COMPLIASSET

POLÍTICA

POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Índice

Índice 0
Objetivo 2
Conceitos e Premissas da Segurança da Informação 4
Responsabilidades 5
Procedimento para backup 5
Solução Vigente 6
1) Redundância 6
2) Backup 7
3) Restauração de Dados 7
4) Mecanismos de Verificação da Situação Vigente 8
Contingência Interna e Comunicação 8
Confidencialidade 9
Controles de acesso a Informações Confidenciais 10
Barreiras de controle de informações 11
Ativos da Compliasset – Uso de redes e sistemas 12

Política de E-mails **12**
1) Regras de Utilização 12
2) E-mails Pessoais 13
Política de Internet **14**
1) Regras de Utilização 14
Rede **15**
Firewall **16**
Atualizações: antivírus, sistema operacional e segurança **16**
Ativos **16**
Acesso Remoto **17**
Boas práticas **17**
Solicitação de Acesso Remoto **18**
Aprovação do Acesso Remoto **18**
Responsabilidades **19**
Processo disciplinar de não-conformidade com as diretrizes estabelecidas nesta Política **19**
Histórico de Versões **21**
ANEXO I **22**
TERMO DE COMPROMISSO **22**

Maio/2023 Versão
2.1

Este material foi elaborado pela Compliasset Software e Soluções Digitais Ltda. (“Compliasset”) e não pode ser copiado, reproduzido ou distribuído sem prévia e expressa concordância desta. A Compliasset é a empresa desenvolvedora e licenciadora do software Compliasset (“Sistema”).

Objetivo

Esta Política tem por objetivo o adequado gerenciamento das informações de posse temporária ou de propriedade da Compliasset, bem como os ativos da empresa com relação ao uso de redes e sistemas, sendo aplicável a todos os colaboradores, independentemente do nível hierárquico, função ou tipo de vínculo (empregatício ou prestação de serviços) com a empresa ("Colaboradores"), que devem atestar sua ciência e aderência por meio do Anexo I – Termo de Compromisso.

As regras aqui formalizadas visam assegurar a proteção dos ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança ou cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo, por meio da conscientização dos Colaboradores a respeito.

Os processos de segurança de dados e da informação devem assegurar:

- A integridade - garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- A disponibilidade - garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário; e
- A confidencialidade dos ativos de informação - garantia de que o acesso à informação seja obtido somente por pessoas autorizadas pelA Compliasset, observadas as regras de sigilo e confidencialidade constantes desta Política.

Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Compliasset poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

A Compliasset exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus

Colaboradores e Clientes, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Conceitos e Premissas da Segurança da Informação

Para efeito desta Política, os termos aqui expressos terão os seguintes significados:

- Segurança da Informação é um termo que se refere essencialmente à proteção contra divulgação, acesso, uso ou modificação não-autorizada e também contra apropriação indevida, furto, destruição, dano ou perda dos ativos de uma empresa ou pessoa, assegurando a confidencialidade, integridade e disponibilidade de informações;
- A confidencialidade é a garantia de que as informações sejam acessadas somente por indivíduos autorizados pelo proprietário da informação; a integridade, garantia de que as informações não sejam alteradas sem autorização ou conhecimento de seu proprietário e a disponibilidade, garantia de que as informações estejam disponíveis quando seu proprietário ou usuário necessitar, representam os principais atributos que orientam a análise, o planejamento e a implementação da segurança para as informações; e

Como premissa para a execução desta Política, o fornecimento e trânsito das informações entre os Clientes e a Compliasset através do Sistema estarão devidamente protegidas por programas e/ou recursos de proteção que busquem evitar qualquer acesso não autorizado aos dados do Cliente.

A Compliasset realiza avaliações e testes periódicos de vulnerabilidade, visando assegurar a segurança lógica dos dados que são acessados, transmitidos e armazenados através da utilização do sistema, comprometendo-se a imediatamente sanar eventuais vulnerabilidades identificadas. Essas avaliações e testes são feitas de acordo com a Política de Gerenciamento de Vulnerabilidades.

A Compliasset possui procedimentos de Gerenciamento de Chaves Criptográficas, Gerenciamento de Regras de Firewall e Gerenciamento de Incidentes de Segurança que visam mitigar, dentre outros, os riscos suscitados nesta Política.

A Compliasset tem o dever de comunicar ao Cliente quaisquer eventos e incidentes de segurança da informação que possam comprometer a confidencialidade, integridade e disponibilidade das informações do Cliente sob sua responsabilidade.

A Compliasset detém mecanismos de contingência relativos à Segurança da Informação, que são documentados, periodicamente testados e atualizados.

Responsabilidades

O Diretor de Tecnologia (Chief Technology Officer – CTO) é o responsável por esta Política, devendo tratar e responder questões de segurança da informação, bem como implementar e revisar as regras e normas aqui estabelecidas.

Procedimento para backup

Faz-se necessário, como empresa de software, garantir o serviço mais estável possível para os Clientes finais da Compliasset.

Da mesma forma, as informações inseridas pelos Clientes precisam ser mantidas em ambientes seguros a prova de desastres e emergências.

A aplicação possui três conjuntos de dados distintos que precisam ser preservados:

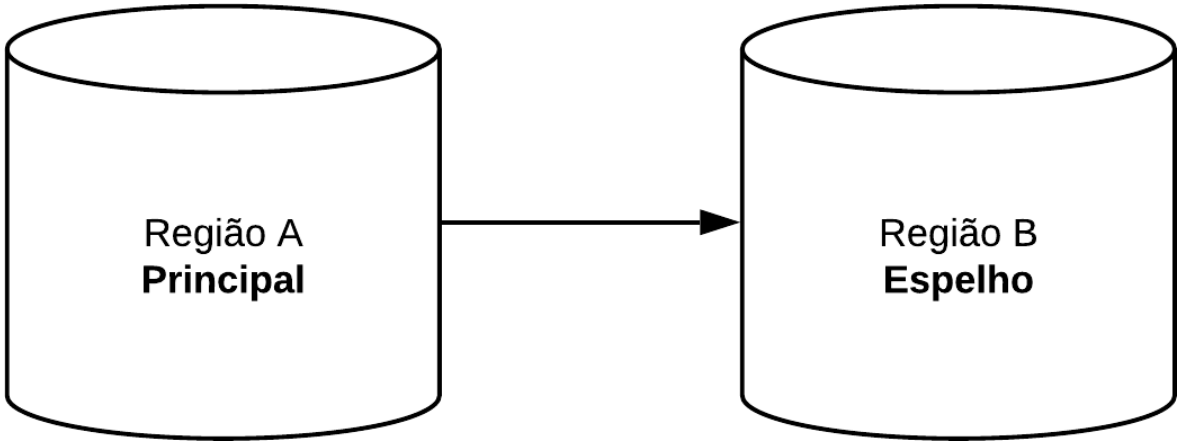
1. Banco de dados
2. Arquivos inseridos por usuários finais
3. Arquivos da aplicação

Solução Vigente

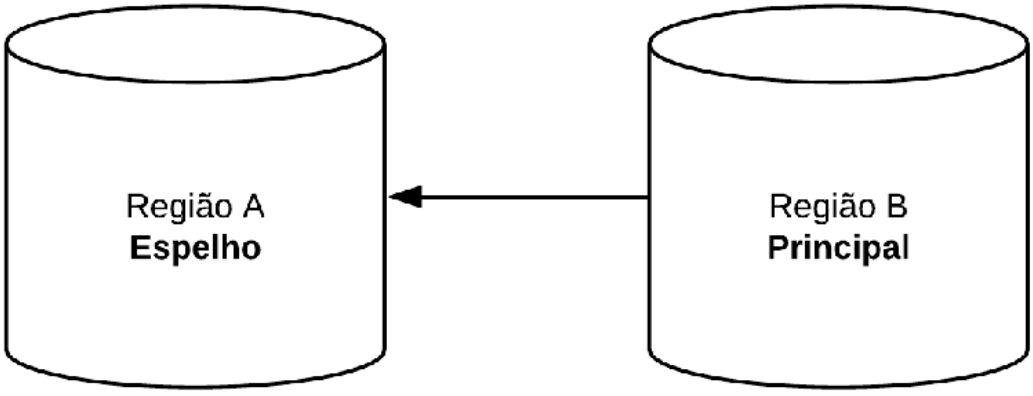
1) Redundância

A Compliasset contrata os serviços da Amazon AWS Services ("AWS") como servidor do Sistema.

Nos data centers da AWS se encontram o banco de dados e os arquivos do Sistema. São servidores da aplicação as duas zonas da AWS no Brasil, chamados de Região A e Região B.



A Região A serve como repositório principal. A Região B serve como um 'espelho' da Região A, ou seja, é uma cópia fiel em tempo real da Região A. Em casos onde a Região A venha a falhar, a Região B assume a aplicação de forma transparente para o Cliente final até que a situação se normalize na Região A.



2) Backup

Além da redundância descrita acima, é feito um backup diário (entre 3:00 e 3:39) de toda a aplicação em outro ambiente da AWS diferente das Regiões A e B, para o caso da improvável falha em ambas Regiões.

Para os arquivos da aplicação, mantemos os mesmos em um serviço próprio para desenvolvedores que fazem o commit de código de programação com melhorias na aplicação em si. O serviço utilizado pela Compliasset se chama BitBucket que garante à Compliasset outras camadas de proteção e restauração destes arquivos.

3) Restauração de Dados

É possível restaurar dados de toda a aplicação ou de alguma parte específica do banco de dados para algum cliente específico através de três formas:

- Usando o backup diário descrito acima;
- Usando a própria Região espelho para períodos inferiores a um dia;
- Utilizando ferramenta de restauração para um momento específico da AWS com intervalo de tempo de 5 minutos;

4) Mecanismos de Verificação da Situação Vigente

Para garantir que a redundância e backups estão funcionando conforme o planejado existe um sistema de alertas diários da AWS. Mensalmente são realizadas verificações mensais do status do Backup.

Contingência Interna e Comunicação

A Compliasset possui um sistema de contingência para atender em caso de:

1) Falha no fornecimento de energia, implantado um nobreak com suporte a operação essencial por um período de 6 horas;

2) Falha no acesso à internet, implantado dois links dedicados com gerenciamento através de firewall o qual ativa automaticamente em caso de falha;

3) Falha no acesso aos servidores, implantado sistema de servidores redundantes, com fontes redundantes, os quais são ativados em caso de falha;

4) RTO - O tempo máximo tolerável para a recuperação dos sistemas e processos críticos após um evento de interrupção são de 12 horas.

5) RPO - O tempo máximo de informações que podem ser perdidas com base no tempo de ocorrência de uma falha e o último backup realizado são de 5 minutos.

6) Falha em estação de trabalho, com a disponibilização de um equipamento preparado no escritório principal para substituição imediata;

7) Inacessibilidade temporária ou permanente do escritório, com a utilização de uma localidade alternativa de trabalho, conforme descrito abaixo;

8) Para os casos de back-up de colaboradores nos casos de doença, existe o trabalho padrão, ou seja, toda atividade está descrita em procedimentos específicos, caso

haja necessidade de substituição de funcionário, temporariamente ou definitivo. O colaborador que assumir determinada atividade vai ter condições de dar continuidade ao negócio, sem que haja interferência na entrega do trabalho ao cliente;

9) Tanto para os cargos gerenciais, como para os cargos das atividades técnicas e regulatórias, existe um backup garantido;

10) Qualquer outra situação que ameace o ambiente seguro do Sistema e da Compliasset, mesmo que não descrita acima.

Confidencialidade

Todas as informações divulgadas pelo Cliente para a Compliasset com a utilização do termo "Informação Confidencial" serão tratadas como confidenciais. O termo Informação Confidencial abrange toda informação escrita, verbal ou de outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a know-how, técnicas, designs, especificações, desenhos, cópias, diagramas, modelos, amostras, fluxogramas, programas de computador, discos, informações sobre Clientes, informações técnicas, financeiras, comerciais ou quaisquer outras que venham a ser reveladas em razão da utilização do Sistema pelo Cliente.

Inclui-se no conceito de Informação Confidencial a integralidade do conteúdo disponibilizado ao Cliente por meio do Sistema.

Toda e qualquer informação ou documento inseridos no Sistema pelo Cliente são e permanecerão de propriedade exclusiva do Cliente.

Informação Confidencial não incluirá:

1) Informação que venha a ser de domínio público sem que seja pela falta ou ação da parte destinatária;

2) Informação que esteja legitimamente disponível à parte destinatária antes de sua divulgação, ou

3) Informação que se torne legitimamente disponível a partir de terceiros, sem qualquer violação de obrigações de confidencialidade.

4) Compliasset reserva-se o direito de monitorar, por meio das ferramentas que julgar pertinentes, o uso não autorizado do seu sistema por terceiros.

Na hipótese de recebimento de ordem judicial solicitando o envio de Informação Confidencial, a parte receptora compromete-se a informar a outra parte sobre o recebimento de ordem antes da disponibilização da informação, de modo que a outra parte possa tomar todas as medidas necessárias à preservação da Informação Confidencial. Caso as medidas tomadas para preservar a Informação Confidencial em questão não tenham êxito, a parte receptora deverá somente enviar a parte das Informações Confidenciais que for necessária ao cumprimento do dever legal.

Controles de acesso a Informações Confidenciais

O controle do acesso a sistemas de informações da Compliasset levará em conta as seguintes premissas:

1) Garantia de que o nível de acesso concedido ao funcionário é adequado ao seu perfil;

2) Cancelamento imediato do acesso concedido a funcionários desligados, afastados ou que tenham sua função alterada na Compliasset;

3) Registro de log de acesso para inclusão, alteração e exclusão de toda e qualquer informação do ambiente tecnológico da Compliasset; e

4) Acesso às trilhas de auditoria.

O dever de confidencialidade dos funcionários com relação às informações que tiverem acesso dentro da Compliasset, subsiste nos casos de desligamento dos mesmos.

Todos os Colaboradores do Compliasset são obrigados a assinar Termo de Confidencialidade ("NDA") antes de iniciar as atividades que demandem o manuseio de informações e dados internos da empresa e dos Clientes.

Barreiras de controle de informações

Os Colaboradores detentores de Informações Confidenciais, em função de seus cargos ou atribuições na empresa Compliasset, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

1) Os Colaboradores devem evitar circular em ambientes externos à Compliasset com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao desenvolvimento do projeto e no interesse do Cliente, devendo essas cópias serem criptografadas ou mantidas através de senha de acesso;

2) O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;

3) As informações que possibilitem a identificação de um Cliente da Compliasset devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da Compliasset ou do próprio Cliente;

4) Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Compliasset, como por exemplo vírus de computador, fraudes, etc.;

5) Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;

6) As senhas de acesso do Colaborador ao Sistemas e rede da Compliasset são pessoais e intransferíveis; e

7) O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Compliasset e poderá ser monitorado pela área de TI sempre que necessário.

Ativos da Compliasset – Uso de redes e sistemas

Política de E-mails

1) Regras de Utilização

Os servidores de e-mail da Compliasset encontram-se protegidos contra vírus e códigos maliciosos, porém, algumas atitudes do usuário são necessárias para contribuir com a segurança da informação:

- Os Coladoradores não deverão em hipótese alguma, anexar com as extensões ".bat", ".exe", ".src", ".lnk" e ".com".
- Os Coladoradores não deverão utilizar contas pessoais para comunicar-se com clientes ou para transmitir qualquer tipo de informação confidencial ou interna.

- Ao trocar e-mails com clientes e parceiros, o conteúdo das mensagens poderá ser considerado posição oficial da Compliasset, portanto, os Colaboradores ficam obrigados a agir com seriedade e profissionalismo.
- Os Coladoradores não deverão enviar mensagens internas ou externas que possam prejudicar a imagem da Compliasset, como piadas, material de caráter sexual, imagens, vídeos (com extensões .mpeg, .avi ou outras), músicas (com extensões .mp3, .wav ou outras), jogos, mensagens ou textos de conteúdo religioso, criminoso, político ou que possa ser interpretado como ofensivo.
- Ao receber e-mails com links, os Colaboradores deverão verificar se correspondem ao endereço que aparece na tela. Para tanto, deverão posicionar o ponteiro do mouse sobre o link (sem clicar). Se o endereço exibido não for o mencionado, o Colaborador não deverá acessar o link.
- Os Colaboradores são rotineiramente instruídos pelo timede DevSecOps a desconfiar de todos os e-mails com assuntos, formulários, destinatário e arte incomuns.
- Os Colaboradores não poderão criar nem passar adiante correntes nas quais o receptor seja induzido a enviar mensagens para outros sem que haja necessidade profissional ou verificação de veracidade e segurança.
- Os Colaboradores não deverão ler, acessar ou divulgar e-mails de outros Colaboradores, clientes e prestadores de serviço sem a devida autorização dos titulares, ressalvados os encaminhamentos de solicitações de clientes às áreas responsáveis por meio dos endereços adequados, ou encaminhamentos de solicitações dos Colaboradores aos Líderes e área de Recursos Humanos para tratar a demanda, bem como encaminhamentos correlatos.
- Os Colaboradores deverão evitar utilizar o e-mail da empresa para assuntos pessoais.
- Se o espaço utilizado pelo Mailbox ultrapassar 400 MB, o usuário ficará impossibilitado de enviar mensagens até que o conteúdo seja reduzido.

- Os Colaboradores deverão evitar anexos muito grandes.
- Os Colaboradores são incentivados a limpar constantemente pastas como Deleted Items e Sent Items.

2) E-mails Pessoais

As contas pessoais de e-mail baseadas na internet (ex.: Gmail, Hotmail, Yahoo, Aol) somente devem ser utilizadas pelos Colaboradores para fins pessoais, sendo proibido o uso de tais contas para conduzir qualquer atividade profissional.

Política de Internet

1) Regras de Utilização

As práticas abaixo são vedadas aos Colaboradores:

- Usar softwares P2P (kazaa, Morpheus, Emule etc);
- Acessar sites de FTP sem autorização da equipe de TI;
- Fazer download ou upload de softwares ou dados não legalizados;
- Usar discos virtuais para armazenamento externo de dados da Compliasset;
- Utilizar informações classificadas como confidenciais ou internas em sites pessoais, linkedin, blogs ou qualquer outro meio de publicação na Internet;
- Navegar na Internet em sites não confiáveis (como os de pornografia, “hackeismo”, dinheiro fácil etc.);
- Fazer download de arquivos não relacionados ao trabalho.

Somente é permitida a navegação convencional. Casos específicos que exijam outros protocolos devem ser solicitados para a equipe de TI e estarão sujeitos à autorização do supervisor imediato e/ou do COO da empresa.

Os Colaboradores com acesso à Internet podem baixar somente programas diretamente relacionados às atividades da Instituição, e devem providenciar o que for necessário para obtenção de licença e registro desses programas.

A Compliasset pode gerar relatórios dos sites acessados, e caso julgue necessário poderá bloquear o acesso a arquivos/domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.

A Compliasset monitora todos os acessos à Internet. Portanto, os Colaboradores deverão utilizar sua infraestrutura de acesso com bom senso e moderação.

Rede

Este tópico visa definir as normas de utilização da rede que englobam desde o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

É proibido acessar a rede da Compliasset para:

- Tentar acesso não autorizado aos servidores;
- Colocar em prova a segurança da rede;
- Tentar fraudar autenticação de usuários;
- Interferir nas atividades de outros usuários, alterando arquivos que não sejam de sua propriedade;
- Expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica e discriminatória através do uso dos recursos da empresa;
- Configurar contas de e-mail particulares.

É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade da empresa. Arquivos deste tipo serão apagados sem aviso prévio.

Cópias de arquivos da rede para dispositivos externos (Pendrives, etc) devem ser solicitadas à equipe de TI e serão executadas apenas com autorização do responsável pela área técnica responsável. A cópia de arquivos para pendrives somente pode ser realizada se para pendrives fornecidos pela área de TI.

Firewall

O acesso à configuração do firewall é restrito ao CTO da empresa, que ao contar com o auxílio de terceiros deverá monitorar e validar qualquer intervenção realizada.

As regras do firewall são configuradas de acordo a evitar qualquer vazamento de informações confidenciais e evitar que agentes externos como vírus e hackers entrem na rede interna e causem eventuais danos à Compliasset. Sendo assim, é permitido apenas o acesso externo da Compliasset a sites não criptografados (protocolo http pela porta 80) sendo esse acesso logado pelo firewall.

Sites criptografados também podem ser acessados, desde que notificados à Diretora de Compliance que deverá comunicar ao CTO da empresa que fará a liberação no firewall, que poderá ser para todos os usuários ou apenas para o usuário que necessita do acesso.

Atualizações: antivírus, sistema operacional e segurança

Todos os equipamentos (desktops) possuem a instalação do software de antivírus Kaspersky e Crowdstrike que estão configurados com a última atualização das definições de antivírus.

Todas as estações de trabalho estão atualizadas com os últimos patches de segurança e atualizações de sistema operacional (Service Packs).

O time de DevSecOps realiza testes de rotina para a avaliação do funcionamento adequado desses sistemas.

Ativos

Os Colaboradores devem proteger os ativos da Compliasset, assim como os ativos de terceiros que estiverem sob sua administração.

Os ativos da Compliasset incluem não somente os ativos financeiros e físicos, mas também relacionamentos com Clientes e propriedade intelectual, como informações sobre produtos, serviços, sistemas e pessoas. Tudo que for criado, obtido ou compilado pela Compliasset, ou em seu nome, incluindo listas de Clientes, diretórios, arquivos, relatórios e materiais de referência, software para computadores, sistemas de processamento de dados, bancos de dados e programas de computador, pertencem à Compliasset.

Os ativos da Compliasset devem ser utilizados somente na condução de seus negócios, exceto quando o uso pessoal for autorizado por esta Política ou por alguma outra política da Compliasset.

Ativos da Compliasset são também materiais, instrumentos e ferramentas oferecidas para o desenvolvimento das atividades dos Colaboradores, que devem evitar desperdícios e utilizar os recursos que lhe são disponibilizados exclusivamente para as atividades profissionais.

Além de bens físicos, financeiros ou não, é também um ativo da Compliasset a sua imagem e reputação. A Compliasset é reconhecida por empreender com ética, por contar com a confiança de seus Clientes, parceiros e concorrentes e por agir sempre com integridade e respeito. Nesse sentido, os Colaboradores têm o dever de aplicar esses valores em suas rotinas de trabalho, bem como de não lesar a reputação do Compliasset.

Acesso Remoto

O acesso remoto permite que os colaboradores trabalhem de forma eficiente e segura a partir de locais externos à empresa, mantendo a produtividade e a continuidade dos negócios.

Estas diretrizes aplicam-se a todos os colaboradores da Compliasset que necessitem acessar recursos corporativos de forma remota.

Boas práticas

Os Colaboradores devem:

- Utilizar somente dispositivos autorizados pela empresa para acessar os recursos corporativos remotamente.
- Manter os dispositivos atualizados com os patches de segurança mais recentes e utilizar soluções de antivírus atualizadas.
- Utilizar conexões seguras, como OPENVPN (Rede Virtual Privada), ao acessar recursos corporativos.
- Não compartilhar senhas ou credenciais de acesso com terceiros e não utilizar senhas óbvias ou facilmente deduzíveis.
- Encerrar a sessão remota após a conclusão do trabalho e garantir que os dispositivos utilizados sejam protegidos por senha.

Solicitação de Acesso Remoto

- Os colaboradores que necessitem da liberação devem preencher o formulário de solicitação de acesso remoto, disponível no Google Drive da empresa.
- A solicitação deve conter as seguintes informações:

1) Nome completo do colaborador
2) Departamento
3) Justificativa para o acesso remoto
4) Duração estimada do acesso remoto
5) Assinatura do colaborador e data

Aprovação do Acesso Remoto

- A aprovação do acesso remoto será feita pelo supervisor direto do colaborador e time de segurança da informação, em conformidade com as políticas e diretrizes da empresa.
- O supervisor deverá avaliar a justificativa e a necessidade do acesso remoto, considerando a segurança da informação e a disponibilidade dos recursos.

Responsabilidades

- Os Colaboradores são responsáveis por
    1) Seguir as boas práticas definidas neste documento.
    2) Manter a confidencialidade das informações acessadas remotamente.
    3) Informar imediatamente o departamento de segurança da informação em caso de perda ou roubo de dispositivos utilizados para acesso remoto.
- O time de DevSecOps é responsável por
    1) Fornecer suporte técnico e orientações sobre o acesso remoto.
    2) Monitorar e auditar o acesso remoto para garantir a conformidade com as políticas de segurança da empresa.

3) Revogar o acesso remoto quando necessário, como em casos de término de contrato ou suspeita de violação de segurança.

Medida disciplinar de não-conformidade com as diretrizes estabelecidas nesta Política

A violação de quaisquer das disposições nesta Política, lei, ou norma relacionada às atividades da Compliasset, bem como a não cooperação com os monitoramentos ou uma investigação interna, podem resultar em medidas disciplinares, como advertência verbal, por escrito ou aplicação das medidas disciplinares previstas em Lei, que serão mensuradas a depender da extensão da lesão às operações da empresa e/ou da reincidência à violação dos termos desta Política. A Compliasset poderá, se a situação assim exigir, despedir o Colaborador sem ou com justa causa.

A utilização da esfera disciplinar interna não visa limitar a efetivação de medidas legais cabíveis para reparar qualquer dano provocado à Compliasset ou seus Clientes, os quais poderão tomar as medidas cabíveis para eventual ressarcimento, inclusive pecuniário, se for o caso.

Histórico de Versões

Datas das atualizações		
Data	**Versão**	**Responsável**
08/Mai/2018	1ª	Nicole Dyskant
09/Dez/2020	2ª	Nicole Dyskant
23/Mai/2023	3ª	Rafael Nogali Machado
14/Jun/2023	4ª	Rafael Nogali Machado

ANEXO I

TERMO DE COMPROMISSO

Eu,_____ , inscrito(a) no CPF/MF sob o nº

_____, na qualidade de Colaborador da Compliasset Software e Soluções Digitais Ltda. ("Compliasset"), pelo presente instrumento, atesto que tenho acesso, li e entendi a Política de Confidencialidade, Segurança da Informação e Cibersegurança da Compliasset e confirmo que tenho conhecimento integral de todas as regras e procedimentos aqui constantes.

Comprometo-me a cumpri-la integralmente, confirmando minha ciência acerca de todos os tópicos nela tratados, em especial, dos monitoramentos e registros de todos os ambientes, sistemas, computadores e redes da empresa, bem como das sanções aplicáveis aos casos de violação da presente Política.

_____ , ____ de_____ de 20___

[Assinatura do Colaborador]

_____