1. OBJETIVO

Esta política estabelece requisitos de uso de dispositivos móveis como Smartphones, Tablets e Notebooks de propriedade pessoal pelos bolsistas, para acessar a rede interna e informações, recursos e/ou serviços do Núcleo de Excelência em Tecnologias Sociais (NEES).

2. AMPLITUDE

Esta política se aplica a todos os bolsistas, incluindo colaboradores terceirizados e estagiários, trabalhando para, ou sob o controle do NEES. Deve ser lida em conjunto com nossa Política de Uso Aceitável.

3. DOCUMENTOS DE REFERÊNCIA

Norma ABNT NBR ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos
Norma ABNT NBR ISO/IEC 27002 – Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.

4. DEFINIÇÕES

- **BYOD ou Bring Your Own Device:** traga seu próprio dispositivo.

5. DIRETRIZES

5.1 Política

Os dispositivos registrados BYOD estão sujeitos a todas as políticas e procedimentos do NEES, relacionados à segurança da informação.
O NEES respeita a privacidade do dispositivo pessoal, e apenas solicita acesso ao dispositivo por técnicos para implementar controles de segurança ou responder a solicitações legítimas de descoberta surgidas em processos administrativos, civis ou criminais. Isso difere da política de uso aceitável e/ou serviços do NEES, onde os bolsistas não têm o direito, nem devem ter a

expectativa de privacidade ao usar os equipamentos e/ou serviços, visando proteger a segurança e a integridade da infraestrutura de dados de tecnologia do NEES. Exceções limitadas à apólice podem ser autorizadas pela Gerência de Infraestrutura devido a variações de dispositivos e plataformas.

Esta política deve ser lida juntamente com a Política de Uso Aceitável e a Política de Dispositivos Móveis do NEES.

5.2 Aprovação, registro e suporte de dispositivos

Os seguintes dispositivos são suportados:

- Notebooks
- Smartphone
- Tablets

Os problemas de conectividade são suportados pelo Suporte de TI, os bolsistas devem entrar em contato com o fabricante do dispositivo ou sua operadora para problemas relacionados ao sistema operacional ou hardware.

Os dispositivos devem ser apresentados ao Suporte de TI, para a configuração adequada de aplicativos padrão, como navegadores, software de produtividade de escritório e ferramentas de segurança, e para serem formalmente aprovados e registrados antes que possam acessar os sistemas e rede interna do NEES.

5.3 Uso aceitável de dispositivos registrados

Usos comerciais aceitáveis são aquelas atividades que apoiam direta ou indiretamente os negócios do NEES.

O uso pessoal aceitável durante a jornada de trabalho é limitado a comunicação pessoal razoável ou recreação.

Os bolsistas são impedidos de acessar sites que não tenham relevância com o trabalho desempenhado enquanto conectados à rede corporativa a critério do NEES.

Os recursos de câmera e ou vídeo dos dispositivos devem ser desativados nas dependências do NEES, exceto durante reuniões ou eventos on-line.

Os dispositivos não devem ser usados a qualquer momento para:

- armazenar ou transmitir materiais ilícitos

- armazenar ou transmitir informações proprietárias
- assediar outros
- participar de atividades de negócios externos enquanto conectados à rede corporativa.

A equipe pode solicitar o uso emergencial e temporário do seu dispositivo para acessar os ativos do NEES, tais como:

- Email
- Calendários
- Contatos
- Documentos

5.4 Reembolso

O NEES não irá contribuir com uma ajuda de custo ou reembolso para uso de dispositivos BYOD.

5.5 Orientações de Segurança da Informação

5.5.1 Acesso não autorizado

- Para evitar acesso não autorizado, os dispositivos registrados devem ser protegidos por senha de acordo com nossa Política de Senha.
- O dispositivo registrado deve travar-se com uma senha ou PIN se estiver ocioso por cinco minutos. Após 5 (cinco) tentativas fracassadas de digitar a senha, o dispositivo será bloqueado automaticamente – levar o dispositivo para o suporte de TI para desbloqueá-lo.
- Dispositivos enraizados (Android) ou jailbroken (iOS) são estritamente proibidos.
- Smartphones e tablets que não estão na lista de dispositivos suportados, não são autorizados a se conectar aos sistemas ou rede do NEES.
- Smartphones e tablets pertencentes a bolsistas que são para uso pessoal não são permitidos a se conectar aos sistemas ou rede interna.
- O acesso da equipe às informações do NEES é automaticamente limitado conforme estabelecido na Política de Controle de Acesso.

- Os bolsistas devem tomar todas as medidas razoáveis para evitar o roubo ou perda de dispositivos registrados.
- Espera-se que os próprios bolsistas mantenham o dispositivo registrado e garantam que seus sistemas sejam regularmente atualizados e corrigidos.
- Espera-se que os bolsistas estejam cientes e cumpram quaisquer requisitos regulatórios ou outros requisitos relativos ao manuseio de dados pessoais.
- Os dispositivos perdidos ou roubados devem ser reportados à Gerência de Infraestrutura assim que for possível e em todos os casos dentro de 24 horas.
- Os bolsistas são responsáveis por notificar sua operadora móvel imediatamente após a perda de um dispositivo registrado.

Situações em que o dispositivo registrado pode ser apagado remotamente:

- Em caso de perda ou roubo do dispositivo
- Se o bolsista deixar de ser um membro da equipe
- Se a Gerência de Infraestrutura detectar violação de dados ou políticas
- Se a Gerência de Infraestrutura detectar vírus ou ameaça semelhante à segurança de infraestrutura de informação ou tecnologia do NEES.

5.5.2 Medidas para posicionamento e proteção de equipamentos

Para garantir a segurança da informação, é crucial que os equipamentos estejam posicionados de forma segura e protegida, tanto em termos de proteção física quanto de segurança cibernética. Desta forma, além da implantação de controles de acesso, os usuários devem estar atentos para: proteção contra riscos ambientais (como incêndios e descargas elétricas), e medidas para evitar a perda ou roubo de equipamentos. A segurança cibernética, por sua vez, exige a implementação de medidas como senhas fortes, autenticação de dois fatores, software antivírus e firewalls, além de backups regulares e testes de recuperação.

5.6 Riscos, Passivos e Isenções de Responsabilidade

A Gerência de Infraestrutura tomará todas as precauções para evitar que quaisquer dados pessoais sejam perdidos no caso de um dispositivo registrado ser remotamente apagado, todos os bolsistas são responsáveis por tomar precauções adicionais, como backup de e-mails, contatos, etc.

- Reservamo-nos o direito de desconectar dispositivos registrados ou desativar serviços sem notificação.
- Espera-se que os bolsistas usem seus dispositivos registrados de forma ética o tempo todo e atendam à Política de Uso Aceitável do NEES.
- Os bolsistas são pessoalmente responsáveis por todos os custos associados com seus dispositivos registrados.

6. REGISTROS

Os registros relacionados com este procedimento estão cadastrados no GLPI.

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO27001/Políticas. Deve ser atualizado anualmente.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	26/04/2024	Criação do documento.	Francisco Meneses
02	12/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e as assinaturas, via sistema INTEGRA	Shirley Vital
03	09/05/2025	Inclusão do item 5.5.2 Medidas para posicionamento e proteção de equipamentos, sendo tratamento da oportunidade de melhoria de auditoria interna.	Francisco Meneses

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-09 18:39
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-12 12:21
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-12 14:41