compliance*, Risco e PLDFT é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A Gestora mantém proteção atualizada contra *malware* nos seus dispositivos e *software* antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da Gestora (por exemplo, vírus, *worms*, *spyware*). Serão conduzidas varreduras mensais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Gestora.

A Gestora utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e *patches*. A Diretora de *Compliance*, Risco e PLDFT é responsável por *patches* regulares nos sistemas da Gestora.

A Gestora mantém e testa regularmente medidas de *backup* consideradas apropriadas pela Diretora de *Compliance*, Risco e PLDFT. As informações da Gestora são atualmente objeto de *backup* diário com o uso de computação na nuvem.

4.3 Monitoramento e Testes Periódicos

A Diretora de *Compliance*, Risco e PLDFT (ou pessoa por ele incumbida) adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para

detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, semestral:

a) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, *fotologs*, *webmails*, entre outros, bem como os e-mails enviados e recebidos; e

b) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a *desktops*, pastas e sistemas, em especial para os mantidos em meio eletrônico, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

A Diretora de *Compliance*, Risco e PLDFT poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

Os testes periódicos realizados devem sempre possibilitar a identificar dos detentores dessas informações para responsabilização, em caso de vazamento, com especial enfoque em segregação lógica, testes de penetração, resposta a eventos de vazamento de dados, rastreabilidade dos *logs* de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela Gestora, em especial os confidenciais.

4.4 Plano de Identificação e Resposta

I. Identificação de Suspeitas:

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada à Diretora de *Compliance*, Risco e PLDFT prontamente.

A Diretora de *Compliance*, Risco e PLDFT determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados. Ademais, a Diretora de *Compliance*, Risco e PLDFT determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

II. Procedimentos de Resposta:

A Diretora de *Compliance*, Risco e PLDFT responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

a) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

b) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

c) Determinação dos papéis e responsabilidades do pessoal apropriado;

d) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

e) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

f) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da Gestora, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

g) Determinação do responsável (ou seja, a Gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo da Diretora de *Compliance*, Risco e PLDFT, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

4.5 Arquivamento de Informações:

De acordo com o disposto nesta Política, os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 18 da Resolução CVM nº 21.

5. DISPOSIÇÕES FINAIS

Todos os Colaboradores receberão esta Política, devendo assinar um termo de adesão na forma do Anexo I, confirmando sua ciência e compreensão das políticas e procedimentos aqui instituídos. Sempre que as políticas e procedimentos forem atualizados, uma nova versão deve ser encaminhada para todos. Uma versão eletrônica atualizada do documento será disponibilizada no diretório da rede da Gestora.

5.1 Consequências do Descumprimento

O descumprimento das políticas e procedimentos estabelecidos na presente Política implicará nas seguintes medidas, segundo o entendimento da Diretora de *Compliance,* Risco e PLDFT (ou, caso a Diretora de *Compliance*, Risco e PLDFT esteja envolvido, de qualquer outro Diretor):

(i) demissão dos Colaboradores envolvidos no descumprimento em questão, incluindo aqueles que tinham conhecimento do descumprimento em questão e foram omissos em reportá-lo a seus superiores; e/ou

(ii) responsabilização dos Colaboradores envolvidos no descumprimento por eventuais danos que a Gestora venha a sofrer em razão de sua conduta.

A aplicação das penalidades acima não isenta, dispensa ou atenua a responsabilidade civil, administrativa e/ou criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos resultantes da infração da legislação em vigor e das políticas e procedimentos estabelecidos nesta Política.

ANEXO I – MODELO DE TERMO DE ADESÃO

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UTILITY GESTORA DE RECURSOS LTDA.

Eu, [nome], [qualificação], declaro que tomei conhecimento dos termos e condições do Política de Segurança da Informação da Utility Gestora de Recursos Ltda. ("Política" e "Gestora", respectivamente), tendo, ao final, recebido uma cópia da referida Política.

Subscrevendo o presente formalizo a minha adesão à Política, comprometendo-me a cumprir com todos os seus termos e condições, adotando, nas situações de dúvida, a posição mais conservadora possível, submetendo as dúvidas a respeito do cumprimento da Política e da legislação e regulamentação em vigor à Diretora de *Compliance*, Risco e PLDFT.

São Paulo, [=] de [=] de [=].

_____

[=]

Testemunhas:

1. _____	2. _____
Nome:	Nome:
RG:	RG:
CPF:	CPF: