NOR 005 – Norma de gestão de acesso

Sumário

1. Objetivo

Esse documento define as regras de segurança a serem observadas para regulamentar a gestão de usuários, sua identificação e acesso a sistemas da TRANSPORTES LUFT LTDA.

2. Âmbito de Aplicação

2.1. A presente norma aplica-se ao GRUPO LUFT e 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 de recursos e sistemas tecnológicos da empresa.

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, ao GRUPO LUFT efetua o monitoramento de todos os ativos da informação e ativos de tecnologia.

3.4. Durante o monitoramento, ao 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

O acesso aos dados e informações da rede, sistemas informatizados e demais recursos tecnológicos disponibilizados pelo GRUPO LUFT devem ser registrados, identificados e controlados.

Todos os sistemas que necessitarem de autenticação devem utilizar autenticação forte, isto é, um meio no qual garanta que as credenciais não sejam enviadas através da rede em texto puro.

Os perfis de acesso deverão ser atribuídos e autorizados com base nos requisitos do negócio do GRUPO LUFT.

O controle de cada identidade deverá permitir o rastreamento de suas atividades que poderá ser utilizado para fins de auditoria interna, bem como para instruir processos judiciais**.**

Todos os dispositivos de identificação utilizados no GRUPO LUFT, tais como número de registro, crachá, *logins* de acesso aos sistemas, certificados e assinaturas digitais e dados biométricos, devem estar associados a uma pessoa física, inequivocamente, atrelada aos seus documentos oficiais (CPF e RG).

Deverá existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acesso em todos os sistemas de informação e serviços do GRUPO LUFT.

O acesso a sistemas críticos deverá ocorrer mediante segregação de função.

As contas de acesso à rede só poderão ser criadas após assinatura do termo de ciência e responsabilidade pelos respectivos usuários.

No caso de prestador de serviço terceirizado, o mesmo deverá ser concedido apenas mediante autorização expressa do diretor ou coordenador responsável e assinatura de Termo de Ciência e Responsabilidade em relação à PSI e Normas.

Cada gestor de área deverá providenciar anualmente uma análise crítica dos direitos de acesso por sua equipe.

Será de responsabilidade da área de tecnologia revisar semestralmente se os perfis de acessos e contas de usuários estão em conformidade com a suas respectivas funções.

É expressamente proibido o compartilhamento de dispositivo de identificação pessoal com outras pessoas.

Nos casos de suspeita de acesso indevido ao seu *usuário e* /senha, desbloqueio e esquecimento de senha, o colaborador deverá entrar em contato com a área de TI.

As contas inativas pelo período de 07 (sete) dias deverão ser bloqueadas com envio de notificação para o gestor da área em que estava alocado o colaborador.

Após 30 (trinta) dias do bloqueio, não havendo justificativa ou motivação formal, a conta deverá ser excluída, devendo o Gestor, da respectiva área, receber nova notificação.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a área de RH deverá imediatamente comunicar a área de TI, a fim de que o acesso seja bloqueado imediatamente.

A mesma se aplica aos usuários cujo contrato ou prestação de serviços tenham se encerrado, bem como os usuários de testes e outras situações similares.

7. Disposições Finais

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

8. Controle e histórico de versões

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

9. Aprovações

Código	Descrição	Versão	Vigência
NOR-005	Norma de gestão de acesso	001	

Emissor(es):

Revisor(es):

Aprovador(es):