Brookfield
Renewable Partners

Brookfield Renewable Partners

POLÍTICA DE USO ACEITÁVEL PARA ATIVOS DE TECNOLOGIA

NOVEMBRO DE 2024

Índice

1 Histórico de revisões

1.1 Tabela de versão

Versão	Data	Preparado por	Comentário
1.14	2022/09/21	Hani Pherawn Camilo Romero	• Cruzou o documento com o Código de Conduta e Ética Empresarial do BEP • Apêndice A atualizado
1.15	2023/04/05	Hani Pherawn	• Removida a referência cruzada ao Código de Conduta e Ética Empresarial do BEP
1.16	2023/05/10	Charles Fowler	• Informações de contato atualizadas de acordo com a direção da Gerência de Portfólio
2.0	2023/12/20	Leonardo Ovidio Hani Pherawn	• Nova sessão sobre IA generativa • Nova sessão sobre Cibersegurança (Phishing) • Subseção para políticas relevantes e segurança de informações e dados • Referências à política de privacidade e dados privados
2.1	2024/11/12	Leonardo Ovidio	• Substituiu negócios operacionais por empresas de portfólio • Atualização da tabela de definições, incluindo Phishing e Inteligência Artificial (IA) Generativa • Contatos atualizados da chave de TI/OT • Linhas de denúncia de ética atualizadas

1.2 Aprovação

Versão	Data	Aprovado por	Papel
1.14	2023/01/11	Mark Reid	Vice-presidente de segurança e conformidade de TI
1.15	2023/05/01	Mark Reid	Vice-presidente de segurança e conformidade de TI
1.16	2023/05/18	Mark Reid	Vice-presidente de segurança cibernética e conformidade de TI
2.0	2023/12/21	Mark Reid	Vice-presidente de segurança cibernética e conformidade de TI
2.1	2024/11/19	Mark Reid	Vice-presidente de segurança cibernética e conformidade de TI

2 Definições

Prazo	Definições
Brookfield renovável Parceiros (BEP)	Brookfield Renewable Partners (BEP) refere-se a empresas corporativas e do portfólio BEP

Serviços de TI	Refere-se aos departamentos de TI do BEP, incluindo Service Desk de TI, Infraestrutura, Aplicativos ou outra equipe de serviço de suporte de TI.
Ativos de tecnologia	Inclui, mas não se limita a todos os sistemas, infraestrutura, dispositivos e/ou serviços gerenciados de Tecnologia da Informação (TI) e Tecnologia Operacional (OT)
	e/ou de propriedade da BEP. Isso inclui todos os ambientes de rede com e sem fio, serviços de Internet, sistemas telefônicos, impressoras, servidores, estações de trabalho (desktop ou laptop), dispositivos móveis (tablet, telefone celular ou outros dispositivos portáteis), sistemas de armazenamento, serviços de e-mail, recursos de informação, serviços em nuvem (interface de desktop virtual, rede privada virtual, máquinas virtuais, etc.), sistemas de inteligência artificial ou outros ativos técnicos. Todos os ativos de TI e OT nos ambientes de controle/operações da planta BEP estão incluídos nesta definição.
Malware	Software projetado para explorar, infiltrar ou danificar Ativos de Tecnologia sem o consentimento informado do Usuário. Também inclui vírus de computador, worms, cavalos de Tróia, rootkits, spyware, ransomware, adware desonesto e outros softwares indesejados.
Pessoal	Qualquer funcionário, contratado, indivíduo ou prestador de serviços que tenha sido autorizado a acessar ou usar um Ativo de Tecnologia BEP
Gerador Artificial Inteligência (IA)	Refere-se a sistemas de inteligência artificial que podem criar conteúdo como texto, imagens, vídeos ou áudio que se assemelham muito a saídas criadas por humanos. Esses sistemas usam tecnologia avançada para analisar grandes quantidades de dados e produzir resultados realistas e criativos.
Phishing	É uma tentativa maliciosa de enganar os indivíduos para que forneçam informações confidenciais, como nomes de usuário, senhas ou detalhes financeiros, fingindo ser uma fonte confiável em comunicações eletrônicas.

3 Finalidade

O objetivo desta política é delinear o uso aceitável dos ativos de tecnologia da BEP. Os padrões descritos neste documento estão em vigor para proteger o pessoal, clientes, parceiros e contrapartes da BEP contra danos causados pelo uso indevido de Ativos de Tecnologia, bem como impor o uso legal, ético e comercial de Ativos de Tecnologia.

Cada empresa do portfólio também pode definir políticas e diretrizes suplementares específicas para suas necessidades, que complementarão esta política. No entanto, esta política substituirá qualquer política suplementar de TI/OT da empresa do portfólio no caso de quaisquer inconsistências entre os documentos.

4 Escopo de Aplicação

Esta política se aplica a todos os funcionários, contratados, consultores, clientes e outros funcionários terceirizados que tenham acesso aos ativos de tecnologia BEP. O não cumprimento desta política pode resultar em ação disciplinar de acordo com as políticas de recursos humanos da empresa do portfólio, incluindo suspensão ou rescisão do acesso aos ativos da BEP Technology, instalações e/ou rescisão do contrato de trabalho ou contrato.

5 Responsabilidades

A Cibersegurança Corporativa e Compliance de TI é responsável pelo conteúdo e manutenção desta política.

Os Chefes de TI/OT são responsáveis pela disseminação, treinamento, monitoramento e aplicação associados a esta política dentro de suas áreas de responsabilidade.

6 Política

6.1 Uso de ativos de tecnologia

Os ativos de tecnologia são fornecidos como facilitadores operacionais e de negócios para o pessoal apoiar as metas e objetivos da organização. Assim, apenas os Ativos de Tecnologia autorizados pela empresa devem ser usados na execução de deveres e responsabilidades de maneira consistente com esta política e outras políticas de BEP.

O uso pessoal incidental de Ativos de Tecnologia para fins não comerciais é permitido se não:

- Consumir uma quantidade mínima de recursos de computação ou rede.
- Interferir na produtividade.
- Antecipe qualquer atividade comercial.
- Causar angústia, problemas legais ou éticos para outras pessoas ou BEP.

O uso indevido de ativos de tecnologia BEP não será tolerado. Não é permitido usar os Ativos de Tecnologia para qualquer finalidade inadequada ou ilegal. Atividades inaceitáveis que constituem uso indevido incluem, mas não estão limitadas ao seguinte:

- Envolver-se em conduta ilegal, fraudulenta ou maliciosa.
- Possuir, armazenar, exibir ou transmitir qualquer material que possa ser ofensivo por causa de seu conteúdo sexual, racista, violento ou discriminatório, incluindo material que viole qualquer assédio ou leis do local de trabalho.
- Baixar, copiar, compartilhar ou armazenar dados da empresa em qualquer repositório de dados não aprovado ou com pessoal não autorizado.
- Acesso não autorizado a sistemas ou software restritos.
- Uso de dispositivos não autorizados na rede da empresa ou para acessar ativos e recursos da empresa.
- Adulterar intencionalmente ou interferir de outra forma na operação normal do ambiente de TI/OT, incluindo a propagação de vírus de computador ou outro malware.
- Alterar intencionalmente a configuração de ativos de tecnologia, ignorar restrições de acesso, adquirir ou instalar software sem autorização específica do pessoal de TI/OT apropriado.
- Uso de ativos de tecnologia para ganho pessoal ou para atividades comerciais não relacionadas ao BEP.
- Realizar atividades não relacionadas aos negócios que possam afetar o desempenho da rede da organização, como streaming de áudio/vídeo, videogame online, download, compartilhamento de arquivos, hospedagem na web, etc., ou que possam afetar negativamente a reputação da organização.

- Realizar qualquer atividade que possa afetar negativamente a postura de segurança da organização. Isso inclui o estabelecimento de redes não autorizadas ou outros sistemas multiusuários para exfiltração de dados, bem como o uso de ferramentas de hardware ou software para reconhecimento, coleta de dados, avaliação, comunicação ou comprometimento dos controles de segurança implementados.
- Infringir a propriedade intelectual ou os direitos de privacidade de terceiros.
- Compartilhar informações pessoais de conta e senha ou usar as credenciais de outra pessoa.
- Compartilhar, divulgar, processar dados pessoais para atividades não relacionadas aos negócios sem o consentimento apropriado de maneira inconsistente com a política de Privacidade Corporativa.
- Deixar os ativos de tecnologia desprotegidos contra roubo oportunista fora das instalações do BEP.
- Abrir e-mails, anexos ou links não solicitados em e-mails de partes desconhecidas.
- Gerar ou encaminhe e-mails em cadeia que não sejam de negócios.
- Provisionar serviços em nuvem para armazenar, processar, compartilhar ou gerenciar informações BEP sem autorização específica da equipe de TI/OT. Isso inclui o encaminhamento de mensagens para uma conta de e-mail pessoal que não seja BEP por conveniência. Além disso, as assinaturas de serviço de nuvem devem ter autorização documentada pela equipe de segurança de TI/OT antes que o serviço seja ativado.

6.2 Segurança Informática

Se você recebeu um computador ou dispositivo móvel BEP, você é o custodiante desse ativo. Você deve ter cuidado no manuseio e manutenção segura dos ativos em sua posse, especialmente fora das instalações do BEP. Se um ativo foi danificado, perdido, roubado ou está indisponível para atividades comerciais, você deve informar imediatamente seu gerente, bem como os Serviços de TI da BEP. Equipamentos de informática, exceto laptops ou dispositivos móveis atribuídos, não devem ser movidos ou realocados sem a aprovação expressa da BEP IT Services.

Você deve manter as informações da conta, como IDs de login e senhas, seguras. Você também é responsável pelas atividades realizadas no contexto das contas que lhe são atribuídas. Ao criar senhas, você deve empregar as práticas recomendadas na criação de senhas complexas que estejam em conformidade com a política de senha do BEP. As senhas não devem ser anotadas.

Todas as estações de trabalho BEP são protegidas com um recurso de bloqueio automático de inatividade. No entanto, você deve bloquear ou fazer logoff de qualquer computador que seja deixado sem supervisão por qualquer período.

6.3 Segurança da Informação / Dados

O ambiente de TI/TO do BEP contém informações confidenciais, confidenciais e potencialmente privadas. Você tomará todas as medidas necessárias para impedir o acesso não autorizado ou a divulgação dessas informações. É sua responsabilidade garantir que todos os dados, incluindo informações confidenciais, confidenciais, privadas, valiosas ou críticas, sejam armazenados adequadamente na rede BEP ou em um sistema ou repositório aprovado. Além disso, quando as informações são transmitidas, é sua responsabilidade garantir que as salvaguardas apropriadas estejam em vigor para garantir a confidencialidade e a integridade das informações.

Mídias removíveis contendo informações sensíveis, confidenciais ou privadas devem ser manuseadas com cuidado, conforme descrito abaixo.

6.4 Mídia removível

Mídias removíveis, incluindo CD/DVD, unidades USB e outras mídias de armazenamento portáteis são fontes frequentes de incidentes de segurança, como infecções por malware e violações de dados. Portanto, observe:

- Não conecte mídia removível de uma fonte desconhecida a um computador BEP. Embora os computadores BEP sejam protegidos com proteção de endpoint, isso pode não impedir contra malware incorporado em mídia removível e outras ameaças de dia zero.
- Não armazene informações sensíveis ou confidenciais em texto não criptografado (não criptografado) em mídia removível, pois a perda pode resultar em uma violação de informações. As informações sensíveis ou confidenciais que precisam ser trocadas por meio de mídia removível devem ser criptografadas usando uma ferramenta aprovada pela BEP IT.
- Mídias removíveis contendo informações confidenciais não devem ser deixadas ao ar livre ou vulneráveis a roubos oportunistas.

6.5 Inteligência Artificial (IA) Generativa

O uso da IA generativa pode trazer grandes benefícios para o BEP e seus usuários. No entanto, como qualquer outra tecnologia/ferramenta, está sujeita a limitações e riscos. Se não for bem gerenciado, afetará negativamente o BEP e seus usuários.

As ferramentas de IA generativa serão usadas de forma ética, responsável, consistente e em conformidade com os regulamentos aplicáveis e as políticas, padrões, diretrizes e melhores práticas corporativas do BEP com supervisão apropriada.

Seguiremos os seguintes princípios para garantir que a IA generativa seja usada de maneira ética e responsável.

- Antes de introduzir ou implantar casos de uso de IA generativa, certifique-se de realizar avaliações de impacto adequadas e obter as permissões necessárias.
- Não use IA generativa para fins que não cumpram os requisitos regulatórios e/ou violem as políticas corporativas sobre segurança cibernética, governança de dados, privacidade e outras áreas relacionadas.
- Não crie, armazene, compartilhe ou use informações confidenciais ou sensíveis, incluindo, mas não se limitando a informações pessoais, financeiras, proprietárias ou intelectuais para produzir conteúdo de IA generativa sem as aprovações apropriadas.
- Programas completos de treinamento ou educação relacionados ao uso de IA generativa, proteção de dados e segurança da informação são necessários para todos os usuários.
- O BEP reserva-se o direito de monitorar e auditar o uso de IA generativa para garantir a conformidade com as políticas e regulamentos aplicáveis, incluindo obrigações de manutenção de registros.

7 Segurança cibernética (phishing)

Os funcionários têm um papel fundamental na proteção de sua organização contra ataques de phishing. É sua responsabilidade exercer vigilância e cautela ao lidar com e-mails, links e anexos e seguir os protocolos de segurança estabelecidos. Eles devem abster-se de compartilhar informações confidenciais ou clicar em links suspeitos e relatar possíveis tentativas de phishing ao departamento de TI. O não cumprimento dessas responsabilidades pode ter consequências profundas (ref seção 10). Não só pode comprometer a segurança dos dados da organização, mas também pode resultar em perdas financeiras, danos à reputação da empresa e até ramificações legais. Portanto, é essencial que os funcionários sejam proativos e responsáveis em sua abordagem às ameaças de phishing, pois suas ações podem afetar significativamente a segurança geral e o bem-estar da organização.

8 Monitorização

Todas as informações contidas no ambiente BEP TI/TO e/ou armazenadas nos Ativos de Tecnologia BEP são propriedade do BEP. A BEP mantém o acesso e reserva-se o direito de acessar e monitorar o conteúdo em ou dentro de qualquer Ativo de Tecnologia BEP a qualquer momento, e pode recuperar, revisar, auditar, interceptar, divulgar ou restringir qualquer informação em tais sistemas, incluindo, mas não se limitando a e-mail, mensagens instantâneas, arquivos e registros de uso da Internet, sem a permissão do titular da conta.

Os motivos pelos quais o BEP ou outros autorizados pelo BEP podem acessar dados ou sistemas incluem, mas não estão limitados a determinar se ocorreu uma violação desta política ou de outra política do BEP; investigar uma falha ou erro em um sistema; monitoramento da utilização do sistema ou da rede, obtenção de informações solicitadas por terceiros em litígio ou em resposta a uma investigação governamental e no curso normal dos negócios.

9 Relatórios

Todos os funcionários e terceiros internos tem a obrigação de aderir a esta Política. Se você testemunhar o comportamento de outros funcionários do BEP ou de qualquer terceiro que você acredite que possa representar uma violação desta Política, você deve denunciá-lo imediatamente. Os relatórios internos são importantes para a organização e são esperados e valorizados.

A BEP leva todos os relatórios a sério; Todas as denúncias recebidas serão avaliadas e, quando necessário, serão realizadas as investigações apropriadas. A confidencialidade das violações relatadas será mantida sempre que possível, de acordo com a necessidade de realizar uma revisão adequada e sujeita à lei aplicável.

Os relatórios devem, em primeira instância, ser feitos ao chefe de TI/TO da empresa do portfólio, que garantirá que as informações sejam tratadas adequadamente e escalonadas conforme necessário. Se este não parecer ser um caminho apropriado devido à natureza ou ao conteúdo do relatório, ele deve ser enviado para a Linha de Denúncia de Ética ou para o Site de Denúncia de Ética. A Linha de Denúncia de Ética/Site é gerenciada por um terceiro independente e permite denúncias anônimas. Os relatórios podem ser feitos em inglês, francês e português, entre outros idiomas, e estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana. Consulte o Apêndice "A" para saber como você pode entrar em contato com a Linha de Denúncia de Ética/Site.

Nenhuma retribuição ou retaliação será tomada contra qualquer pessoa que tenha feito uma denúncia com base na crença razoavelmente boa de que ocorreu uma violação desta Política.

10 Aplicação e Ação Disciplinar

Qualquer violação desta política é motivo para o BEP:

- Revogar e/ou restringir o acesso aos ativos de tecnologia BEP.
- Tomar medidas disciplinares, incluindo rescisão do contrato de trabalho ou contrato.
- Iniciar uma ação legal contra o Indivíduo e/ou outras pessoas que possam estar envolvidas.

11 Políticas Relevantes

- Política de Segurança da Informação Corporativa
- Política de Uso de Dispositivo Pessoal
- Norma de Prevenção à Perda de Dados
- Norma de Gestão de Backup

APÊNDICE A

INFORMAÇÕES DE CONTATO PARA POLÍTICA

Informações de contato para a política

Consulte o documento "Contatos-chave de TI/OT em todo o mundo", gerenciado pela BEP Cybersecurity and Compliance.

LINHA DE DENÚNCIA ÉTICA:

Austrália – 1-800-957963	Luxemburgo – 800 27 819
Barbados – 1-833-388-0834	México – 01800-436-0065
Bermudas - 1-833-388-0833	Nova Zelândia – 0800-450-194
Brasil – 0800-550-0049	Peru – 0800-74879
Canadá - 1-800-665-0831	Portugal – 800-815-087
Ilhas Cayman - 833-425-1502	Catar – 800-0249
Chile – 800914483	Cingapura – 800-492-2253
China – 86 21 8036 5429	Coreia do Sul – 080-880-0303
Colômbia – 01800-5189736	Espanha – 900-751-347
França – 0800-91-2964	Suíça – 0800-225-163
Alemanha – 0800-182-1227	Emirados Árabes Unidos – 800 012-0127
Hong Kong – 800-967-085	Reino Unido e Irlanda do Norte – 0800-652-6598
Índia – 000-800-0502-237	Estados Unidos - 1770-613-6339
Irlanda - 1800-849-310	Uruguai - 000-416-205-6408
Japão – 0800-123-9234	

Online (Resto do mundo)
www.brookfield.ethicspoint.com
Online (Elera) - www.canalconfidencial.com.br/elera
Online (China, exceto Hong Kong) – https://brookfield.whispli.com.cn/pages/renewables

Observação: O tipo de denúncia que pode ser feita à Linha de Denúncia de Ética e ao Site pode ser restrito em certas jurisdições de acordo com a legislação local aplicável. Entre em contato com a Rede para obter mais detalhes sobre essas restrições.