Política de Segurança da Informação

Introdução

O objetivo desta Política de Segurança da Informação é garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas de informação sob o controle da L&L Products. Esta política define os princípios e regras para proteger contra acesso não autorizado, divulgação, alteração e destruição de informações confidenciais.

Aplicabilidade

Esta política aplica-se a todos os funcionários, contratados e entidades terceiras com acesso aos sistemas de informação e dados da L&L Products. Todos os indivíduos aos quais foi concedido acesso ("Usuários") são responsáveis por aderir às regras descritas nesta política e seus controles, processos e procedimentos de suporte, e relatar qualquer acesso não autorizado ou possíveis incidentes de segurança imediatamente.

Objetivos de Segurança da Informação

- Garantir a confidencialidade das informações sensíveis.
- Manter a integridade dos dados e sistemas de informação.
- Garantir a disponibilidade dos sistemas e serviços de informação.
- Proteger contra acesso não autorizado, divulgação, alteração e destruição de informações.
- Cumpra as leis, regulamentos e padrões relevantes do setor.

Âmbito

Esta política e seus controles, processos e procedimentos de suporte se aplicam a todos os sistemas de informação, redes e dados de propriedade ou operados pela L&L Products em todo o mundo. Ele abrange todos os funcionários, contratados e entidades terceirizadas que acessam, gerenciam ou mantêm recursos de informações, independentemente do local físico a partir do qual o acesso ocorre.

Classificação das informações

Todos os ativos de informação devem ser classificados com base na sua sensibilidade e devem ser aplicados controles de segurança adequados de acordo com a sua classificação.

- C1-Informação: Informação destinada e disponível ao público em geral.
- C2-Informação: Informação que não se destina a ser abertamente acessível ao público, mas que não causa impacto negativo na organização se vier a tornar-se pública.
- C3-Informação: Informações que podem causar pequenos danos à organização se perdidas, alteradas ou divulgadas.

- C4-Informação: Informações que podem causar danos significativos à organização se perdidas, alteradas ou divulgadas.

Controles de Acesso

Todos os Usuários devem usar um ID exclusivo para acessar os sistemas e aplicativos da L&L Products e senhas fortes em conformidade com a política de senha definida.

Sempre que possível, a Autenticação Multifatorial (MFA) será usada para acessar sistemas e dados confidenciais.

Os privilégios de acesso serão fornecidos com base nos seguintes princípios:

- Necessidade de saber – Os usuários ou recursos terão acesso aos sistemas necessários para cumprir suas funções e responsabilidades.
- Privilégio mínimo – Os usuários ou recursos receberão os privilégios mínimos estritamente necessários para concluir suas funções e responsabilidades.

As solicitações de contas de Usuários e privilégios de acesso devem ser formalmente documentadas e aprovadas pelo proprietário dos dados.

As solicitações de contas externas e privilégios de acesso devem ser claramente notificadas na solicitação e ser formalmente documentadas.

As solicitações de contas de serviço e privilégios de acesso devem ser formalmente documentadas e aprovadas pelo Diretor de Segurança da Informação (CISO) ou designado.

As solicitações de contas de administrador e privilégios de acesso devem ser formalmente documentadas e aprovadas pelo CISO ou designado. Revisões anuais dos privilégios de acesso serão realizadas para garantir o alinhamento com as funções e responsabilidades do Usuário.

Procedimentos de rescisão:

O acesso aos sistemas são prontamente revogados após o término do usuário ou quando o acesso não é mais necessário para as responsabilidades do trabalho.

As entrevistas de saída incluem uma revisão dos direitos de acesso e a devolução de todos os ativos da organização .

Acesso Remoto:

O acesso remoto aos sistemas da organização requer uma conexão segura e criptografada, como redes virtuais privadas (VPNs).

As atividades de acesso remoto estão sujeitas aos mesmos controles de segurança que o acesso no local.

Proteção de Dados e Privacidade

As informações pessoais e/ou confidenciais devem ser tratadas de acordo com as leis e regulamentos de privacidade aplicáveis e protegidas em conformidade.

Resposta e Relatórios de Incidentes

O acesso aos sistemas da organização é registrado e monitorado regularmente em busca de atividades suspeitas.

As contas de usuário e os direitos de acesso existentes serão revisados pelo menos anualmente para detectar contas inativas e contas com privilégios excessivos. Exemplos de contas com privilégios excessivos incluem:

- Uma conta ativa atribuída a contratados, fornecedores ou funcionários externos que não trabalham mais para a L&. Products.
- Uma conta ativa com direitos de acesso para os quais as funções e responsabilidades do Usuário não exigem acesso.
- Direitos ou permissões administrativas do sistema (incluindo permissões para alterar as configurações de segurança ou de desempenho de um sistema) concedidos a um usuário que não é administrador.
- Contas ativas desconhecidas.

Todos os eventos ou incidentes de segurança devem ser reportados imediatamente ao departamento de TI.

Segurança Física

O acesso físico a sistemas de informação, data centers e outras áreas sensíveis deve ser restrito e monitorado.

Os equipamentos que contenham informações sensíveis devem estar fisicamente protegidos.

Conscientização e treinamento em segurança

Os funcionários receberão treinamento regular sobre políticas, procedimentos e melhores práticas de segurança da informação.

Devem ser realizadas campanhas de conscientização sobre segurança para promover uma cultura de segurança.

Conformidade e Auditoria

Devem ser realizadas auditorias e avaliações de segurança regulares para garantir a conformidade com esta política e regulamentos relevantes.

A não conformidade deve ser tratada por meio de ações corretivas e, se necessário, medidas disciplinares.

Execução

Violações desta Política de Segurança da Informação e seus controles, processos e procedimentos de suporte podem resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho ou ação legal. A não conformidade com esta política também pode resultar na revogação de privilégios de acesso ao sistema.

Perguntas

Perguntas sobre esta Política podem ser endereçadas ao seu Departamento de TI.

Data de vigência: 01/03/2024

Data da próxima revisão: 01/03/2026

Christophe Carré

CEO