POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNA

NDD TECH LTDA

Diretrizes

Estes são os princípios básicos que regem a Política de Segurança da NDD Tech, estabelecidos de acordo com as necessidades da empresa:

1. À NDD é atribuída a guarda de informações de seus clientes diretos e indiretos, fornecedores e empregados. Portanto, a criação de um ambiente que garanta a disponibilidade e proteção é essencial para a continuidade de negócio da Companhia.

2. Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade, integridade e disponibilidade, independente da sua forma de armazenamento, digital ou não.

3. Dados Pessoais e informações relacionadas a pessoa natural identificada ou identificável, devem obrigatoriamente ser protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD) e tratados como confidenciais quando não houver justificativa legitima em contrário.

4. Cuidados redobrados devem ser tomados em relação aos Dados Pessoais Sensíveis, aqueles que podem revelar origem racial, étnica, opinião política, convicção religiosa, filosófica, filiação sindical, dados genéticos ou biométricos, relacionados a saúde ou orientação sexual.

5. As informações devem ter o ciclo de vida programado. Informações consideradas confidenciais, quando não mais necessárias, devem ser destruídas através de mecanismos apropriados. O descarte ou reutilização de mídias contendo essas informações deve ser feito de forma a inviabilizar a sua recuperação.

6. Todo o indivíduo que tenha acesso as dependências da NDD deverá ser identificado. O acesso de terceiros em áreas onde exista o processamento físico ou digital de informações, deverá ser fundamentado pela estrita necessidade e deverá ocorrer sempre com o acompanhamento de funcionário da NDD, responsável pelas informações naquele setor.

7. Todos os equipamentos na Companhia deverão estar inventariados e identificados de forma individual.

8. Credenciais de acesso, ou crachá de acesso as instalações e/ou sistemas são pessoais, não compartilháveis e intransferíveis. O usuário é responsável por todas as atividades desenvolvidas mediante autenticação com sua credencial, por isso deve zelar por sua proteção e sigilo, e realizar as ações de manutenção apropriadas para cada tipo de credencial, como a troca periódica de senhas.

9. Os funcionários da NDD, durante a vigência e após o término do contrato de trabalho ou prestação de serviço, não podem se apropriar de informações ou de mídias, equipamentos, componentes ou acessórios que as contém, como por exemplo: e-mails corporativos, planilhas, arquivos de dados ou vídeos.

10. A responsabilidade de manter a segurança é compartilhada por todos os funcionários. A NDD deverá ministrar treinamentos para promover a conscientização e preparo. As Violações das normas abaixo relacionadas, incidentes ou falhas de segurança devem ser notificadas imediatamente à equipe de Segurança da Informação da NDD.

11. Se houver mera possibilidade de vazamento de Dados Pessoais, deve ser notificado também imediatamente o Encarregado de Processamento de Dados (DPO).

Segurança Física

1. Todo o indivíduo ao ingressar nas instalações da NDD deverá usar crachá de identificação.

2. Pessoas externas à Companhia deverão ser identificadas na recepção e o seu ingresso nas instalações da NDD será realizado mediante autorização e acompanhamento do empregado da Companhia.

3. Todo computador ou notebook que sair da NDD, precisará de autorização prévia do gestor responsável.

4. Os prestadores de serviços da NDD são responsáveis pelas ações ou prejuízos causados por seus empregados ao patrimônio da NDD, bem como deverão garantir a manutenção da confidencialidade das informações acessadas.

5. Documentos ou papéis contendo informações confidenciais, quando não mais necessários, devem ser triturados ou destruídos de forma a impossibilitar leitura.

6. Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc) contendo informações confidenciais, quando não mais necessárias, devem ser quebradas ou destruídas de forma a impedir seu uso indevido.

7. Mídias regraváveis (drives HD ou SSD, pen drives, cartões SD, fitas, discos CD ou DVD do tipo RW, ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas com o procedimento seguro adequado indicado pela equipe de Segurança da Informação antes de seu reuso ou descarte.

8. Os equipamentos e seus componentes internos serão inventariados periodicamente e somente funcionários autorizados podem fazer remanejo de equipamentos e peças.

Credenciais de Acesso

1. Credenciais, identificações e senhas de acesso devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.

2. Cada funcionário trocará sua senha de forma sistêmica e automática, com validade máxima de 42 (quarenta e dois) dias e é de sua responsabilidade escolher senhas robustas, complexas e longas.

3. As senhas devem ser diferentes entre os sistemas utilizados, devem ter números, letras maiúsculas, minúsculas e caracteres especiais.

4. A NDD adota o conceito de privilégio mínimo, no qual os colaboradores devem ter acesso apenas à informação estritamente necessária para o cumprimento de suas atribuições.

5. Os processos de concessão e revogação de acesso são de responsabilidade das equipes de SRE (Site Reliability Engineering) e Infraestrutura de TI e devem ser centralizados nessas equipes e executados conforme os fluxos documentados.

Uso da Rede

1. O acesso a Internet é fornecido para atividades e finalidades da Companhia. Acessos com fins particulares lícitos podem ser feitos ocasionalmente, preferencialmente fora do horário de expediente, desde que não violem as demais normas.

2. É proibido usar a rede para acessar ou enviar conteúdo pornográfico, ofensivo ou difamatório, bem como para constranger terceiros, sejam eles funcionários ou não.

3. O uso para fins particulares de redes sociais como Facebook ou Twitter e sites de vídeos como YouTube, Vimeo e Netflix durante o horário de expediente é considerado inadequado e pode estar bloqueado a qualquer horário a critério da Companhia.

4. Qualquer site conhecido de conteúdo vedado ou inadequado pode estar em listas de bloqueio automático. Eventuais erros na classificação de determinado sítio podem ser comunicados à equipe responsável pelos proxys para retificação.

5. Os acessos à Internet podem e serão monitorados e registrados pela Companhia. Os registros ficam a disposição da Companhia pelo tempo que esta julgar adequado.

6. Não é permitido instalar, usar ou configurar equipamentos (hardware ou software) que deem acesso à rede corporativa sem autorização formal e conhecimento da Equipe de Segurança da Informação. Em especial, não é permitida a instalação de ponto de acesso wifi, bluetooth, modem, hub, switch, vpn, roteador ou software de acesso remoto para fins pessoais.

7. O correio eletrônico corporativo é mantido pela NDD e deve estar com a proteção anti-spam permanentemente ativa.

8. Todas as mensagens enviadas por correio eletrônico com o endereço profissional são de propriedade da Companhia, portanto devem ser usadas para assuntos de interesse da NDD e não se deve manter qualquer expectativa de privacidade de seus conteúdos.

9. É vedado o envio ou participação em correntes, mesmo de solidariedade, premiações ou informações com o e-mail corporativo disponibilizado pela NDD.

10. É vedado o envio de mensagens com conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política.

11. Não é permitido distribuir, via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo “corrente” e mensagens em massa, comerciais, de propaganda política ou o envio de correio eletrônico não solicitado.

12. Notebooks, laptops, tablets e outros equipamentos pessoais ou de terceiros não devem ser ligados diretamente na rede da Companhia sem autorização. Tais equipamentos, quando autorizados, podem ser conectados à rede wifi e ter acesso a serviços internos via VPN gerenciada pela Companhia.

Proteção de Estações e Servidores

1. Todos os computadores e servidores da NDD devem ter instalados o antivírus.

2. O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da equipe de administração do antivírus.

3. Constatado qualquer problema com o antivírus, o usuário deverá comunicar imediatamente a equipe de Infraestrutura que tomará as providencias cabíveis.

4. Todos os computadores e servidores da NDD devem estar instalados os agentes de monitoramento, estes não devem ser desinstalados sem a autorização da equipe de Infraestrutura e Segurança da Informação.

Utilização de Programas

1. As estações de trabalho são disponibilizadas com os programas - sistema operacional e aplicativos - mínimos necessários para o desempenho de sua função básica na NDD.

2. São considerados legítimos os softwares instalados e utilizados conforme suas licenças de uso e que não contrariem as demais regras da NDD e a legislação.

3. Não é permitida a instalação nos equipamentos da NDD de qualquer software, gratuito ou não, sem a autorização da equipe de Infraestrutura e Segurança da Informação. Caso necessite de algum software específico, entre em contato através de chamado aberto no portal Helpdesk (clicando aqui).

4. O uso ou instalação de software sem licença de uso ou em nome de outros sem autorização caracteriza crime de pirataria, ficando o usuário e o instalador sujeitos às sanções administrativas, legais e penais da legislação.

5. Ocasionalmente serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software permitindo identificar desvios das normas.

Cópias de Segurança ou Backup

1. Cada usuário é responsável por realizar as cópias de segurança de seus arquivos laborais no Sharepoint e sistemas de arquivos disponibilizados pela NDD.

2. Arquivos gerados nas estações de trabalho devem ser salvos no Sharepoint, pois só lá é feito o backup e em caso de exclusão acidental podem ser rapidamente recuperadas. Caso algum arquivo ou pasta seja salvo apenas no computador e existir uma exclusão acidental não é possível sua recuperação.

3. Não é permitida a cópia de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não autorizados pela NDD ou seus clientes.

4. Sempre que possível, os dados confidenciais devem estar criptografados nos backups.

5. Todo o backup deve periodicamente passar por teste de restauração.

6. Meios de armazenamento devem ser guardados em local seguro, armário, nuvem, cofre ou sala com chave ou controle de acesso e devem ser respeitados os tempos de vida útil sugeridos pelo fabricante.

7. Alguns backups têm tempo de vida determinado por lei, portanto a equipe responsável pelos backups deve ser informada e zelar por mantê-los disponíveis durante esse tempo, bem como os equipamentos necessários para sua recuperação quando necessário.

Sistemas e Aplicações

1. Não é permitida a transferência de dados para processamento ou armazenamento em serviços externos, de terceiros não autorizados expressamente pela NDD ou clientes.

2. Armazenamento e transferências de dados confidenciais devem ser sempre criptografadas com mecanismos aprovados pela Companhia.

3. A NDD optará preferencialmente por soluções/aplicações que se utilizem de protocolos seguros, tanto na transferência quanto no armazenamento de informação. Aplicações que não façam uso desses recursos devem ser validadas pela equipe de segurança da informação antes do início da sua utilização.

4. A NDD optará preferencialmente pela utilização de sistemas de duplo ou múltiplos fatores de autenticação (MFA/2FA). Aplicações que não façam uso desses recursos devem ser validadas pela equipe de segurança da informação antes do início da sua utilização.

5. Os sistemas deverão gerar registros (logs) de eventos de segurança. Devem ser utilizados para este fim funções do Sistema de Segurança em uso, recursos do sistema operacional, recursos de banco de dados e/ou recursos da aplicação. Os registros deverão conter ao menos as seguintes informações:

- identificação da aplicação e função;
- momento da ocorrência (timestamp);
- informações que identifiquem a máquina ou local da ocorrência;
- Dados relevantes manipulados pela aplicação.

O Sistema de Segurança poderá se encarregar do registro de algumas dessas informações.

6. No desenvolvimento e manutenção de sistemas é obrigatório o uso de software e repositório de controle e versionamento de arquivos (como fontes, modelos, documentos, diagramas, páginas web) aprovado pela Companhia.

7. Cada desenvolvedor é responsável pela integridade dos arquivos de sistema que estão sendo trabalhados, devendo utilizar preferencialmente áreas de trabalho em servidores designados.

8. Todo o desenvolvedor de aplicações deverá seguir, quando disponíveis e forem aplicáveis, as recomendações de segurança para o desenvolvimento.

Administração de Servidores

1. Todas as instalações de novos servidores deverão seguir procedimentos padrões e incluir pacotes, Service Packs, Hot Fixes obrigatórios.

2. A instalação das atualizações de segurança deverá ser realizada pelo responsável direto de cada servidor, seguindo as orientações de segurança no que tange ao backup antes do procedimento, adequação de horário e plano de recuperação de falhas.

3. Acessos remotos devem ser feitos sempre usando mecanismos criptografados. Devem ser desativados os serviços de acesso remoto que não usam criptografia.

4. Os equipamentos utilizados devem possuir sistema operacional atualizado e com recursos de segurança implantados.

5. A ativação de novos serviços de rede será condicionada a uma análise de riscos (a ser realizada pela Equipe de Segurança e Infraestrutura), onde, no mínimo, os seguintes aspectos serão considerados: requisitos de segurança do serviço, objetivo, alvo do serviço, forma de acesso, forma da administração e volume de tráfego.

6. Não é permitida a instalação de serviços de rede não autorizados pela Equipe de Segurança e Infraestrutura.

7. Todo o tráfego de informações confidenciais por meio compartilhado será protegido através de criptografia.

8. A equipe de Segurança da Informação pode indicar e usar ferramentas de detecção e prevenção de intrusos, para emitir alertas e registrar possíveis tentativas de invasão.

Desenvolvimento Seguro

1. Desenvolver conforme as boas práticas de SDL (Ciclo de Vida do Desenvolvimento de Segurança), TOP10 da OWASP (Open Web Application Security Project) e TOP25 da SANS (sans.org).

2. Desenvolver aplicando os princípios de Privacy by Desgin e Privacy By Default, buscando a segurança e a proteção dos dados tratados.

3. Capacitar o time de desenvolvimento para as práticas de desenvolvimento seguro.

4. A NDD possui uma política interna específica para o desenvolvimento seguro de seus produtos seguindo as melhores práticas de mercado.

Registros e Auditoria

1. Os Administradores devem habilitar, sempre que possível, os registros de segurança (logs) para auxiliar na análise em caso de possíveis falhas e/ou na execução de auditorias.

2. Os registros de segurança deverão ser analisados periodicamente (manual ou automaticamente).

Cód. do Procedimento:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL.EX.001	**SIG E TI**	**23/05/2023**	**003**

Aprovador(es):
DIRETORIA