POLÍTICA DA SEGURANÇA DA INFORMAÇÃO, TECNOLOGIA, COMUNICAÇÃO E PROTEÇÃO DE DADOS

Julho 2022

Versão - 3

Data de Vigência: 05/07/2022

1 OBJETIVO

Esta Política da Segurança da Informação, Tecnologia, Comunicação e Proteção de Dados ("Política") tem o objetivo de estabelecer diretrizes gerais para o uso dos Recursos de Tecnologia e das Informações da EOS Investimentos Ltda. ("EOS") e fornecer procedimentos mínimos para proteger as informações e a imagem da empresa em condições de crise, de perda de ativos e outras situações adversas.

Em atenção aos dispositivos da Instrução CVM n.º 21/2021, do Código ANBIMA de Administração de Recursos de Terceiros e da Lei 13.709, de agosto de 2018 ("LGPD"), a EOS procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

Sendo assim, nenhuma Informação Confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da EOS, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a EOS, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Compliance.

2 ABRANGÊNCIA E APLICABILIDADE

Esta Política aplica-se a todos os Colaboradores da EOS, ou seja, seus funcionários, estagiários, trainees e sócios, no desempenho de suas atividades funcionais, funcionários terceirizados, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da EOS, ou que acesse informações a ela pertencentes.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela EOS, sendo de responsabilidade individual e coletiva o seu cumprimento. A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos ativos disponibilizados pela EOS ao Colaborador.

Qualquer informação sobre a EOS, ou de qualquer natureza relativa as atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Compliance.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de Compliance da EOS, sob a direção do Diretor de Compliance da instituição.

Ademais, para implementação e monitoramento contínuo da presente Política, a EOS conta com o suporte e assessoria da empresa terceirizada de TI.

3 DEFINIÇÃO

Recurso de Informação: Toda e qualquer informação inerente às atividades de negócio e aos clientes da EOS que possam ser de conhecimento dos Colaboradores da EOS e de seus parceiros.

Recursos de Tecnologia: Todo recurso eletrônico utilizado para transportar, modificar, gravar ou fazer qualquer tipo de manipulação em dados e informações inerentes aos processos de negócio da EOS.

Recursos de Comunicação: Todo recurso que possa ser utilizado para receber, transferir, enviar qualquer tipo de dado ou informação (por voz, escrita, meio digital, etc.).

Recursos de RITC: Recurso de Informação, Recurso de Tecnologia e Recurso de Comunicação, quando mencionados em conjunto.

4 POLÍTICA DE USO RITC

Entendem-se como Recursos de RITC (Informação, Tecnologia e Comunicação) todos os instrumentos utilizados nas atividades de trabalho dos Colaboradores, funcionários terceirizados e parceiros que podem ser ou não de propriedade da EOS, e que possuem valores ou informações relevantes para as atividades de negócio da EOS.

A política de uso de Recursos de RITC visa disciplinar o uso de tais recursos na EOS, bem como, orientar para que os riscos de falhas nos Recursos de RITC sejam minimizados e regular a responsabilidade decorrente do seu uso.

A presente Política consiste em assegurar as informações da EOS, visando garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações, de forma que nenhuma Informação Confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da EOS, que não necessitem, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Ademais, a presente Política também tem o objetivo de cumprir com o art. 24, incisos I, II e III, da Instrução CVM n.º 21/2021, assegurando o controle das Informações Confidenciais a quem tenha acesso, bem como dispor de suas regras de cibersegurança, em linha com Guia de Cibersegurança da ANBIMA, datado de 2021.

5 NORMAS E CONCEITOS BÁSICOS

(i) Identificação de Riscos:

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em

termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- *Malware* – *softwares* desenvolvidos para corromper computadores e redes:
    - Vírus: *software* que causa danos a máquina, rede, *softwares* e banco de dados;
    - Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
    - *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
    - *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia Social – métodos de manipulação para obter Informações Confidenciais, como senhas, dados pessoais e número de cartão de crédito:
    - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
    - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter Informações Confidenciais;
    - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter Informações Confidenciais;
    - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter Informações Confidenciais;
    - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de DDoS (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a EOS pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

(ii) Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para a EOS, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para EOS, em caso de incidente de segurança.

Deste modo, a EOS segrega as informações geradas pela Gestora, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:

- Quaisquer informações e/ou dados que a Gestora teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag*:

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag*:

- Todas as Informações Confidenciais, a saber:
  - know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela EOS;
  - operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela EOS; e
  - estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da EOS e/ou de seus sócios e clientes.

A partir da definição acima, a EOS se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag*, *Yellow Flag* e *Green Flag*.

(iii) Disponibilização e Normas de Uso

Os Recursos de RITC são fundamentais para as atividades da EOS e seu uso incorreto poderá trazer significativos prejuízos para a empresa.

Todos os computadores disponibilizados para os Colaboradores da EOS têm por objetivo o desempenho das atividades profissionais na EOS, não devendo ser utilizado para quaisquer outros fins. Todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela área responsável, mediante aprovação do Diretor de Risco e Compliance.

A disponibilização e uso dos computadores da EOS respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de Compliance autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;

- O usuário é responsável pelo recurso em uso (RITC), no entanto a instalação de programas nos dispositivos deve ser realizada sob a consulta do Diretor de Compliance, bem como é responsabilidade do usuário assegurar que estes programas são de origem confiável e não causarão danos a estes dispositivos, sendo de responsabilidade do usuário qualquer aplicativo instalado, executado ou em execução durante o período de uso dos dispositivos;

- Toda e qualquer alteração realizada em um computador ou outro dispositivo fornecido pela EOS será de responsabilidade do usuário/dono deste dispositivo.

- Todos os equipamentos, *softwares* e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão e aprovação do Diretor de Compliance;

- O Diretor de Compliance autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;

- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável, mediante supervisão e aprovação do Diretor de Compliance;

- Os dispositivos devem ser protegidos por senha individual, e fica proibido o compartilhamento da senha de acesso. Usuários que utilizam dispositivos pessoais para acessar, compartilhar ou manipular informações devem seguir o mesmo padrão de segurança, utilizando senha de acesso ao dispositivo sem expor estes dispositivos a acesso de terceiros. A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela EOS é sua assinatura eletrônica no servidor da EOS;

- Será apenas permitida senha com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes;

- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela EOS, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;

- É permitida apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação ao Diretor de Risco e Compliance;

- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração da mesma; e

- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Risco e Compliance à área responsável.

É de responsabilidade do usuário a proteção dos Recursos de RITC concedidos pela EOS, assim como das informações que podem estar contidas em dispositivos e meios de comunicação.

Fica estabelecido que toda informação adquirida e criada pelo processo de negócio da EOS, é de propriedade da EOS.

O uso dos ativos da EOS pode ser supervisionado, monitorado ou retido para auditoria sem aviso prévio, por isto o uso destes recursos para fins pessoais deve ser evitado e não devem ser utilizados como meio de armazenamento pessoal de informações.

Deve-se observar que o uso destes recursos não coloque em risco a confidencialidade, integridade e disponibilidade das informações da EOS, bem como a capacidade funcional dos dispositivos usados.

Todas as informações devem ser armazenadas na nuvem, nas pastas previamente definidas.

A utilização de mídias removíveis (Pendrive, CD/DVD, cartão de memória) deve ser autorizada pelo Diretor de Compliance.

Fica declarado proibido, o empréstimo, aluguel, compartilhamento dos Recursos de RITC disponibilizados pela EOS com terceiros, concorrentes, ou qualquer outro indivíduo ou empresa que não esteja formalmente autorizado pela Área de Compliance da EOS.

A utilização de técnicas de acesso remoto nos dispositivos, para qualquer fim, seja acesso a informações ou manutenção do dispositivo, deve ser aprovado pelo Diretor de Compliance da EOS.

Usuários da EOS são responsáveis por toda e qualquer informação que está sob seu controle, desta forma deve ser aplicar o descarte seguro de informações impressas (triturar arquivos confidenciais), zelar pelas informações que são faladas em público, ser crítico quanto a confidencialidade da informação antes de compartilhar com outras pessoas. Estar atento ao armazenamento de documentos que contenham Informações Confidenciais sob chaves (ser rigoroso com a política de mesa limpa).

O acesso à rede de internet cabeada deve ser utilizado prioritariamente para fins de execução das atividades de trabalho. Os usuários da EOS devem se conectar exclusivamente na rede sem fio disponibilizada para uso interno. É proibido o uso de conexões de rede públicas nestes dispositivos, sejam elas cabeadas ou sem fio. O usuário das redes da EOS é responsável pelo uso

seguro e correto, bem como serão responsabilizados pelo uso e suas consequências pela EOS e, se necessário, pela lei.

A utilização do nome da EOS em redes sociais ou outros meios de mídia deverão ser formalmente aprovados pela Área de Compliance da EOS, bem como a exposição de qualquer outra informação que seja de propriedade ou esteja sob a tutela da EOS.

Para preservar o ciclo de vida dos dispositivos elétricos/eletrônicos, é sugerido que estes sejam desligados após a rotina de trabalho.

No caso de perda/roubo/furto ou outro evento de perda de posse/controle pessoal sobre o equipamento, o usuário deve notificar a EOS, pelo endereço de e-mail: compliance@eosinvest.com.br para que as devidas providências sejam tomadas para a prevenção da perda de informações.

A identificação, pela EOS, do uso incorreto dos Recursos de RITC poderá gerar advertências ou penalidades, definidas no comitê de sócios, dependendo de sua gravidade.

(iv) Normas de Uso para Visitantes

Denominam-se visitantes aqueles que esporadicamente visitam o escritório da EOS.

Os usuários visitantes devem utilizar exclusivamente a rede de visitantes, obedecendo a Política da EOS. No momento da concessão de acesso à rede de visitantes, algum funcionário da EOS deverá orientá-lo do uso correto.

Responsabilidades do usuário conectado à rede visitantes da EOS:

- A utilização da rede visitante da EOS para fim comercial é expressamente proibida;
- É proibida a utilização da rede para acesso a conteúdos pornográficos;
- Todo e qualquer tipo de conteúdo acessado a partir da rede sem fio de Visitantes da EOS é de plena responsabilidade do usuário, inclusive responsabilidade judicial em caso da utilização do acesso para participação em crimes (virtuais ou não), acesso e disseminação de conteúdo de pedofilia, difamação e injúria, ou qualquer outra ação que não esteja nas conformidades da lei;
- É proibida a divulgação de conteúdos inerentes a EOS na internet a partir deste acesso;
- O dispositivo utilizado para conexão pode ser confiscado, em caso de suspeita de uso incorreto;
- O acesso pode ser revogado sem aviso prévio e pode ser solicitado ao usuário esclarecimento sobre o uso do acesso à internet através da rede visitantes;
- O acesso pode ser monitorado e os *logs* (evidências) coletadas podem ser utilizadas como prova de infração à lei ou a este termo de responsabilidade;
- É de responsabilidade do usuário visitante fazer uso seguro da rede, desta forma contribui para que não cause ônus a EOS e a si mesmo;

- Em caso de dano causado através do uso da rede de visitante o usuário será responsabilizado e arcará com todas as despesas necessárias para reparo do dano, indiferentemente da complexidade ou gênero do dano;

- É de responsabilidade do usuário visitante desconectar o dispositivo utilizado na rede da EOS no fim do período de visita, bem como é proibido o compartilhamento deste acesso com outros indivíduos;

- É expressamente proibido que usuários visitantes utilizem gravadores de voz, câmeras de vídeo ou fotográfica (ou qualquer outro dispositivo de captura de dados) nas dependências da EOS para capturar informações sem o prévio conhecimento da diretoria; e

- Aquele visitante que, por força de trabalho, utilize do ambiente e infraestrutura da EOS para executar qualquer atividade, se qualifica como prestador de serviço e deve respeitar todas as cláusulas de todas as sessões desta norma.

(v) Uso de correio eletrônico particular

O correio eletrônico disponibilizado (usuário@eosinvest.com.br) é de propriedade da EOS, bem como todas as informações contidas no mesmo. É expressamente claro que, a EOS pode requerer a qualquer momento a posse destes correios, bem como todas as informações armazenadas no mesmo sem qualquer exceção ou aviso prévio.

É proibido a utilização profissional de correio eletrônico particular.

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à EOS.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a EOS.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Compliance.

(vi) Endereço eletrônico de programas ou de comunicação corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da Área de Compliance responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da EOS, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da EOS.

(vii) Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela EOS mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da EOS.

(viii) Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na EOS.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a EOS, a sugestão deve ser encaminhada para a Área de Compliance, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da EOS; e
- Sejam incoerentes com o Código de Ética Corporativa da EOS.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da EOS é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da EOS.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos; e
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

(ix) Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Compliance. Em paralelo, a EOS também manterá uma cópia dos e-mails a partir de armazenamento em nuvem.

(x) Armazenamento em Nuvem (Cloud)

A EOS poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados em Nuvem (*Cloud*).

No caso de contratação de fornecedores ou prestadores de serviços ("Terceiros") para o serviço em Nuvem, tal contratação pode representar uma fonte significativa de riscos para a EOS em relação à cibersegurança. Neste sentido, necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de armazenamento na Nuvem.

Necessário iniciar um devido processo de *Due Diligence* do Terceiro antes da contratação, devendo constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e cibersegurança, bem como à proteção de dados pessoais.

Antes da contratação desse serviço, a empresa poderá ser requisitada a enviar a EOS:

(i) Documentos que atestem a existência dos respectivos procedimentos de cibersegurança e proteção de dados pessoais;

(ii) Último relatório de teste/auditoria periódica; e

(iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

A Área de Compliance analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados pela EOS. Somente após a aprovação pela Área de Compliance, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de incidente constatado pelo Terceiro, este deverá enviar uma notificação relatando o ocorrido à EOS, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de *Due Dilligence* aos provedores destes serviços, tal como, porém não exclusivamente:

a. *Software as a Service* (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;

b. *Platform as a Service (PaaS)* – desenvolvimento, teste, uso e controle sobre softwares próprios; e

c. *Infrastructure as a Service (IaaS)* – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

6 CONTROLE, MONITORAMENTO E TESTES DE CONTINGÊNCIA

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela área responsável, sob supervisão do Diretor de Compliance. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

O monitoramento de acessos de internet, telefone e dos Recursos de RITC se torna de conhecimento dos Colaboradores e terceiros que venham a usufruir destes recursos a partir desta Política.

A EOS manterá diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções de cada Colaborador e poderá monitorar o acesso dos mesmos a tais pastas e arquivos com base na senha e login disponibilizados.

Convém conferir que os documentos e outras informações dos clientes que estejam sob a égide da distribuição realizada pela própria EOS estarão em pasta segregada, de forma que somente aqueles Colaboradores que desempenhem atividade nessa área podem ter acesso, e devem contar com aprovação do Diretor de Distribuição para tal. Pela natureza das atividades, o Diretor de Compliance também possui acesso aos documentos e informações.

A EOS também possui câmeras instaladas em alguns pontos de seu escritório, que funcionam de forma ininterrupta e cujas imagens ficam gravadas em local apropriado, para consulta mediante necessidade.

Em função da natureza das operações realizadas pela EOS, alguns ramais estão ligados a sistema de gravação de voz. Tais gravações permitem a solução de eventuais conflitos que surjam nas negociações realizadas pela EOS e suas contrapartes, bem como possibilita a identificação de situações de não conformidades, em linha com os normativos que as gestoras devem observar para realizar a atividade de distribuição de cotas dos fundos de investimento sob gestão.

Nessa esteira, destacamos que as comunicações com os clientes de assunto correlato à distribuição devem ser realizadas nessas linhas de telefone que contenham esse tipo gravação com proteção.

Toda e qualquer ordem recebida pelos Colaboradores da EOS proveniente de seus clientes devem ter o seu armazenamento realizado pelo período não inferior a cinco anos.

A EOS dará tratamento sigiloso às informações decorrentes do monitoramento, e não poderá divulgá-las nem para membros da EOS que não tenham a incumbência de fazer este monitoramento, nem para terceiros, salvo por força de disposição legal, ordem judicial ou, ainda, para os fins exclusivos de se adotar as medidas necessárias para fazer cumprir esta Política.

A EOS mantém um registro de *logs*, que através da utilização do usuário e senha de cada Colaborador, é capaz de identificar o Colaborador que realizou alterações nos arquivos e documentos, sendo possível manter a rastreabilidade e auditabilidade. A EOS poderá manter por 5 anos todos os *logs*, e poderá verificar regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados.

A EOS institui esta Política para se resguardar de qualquer ônus causado pelo seus Colaboradores e parceiros, assim como se espera que todos façam o uso consciente dos recursos disponibilizados para que não seja necessário o desgaste da adoção de medidas drásticas para recorrer de qualquer problema futuro.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a EOS esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da EOS.

Ademais, serão realizados Testes Periódicos de Segurança da EOS, 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 EOS, em especial os confidenciais. Referidos testes serão realizados, com periodicidade mínima semestral, pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos da EOS.

7 PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a EOS desenvolveu um Plano de Resposta para indícios, suspeitas fundamentadas, vazamentos de Informações Confidenciais ou outras falhas de segurança.

No caso de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

Estas providências consistem em:

<u>Empresa de TI Terceirizada (Sob Supervisão do Compliance):</u>

a) Verificação e Auditoria dos *Logs*;

b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;

c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;

d) Desinstalação de software;

e) Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;

f) Formatação e reconstrução do sistema operacional;

g) Substituição física de dispositivos de armazenamento

h) Reconstrução de sistemas e redes;

i) Restauração de dados provenientes do *backup* realizado diariamente;

j) Entre outros.

Compliance ou Jurídico Contratado:

a) Criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;

b) Em caso de confirmação de qualquer incidente de segurança, principalmente algum que afete os dados pessoais que a EOS realize o tratamento, ou em caso de eventual vazamento de Informações Confidenciais, elaborar notificação aos clientes afetados e à Autoridade Nacional de Proteção de Dados (“ANPD”) informando o ocorrido.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia.

b) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da Gestora resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados, bem como ser formalizado no Relatório de Controles Internos da EOS.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da EOS.

8 PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

A EOS está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da EOS, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a EOS.

Importante observar que o escopo da proteção de dados pessoais no âmbito da EOS está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas, com especial menção ao cumprimento da regulação aplicável à gestão de recursos de terceiros. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Gestora, de fornecedores e outros com os quais a EOS manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela EOS está pautado nos requisitos do artigo 7º da LGPD, assim como nas premissas do artigo 11 da mesma lei, quando aplicável.

Princípios Norteadores:

A EOS compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da LGPD:

(i) Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(ii) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

(iii) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

(iv) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

(v) Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vi) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(vii) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

(viii)Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

(ix) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

(x) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18 da LGPD, o titular dos dados pessoais poderá solicitar à EOS, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue.

a) Confirmação de existência de tratamento;

b) Acesso aos dados;

c) Correção de dados incompletos, inexatos ou desatualizado;

d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;

e) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

f) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;

g) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

i) Revogação do consentimento, nos termos da Lei.

A EOS disponibiliza canal de comunicação, através do endereço compliance@eosinvest.com.br, por meio do qual o seu Encarregado pelo Tratamento de Dados Pessoais receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados em consonância a sua Política de Privacidade. O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a EOS, os titulares dos dados (pessoas físicas) e a ANPD.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela EOS durante tempo necessário para o atingimento dos objetivos para os quais foram coletados. De todo modo, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual, pelo que, nestas hipóteses o prazo mínimo de armazenamento será de 5 (cinco) anos.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a EOS estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à EOS, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a EOS cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança:

As matérias relacionadas aos dados pessoais, dados sigilosos e ao tratamento destes serão apresentadas ao Encarregado pelo Tratamento de Dados Pessoais, para avaliação e eventual deliberação e, nos casos em que este julgar serem mais complexos, tais matérias serão submetidas ao Comitê de Gestão de Riscos e de Compliance.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da EOS para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a ANPD, bem como todos os que porventura possam ter sido afetados pelo referido evento.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, quando aplicável, inclusive de dados sensíveis, nos termos do artigo 38 da LGPD.

Treinamento:

A EOS treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com a sua Política de Treinamento e Reciclagem de Colaboradores.

9 TERMO DE CONFIDENCIALIDADE

Conforme estabelecido no Termo de Responsabilidade e Confidencialidade constante no Anexo I a esta Política, nenhuma Informação Confidencial deve, em qualquer hipótese, ser divulgada à terceiros não Colaboradores da EOS. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de *compliance* da EOS.

Qualquer informação sobre a empresa, seu know-how, técnicas, cópias, diagramas, modelos, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela EOS, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela nossa instituição, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da EOS e/ou de seus sócios e clientes, obtida em decorrência do desempenho das atividades do Colaborador na, ou para a, EOS, só poderá ser fornecida à terceiros, ao público em geral, aos meios de comunicação de massa ou demais órgãos públicos ou privados se assim for previamente autorizado pelo Diretor de Compliance e ou pelo Diretor Geral.

A informação obtida em decorrência da atividade profissional exercida na EOS não pode ser divulgada, em hipótese alguma, a terceiros não Colaboradores. Enquadram-se neste item, por exemplo, estratégias de investimento ou desinvestimento, relatórios, estudos realizados de análise de investimentos – independentemente destas análises terem sido realizadas pela EOS ou por terceiros contratados –, opiniões internas sobre ativos financeiros, informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimento geridos pela EOS, transações realizadas e que ainda não tenham sido divulgadas publicamente, além daquelas estabelecidas no Anexo I - Termo de Responsabilidade e Confidencialidade.

A utilização ou divulgação de qualquer Informação Privilegiada, "*Insider Trading*", Divulgação Privilegiada e/ou "Front Running", sujeitará os responsáveis às sanções previstas neste Código, inclusive desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da EOS, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da EOS, e sujeito ainda às consequências legais cabíveis.

10 VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada periodicamente, pelo menos 01 (uma) vez ao ano, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

O objetivo principal do processo de revisão dessa Política é manter sempre atualiza a metodologia de avaliação de risco, as implementações de proteção e prevenção, os monitoramentos e testes e os planos de resposta.

11 ADMINISTRAÇÃO DESTA POLÍTICA

Esta Política é administrada pelo Diretor de Compliance da EOS, sob a supervisão direta da diretoria.

Eu _____, inscrito no CPF/ME sob o nº _____ me declaro ciente de todas as regras de uso dos recursos de informação, tecnologia e comunicação (RITC) disponibilizados pela EOS.

Comprometo-me em cumprir todas as regras estabelecidas, bem como tenho ciência de todas as responsabilidades e sanções às quais poderei ser submetido em caso de descumprimento desta Política ou em causa de ônus a EOS Investimentos Ltda.

São Paulo, ____ de _____ de _____.

_____

COLABORADOR

ANEXO I

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Através deste instrumento eu, ..., portador da Cédula de Identidade RG n.º ....., expedida pelo ....., inscrito no CPF/ME sob o n.º ..... e/ou com Carteira de Trabalho e Previdência Social n.º ....., série ..... ("Colaborador"), e EOS Investimentos Ltda., inscrita no CNPJ/ME sob o n.º 09.555.837/0001-71 ("EOS"), resolvem, para fim de preservação de informações pessoais e profissionais dos clientes e da EOS, celebrar o presente Termo de Responsabilidade e Confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais ("Informações Confidenciais"), para os fins deste Termo:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: *know-how*, técnicas, cópias, diagramas, modelos, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela EOS, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela EOS, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da EOS e a seus sócios ou clientes, independente destas informações estarem contidas em *pen-drives*, HDs, outros tipos de mídia ou em documentos físicos.

b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na EOS, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, funcionários e estagiários da EOS e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela EOS ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

1.1 Não são consideradas Informações Confidenciais, quaisquer informações que: (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador; (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Termo; (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade; (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente o Diretor de Compliance da EOS para que as medidas legais cabíveis sejam tomadas, observado o disposto no item 5 deste Termo.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na EOS, comprometendo-se, portanto, observadas as disposições do Código de Ética e Conduta Profissional ("Código") e desta Política, a não divulgar tais Informações Confidenciais para quaisquer fins ou pessoas estranhas à EOS, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1 O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na EOS.

2.2 As obrigações ora assumidas ainda persistirão no caso do Colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela EOS.

2.3 A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.

3 O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a EOS e terceiros, ficando deste já o Colaborador obrigado a indenizar a EOS, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1 O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, e desligamento ou exclusão por justa causa do Colaborador se este for sócio da EOS, sem prejuízo do direito da EOS de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

3.2 A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens 2 e 2.1 acima.

3.3 O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na EOS são e permanecerão sendo propriedade exclusiva da EOS e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na EOS, devendo todos os documentos permanecer em poder e sob a custódia da EOS, salvo se em virtude de interesses da EOS for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da EOS;

b) Em caso de rescisão do Contrato Individual de Trabalho, desligamento ou exclusão do Colaborador, o mesmo deverá restituir imediatamente à EOS todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da EOS, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a

disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

d) É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela EOS no equipamento do mesmo.

e) A senha que foi fornecida para acesso à rede de dados institucionais é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

f) O software antivírus, instalado no equipamento do Colaborador jamais deverá ser desabilitado, exceto com prévia anuência.

5. Ocorrendo a hipótese de o Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a EOS, permitindo que a EOS procure a medida judicial cabível para atender ou evitar a revelação.

5.1 Caso a EOS não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela a que o Colaborador esteja obrigado a divulgar.

5.2 A obrigação de notificar a EOS subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a EOS, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

6.1 A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da EOS.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

São Paulo, _____ de _____ de _____ .

_____

[COLABORADOR]

Testemunhas:

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