POLÍTICA DE CONTROLE DE ACESSO LÓGICO

- PROGRAMA DE GOVERNANÇA EM PRIVACIDADE SMARTSYSTEMIT –

HISTÓRICO DE VERSÕES

POLÍTICA DE CONTROLE DE ACESSO LÓGICO	Código: PCAL	
Documento desenvolvido pela Paliares & Sanchotene Advogados Associados especificamente para SMARTSYSTEMIT.	Data de Criação: 04/04/2024	Versão: 00
Revisão PS Advogados Associados	Data de Revisão 15/07/2024	Versão: 01

SUMÁRIO

A SMARTSYSTEMIT SOLUÇÕES EM INFORMÁTICA LTDA **(“**SMARTSYSTEMIT**”)** possui o compromisso de resguardar e proteger as informações e os dados, sejam eles pessoais ou não, que estão sob sua guarda.

Nesse contexto, a segurança da informação é uma atividade essencial de proteção de todos os ativos tangíveis e intangíveis da SMARTSYSTEMIT.

Dessa forma, a presente POLÍTICA DE CONTROLE DE ACESSO LÓGICO (“Política”) apresenta diretrizes gerais de conduta, para possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas no âmbito de atividades da SMARTSYSTEMIT.

Esta Política está de acordo com as leis vigentes em nosso país, bem como está alicerçada nas recomendações das normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e ABNT NBR ISO/IEC 27003:2020 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações.

Esta Política aplica-se à alta gestão, colaboradores, terceirizados, estagiários, aprendizes, usuários da rede visitante (sem fio), parceiros e/ou empresas contratadas pela SMARTSYSTEMIT.

1. ACESSO

O acesso às informações rotuladas como públicas e de uso interno não é restringido com controles de acesso que discriminam o usuário.

O acesso às informações confidenciais e restritas serão permitidas apenas quando uma necessidade de trabalho tiver sido identificada e, tal acesso aprovado pelo gestor do contrato ou responsável pelo setor ou departamento de lotação.

O acesso a alguns equipamentos de hardware e/ou software especiais (tais como equipamentos de diagnóstico de rede) é restrito aos profissionais do Departamento de Tecnologia da Informação, com uso registrado, baseado nas necessidades da SMARTSYSTEMIT.

Será dado a todos os usuários da SMARTSYSTEMIT, o acesso aos serviços básicos (e-mail, sistema, etc.), quando este for o caso.

Estas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela autoridade competente.

Todos os outros recursos dos sistemas serão providos via perfis de trabalho ou por solicitação feita ao proprietário da informação envolvida.

Quaisquer questões sobre controle de acessos privilegiados deverão ser direcionadas ao gestor do contrato ou responsável pelo setor ou departamento de lotação.

2. TERMOS DE DEFINIÇÕES

Os seguintes termos são utilizados nesta Política aos ativos e aos sistemas de informação da SMARTSYSTEMIT com os significados específicos que se seguem:

i. **Arquivo**: agrupamento de registros que, geralmente, seguem uma regra estrutural e que possuem informações (dados).
ii. **Autenticidade**: garantia de que uma informação, produto ou documento é do autor a quem se atribui.
iii. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
iv. **Credenciais de acesso**: conjunto composto pelo nome de conta e respectiva senha, utilizado para o ingresso ou acesso (login) em equipamentos, rede ou sistema.
v. **Criptografia**: arte e ciência de esconder o significado de uma informação de receptores não desejados.
vi. **Disponibilidade**: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado.
vii. **Estações de trabalho**: computador pessoal utilizado para trabalho nas dependências da empresa.
viii. **Gestor/Responsável**: colaborador oficialmente designado como gestor de determinado setor ou sistema de informação.
ix. **Integridade**: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades.
x. **Ponto de acesso sem fio**: equipamento que compõe uma rede sem fio (wireless), concentrando as conexões de um ou mais equipamentos.
xi. **Privilégio mínimo**: conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades.

xii. **Programa**: coleção de instruções que descrevem uma tarefa a ser realizada por um computador.

xiii. **Recursos de armazenamento de dados corporativos**: armazenamento de massa projetado para ambientes de grande escala e alta tecnologia.

xiv. **Recursos de TI**: todo equipamento ou dispositivo que utiliza tecnologia da informação, bem como qualquer recurso ou informação que seja acessível por meio desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local, internet, VPN (rede particular virtual), pendrives, smartcards, tokens, smartphones, modens sem fio, desktops, pastas compartilhadas em rede, entre outros.

xv. **Rede local da SMARTSYSTEMIT**: conjunto de recursos compartilhados por meio dos servidores de rede, switches e computadores clientes, por onde circulam as informações corporativas da SMARTSYSTEMIT.

xvi. **Rede sem fio (wireless)**: sistema que interliga equipamentos utilizando o ar como via de transmissão por meio de ondas eletromagnéticas.

xvii. **Sistema de informação**: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação.

xviii. **Sistemas de mensageria**: sistemas que permitem o envio e a recepção de mensagens de correio eletrônico ou de mensagens instantâneas entre usuários, dentro e fora da instituição.

xix. **Storages**: rede de área de armazenamento projetada para agrupar dispositivos de armazenamento de computador.

xx. **TI**: Tecnologia da Informação.

xxi. **TIC**: Tecnologia da Informação e Comunicação são um conjunto de recursos tecnológicos utilizados de forma integrada com um objetivo comum.

xxii. **Departamento**: unidade em que está lotado o colaborador, assessor, terceirizado, estagiário ou aprendiz.

xxiii. **Usuário**: pessoa física ou jurídica que opera ou tem acesso a algum sistema informatizado da SMARTSYSTEMIT.

xxiv. **Web**: Rede Mundial de Computadores.

xxv. **Webconferência**: reunião ou encontro virtual realizado pela internet por meio de aplicativos ou serviço com possibilidade de compartilhamento de apresentações, voz, vídeos, textos e arquivos por meio da web.

3. CADASTRAMENTO DE USUÁRIOS

A criação de novas contas de acesso à rede ou sistemas se dará da seguinte forma:

i. **colaboradores**: diretamente pelo responsável pelo setor ou do departamento de lotação, informando o nome completo, a função e a matrícula do colaborador;
ii. **estagiários e menores aprendizes**: diretamente pelo responsável pelo setor ou do departamento de lotação, informando o nome completo, a função e a matrícula do estagiário ou menor aprendiz e a vigência do contrato;
iii. **prestadores de serviço**: diretamente pelo gestor do contrato, informando o nome completo, departamento de lotação, número e vigência do contrato, nome da empresa contratada e matrícula na empresa contratada (ou outro documento legalmente válido).

Nas eventuais substituições, caberá ao responsável a configuração adequada do período de acesso do colaborador, estagiário, menor aprendiz ou prestador de serviço.

As contas dos estagiários, menores aprendizes e prestadores de serviço serão configuradas para expiração automática, concomitantemente à vigência do contrato, salvo nos casos de desligamento antes do prazo estipulado na contratação, hipótese na qual o responsável pelo setor ou do departamento de lotação deve providenciar seu desligamento.

Caberá ao gestor do contrato ou responsável pelo setor ou departamento de lotação, quando for o caso, solicitar ao Departamento de TI a liberação ou restrição de privilégios de acesso aos documentos de sua unidade, essa solicitação deverá ser realizada via e-mail.

Para evitar a expiração automática da conta de estagiários, menores aprendizes ou de prestadores de serviços, deverá o gestor do contrato ou responsável pelo setor ou departamento de lotação, tomar as devidas providências com antecedência mínima de 72 (setenta e duas) horas à expiração da conta.

Todos os usuários que utilizam aplicações e sistemas da SMARTSYSTEMIT devem assinar o TERMO DE RESPONSABILIDADE (“Termo”) sobre o conhecimento da Política de Controle de Acesso Lógico da SMARTSYSTEMIT.

A assinatura do documento Termo indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos da SMARTSYSTEMIT relacionados ao ambiente de TI, incluindo as instruções contidas nesta Política, bem como as implicações legais decorrentes do não cumprimento do disposto no termo.

O gestor do contrato ou responsável pelo setor ou do departamento de lotação, ficará responsável por recolher a assinatura deste Termo sobre o conhecimento da Política de Controle de Acesso Lógico da SMARTSYSTEMIT.

É de responsabilidade do gestor do contrato realizar o cancelamento da conta de acesso quando do desligamento ou afastamento do prestador de serviço.

Não haverá identificação genérica e de uso compartilhado para acesso aos recursos de rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer gestor do contrato ou responsável pelo setor ou do departamento de lotação, acerca da possibilidade de aceitação dos riscos associados.

As contas de acesso à rede ou sistemas serão compostas pelo nome do respectivo departamento e/ou cargo/função ocupado, sendo a forma padrão, separados por ponto quando necessário.

Caso a forma padrão incorra em repetição com conta já existente, será acrescido numeral sequencial.

No ato da criação de conta de acesso à rede ou sistemas, será automaticamente criada conta dos serviços de correio eletrônico (e-mail), mensageria e agenda correspondente, bem como de outros serviços que utilizem a mesma base de dados para autenticação.

Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.

No descumprimento dos casos tratados no item acima, os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis, tanto o titular das credenciais quanto aquele que as utilizar indevidamente.

4. POLÍTICA DE SENHAS

A identificação de usuários que operam a rede local ou sistemas da SMARTSYSTEMIT deve ser feita mediante a autenticação usuário-senha.

A senha cadastrada é pessoal, intransferível e confidencial.

A senha deverá observar as seguintes regras de formação:

1. não pode conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos;

2. deve conter, no mínimo, 08 (oito) caracteres;
3. deve conter caracteres de três das quatro categorias seguintes:

    a) caracteres alfabéticos maiúsculos;

    b) caracteres alfabéticos minúsculos;

    c) caracteres numéricos; e

    d) caracteres especiais, não alfabéticos (por exemplo: !, $, #, %).

Nos casos de troca de senha, a nova senha não poderá ser igual às últimas 3 (três) senhas anteriormente utilizadas.

Após 3 (três) tentativas erradas, o usuário ficará bloqueado, necessitando solicitar orientações ao gestor do contrato ou responsável pelo setor ou do departamento de lotação.

Em caso de suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

Em caso de comprometimento comprovado de segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

Independentemente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

5. DO ACESSO À REDE

Apenas poderão ser conectadas à rede cabeada da SMARTSYSTEMIT microcomputadores e *notebooks* previamente autorizados pelo gestor do contrato ou responsável pelo setor ou departamento de lotação.

Exceções devem ser comunicadas à alta gestão ou Departamento de Tecnologia da Informação, justificando a necessidade e o prazo de utilização.

As exceções autorizadas deverão, obrigatoriamente, adotar os padrões definidos pela Política de Segurança da Informação da SMARTSYSTEMIT, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, uma vez que a SMARTSYSTEMIT não fornecerá licenças para o funcionamento de microcomputadores particulares.

Microcomputadores e dispositivos portáteis poderão acessar a rede sem fio específica para esse fim.

O usuário, antes de acessar a rede visitante, deverá se identificar e concordar com o termo de uso da rede sem fio.

Poderá ser desconectado das redes cabeada e sem fio qualquer dispositivo que constitua ameaça à segurança da informação.

Computadores com acesso à rede deverão ser desligados ou bloqueados na ausência do usuário.

6. DO ACESSO À INTRANET E À INTERNET

Os acessos aos portais da internet e aos demais serviços disponíveis na intranet da SMARTSYSTEMIT serão efetuados, preferencialmente, por meio da rede local e deverão ser identificados por usuário.

Os rastros de acesso deverão, no mínimo, identificar usuários, endereço IP, URL acessada, data e hora.

O Departamento de Tecnologia da Informação deverá reter os rastros de acesso pelo prazo mínimo de 60 (sessenta) dias.

É proibido o acesso a sites que tratem de pornografia, pedofilia, erotismo e correlatos; de racismo; de ferramentas para invasão e evasão de sistemas; de compartilhamento de arquivos que tratem destes assuntos; e de apologia e incitação a crimes.

O Departamento de Tecnologia da Informação poderá utilizar *software* específico que realizará o bloqueio automático desses sítios.

Os acessos a *sites* e serviços disponíveis na internet serão controlados por filtros de conteúdo e reguladores de tráfego implementados nos dispositivos de segurança da rede da SMARTSYSTEMIT, cuja operacionalização é de responsabilidade do Departamento de Tecnologia da Informação.

O gestor do contrato ou responsável pelo setor ou do departamento de lotação, deve definir, com base nas categorias de conteúdo fornecidas pelo Departamento de Tecnologia da Informação, os perfis de acesso à rede a serem aplicados a cada um de seus colaboradores.

As solicitações de criação ou alteração nas permissões de acesso deverão ser formalizadas via e-mail e arquivadas em meio eletrônico pelo respectivo departamento.

O gestor do contrato ou responsável pelo setor ou do departamento de lotação, deve fiscalizar o bom uso dos acessos à internet e solicitar ajustes e restrições, em caso de má utilização.

Mediante solicitação do gestor do contrato ou responsável pelo setor ou do departamento de lotação, o Departamento de Tecnologia da Informação poderá fornecer relatórios mensais dos acessos para permitir o devido controle.

O Departamento de Tecnologia da Informação poderá, eventualmente e quando necessário, fazer ajustes temporários no controle de banda para viabilizar eventos específicos como vídeo conferências e acesso a visitantes.

Todas as operações de acesso realizadas serão registradas para fins de auditoria.

Não será admitido burlar ou tentar burlar os filtros de conteúdo ou restrições de acesso à internet, sob pena de responsabilização dos envolvidos, que estarão sujeitos às sanções administrativas e penais cabíveis.

7. ACESSO REMOTO A SISTEMAS DE INFORMAÇÃO

O acesso remoto à rede corporativa da SMARTSYSTEMIT deve ser realizado somente para atender aos interesses de trabalho.

Compete ao Departamento de Tecnologia da Informação definir os perfis de acesso, aplicando técnicas de autenticação e de segurança.

i. o acesso remoto, no âmbito da rede corporativa, deve ser provido por meio de canal criptografado, preferencialmente utilizando as recomendações da ICP-Brasil;

ii. o acesso remoto à rede corporativa terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

iii. a permissão para se realizar acesso remoto à rede corporativa deve ser solicitada à área de administração da rede pela Coordenação ou área superior a que o usuário da rede está subordinado, com horários para se realizar o acesso; e

iv. o acesso remoto à rede corporativa será gravado, para posterior auditoria, em *logs* contendo data e hora, serviço utilizado, usuário e informações específicas que facilitem o rastreamento da ação tomada.

Quaisquer computadores que tenham comunicação remota em tempo real com os sistemas da SMARTSYSTEMIT devem se submeter ao mecanismo de controle de acesso, levando-se em consideração os privilégios necessários ao acesso a cada tipo de informação.

Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação ao gestor do contrato ou responsável pelo setor ou do departamento de lotação.

Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, o Gestor de Privacidade da SMARTSYSTEMIT deverá ser imediatamente acionado para tomar as providências necessárias a sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação da SMARTSYSTEMIT.

Os casos omissos serão resolvidos pelo Gestor de Privacidade da SMARTSYSTEMIT.

8. UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

O correio eletrônico é o recurso corporativo para comunicação a ser utilizado de modo compatível com o exercício da função, sem comprometer a imagem da SMARTSYSTEMIT nem o tráfego de dados na rede de computadores da instituição.

Todas as mensagens eletrônicas enviadas e recebidas nos domínios da SMARTSYSTEMIT terão registrados os dados: data e hora do envio ou recebimento, remetente e destinatário.

O Departamento de Tecnologia da Informação deverá implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

O Departamento de Tecnologia da Informação poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por Departamento e por usuário.

O Departamento de Tecnologia da Informação não acessará mensagens individuais de caixas de *e-mail*, salvo para atender aos seguintes objetivos:

i. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da Alta Gestão da SMARTSYSTEMIT;

ii. recuperar conteúdo de interesse da SMARTSYSTEMIT, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Alta Gestão da SMARTSYSTEMIT;

iii. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Alta Gestão da SMARTSYSTEMIT;

iv. atender à determinação judicial; e

v. realizar a recuperação de mensagens do *backup*, a pedido do próprio usuário.

O envio de mensagens a componentes da lista de endereços e grupos de *e-mails* da SMARTSYSTEMIT restringir-se-á a assuntos de interesse da SMARTSYSTEMIT.

A exclusão de caixas postais poderá ocorrer com o desligamento do usuário, mediante autorização da Alta Gestão da SMARTSYSTEMIT.

São vedadas as seguintes ações relacionadas à utilização do correio eletrônico:

i. acesso ou tentativa de acesso à caixa postal em desacordo com as diretrizes desta Política;

ii. envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições do usuário, incluindo as que contém ofensas, comentários discriminatórios e pornografia; e

iii. adulteração de dados referentes à origem da mensagem nos campos de controle e cabeçalho.

Considera-se armazenado o *e-mail* aberto e mantido na caixa postal do usuário.

O Departamento de Tecnologia da Informação prestará suporte para a configuração e utilização da tecnologia adotada para o serviço de correio eletrônico corporativo.

9. UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

O sistema de arquivos compreende um conjunto de pastas armazenadas em servidor de arquivos e compartilhadas em rede, que podem ser compartilhadas entre todos os usuários ou restrito a usuários de determinado departamento ou de determinado projeto.

O Departamento de Tecnologia da Informação realizará o *backup* dos arquivos armazenados no servidor de arquivos, conforme discriminado na Política de Segurança da Informação (backup).

O *backup* de arquivos de pastas de usuário armazenadas nas estações de trabalho é de responsabilidade do usuário.

O Departamento de Tecnologia da Informação poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas dos departamentos.

O Departamento de Tecnologia da Informação não acessará os arquivos armazenados nas pastas dos departamentos e dos usuários, salvo nas seguintes situações:

i. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da Alta Gestão da SMARTSYSTEMIT;

ii. recuperar conteúdo de interesse da SMARTSYSTEMIT, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Alta Gestão da SMARTSYSTEMIT;

iii. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Alta Gestão da SMARTSYSTEMIT;

iv. atender à solicitação judicial; e realizar a recuperação de arquivos do *backup*, a pedido do usuário.

Os casos omissos serão dirimidos pelo Gestor de Privacidade da SMARTSYSTEMIT.

Essa Política é parte do Programa de Governança e Proteção de Dados da SMARTSYSTEMIT e complementa demais normas e procedimentos vigentes.

Campinas, 04 de abril de 2024.

_____

SMARTSYSTEMIT SOLUÇÕES EM INFORMÁTICA LTDA

Rua José Paulino, no 416, Sala 105, Centro, Campinas / SP

CEP: 13013-000

(19) 3236-1117