NOR 011 – Norma de penalidades

Sumário

1. Objetivo

Esse documento define as regras para classificar as infrações e regulamentar as penalidades.

2. Âmbito de Aplicação

2.1. A presente norma aplica-se ào GRUPO LUFTe às empresas controladas ou a ela afiliadas, cada qual doravante individualmente designada “Empresa”.

2.2. As regras definidas neste documento aplicam-se a todos os usuários que utilizam recursos e serviços tecnológicos fornecidos pelo GRUPO LUFT, incluindo funcionários, terceiros e parceiros.

3. Considerações Gerais

3.1. O conteúdo desta norma é propriedade da Empresa, e é destinado para uso interno. Para garantir que seja sempre considerada a versão mais atualizada, não é recomendado que este documento seja reproduzido, armazenado ou transmitido, em qualquer formato ou por quaisquer meios, sejam eletrônicos ou físicos.

3.2. O conteúdo desta norma deve ser conhecido e observado por todos os funcionários e terceiros que trabalhem internamente nos ambientes da empresa, sendo o seu descumprimento passível de aplicação de medidas legais e disciplinares.

3.3. Com o objetivo de proteger suas informações e validar se o comportamento de seus colaboradores está de acordo com a política e normas, o GRUPO LUFT efetua o monitoramento de todos os ativos da informação e ativos de tecnologia.

3.4. Durante o monitoramento, o GRUPO LUFT, sem qualquer notificação ou aviso poderá interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar a pessoas autorizadas qualquer tipo de informação relacionada ou contida nos recursos ou serviços de tecnologia da informação.

3.5. Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente norma, os Funcionários devem consultar o seu Gestor imediato e/ou a Área de Compliance.

3.6. A infração a esta norma estará sujeita às regras estabelecidas na Norma de Penalidades.

3.7. Os casos omissos serão decididos pelo Comitê de Conduta.

4. Vínculos

PS01 - Política de Segurança da Informação

5. Conceitos

5.1 Funcionário – Refere-se a todo e qualquer conselheiro, administrador, diretor e funcionário que compõe o quadro da Empresa.

5.2 Informação – É todo e qualquer dado, informe, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oralmente ou de qualquer outra forma, gravados ou não com a expressão “confidencial”, em decorrência do desenvolvimento das atividades profissionais da Empresa.

5.3 Recursos de Tecnologia da Informação (“TI”) – São ferramentas de tecnologia da informação disponibilizadas ao Funcionário ou Terceiro para utilização a serviço da Empresa, tais como, mas não se limitando a: internet, intranet, rede corporativa com seus respectivos diretórios, correio eletrônico (e-mail), notebooks, computadores, impressoras, scanners, softwares e sistemas aplicativos.

5.4 Terceiro – Refere-se, mas não está limitado, a toda e qualquer pessoa física ou jurídica, que a Empresa se relacione ou venha a se relacionar, prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, independentemente de contrato formal ou não, incluindo aquele que utiliza o nome da Empresa para qualquer fim ou que presta serviços, fornece materiais, interage com Funcionário Público, com o Governo ou com outros Terceiros em nome da Empresa.

5.5 Usuário – Qualquer Funcionário, Terceiro ou qualquer outra pessoa que venha a ter acesso à Informação ou Informação Confidencial que transitam no âmbito dos Recursos de Tecnologia da Informação da Empresa, seja através de uma Conta de Usuário ou de uma Conta de Terceiro.

6. Diretrizes

Toda e qualquer infração à PSI e às Normas de Segurança da Informação deverá ser informada ao Comitê de Conduta e, por conseguinte, apurada através de procedimentos internos, que deverão ser conduzidos pelo gestor da área em que se encontra alocado o profissional que cometeu a infração, em conjunto com a Gerência do RH do GRUPO LUFT e/ou demais membros destas equipes que venham a ser indicados pelos respectivos gerentes.

Caso o Comitê de Conduta julgue cabível, o colaborador envolvido poderá, enquanto durar o processo de apuração interna, ser afastado da função ou suspenso, conforme classificação da sua infração.

Ao colaborador suspeito de cometer violações à Política e Normas de Segurança da Informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração, deverá ser aplicada com proporcionalidade à ocorrência.

7. Procedimentos

A Matriz de Classificação de Infrações deve ser entendida como regra geral a ser utilizada no processo disciplinar em conjunto com a análise específica de cada caso.

Abaixo são exemplificados os tipos de infrações.

INFRAÇOES LEVES

Uso dos recursos e serviços fornecidos por TI para:

- Encaminhamento de correntes e/ou piadas;
- Envio de correio eletrônico por engano, sem conteúdo confidencial;
- Uso de recursos da empresa para fins pessoais em desacordo com a Norma de acesso e utilização de e-mail.

INFRAÇOES GRAVES

Uso dos recursos e serviços fornecidos por TI para:

- Empréstimo de senha;
- Utilização de *login* e senha de outra pessoa;
- Anotação de senhas em lugares visíveis ou arquivos eletrônicos;
- Envio de *email* por engano com conteúdo confidencial que não tenha causado dano à empresa ou a terceiros;
- Envio de mensagem por correio eletrônico a partir do endereço de seu departamento ou usando o nome de usuário de outra pessoa que não seja o seu próprio *email* para fins pessoais;
- Envio de mensagens não solicitadas para múltiplos destinatários;
- Envio de mensagem que contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da empresa;
- Envio de mensagem que contenha ameaças eletrônicas (tais como, mas não limitados a *spam*, vírus, *etc*), arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Envio de mensagens que tenham fins políticos locais ou do país (propaganda política) e religiosos;
- Acesso remoto por máquinas sem antivírus;
- Prática de atividades comerciais paralelas, isto é, alheias ao interesse da empresa, durante o período de trabalho e/ou com ferramentas de trabalho pertencentes à empresa;
- *Download* e/ou armazenamento de vídeos ou músicas nas ferramentas da empresa, por exemplo, *desktop*, *notebook*, *tablets* e/ou celulares.

INFRAÇOES MUITO GRAVES

Uso dos recursos e serviços fornecidos por TI para:

- Empréstimo de senha por administrador de sistemas;
- Anotação de senha em lembretes físicos ou eletrônicos sem proteção (por administrador de sistemas);
- Tentativa de acesso a ambientes virtuais controlados aos quais o colaborador não tenha permissão (ex.: tentativa de invasão a ambiente, ao qual não tenha permissão de acesso);
- Envio e/ou publicação de mensagens para fins de difamação, injúria, calúnia ou ameaça a terceiros;
- Envio de e-mail por engano com conteúdo confidencial que tenha causado dano à empresa ou a terceiros;
- Manuseio de imagens ou acesso a sites de pornografia;
- Manuseio de imagens ou acesso a sites de pedofilia;
- Fraudes de qualquer tipo;
- Instalação de softwares peer to peer;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- Divulgação de informação e/ou documentos protegidos (ex. publicação em redes sociais ou enviá-las por email);
- Prática de Cyberbullying corporativo;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das empresas estiver sujeita a algum tipo de investigação.
- Aproveitar-se da sua função para cópia e/ou divulgação de informações que sejam do interesse da empresa;
- Utilizar os recursos tecnológicos da empresa para manusear fotos e vídeos de terceiros, fazendo montagens para fins ilícitos;
- Produzir e/ou transmitir mensagem que:
    - Inclua imagens criptografadas ou de qualquer forma mascaradas consideradas ilegais;
    - Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
    - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos, incluindo, mas não se limitando, a textos e imagens.

A título de orientação, o Comitê de Conduta, ao deparar-se com uma situação de comprovada violação de qualquer dispositivo constante da PSI ou NORMAS, poderá valer-se, em sua deliberação de julgamento, dos seguintes critérios:

- INFRAÇÃO LEVE – ADVERTÊNCIA E ANOTAÇÃO EM PRONTUÁRIO;
- INFRAÇÃO GRAVE - ADVERTÊNCIA E ANOTAÇÃO EM PRONTUÁRIO;
- INFRAÇÃO MUITO GRAVE – DEMISSÃO POR JUSTA CAUSA.

É muito importante ressaltar que:

- 2 (duas) infrações leves equivalem a 1 (uma) infração grave.
- 2 (duas) infrações graves equivalem a 1 (uma) infração gravíssima.

8. Disposições Finais

Esta norma entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

9. Controle e histórico de versões

Data	Versão	Sumário
01/07/2021	001	Criação do instrumento normativo

10. Aprovações

Código	Descrição	Versão	Vigência
NOR-011	Norma de penalidades	001	01/07/2021

Emissor(es):

Revisor(es):

Aprovador(es):