**POLÍTICA DE SEGURANÇA INFORMÁTICA**

**INTRODUÇÃO**

Este documento possui função organizacional dentro da empresa NNTECHNICAL, responsável por definir, especificar e destacar as principais questões organizacionais dentro da corporação de funcionários, bem como com o compromentimento da Empresa para com seus colaboradores.

Sendo a segurança a pauta mais importante dentre as funcionalidades da Empresa NNTECHNICAL, deste o ano 2013, serão apresentadas, abaixo, normas, instruções e procedimentos que coicidem a melhor actuação em conjunto da equipe de funcionários e dos indivíduos responsáveis pela gestão da organização. Nós, directores da Empresa NNTECHNICAL tratamos com zelo a sua segurança.

**A EMPRESA NNTECHNICAL E A POLÍTICA DE SEGURANÇA**

As instruções alistadas neste documento deverão ser seguidas à risca por todo o conjunto corporativo de funcionários e membros da equipe da empresa, assim como parceiros e os demais prestadores de serviço para a organização.

É da responsabilidade da nossa empresa garantir que a Integridade, Confiabilidade, Disponibilidade, Autenticidade, façam parte dos nossos serviços para com os nossos clientes.

Ao receber uma cópia da Política de Segurança da Empresa NNTECHNICAL, (a) SR. (a) compromete-se a colaborar em conjunto com a gestão de Segurança do Trabalho da empresa, respeitando todas as normas e procedimentos aqui estabelecidos, cliente, ademais, de que poderá ser responsabilizado pelo não cumprimento efectivo das regras dispostas neste documento.

**DESCOBRIMENTO DAS POLÍTICAS DE SEGURANÇA**

O não cumprimento das normas estabelecidas neste documento poderá acarretar em sanções administrativas, resultando, possivelmente, no desligamento do funcionário perante a Empresa NNTECHNICAL, conforme a gravidade da ocorrência e seus devidos desdobramentos com a legislação vigente.

**UTILIZAÇÃO DOS EQUIPAMENTOS**

Todos os materiais e equipamentos utilizados conforme a necessidade do funcionário são de prioridade da Empresa NNTECHNICAL, assim deverão ser manejeados e ocupados de modo a não causar danos aos materiais e às suas funcionalidades.

Os computadores, bem como as máquinas de uso comum utilizam a autentificação dos funcionários por meio de senhas que deverão conter, no mínimo, oito (8) caracteres para a criação de senha, caractertes alfanuméricos, composto por letras e números, visando maior segurabilidade dos equipamentos. Senhas com combinações simples e óbvias deverão ser evitadas, a criação coerente e segura é um meio seguro de acesso aos sistemas de informação da organização. Não é permitido o uso de qualquer material ou equipamento para fins ilícitos.

**POLÍTICA DE USO DOS SISTEMAS DE TRABALHO**

Não deverão ser instalados ou manuseados tipos de software ou hardware sem autorização prévia da equipe de tecnologia e informação ou de segurança, ressalvados os sistemas que já venham instalados nos equipamentos e computadores, bem como o próprio sistema de uso da organização.

Todos os dados correspondentes à empresa deverão ser mantidos e arquivados no servidor que, por meio de backups diários, disponibilizará as documentações aos demais usuários.

Não é permititdo divulgar, compartilhar ou armazenar em sstema próprio nenhuma informação confidencial da Empresa para parrceiros, ou até, mesmo, parceiros sem autorização prévia.

**POLÍTICAS DE RELACIONAMENTO**

Não pode mencionar ou revelar nossa política de Segurança com terceiros ou em locais públicos, zelando pela confidencialidade dos assuntos empresariais da organização .

Não compartilhar senhas pessoais com ninguém e deve-se manter todas as documentações que estiverem em posse pessoal em local seguro e adequado.

Não aceitar ajuda técnica de qualquer outro colaborador que não seja da equipe técnica da Empresa.

**POLÍTICAS DE ACESSO A INTERNET**

O uso recreeativo de internet não deve se dar no horário de expediente.

Acesso a sites com conteúdo pornográfico, jogo, bate-papo, apostas, e assemelhados estará bloqueado e monitorado. O acesso a internet é permitido para o uso interno a todos os funcionários da Empresa.

**VÍRUS E CÓDIGOS MALICIOSOS**

Manter o anti-vírus actualizado. A nossa equipe técnica irá se encarregar disso, mas caso perceba que a actualização não esta funcional, entre em contacto com a mesma para que a situação possa ser corrigida.

Não traga disquetes ou CDs de fora da empresa.

**TÉNICAS DE DEFESA CONTRA CIBERATAQUES**

Para a segurança contra ataques cibernéticos deverão ser feitas cópias de segurança, para garantir a disponibilidade da informação.

Redundância de sistemas,para a alta disponibilidade das informações.

Eficácia no controle de acesso, usando mecanismos físicos ou lógicos.

Deve-se usar um mecanismo de controle de tráfego de dados entre computadores de uma rede interna e destes com as outras rede externas usando Firewall.

**CONTINUIDADE DE NEGÓCIOS**

Um dos factores muito importante para a nossa empresa e a disponibilidade, pois de nada adianta uma informação segura se a amesma estiver indisponível para quem necessita dela. Por esse motivo nossas equipes técnicas e de segurança contam com a sua colaboração para manter nossa empresa como líder de mercado. Entre sempre em contacto connosco sempre que julgar necessário.

**ACEITAÇÃO**

Este documento entra em vigor Na data de sua assinatura pelas partes e permanece válido por tempo indeterminado ou ate que advenha outros termos que revoguem por acordo mútuo entre partes.

**Membros da Equipe Técnica**

Nome: Nirma Suzardo Nhantumbo.

E-mail:nirmanhantumbo49@gmail.com

Número de celular: 848861184

**Membros da Equipe de Segurança:**

Nome:Suzardo Armando

E-mail: SuzardoArmand@ogmail.com

Número de celular:842255650

**O Sr. (a) Empregado** **O Sr. (a) Técnico (a)**

**––––––––––––––––––––– ––––––––––––––––––––**

Anabela Francisco Nirma Nhantumbo

Nampula, 16 de Fevereiro de 2013.