1. APRESENTAÇÃO

Atuando desde 2004 na área de Tecnologia da Informação e Comunicação, a Plenatech prima pela qualidade e segurança de seus sistemas e equipamentos. Para que possamos aprimorar cada vez mais nossos produtos e serviços, é essencial nos mantermos sempre atentos à regulamentação vigente e às melhores práticas do mercado. Por isso, elaboramos essa Política de Segurança Cibernética, que deve nortear as ações da nossa empresa tanto no desenvolvimento de novos projetos quanto na melhoria contínua dos que já estão em andamento.

2. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores e fornecedores envolvidos no desenvolvimento de produtos e sistemas na Plenatech.

3. OBJETIVO

O objetivo desta Política é garantir a segurança dos usuários dos produtos e sistemas da Plenatech por meio da plena observância dos princípios de *security by design* (segurança desde a concepção) e *security by default* (segurança por padrão) e das demais diretrizes aqui estabelecidas.

4. REFERÊNCIAS

I. Ato nº 77, de 5 de janeiro de 2021, da Anatel

II. Resolução nº 715, de 23 de outubro de 2019, da Anatel

III. Ato nº 2436, de 7 de março de 2023, da Anatel

IV. Política de Divulgação Coordenada de Vulnerabilidades da Plenatech

V. Política de Suporte aos Produtos da Plenatech

VI. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

5. CONCEITOS E DEFINIÇÕES

Algoritmos de criptografia: algoritmos baseados na ciência da criptografia, abrangendo algoritmos de encriptação/decriptação, algoritmos de *hash* criptográficos, algoritmos de assinatura digital e algoritmos de trocas de chaves.

Backdoor: mecanismo não documentado contido no *software/firmware* do produto que possibilita acesso não autorizado ao equipamento. A presença de *backdoors* no produto final pode ser intencional ou acidental.

Dados pessoais: informação relacionada a pessoa natural identificada ou identificável.

Dados pessoais sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Firmware: *software* acessível somente para leitura, programado em um *hardware* de propósito específico e armazenado de forma funcionalmente independente do armazenamento principal do equipamento.

Hashing: algoritmo matemático baseados em padronização internacionalmente reconhecida que mapeia dados de comprimento variável na entrada de uma função para um conjunto de dados de comprimento fixo na saída da função.

Métodos adequados de autenticação: protocolos ou algoritmos de autenticação baseados em padronização internacionalmente reconhecida, em suas versões atualizadas.

Senha fraca: senha que não possui, no mínimo, 8 caracteres e não contém pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.

Usuário: aquele que manipula, configura, se aproveita das utilidades e está sujeito aos impactos resultantes de vulnerabilidades e falhas apresentadas por equipamentos para telecomunicações.

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

6. PRINCÍPIOS E DIRETRIZES

I. Serão disponibilizados os recursos humanos, técnicos e financeiros necessários para a efetividade desta Política.

II. Serão conduzidos treinamentos periódicos para que todos na Plenatech conheçam e compreendam esta Política e as demais normas a ela relacionadas.

III. A Plenatech deseja e encoraja que toda pessoa que tenha conhecimento de falhas ou vulnerabilidades em seus sistemas e equipamentos comuniquem o fato nos canais disponíveis.

IV. Todas as comunicações de falhas e vulnerabilidade recebidas serão tratadas com zelo e seriedade.

V. Serão empregados todos os esforços economicamente razoáveis para manter os usuários protegidos contra falhas e vulnerabilidades de nossos produtos.

VI. Sempre que julgar necessário, a Plenatech poderá envolver agentes externos no processo de investigação e apuração das vulnerabilidades, incluindo consultores, peritos, auditores, advogados e quaisquer terceiros que julgue necessários.

VII. Serão disponibilizados os canais apropriados para que qualquer pessoa possa submeter a comunicação de falhas e vulnerabilidades identificadas em nossos sistemas e equipamentos.

VIII. As comunicações serão apuradas em prazo razoável, conforme processos e procedimentos internos, e serão priorizadas as que apresentam maiores riscos para a empresa e seus clientes.

IX. Sempre que a vulnerabilidade puder trazer riscos significativos à Plenatech, seus colaboradores, clientes ou fornecedores, a empresa adotará as medidas que considerar necessárias para mitigar imediatamente os riscos, incluindo o eventual bloqueio ou suspensão de acessos aos seus sistemas e quaisquer outras medidas que julgar apropriadas.

X. As informações recebidas por meio dos canais de comunicação de falhas e vulnerabilidades, bem como os processos e procedimentos posteriores, serão considerados segredo industrial e, portanto, confidenciais, não podendo ser revelados a quem quer que seja.

XI. Conforme o caso concreto, a Plenatech poderá solicitar ao comunicante que preste informações adicionais necessárias para a avaliação da falha ou vulnerabilidade identificada.

XII. Serão envidados todos os esforços necessários para atender as solicitações das autoridades competentes nos prazos estabelecidos nas leis e normas em vigor.

XIII. A Plenatech envidará todos os esforços razoáveis para manter seus sistemas e equipamentos atualizados de forma a atender as exigências legais, normativas e administrativas no menor tempo possível, considerados o estado da técnica, o desenvolvimento tecnológico e o surgimento de novas ameaças e vulnerabilidades.

XIV. Todos os equipamentos terminais desenvolvidos pela Plenatech que se conectem à Internet terão mecanismos automatizados e seguros para atualização de *software*/*firmware*, que empregarão métodos de criptografia, autenticação e verificação de integridade adequados às características do produto.

XV. A Plenatech garantirá aos usuários de seus sistemas e equipamentos a possibilidade de verificação manual da disponibilidade de atualizações de *software*/*firmware*, as quais poderão ser implementadas com facilidade.

XVI. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet deverão contar com mecanismos para informar ao usuário as alterações de *software/firmware* implementadas devido às atualizações, especialmente as relacionadas à segurança.

XVII. As atualizações disponibilizadas deverão preservar as configurações existentes no equipamento após finalizado o procedimento de atualização, salvo quando as alterações resultarem em melhorarias na segurança do dispositivo.

XVIII. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet terão mecanismo para gerenciamento e administração remotos que empreguem métodos adequados de autenticação e criptografia e tenham mecanismos de controle de acesso às interfaces de gerenciamento e administração remotos.

XIX. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet terão rotinas simplificadas adequadas para sua instalação e configuração, evitando potenciais falhas de segurança não intencionais e serão, por padrão de fábrica, configurados de forma restritiva ao invés de forma permissiva (*security by default*).

XX. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet terão mecanismo de monitoramento de comportamentos não usuais do *software/firmware* que alertem o usuário ou se reiniciem automaticamente caso um comportamento suspeito seja detectado.

XXI. Os equipamentos produzidos pela Plenatech terão ferramenta de registro de atividades (logs) relacionadas à autenticação de usuários, alteração de configurações do sistema e funcionamento do sistema.

XXII. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet não utilizarão credenciais e senhas iniciais padrão para acesso às suas configurações nem que sejam derivadas de informações de fácil obtenção por métodos de escaneamento de tráfego de dados em rede.

XXIII. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet deverão forçar, na primeira utilização, a alteração da senha inicial de acesso à configuração do equipamento e não permitirão o uso de senhas em branco ou senhas fracas.

XXIV. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet possuirão mecanismos de defesa contra tentativas exaustivas de acesso por força bruta e terão mecanismos de recuperação de senha robustos contra tentativas de roubo de credenciais.

XXV. Os sistemas e *firmwares* desenvolvidos pela Plenatech não utilizarão credenciais, senhas e chaves criptográficas definidas no próprio código fonte do e que não podem ser alteradas (*hard-coded*).

XXVI. Os equipamentos desenvolvidos pela Plenatech terão ferramentas que protejam senhas, chaves de acesso e credenciais armazenadas ou transmitidas utilizando métodos adequados de criptografia ou *hashing* e terão rotinas de encerramento de sessões inativas (*timeout*).

XXVII. É terminantemente proibida a inserção de qualquer ferramenta de teste ou *backdoor* nos processos de desenvolvimento do produto que não sejam absolutamente necessários à sua operação usual.

XVIII. Todas as comunicações realizadas nos serviços de comunicação de dados desenvolvidos pela Plenatech serão documentadas, incluindo aquelas para envio de

informações de perfil de uso do equipamento para fabricantes ou para terceiros (telemetria).

XXIX. Os serviços de comunicação de dados desenvolvidos pela Plenatech deverão ser fornecidos com serviços de comunicação de dados com as portas não usualmente utilizadas desabilitadas, de forma a reduzir a superfície de ataque.

XXX. Os serviços de comunicação de dados desenvolvidos pela Plenatech permitirão ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais à operação ou ao gerenciamento do equipamento.

XXXI. Os sistemas desenvolvidos pela Plenatech que trafegarem dados pessoais observarão integralmente a legislação concernente à proteção de dados pessoais, especialmente a Lei nº 13.709/2018 (LGPD).

XXXII. Os sistemas desenvolvidos pela Plenatech que trafegarem dados pessoais possibilitarão a utilização de métodos adequados de criptografia para a transmissão e armazenamento de informações sensíveis, incluindo dados pessoais.

XXXIII. Os sistemas desenvolvidos pela Plenatech que trafegarem dados pessoais permitirão que os usuários deletem facilmente seus dados pessoais e sensíveis armazenados, possibilitando o descarte ou a substituição do equipamento sem riscos de exposição de informações pessoais.

XXXIV. Todos os produtos e sistemas desenvolvidos pela Plenatech conterão em sua documentação informações ao usuário sobre quais dados pessoais, sensíveis ou não, são coletados, utilizados e armazenados.

XXXV. Os sistemas e equipamentos desenvolvidos pela Plenatech terão mecanismos para limitação da taxa de transmissão de dados de saída (*upload*), além do usualmente necessário, de forma a minimizar sua utilização como vetor em ataques a outros equipamentos ou sistemas (ataque de negação de serviço –DDoS).

XXXVI. Os sistemas e equipamentos desenvolvidos pela Plenatech terão mecanismos para validação do endereço de origem dos pacotes de dados, filtrando pacotes com endereço de origem falsificados (filtro *antispoofing*).

XXXVII. A Plenatech manterá e disponibilizará publicamente uma Política de Suporte aos Produtos com vistas a garantir transparência quanto às coberturas gerais, os tempos

mínimos de disponibilização de atualizações de segurança e os canais de comunicação disponíveis para a notificação de falhas e vulnerabilidades de segurança.

XXXVIII. A Plenatech manterá e disponibilizará publicamente uma Política de Divulgação Coordenada de Vulnerabilidades que indique (i) seus objetivos, suas responsabilidades e o que espera das demais partes interessadas; (ii) as formas de notificação de vulnerabilidade e seus respectivos contatos; (iii) o detalhamento das opções de comunicação segura; (iv) as informações que o notificador deve incluir na notificação; (v) o que o notificador deve esperar após reportar uma vulnerabilidade; e (vi) orientações sobre o que está no escopo do processo de notificação.

XXXIX. A Plenatech manterá um canal público de suporte para informar e manter um histórico sobre as vulnerabilidades identificadas em seus produtos e sistemas, as medidas de mitigação adotadas, as correções de segurança associadas.

XL. O canal de suporte disponibilizará acesso às correções de segurança e/ou às novas versões de *software/firmware* para seus produtos, além de manuais e materiais orientativos relativos à configuração, atualização e uso seguro dos equipamentos.

XLI. A proteção e a segurança do usuário sempre terão prioridade no desenvolvimento dos produtos e sistemas da Plenatech.

7. INDICADORES DE EFETIVIDADE

I. Número de comunicações recebidas.

II. Número de falhas e vulnerabilidades confirmadas.

III. Desempenho colaboradores em avaliações periódicas que meçam o grau de conhecimento desta Política e demais normas internas a ela relacionadas.

IV. Tempo médio para a correção de falhas e vulnerabilidades.

8. RESPONSABILIDADES

São responsabilidades da Direção:

- Garantir a disponibilidade dos recursos necessários para a efetivação desta Política.
- Aprovar ou não qualquer alteração desta Política.
- Acompanhar os indicadores de efetividade.

- Propor melhorias e revisões a esta Política e às demais normas internas a ela relacionadas.
- Esclarecer dúvidas relacionadas a esta Política e às demais normas a ela relacionadas.
- Deliberar sobre a necessidade de adoção de medidas preventivas ou corretivas destinadas a prevenir riscos decorrentes de falhas e vulnerabilidades identificadas.

São responsabilidades dos colaboradores e terceiros:

- Observar integralmente as disposições desta Política e demais normas a ela relacionadas.
- Denunciar condutas que violem a legislação vigente e/ou as normas internas e processos da Plenatech relativos à segurança cibernética.
- Conhecer as disposições desta Política e das demais normas a ela relacionadas.

São responsabilidades dos líderes:

- Fazer com que seus liderados conheçam e compreendam esta Política e as demais normas a ela relacionadas.

9. DISPOSIÇÕES FINAIS

Para cumprir com o seu compromisso com o desenvolvimento de produtos e sistemas seguros, a Plenatech manterá um programa de adequação progressiva a esta Política.

Sempre que houver alteração, as partes interessadas receberão, na medida do possível, a versão atualizada e serão informadas sobre as mudanças realizadas.

É obrigação das partes interessadas buscar a versão mais atual desta Política sempre que necessário.

Nos colocamos à disposição pelo e-mail suporte@plenatech.com para esclarecer dúvidas relativas à interpretação dos termos ou diretrizes aqui estabelecidos e para receber sugestões de melhoria.

10. CONTROLE

Esta Política foi finalizada e validada no dia 24 de abril de 2024 e homologada pela Diretoria no dia 24 de abril de 2024 com vigência a partir do dia 24 de abril de 2024, devendo ser revisada anualmente ou sempre que necessário.