Política de Segurança da Informação

Sumário

OBJETIVO

Estabelecer diretrizes para estruturar um sistema normativo de Segurança da Informação, visando garantir a proteção e confidencialidade aos dados e recursos de informação do Grupo Mafra, seus colaboradores, clientes, parceiros, fornecedores e demais agentes envolvidos direta ou indiretamente com o Grupo Mafra.

ABRANGÊNCIA

A presente Política aplica-se a todos os Agentes de Segurança da Informação, conforme definidos na seção 5 abaixo.

É missão e responsabilidade de cada Agente de Segurança da Informação, observar e seguir as políticas, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação, de forma que, é imprescindível que cada Agente de Segurança da Informação tenha conhecimento dessa política e compreenda o papel da Segurança da Informação em suas atividades diárias e a importância desta para o Grupo Mafra.

Essa política é aplicável tanto ao ambiente informatizado quanto aos meios convencionais de processamento, comunicação e armazenamento da informação. Abrange todos os equipamentos e recursos possuídos ou utilizados pelo Grupo Mafra

A Diretoria de Operações é responsável por editar as políticas e padrões que apoiam a todos na proteção da informação, e está preparada para auxiliar na resolução de problemas relacionados ao tema.

Os colaboradores e terceiros que tenham acesso aos recursos do Grupo Mafra somente os utilizarão seguindo os princípios de segurança aqui estipulados e sem afetar ou causar prejuízo a outrem.

Quaisquer dos Agentes de Segurança da Informação que observarem desvios às diretrizes desta Política de Segurança da Informação ou ao Código de Conduta do Grupo Mafra deverão comunicar tais fatos no Canal de Ética - (https://portal.mafrahospitalar.com.br/compliance/ - 0800 721 9152).

Verificações de cumprimento da política serão efetuadas para checar o nível de segurança das áreas e elaborar projetos para melhoria dos índices de conformidade.

Toda violação ou desvio é investigado pela Diretoria de Operações para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Internamente, o descumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos Agentes que a descumprirem, conforme a respectiva gravidade do descumprimento. Não obstante, estarão todos os Agentes de Segurança da Informação sujeitos às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

Informações, como definida na seção 5 abaixo, precisam ser preservadas observando três princípios básicos de Segurança da Informação:

- Integridade — a Informação deve ter seu conteúdo original mantido, sendo protegida contra alterações indevidas, seja de forma intencional ou acidental;

- Confidencialidade — somente pessoas devidamente autorizadas podem ter acesso às informações;

- Disponibilidade — o acesso à Informação deve ser garantido às pessoas autorizadas sempre que for necessário.

É de propriedade exclusiva do Grupo Mafra toda informação, ideias e métodos gerados utilizando-se integralmente ou parcialmente seus recursos.

O Grupo Mafra, como custodiante de dados e informações, os considera sigilosos, logo serão tratados assim pelos seus colaboradores e todos que tenham acesso a estes.

As Informações, independentemente da forma apresentada, compartilhada ou armazenada, são de responsabilidade de quem as gerou, recebeu ou armazenou e, devem ser utilizadas apenas para sua finalidade original, estando sujeitos a monitoramento e auditoria.

É proibida a modificação, divulgação e destruição não autorizadas das Informações, quer oriundas de erros, ou mesmo fraudes, vandalismo, espionagem ou sabotagem.

Igualmente, as Informações Confidenciais, como definida na seção 5 abaixo, deverão ser mantidas em caráter sigiloso, com acesso restrito, sendo controladas suas cópias, dados e reproduções, não podendo ser repassadas para terceiros sem consentimento por escrito do Grupo Mafra.

É também objetivo desta Política, a Segurança Cibernética que visa prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente virtual.

O Grupo Mafra adotará ferramentas, procedimentos e controles para reduzir sua vulnerabilidade a incidentes e atender aos objetivos de Segurança Cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

Equipamentos particulares/privados como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às

redes do Grupo Mafra, ressalvadas as hipóteses devidamente autorizadas pelo gestor da área, que, em caso necessário, entrará em contato com o setor de Tecnologia.

Nenhuma Informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Os Agentes de Segurança da Informação não devem discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto.

Com relação aos prestadores de serviços e terceiros que tenham acesso às instalações, informações e dados do Grupo Mafra, os instrumentos legais que regulamentam a relação entre as partes deve conter cláusulas que contemplem a responsabilidade destes no cumprimento desta Política de Segurança da Informação, suas normas e procedimentos.

PROCESSO DE SEGURANÇA DA INFORMAÇÃO

FICA A CARGO DA DIRETORIA DO GRUPO MAFRA:

Dar anuência ao Plano de Segurança da Informação, proposto pela Presidência e Diretoria de Operações do Grupo Mafra quanto a Informação e os testes periódicos de análise de vulnerabilidade, realizados pelo Grupo Mafra ou por empresas externas.

Aprovar os investimentos necessários a serem aplicados no Grupo Mafra para a garantia dos níveis adequados da Segurança da Informação.

Gerenciar, conjuntamente, os riscos à informação considerados críticos e importantes para o negócio da empresa e que tenham que ser acompanhados no nível máximo da empresa.

Aprovar proposta da Diretoria de Operações de procedimentos e controles em níveis de complexidade, abrangência e precisão voltados à prevenção e ao tratamento dos incidentes a serem adotados pelo Grupo Mafra e por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais do Grupo Mafra.

FICA A CARGO DA DIRETORIA DE OPERAÇÕES:

Gerenciar a Segurança de Tecnologia da Informação no mais alto nível organizacional da empresa, de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio do Grupo Mafra.

Elaborar e revisar anualmente um procedimento operacional de Segurança da Informação contendo: Objetivo, escopo, definição de funções e responsabilidades, investimentos necessários e riscos envolvidos.

Assegurar atendimento em tempo integral, eficiente e autônomo para atender e orientar nos casos de incidentes que possam colocar em risco a Segurança da Informação da Empresa, bem como de seu patrimônio.

Assegurar que os Agentes de Segurança da Informação estejam cientes das ameaças e das preocupações que possam intervir na segurança e que sejam orientados para apoiar esta Política.

Alertar aos Agentes de Segurança da Informação que qualquer Informação ou sistema de Informação é passível de monitoramento, desde que, seja feito através de um processo formal e sistemático.

Definir os parâmetros a serem utilizados na avaliação de relevância dos incidentes, registrar a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Grupo Mafra

Efetuar testes e elaborar cenários de incidentes aos serviços e canais eletrônicos de Informações.

Estabelecer procedimentos e controles em níveis de complexidade, abrangência e precisão voltados à prevenção e ao tratamento dos incidentes a serem adotados pela Companhia e por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Companhia.

Informar como a confidencialidade e integridade serão mantidas, e como a disponibilidade dos serviços será assegurada em caso de incidente ou desastre;

Manter a segurança quanto aos aspectos dessa norma, quanto a responsabilidade pelo processo, auditando-os periodicamente, buscando a certificação do cumprimento dos requisitos de segurança.

Assegurar que os recursos de tecnologia colocados à disposição dos Agentes de Segurança da Informação sejam utilizados apenas para as finalidades aprovadas pela Empresa.

Analisar periodicamente os ativos da Informação, de forma que estejam devidamente inventariados, protegidos, tenham um responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança.

Garantir que a aquisição de novos produtos, a seleção de mecanismos de segurança e a aquisição de bens e/ou serviços de tecnologia levem em consideração o balanceamento de risco, tecnologia, custo, qualidade, velocidade e impacto nas atividades do Grupo Mafra.

Assegurar que se evite quaisquer ações ou situações que possam expor a Empresa a riscos de perda financeira, material ou humana, direta ou indiretamente, potenciais ou reais, comprometendo suas atividades.

Assegurar que medidas preventivas sejam tomadas para diminuir risco de ocorrência de fraudes internas ou externas, mantendo um forte processo de avaliação de riscos de Segurança da Informação e implementação de respectivos requisitos, utilizando-se de tecnologia de ponta e de um serviço de inteligência apropriado, bem como, uma equipe

competente e preparada para dar tratamento a casos deste tipo, com agilidade e eficiência.

Adotar mecanismos para disseminação da cultura de segurança cibernética no Grupo Mafra (programas de capacitação/rotinas de Informação a usuários finais/novos usuários sobre esta Política/precauções na utilização de ferramentas eletrônicas/ comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética), bem como, para verificação do cumprimento desta Política.

Monitorar para que todos os Agentes de Segurança da Informação conheçam as normas e demais decisões administrativas oriundas dos órgãos de administração do Grupo Mafra especificamente com relação à Segurança da Informação, bem como obrigações estatutárias.

Na relação com terceiros contratados, esclarecer que o Grupo Mafra tem o direito de auditar o uso de recursos de Tecnologia de Informação do terceiro, sempre que entender necessário, desde que devidamente aprovado pelos gestores diretos de ambas as partes.

Garantir a observância, pelos terceiros contratados, desta Política e dos requisitos legais e regulamentos internos do Grupo Mafra;

Adotar providências de forma a reduzir as possibilidades de erro humano, falhas de equipamentos e dispositivos, ou qualquer outro tipo de incidente que possa causar a perda da integridade das informações.

Controlar os acessos aos ambientes tecnológicos e de informação do Grupo Mafra através de um processo formal, físico e lógico ao ambiente ou serviços disponíveis em servidores, devendo as autorizações de acesso ser revistas, auditadas, confirmadas e continuadamente registradas.

Monitorar o tráfego efetuado em ambientes, recursos de Tecnologia de Informação e acordos de níveis de serviço rastreando eventos críticos e evidenciando possíveis ocorrências, dando ampla e geral divulgação dessa atividade e da possibilidade de uso desse recurso em casos de incidentes.

Prever no orçamento anual do Departamento, os recursos necessários para atendimento a esta Política, bem como, manter os níveis adequados em Segurança da Informação.

FICA A CARGO DOS COLABORADORES DO GRUPO MAFRA:

Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.

Cumprir as determinações desta Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis.

Utilizar recursos e sistemas de informações do Grupo Mafra somente para os fins profissionais.

Responder, por todo e qualquer acesso, aos recursos bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado.

FICA A CARGO DOS DIRETORES E GESTORES DO GRUPO MAFRA:

Gerenciar o cumprimento desta Política, por parte de seus supervisionados.

Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

Zelar, em nível físico e lógico, pelos ativos de informação e de processamento do Grupo Mafra relacionados com sua área de atuação.

Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações.

Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI (Tecnologia da Informação), que acessos e permissões devem ter os colaboradores, sob sua supervisão, a informações e sistemas.

Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de TI (Tecnologia da Informação), quais os colaboradores demitidos ou transferidos, para exclusão de permissões no cadastro dos usuários.

Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI (Tecnologia da Informação), aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

CONCEITOS

Agentes de Segurança da Informação: administradores (diretores, membros do Conselho de Administração e membros dos demais comitês do Grupo Mafra), membros do Conselho Fiscal, colaboradores, fornecedores, clientes e quaisquer outros envolvidos direta ou indiretamente em processos internos do Grupo Mafra.

Informação: é todo o conjunto de dados e elementos gerados ou desenvolvidos pelo e para o Grupo Mafra, de propriedade ou não deste, podendo estar presentes em sistemas de informação, arquivos digitais, equipamentos, conversas, diretórios de rede, bancos de dados internos ou externos, mídia impressa, magnética ou ótica, dispositivos eletrônicos móveis, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral que, independentemente da forma apresentada, compartilhada ou armazenada, devem ser adequadamente manuseadas e protegidas, e utilizadas apenas para a sua finalidade originária.

Informação Confidencial: Informação não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbal ou de outra forma emitidas, reveladas e obtidas pelo Grupo Mafra.

Segurança da Informação: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger as informações do Grupo Mafra.

Segurança Cibernética: Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado.

Canal de Ética – Canal de comunicação do Grupo Mafra para recebimento de denúncias relacionadas ao não atendimento desta Política.

Grupo Mafra: Grupo empresarial controlado pela empresa CM Hospitalar S.A., e suas empresas subsidiárias.

DOCUMENTOS ASSOCIADOS

Documentos de normas e procedimento internos sobre:

- Anexo I - Política de senhas
- Anexo II - Política de uso do e-mail corporativo
- Anexo III - Política de acesso à Internet
- Anexo IV - Política de uso da estação de trabalho
- Anexo V – Política de controle de acesso

Documentos e Normas externas:

- NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;
- Lei Geral de Proteção de Dados – Lei 13.709/18
- PCI - Data Security Standard

DISPOSIÇÕES GERAIS

No que se refere a Informações, confidenciais ou não, em custódia ou não, é proibido tudo aquilo que não esteja previamente autorizado por esta política e demais documentos normativos.

É competência do Conselho de Administração da empresa CM Hospitalar S/A, alterar esta Política sempre que se fizer necessário.

Esta Política entra em vigor na data de sua aprovação pelo Conselho de Administração da empresa CM Hospitalar S/A.

APROVAÇÕES

Elaboração	Revisão	Aprovação
Compliance, Controles Internos, Jurídico, Tecnologia da Informação	V00	Comitê de Auditoria, Gestão do Risco, Compliance e de Recursos Humanos Conselho de Administração

POLÍTICA DE SENHAS

A autenticação nos sistemas de informática será baseada em uma senha.

Uma senha segura deverá conter no mínimo 8 caracteres sendo (letras maiúsculas, letras minúsculas, números e caracteres especiais).

As senhas terão um tempo de vida útil determinado pela equipe de segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas.

Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades são pessoais e intransferíveis.

Os Agentes de Segurança da Informação são responsáveis por todos os atos executados com seu identificador (login), que é único e requer senha exclusiva para identificação/autenticação individual no acesso à Informação e aos recursos de tecnologia.

Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.

ANEXO II – Política de Uso de E-mail Corporativo

POLÍTICA DE USO DE E-MAIL CORPORATIVO

APLICAÇÃO

Esta política é válida para: todos os colaboradores do Grupo Mafra ("colaboradores"), conforme abrangência definida no Código de Conduta Profissional ("Código de Conduta").

VIGÊNCIA

Prazo indeterminado até sua revisão pelo Comitê de Auditoria, Gestão do Risco, Compliance e de Recursos Humanos e sua aprovação pelo Conselho de Administração.

PRAZO DE REVISÃO

Será revisada a cada dois anos de vigência da Política ou quando houver alteração na legislação que regulamenta a matéria.

DEFINIÇÕES

1. Usuário: pessoa que acessa ou utiliza de forma legítima e autorizada as informações da empresa.

2. E-mail corporativo: também denominado e-mail, é o sistema de correio cujo domínio identifica a instituição. Ex.: exemplo@mafrahospitalar.com.br.

3. Recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento.

CAMPO DE APLICAÇÃO

Esta política se aplica no âmbito do Grupo Mafra, neste documento constam princípios, orientações e regras de conduta que devem ser observados por todos os usuários de e-mail corporativo do grupo, de forma a garantir o uso responsável do e-mail através dos recursos disponibilizados.

OBJETIVO

1. Disponibilização do serviço de e-mail corporativo do Grupo Mafra para os usuários da empresa;

2. Definir os requisitos e as regras de segurança para o uso do e-mail corporativo.

PRIVACIDADE

1. O usuário não deve manter qualquer expectativa de privacidade sobre as mensagens criadas, armazenadas, enviadas ou recebidas através do sistema de e-mail corporativo;

2. O Grupo Mafra, como proprietária do sistema de e-mail corporativo, poderá, a qualquer tempo e sem aviso prévio, monitorar o uso do sistema e inclusive o conteúdo das mensagens quando julgar necessário;

3. Os e-mails corporativos são disponibilizados aos usuários como ferramenta de trabalho e, portanto, são propriedades do Grupo Mafra.

FINALIDADE

O serviço de e-mail corporativo tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do Grupo Mafra.

CRIAÇÃO/DESATIVAMENTO DE CONTAS DE E-MAIL

A concessão de contas de e-mail corporativo depende de pedido formal do responsável pela área, através do portal chamados.mafrahospitalar.com.br, informando: nome completo do usuário, matrícula, cargo, empresa, unidade, setor no qual está desempenhando suas atividades e justificativa da necessidade da conta de e-mail.

Assim que criado o e-mail, será respondido o chamado com o nome do e-mail corporativo, a senha provisória e a Política de uso do e-mail.

Em caso de desligamento do colaborador, o Departamento de RH deverá informar ao time responsável pela manutenção dos e-mails, que deverá imediatamente desativar o e-mail que era utilizado pelo colaborador.

RESPONSABILIDADE

O usuário é responsável por:

1. Conteúdo de mensagens enviadas via e-mail corporativo sob sua identificação;

2. Proteger a confidencialidade de sua senha de acesso – ela não pode ser compartilhada, sendo de uso pessoal, intransferível e deverá ser trocada no primeiro acesso ao e-mail;

3. Verificar se a origem da mensagem recebida é de fonte confiável e de interesse da empresa, a fim de evitar algum dano aos recursos tecnológicos;

4. Para fins de isenção de responsabilidade, todo e qualquer e-mail corporativo deverá sair com a seguinte comunicação:

> **Aviso 1**: Este e-mail pode conter informações e documentos confidenciais e/ou protegidos por lei. Se você não for o efetivo destinatário, pedimos, por favor, que desconsidere completamente o seu conteúdo e os devolva ao seu remetente e os apague imediatamente, ficando proibida a sua cópia e/ou encaminhamento para terceiros.
>
> **Aviso2**: Apesar do Grupo Mafra tomar todas as cautelas necessárias para evitar que nenhum vírus esteja presente nessa mensagem, ele não se responsabiliza por eventuais perdas ou danos eventualmente causados por esse e-mail ou seus anexos.

INFORMAÇÕES

O acesso indevido às informações tramitadas por meio do e-mail corporativo do Grupo Mafra ou contidas em seus ambientes, será punido na forma da lei.

Caso receba uma mensagem originada da Internet de um remetente desconhecido, você deve remover essa mensagem da sua caixa de entrada, preferencialmente antes mesmo de abri-la.

Não responder caso receba mensagens contendo texto ou imagem não profissional ou de propaganda. Nem mesmo que seja para solicitar o cancelamento do envio de spam, exemplo: "Clique Aqui caso não queira mais receber este e-mail.", este é um tipo de ataque que consiste em enviar e-mails para uma lista e caso o usuário cadastre que não queira mais receber este e-mail o hacker fica sabendo que este é um e-mail válido e vende a lista de e-mails para empresas de marketing digital, propagando ainda mais o spam.

Ao enviar ou responder uma mensagem para um destinatário com cópia para várias pessoas, tenha certeza de que todas as pessoas realmente devem receber a mensagem. A facilidade de se copiar uma mensagem no e-mail corporativo nos leva a endereçar cópias para muitas pessoas. Cópias desnecessárias sobrecarregam os recursos tecnológicos.

Quando enviar e-mails com anexo tome cuidado com o tamanho máximo da mensagem e anexos, o tamanho máximo do e-mail com os anexos será de 20 MB, porém alguns servidores de e-mails externos (gmail, yahoo, uol, etc) restringem o tamanho das mensagens em 20 MB ou até menos.

Tenha o hábito de excluir com frequência e-mails desnecessários, inclusive e-mails da lixeira e da pasta mensagens enviadas, para não sobrecarregar os recursos tecnológicos.

Em caso de férias, suspensão ou qualquer outra maneira de afastamento temporário do colaborador por mais de 48h, ele deverá adotar as providências necessárias para que as mensagens enviadas ao seu e-mail sejam automaticamente redirecionadas para o e-

mail de outro colaborador – cuja determinação ficará a cargo do gerente responsável pela área – enquanto estiver afastado de suas atividades.

Em caso de férias, o colaborador deverá ativar uma resposta automática informando o período de sua ausência, a previsão de volta às atividades e os contatos dos colaboradores que poderão responder durante o período que estiver afastado de suas atividades.

Caso ocorra constatação de má utilização do e-mail corporativo, o Grupo Mafra reserva-se o direito de investigar o acesso do usuário.

O Grupo Mafra poderá suspender o acesso do usuário em caso de comprovação de utilização inadequada ou para averiguação de fatos.

O usuário não possui o direito de fazer cópias (backups) dos e-mails em caso de desligamento da instituição.

Não utilizar o e-mail corporativo para cadastro em sites de compras, em listas tipo FEEDS e NEWS (ex.: sacks, barataoweb, baratocoletivo, mercadolivre), pois são malas direta para envio de SPAMS, responsáveis por problemas que podem ocasionar o bloqueio do domínio (*.mafrahospitalar.com.br) para envio de mensagens.

Deve evitar todo e qualquer procedimento de uso do e-mail não previsto nesta Política, que possa afetar de forma negativa o Grupo Mafra.

VEDAÇÕES

É vedado ao usuário o uso do e-mail corporativo com o objetivo de:

1. Praticar crimes e infrações de qualquer natureza;

2. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

3. Executar ações nocivas contra outros recursos computacionais do Grupo Mafra ou de redes externas;

4. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede do Grupo Mafra;

5. Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

6. Enviar arquivos de áudio, vídeo ou animação, salvo os que tenham relação com as funções institucionais desempenhadas pelo Grupo Mafra;

7. Divulgar, no todo ou em parte, os endereços eletrônicos corporativos;

8. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema ou a imagem do Grupo Mafra;

9. Reproduzir qualquer material recebido pelo e-mail corporativo ou outro meio que possa infringir direitos autorais, marcas, licença de software ou patentes existentes, sem que haja permissão comprovada do criador do trabalho;

10. Encaminhar mensagens que representem a opinião pessoal do autor, colocando-a em nome do Grupo Mafra;

11. Utilizar o e-mail corporativo para cadastro em sites de compras, em listas tipo FEEDS, NEWS, em sites de relacionamento ou redes sociais.

12. Forjar ou tentar forjar a identidade de outros usuários (por exemplo, usar o endereço de outro usuário para envio de e-mails).

SANÇÕES

Havendo descumprimento de quaisquer das normas objeto desta Política, o infrator estará sujeito às sanções estabelecidas no Código de Conduta, no respectivo contrato individual e/ou na legislação.

O Grupo Mafra conta com canais de comunicação, gerenciados pelo seu Comitê de Compliance, por meio dos quais os colaboradores e demais terceiros interessados podem denunciar, de forma anônima ou identificada, práticas irregulares eventualmente ocorridas na empresa. Os Canais de Comunicação são acessíveis a todos os interessados, que deverão procurar o Comitê de Compliance por algum dos seguintes meios:

- E-mail: eticagrupomafra@deloitte.com.br
- Telefone: 0800-7219152
- Contato pessoal com integrantes do Comitê
- www.ethicsdeloitte.com.br/grupomafra
- Endereço de correspondência: Avenida Luiz Maggioni, nº 2727, Distrito Empresarial Luiz Roberto Jábali, CEP 14.072-055, Ribeirão Preto/SP (A/C Comitê de Compliance).

POLÍTICA DE ACESSO À INTERNET

O uso recreativo da internet não deverá se dar no horário de expediente.

Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do supervisor do departamento local.

Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado

É proibido o uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança

Lembrando novamente que o uso da internet será auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

POLÍTICA DE USO DE ESTAÇÃO DE TRABALHO

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, ressalvadas as exceções em que o colaborador compartilha a estação de trabalho com um turno distinto, cada colaborador tem sua estação própria de trabalho.

Tudo que venha a ser executado de sua estação e identificado com sua senha acarretará responsabilidade sua.

Por isso sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou travou o console.

Não instale nenhum tipo de software/hardware sem autorização da equipe técnica ou de segurança.

Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria

Mantenha na sua estação somente o que for supérfluo ou pessoal.

Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica

ANEXO V – Política de Controle de Acesso

POLÍTICA DE CONTROLE DE ACESSO

OBJETIVO

Estabelecer as regras que norteiam as atividades de Controle de Acesso no Grupo.

Campo de aplicação

Esta política é válida para: todos os colaboradores do Grupo Mafra ("colaboradores"), conforme abrangência definida no Código de Conduta Profissional ("Código de Conduta").

Definições

Acesso – Ato de ingressar, transitar, conhecer ou consultar a informação, seja local, ou remotamente, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

Ativos de Informação – Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Bloqueio de Acesso – Processo que tem por finalidade suspender temporariamente o acesso.

Contas de Serviço – Contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, *script* etc.) sem qualquer intervenção humana no seu uso.

Credenciamento de Acesso – Processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia.

Credenciais ou Contas de Acesso – Identificações concedidas após o processo de credenciamento de acesso, que permitam habilitar determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão, credencial biométrica ou lógica como identificação de usuário e senha.

Equipamentos - Instrumentos necessários para determinada função.

Exclusão de Direito de Acesso – Processo que tem por finalidade suspender definitivamente o acesso.

Exclusão de Conta de Acesso – Processo que tem por finalidade o cancelamento do código de identificação e do perfil de acesso.

Gestão de Riscos de Segurança da Informação e Comunicações – Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Gestor do ativo de informação – indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Identificação do Usuário ou Nome do Usuário – forma pela qual o usuário é conhecido no ambiente de informática da CM Hospitalar S/A. O usuário recebe as permissões de utilização dos recursos computacionais em função de sua Identificação, que deve ser validada com o uso de uma Senha.

Menu – Lista de opções ou entradas postas à disposição do usuário, que aparece no vídeo de um terminal de computador com as funções que este poderá realizar por meio de um programa ou de um *software*.

Necessidade de Conhecer – Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

Perfil de Acesso – Conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

Quebra de Segurança – Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

Usuário – Qualquer empregado ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da CM Hospitalar S/A.

Conformidade

1.1. Ao usuário de informações não é dado o direito de desconhecimento da Política de Segurança da Informação, devendo seguir rigorosamente o disposto nas regras.

1.2. Esta política é comunicada para todo o pessoal envolvido e largamente divulgada, garantindo que todos a conheçam e apratiquem.

1.3. A inobservância das políticas e normas de segurança sujeita o usuário a sanções

internas e, nos casos cabíveis, às leisvigentes.

2. Verificações de cumprimento da política devem ser efetuadas, para verificar o nível de segurança das áreas e elaborar projetos para melhoria dos índices de conformidade.

Descrição

O processo de concessão de credenciais de acesso aos ativos de informação da CM Hospitalar S/A deve levar em conta os resultados da análise de risco de Segurança da Informação e Comunicações e o processo de concessão de acesso à informação deve levar em conta a autenticidade dessas credenciais de acesso.

Controle de Acesso

Conjunto de procedimentos, recursos e meios utilizados pela Empresa com a finalidade de conceder ou bloquear o acesso aos ativos de informação a usuários autorizados ou não.

Papeis e responsabilidades

Setor de tecnologia da informação TI

Definir, implementar e gerenciar um sistema de controle de acesso para todos os ativos de informação da CM Hospitalar S/A, não importando sua localização física.

Prover o controle e a autenticação das conexões externas dos usuários e viabilizar a segurança da informação quando for necessária a utilização de computação móvel e demais recursos de trabalho remoto.

Estabelecer procedimentos que garantam a segurança da informação para o acesso aos sistemas (logon).

Prover a segurança da informação quando da utilização de programas utilitários que sejam capazes de sobrepor os controles dos sistemas e aplicações.

Assegurar que o acesso à informação e às funções dos sistemas de aplicação, por parte dos usuários, seja baseado nos requisitos de restrição de acesso do negócio.

Criar contas de serviço observando-se a premissa do menor privilégio possível, os requisitos do negócio, e o resultado da análise de risco.

Monitorar o acesso e o uso dos sistemas para os fins desta Norma.

Usuários

Zelar pela integridade e confidencialidade de suas credenciais de acesso aos recursos computacionais da CM Hospitalar S/A (identificação de usuário e senha).

Zelar e contribuir para um efetivo controle de acesso aos recursos computacionais da CM Hospitalar S/A, de forma a prevenir o acesso não autorizado aos ativos informacionais e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.

Assegurar a segurança da informação ao utilizar computação móvel e demais recursos de trabalho remoto.

Criação ou Bloqueio de Conta de Acesso

A solicitação para criação ou bloqueio de contas de acessos de usuários, quando do início ou término da prestação de serviço, pode ser realizada pelas áreas do quadro abaixo.

A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento de acesso para qualquer usuário.

Área Responsável pela Solicitação de Criação ou Bloqueio de Conta de Acesso	Categorias de Usuário Para os Quais Pode Solicitar a Criação ou Bloqueio de Conta de Acesso
Área de Recursos Humanos	Empregados e estagiários
Gerentes e outros hierarquicamente equiparados	Prestador de Serviço Terceirizado
Diretor da área que estiver vinculado	Outros usuários

Exclusão de conta de acesso

A exclusão de conta de acesso de um usuário somente poderá ser executada caso sua identificação não tenha sido criada corretamente e não existam registros de *logs* gerados pelos acessos aos ativos de informação da organização. Caso tenha ocorrido pelo menos um registro de acesso aos ativos de informação, a conta de acesso deve ser bloqueada indefinidamente.

Análise Crítica do Direito de Acesso

Cabe ao Gestor da Informação realizar a cada 6 (seis) meses uma análise crítica dos direitos de acesso do usuário aos ativos de informação sob sua gestão. Nos casos de ativos de informações sigilosos, esta análise deve ser feita a cada 3 (três) meses.

Integridade e Confidencialidade das Credenciais de Acesso

A fim de zelar pela integridade e confidencialidade de suas credenciais de acesso e efetivamente contribuir para a efetiva gestão do controle de acesso aos recursos computacionais e informacionais da CM Hospitalar S/A, o Usuário deve seguir as seguintes regras:

Manter a confidencialidade de sua senha pessoal.

Trocar de senha na primeira vez que utilizar a conta de acesso aos sistemas.

Solicitar uma nova senha, quando do esquecimento.

Evitar o registro das senhas em qualquer meio.

Alterar a senha sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade.

Criar senhas que sejam fáceis de lembrar, mas que não sejam baseadas em elementos que outras pessoas ou possíveis invasores possam facilmente adivinhar, ou deduzir, a partir de informações pessoais, como, por exemplo:

Nome do usuário;

- Identificador do usuário (ID), mesmo que seus caracteres estejam embaralhados;
- Nome de membros de sua família ou de amigos íntimos;
- Nomes de pessoas ou lugares em geral;
- Nome do sistema operacional ou da máquina que está sendo utilizada;
- Datas significativas, como a do nascimento próprio, de um filho, esposa, etc.;
- Números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- Placas ou marcas de veículos;
- Palavras que constam de dicionários em qualquer idioma;
- Letras ou números repetidos.

Alterar a senha em intervalos regulares e evitar a reutilização de senhas antigas. Escolher suas próprias senhas.

Selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que o obrigue a registrá-la em qualquer outro meio para não serem esquecidas.

Encerrar as sessões ativas ou utilizar-se do mecanismo de bloqueio de acesso (tela de proteção com senha) quando precisar se afastar dos equipamentos, mesmo que seja por um período curto. É vedado a todo usuário:

Incluir senhas em processos automáticos de acesso a sistemas, por exemplo, armazenadas em macros ou nos navegadores da WEB.

Revelar credenciais de acesso ou permitir o acesso a ativos de informação por terceiros por meio dessas credenciais.

Disposições Gerais

Casos omissos ou excepcionais serão submetidos à aprovação da Diretoria Executiva.

A não observância aos dispositivos dessa Norma pode acarretar, nos termos da legislação aplicável, sanções administrativas, civis e/ou penais.

ANEXO VI - Declaração de ciência e concordância

TERMO DE COMPROMISSO

Eu, _____, inscrito no CPF sob o nº _____, portador do RG nº _____, declaro que obtive acesso a Política de Segurança da Informação do Grupo Mafra e estou ciente de todos os seus termos, com os quais tenho total concordância e me comprometo a cumpri-los durante a minha prestação de serviços para qualquer empresa que componha o Grupo Mafra.

Declaro estar ciente de que eventual violação de minha parte a qualquer regra estabelecida nessa política, poderá culminar na aplicação de sanções com base no Código de Conduta, sem prejuízo de eventuais sanções legais.

Por ser verdade, assino o presente termo.

Local/data:_____

_____

Assinatura