1. INTRODUÇÃO

Com a preocupação de mantermos a segurança nas atividades da **Level 4**, apresentamos neste documento um conjunto de instruções e procediemntos para normalizar e melhorar a visão e atuação em segurança.

1.1. A empresa e a Política de Segurança

As regras aqui estabelecidas serão observadas em todos os seus detalhes por todos os colaboradores, parceiros, clientes e prestadores de serviços. Desta forma, quando divulgado e entregue a cópia deste documento, todos os que receberem se comprometem a respeitar todos os tópicos abordados e está ciente da repercussão de tais regras no seu dia-a-dia.

1.2. O não cumprimento da Política de Segurança

O não cumprimento das políticas aqui detalhadas acarretará em sanções administrativas em primeiro momento, podendo na reincidência ou conforme a gravidade do ato contrário à esta política acarretar o desligamento daquele que infringiu regras aqui dispostas.

2. OBJETIVOS

Esta Política de Segurança tem como objetivo estabelecer diretrizes que permitam aos colaboradores, parceiros, clientes e prestadores de serviços da **Level 4** seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Ainda, servirá esta Política de Segurança para nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Por fim, temos ainda como objetivo preservar as informações da **Level 4** quanto à:
• **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.

• **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. DAS RESPONSABILIDADES ESPECÍFICAS

3.1. Dos colaboradores em geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao **Level 4** e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2. Dos colaboradores em regime de exceção (temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

3.3. Dos gestores de pessoas e/ou processos

Devem ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Também devem atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da **Level 4**.

Exigirão dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **Level 4**.

Antes de conceder acesso às informações da instituição, estes deverão exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Por fim, deverão adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

4. DOS CUSTODIANTES DA INFORMAÇÃO

4.1. Da área de tecnologia da informação (TI)

São deveres da área de Tecnologia da Informação e seus prepostos:

a) Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI;
b) Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
c) Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
d) Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a **Level 4**.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, a área de TI deverá garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

É prerrogativa da área de TI da empresa proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Também deverá a área de TI garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Por fim, a área de TI deverá garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

4.2. Da área de segurança da informação

É responsabilidade da área de Segurança da Informação:

a) Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

b) Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da **Level 4**, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
c) Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

5. USO DE CORREIO ELETRÔNICO

O uso do correio eletrônico da **Level 4** é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o **Level 4** e também não cause impacto no tráfego da rede.

Contudo, os usuários não poderão ter expectativa de privacidade com relação as mensagens e anexos na utilização do correio eletrônico da **Level 4**, restando claro neste documento que todos os dados poderão ser gerenciados e monitorados pela área de TI.

6. USO DE INTERNET

Todas as regras atuais da **Level 4** visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da **Level 4** para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

7. DO USO DE DISPOSITIVOS PESSOAIS (BYOD)

O proprietário do equipamento será o único responsável pela manutenção e atualização das licenças dos softwares instalados no seu dispositivo. Todas as licenças dos softwares utilizados nos dispositivos BYOD deverão ser originais e adquiridas pelo usuário para não haver implicações legais em se tratando de pirataria de software. O usuário responderá por qualquer incidente ou processo sobre o uso de software não licenciado em seu dispositivo.

É responsabilidade do proprietário, a guarda e manutenção adequada do dispositivo de seus equipamentos quando utilizados para a execução das atividades nos projetos da LEVEL4.

A LEVEL 4 não se responsabiliza por acessos indevidos ao dispositivo ou danos de hardware e/ou software que possam ocorrer neste quando usado no contexto da

instituição. A responsabilidade de proteção física e lógica do dispositivo BYOD é exclusiva do proprietário.

Em caso de perda, roubo ou furto do dispositivo utilizado, deverá ser informado imediatamente, via endereço de e-mail perda.byod@level4.com.br, onde serão tomadas as medidas cabíveis se tratando de segurança e assim, evitar o uso indevido por terceiros dentro do ambiente da LEVEL 4, do dispositivo extraviado.

É responsabilidade exclusiva do proprietário do dispositivo a segurança dos dados no mesmo para não haver o vazamento de informações ou perda de dados. O proprietário deverá manter todos os meios de segurança, em especial a utilização de software de Firewall e Antivírus. Ainda, recomenda-se a utilização de criptografia nos dados do dispositivo e backup frequente dos dados.

Qualquer utilização de dispositivos BYOD estará sujeita às regras previstas nesta Política de Segurança de Informação.

No caso de finalização das atividades do proprietário para com a LEVEL 4, este se responsabilizará pela exclusão total dos dados armazenados em seu equipamento, que será auditado pela LEVEL 4 para a comprovação de que tais dados foram saneados e totalmente excluídos.

8. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a **Level 4** e/ou terceiros.

Desta forma, o uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

9. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da **Level 4**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.