Voir la

POLITIQUE RELATIVE À L'**UTILISATION ACCEPTABLE DES ACTIFS TECHNOLOGIQUES**

See the

ACCEPTABLE USE POLICY FOR **TECHNOLOGY ASSETS**

Veja o

POLÍTICA DE **USO ACEITÁVEL PARA ATIVOS DE TECNOLOGIA**

POLITIQUE RELATIVE À L'UTILISATION ACCEPTABLE DES ACTIFS TECHNOLOGIQUES

Brookfield

TABLE DES MATIÈRES

1. DÉFINITIONS

TERME	DÉFINITIONS
Brookfield Renewable Partners (BEP)	Brookfield Renewable Partners L.P. s'entend de BEP et de ses filiales, y compris Brookfield Energia Renovavel (BER), le Groupe corporatif de BEP, les plateformes de BEP et Énergie Brookfield Marketing S.E.C. (« ÉBM »).
Actif technologique	Comprend, sans toutefois s'y limiter, tous les équipements/systèmes de technologies de l'information (TI) et de technologie opérationnelle (TO) qui sont détenus par BEP ou fournis par un tiers en vue de son utilisation par BEP (p. ex., logiciel en tant que service, plateforme en tant que service, infrastructure en tant que service) et les applications logicielles hébergées; les réseaux, y compris les réseaux locaux, étendus, Internet, sans fil et mobiles; les périphériques réseau, les systèmes téléphoniques, les imprimantes, les serveurs et systèmes de stockage, les ordinateurs personnels, les portables, les téléphones intelligents, les tablettes et autres appareils mobiles; ainsi que les outils de collaboration, y compris le courrier électronique et la messagerie instantanée. Tous les actifs de TI se trouvant sous le contrôle/dans les environnements des opérations des centrales de BEP sont inclus dans cette définition.
Programme malveillant	Logiciel conçu en vue d'exploiter, d'infiltrer ou d'endommager des actifs technologies sans le consentement éclairé de l'utilisateur. Comprend également les virus informatiques, les vers informatiques, les chevaux de Troie, les trousses administrateur pirate (rootkit), les logiciels espions, les logiciels publicitaires malhonnêtes et les autres logiciels non désirés.
Personnel, membre du personnel	Tout employé, entrepreneur, personne ou fournisseur de services qui a été autorisé à avoir accès à un actif technologique de BEP ou qui utilise un actif technologique de BEP.

2. OBJET

L'objet de la présente politique est de décrire ce qui constitue une utilisation acceptable des actifs technologiques de BEP. Ces normes sont en place afin de protéger le personnel, les clients, les partenaires et les contreparties de BEP contre tout tort causé par l'utilisation abusive des actifs technologiques.

Les plateformes opérationnelles peuvent également établir des politiques et lignes directrices supplémentaires traitant de leurs besoins particuliers, et celles-ci doivent être interprétées de concert avec la présente politique. En cas d'incohérence entre la présente politique et la politique supplémentaire de la plateforme en matière de TI/TO, la présente politique prévaudra.

3. PORTÉE

La présente politique s'applique à tous les membres du personnel et à tous les actifs technologiques de BEP.

4. RESPONSABILITÉS

Le Chef de la direction des technologies de l'information du Groupe corporatif est responsable du contenu et du maintien de la présente politique.

Les Chefs de la direction des technologies de l'information (Groupe corporatif et plateformes) sont responsables de la diffusion, de la formation, de la surveillance et de l'application associées à cette politique au sein de leurs secteurs de responsabilité. Les Chefs de la direction des technologies de l'information (Groupe corporatif et plateforme) communiqueront le contenu de la présente politique à leurs équipes de direction respectives et coordonneront la communication de la politique.

5. POLITIQUE

5.1 Utilisation des actifs technologiques

Les actifs technologies sont fournis au personnel en tant qu'outils habilitants sur le plan opérationnel et commercial afin de soutenir les buts et objectifs de l'organisation. Par conséquent, les actifs technologiques doivent être utilisés dans l'exercice des fonctions et des responsabilités d'une manière conforme à la présente politique et d'autres politiques de BEP, y compris le Code d'éthique et de conduite des affaires, la Politique de milieu de travail positif et la Politique corporative de sécurité informatique.

L'utilisation personnelle accessoire des actifs de TI à des fins non liées à l'entreprise est permise si l'utilisation :

- ne consomme pas plus qu'une quantité négligeable de ressources informatiques et de ressources réseau;
- n'interfère par avec la productivité d'autres personnes;
- n'empêche pas l'exercice de quelque activité de l'entreprise que ce soit;
- ne cause pas de détresse ni de problèmes sur le plan juridique ou moral à d'autres membres du personnel ou à BEP en tant que telle.

L'utilisation abusive des actifs technologiques de BEP n'est pas tolérée. Il est toujours interdit au personnel d'utiliser les actifs technologiques à des fins inappropriées ou illicites. Les activités inacceptables constituant une utilisation abusive comprennent, sans toutefois s'y limiter, ce qui suit :

- Commettre des actes illégaux, frauduleux ou malicieux.
- Posséder, stocker, afficher ou transmettre du matériel qui pourrait être offensant en raison de son contenu sexuel, raciste ou religieux, y compris du matériel qui enfreint les lois sur le harcèlement ou sur le milieu de travail.
- Accéder à des systèmes ou à des logiciels qui sont restreints au personnel des TI/TO.
- Trafiquer intentionnellement le fonctionnement normal de l'environnement des TI, ou interférer d'autre façon dans celui-ci, y compris au moyen de la propagation de virus informatiques ou d'autres programmes malveillants.

- Altérer intentionnellement la configuration des actifs technologiques, contourner les restrictions aux accès, acquérir ou installer des logiciels (lorsque des contrôles ne sont pas en place pour empêcher un tel achat ou une telle acquisition) sans avoir obtenu une autorisation spécifique de la part du personnel des TI/TO.
- Utiliser les actifs technologiques pour obtenir un gain personnel ou exercer des activités non liées à l'entreprise pendant une durée prolongée.
- Exercer des activités non liées à l'entreprise qui sont susceptibles d'influer sur la performance de l'environnement des TI de l'organisation, comme la lecture audio/vidéo en continu, les jeux vidéos en ligne, etc., ou qui sont susceptibles d'avoir une incidence négative sur la réputation de l'organisation.
- Exercer toute activité susceptible d'avoir une incidence sur le niveau de sécurité de l'organisation sans avoir obtenu une autorisation spécifique de la part du personnel des TI/TO. Cela comprend l'installation de réseaux sans fil ou d'autres systèmes multi-utilisateurs pour communiquer de l'information ainsi que l'acquisition, la possession ou l'utilisation d'outils matériels ou logiciels pouvant être employés pour évaluer ou compromettre la sécurité.
- Violer les droits de propriété intellectuelle ou les droits à la vie privée d'autrui.
- Partager des comptes personnels et des mots de passe, ou utiliser le compte d'une autre personne.
- Laisser des actifs technologiques sans protection contre des vols opportunistes à l'extérieur des installations de BEP.
- Ouvrir des courriels non sollicités ou encore des pièces jointes ou des liens contenus dans un courriel provenant de parties inconnues.
- Générer ou transmettre une chaîne de courriels non liée à l'entreprise.
- Obtenir des services d'infonuagique pour stocker, traiter, partager ou gérer des informations de BEP sans avoir obtenu une autorisation spécifique de la part du personnel des TI/TO. Cela comprend transmettre des messages à un compte de courriel personnel n'appartenant pas à BEP à des fins de convenance.

5.2 Sécurité informatique et informations sensibles

Si vous détenez un ordinateur ou un appareil mobile fourni par BEP, vous êtes considéré être le gardien de cet actif. Vous devez en assurer la manipulation et la sauvegarde avec soin, surtout à l'extérieur des installations de BEP. Si un actif a été endommagé, perdu, ou volé ou qu'il ne peut pas être utilisé dans le cadre d'activités liées à l'entreprise pour d'autres raisons, vous devez en informer sans délai votre gestionnaire ainsi que le Centre de services TI. Les ordinateurs, à l'exception des portables ou des appareils mobiles personnellement attribués, ne doivent pas être déplacés ou relocalisés sans l'approbation expresse du service des TI de BEP.

Il vous incombe de vous assurer que toutes les données, y compris les informations sensibles, de valeur ou critiques, sont stockées de façon appropriée sur le réseau de BEP ou dans un système ou un référentiel approuvé.

Vous devez assurer la sécurité des informations sur vos comptes, comme les identifiants de connexion et les mots de passe. Vous êtes également responsable des activités menées dans le contexte des comptes qui vous ont été assignés. Lorsque vous créez des mots de passe, vous

devez employer les pratiques exemplaires consistant à élaborer des mots de passe complexes qui comprennent une combinaison de lettres majuscules et minuscules, de chiffres et de symboles spéciaux. Les mots de passe ne doivent pas être notés par écrit.

Tous les portables et postes de travail sont sécurisés au moyen d'un écran de veille protégé par mot de passe doté d'une fonction d'activation automatique. Vous devez verrouiller ou fermer tout ordinateur qui sera laissé sans surveillance pendant une certaine période.

L'environnement technologique de BEP contient des informations sensibles et confidentielles. Vous devez prendre tous les moyens nécessaires pour empêcher un accès non autorisé à ces informations ou la communication de ces informations, conformément au Code d'éthique et de conduite des affaires et à la Politique de divulgation. Les médias amovibles contenant des informations sensibles doivent être manipulés avec soin, tel qu'il est décrit ci-après.

5.3 Médias amovibles

Les médias amovibles, y compris les CD/DVD, les clés USB et les lecteurs de stockage portables, sont des sources fréquentes d'incidents en matière de sécurité, comme les infections par des programmes malveillants et les atteintes à la protection des données. Par conséquent, vous ne devez pas faire ce qui suit :

- Brancher un média amovible provenant d'une source inconnue à un ordinateur de BEP. Bien que les ordinateurs de BEP soient protégés par des logiciels antivirus, ces derniers n'offrent pas toujours une protection efficace contre les programmes malveillants stockés dans un média amovible.

- Stocker des informations sensibles ou confidentielles en texte clair (sans cryptage) dans des médias amovibles, car la perte de ceux-ci pourrait donner lieu à une atteinte à la protection des informations. Les informations sensibles ou confidentielles qui doivent être échangées par l'entremise de médias amovibles doivent être cryptées à l'aide d'un outil de cryptage approuvé par le service des TI de BEP.

- Laisser les médias amovibles contenant des informations sensibles à la vue de tous ni faire en sorte qu'ils soient susceptibles de faire l'objet d'un vol opportuniste.

6. SURVEILLANCE ET PROTECTION DES RENSEIGNEMENTS PRIVÉS

Toutes les informations contenues dans l'environnement des TI de BEP appartiennent à BEP. Toutes les informations stockées dans des actifs technologiques de BEP ne sont ni privées ni confidentielles, et ce, même si des mots de passe ou d'autres dispositifs de sécurité sont en place. BEP conserve l'accès et se réserve le droit d'accéder au contenu ainsi que de surveiller le contenu se trouvant sur ou dans un actif technologique de BEP en tout temps, et peut récupérer, examiner, auditer, intercepter, communiquer ou restreindre toute information sur de tels systèmes, y compris, sans toutefois s'y limiter, les courriels, les messages instantanés, les fichiers et les journaux d'utilisation d'Internet, sans avoir obtenu la permission du titulaire du compte.

Les raisons pour lesquelles BEP ou d'autres personnes ou entités autorisées par BEP peuvent accéder aux données ou aux systèmes comprennent les suivantes, sans toutefois s'y limiter : déterminer si une infraction à la présente politique ou à une autre politique de BEP est survenue; enquêter sur une défaillance ou une erreur dans le système; surveiller l'utilisation du système ou du réseau; obtenir des informations demandées par un tiers dans le cadre d'un litige, ou en réponse à une enquête menée par le gouvernement et dans le cadre normal des activités.

7. SIGNALEMENT

Nous avons tous l'obligation de respecter la présente politique. Si vous êtes témoin d'un comportement de la part d'un membre du personnel de l'organisation ou d'un tiers qui, pourrait constituer une infraction à la présente politique, vous devez le déclarer sans délai. La déclaration d'une infraction à l'interne est importante pour l'organisation, et est à la fois un devoir et un acte valorisé.

L'organisation prend toutes les déclarations au sérieux, et chaque déclaration reçue sera évaluée et, lorsque cela est nécessaire, une enquête appropriée sera menée. La confidentialité des infractions déclarées sera maintenue lorsque cela est possible, conformément au besoin de mener un examen adéquat et sous réserve des lois applicables.

Les déclarations doivent être faites en premier lieu aux gestionnaires principaux des TI dont le nom figure à l'annexe A ou à un autre gestionnaire principal, qui s'assurera que l'information est traitée de façon appropriée et est portée à l'attention d'un niveau hiérarchique supérieur lorsque cela est nécessaire. Advenant que ce moyen ne semble pas approprié compte tenu de la nature ou du contenu de la déclaration, cette dernière doit être faite par l'entremise de la ligne téléphonique ou le site Web de signalement. La ligne téléphonique et le site Web de signalement, qui sont gérés par un tiers indépendant, The Network, permettent à quiconque d'effectuer un signalement de façon anonyme, et ce, en anglais, en français, en portugais et dans d'autres langues. La ligne téléphonique et le site Web de signalement sont sans frais et disponibles en tout temps. Veuillez consulter l'annexe A pour savoir comment joindre la ligne téléphonique et le site Web de signalement.

Aucune mesure de représailles ne sera prise à l'encontre d'une personne qui effectue une déclaration fondée sur des motifs raisonnables de croire, de bonne foi, qu'une infraction à la présente politique a été commise.

8. APPLICATION ET MESURES DISCIPLINAIRES

Toute infraction à la présente politique constitue un motif justifiant BEP à prendre l'une des mesures suivantes :

- Révoquer et/ou restreindre l'accès aux actifs technologiques de BEP.
- Imposer des sanctions disciplinaires, y compris le congédiement ou la résiliation du contrat.
- Intenter une poursuite à l'encontre de la ou des personnes impliquées.

ANNEXE A
COORDONNÉES POUR L'APPLICATION DE LA POLITIQUE

Steve Little	(819) 561-2722 poste 6661	steve.little@energiebrookfield.com
Yanic Croteau	+55 (21) 2439-5154	yanic.croteau@brookfieldenergia.com
Michelle McClafferty	+353 (21) 422-3637	michelle.mcclafferty@brookfieldrenewable.com
Peter Pilgrim	(819) 561-8636	peter.pilgrim@energiebrookfield.com

LIGNE TÉLÉPHONIQUE DE SIGNALEMENT

The Network, une société du groupe NAVEX Global

Amérique du Nord :	1-800-665-0831
Brésil :	0800-777-0772
Royaume-Uni :	0-808-234-2210
Irlande :	1-800-94-6551
Portugal :	800-78-4717
Ailleurs dans le monde :	770-613-6339

SITE WEB DE SIGNALEMENT

https://brookfieldrenewable.tnwreports.com/

ACCEPTABLE USE POLICY FOR TECHNOLOGY ASSETS

Brookfield

TABLE OF CONTENTS

1. DEFINITIONS

TERM	DEFINITIONS
Brookfield Renewable Partners (BEP)	Brookfield Renewable Partners L.P. refers to BEP and its subsidiaries, including, Brookfield Energia Renovavel (BER), BEP Corporate, the BEP Platforms, and Brookfield Energy Marketing L.P. ("BEM").
Technology Asset	Includes but is not limited to all Information Technology (IT) and Operational Technology (OT) equipment/systems and software that are owned by BEP or provided for BEP's usage by a 3rd party (such as Software as a Service, Platform as a Service, Infrastructure as a Service) and hosted software applications; networks including local, wide-area, Internet, wireless and mobile; networking devices, phone systems, printers, servers and storage systems, personal computers, laptops, smartphones, tablets, other mobile devices; and collaboration tools including email and instant messaging. All IT assets within BEP plant control/operations environments are included within this definition.
Malware	Software designed to exploit, infiltrate or damage Technology Assets without the informed consent of the User. It also includes computer viruses, worms, Trojan horses, rootkits, spyware, dishonest adware and other unwanted software.
Personnel	Any employee, contractor, individual or service provider who has been authorized for access to, or has use of a BEP Technology Asset.

2. PURPOSE

The purpose of this policy is to outline the acceptable use of BEP's Technology Assets. These standards are in place to protect BEP personnel, customers, partners, and counterparties from harm caused through the misuse of Technology Assets.

The Operating Platforms may also define supplementary policies and guidelines specific to their needs which should be read in tandem with this policy. In the event of any inconsistency between this Policy and the supplementary IT/OT policy of a platform, this policy shall apply.

3. SCOPE

This policy applies to all personnel and all BEP Technology Assets.

4. RESPONSIBILITIES

The Chief Information Officer ("CIO") of the Corporate Group is responsible for the content and maintenance of this policy.

The CIOs (Corporate and Platform) are responsible for the dissemination, training, monitoring, and enforcement associated with this policy within their areas of responsibility. The CIOs (Corporate and Platform) will communicate the content of this policy with their respective management teams and coordinate the communication of the policy.

5. POLICY

5.1 Use of Technology Assets

Technology Assets are provided as operational and business enablers for personnel to support the organization's goals and objectives. Accordingly, Technology Assets are to be used in the execution of duties and responsibilities in a manner that is consistent with this policy and other BEP policies; including the Code of Business Conduct and Ethics, the Positive Work Environment Policy, and the Corporate IT Security Policy.

Incidental personal use of IT Assets for non-business purposes is permissible if the use does not:

- Consume more than a trivial amount of computing or network resources
- Interfere with others' productivity
- Pre-empt any business activity
- Cause distress, legal, or morale issues for other Personnel or BEP itself

Misuse of BEP Technology Assets is not tolerated. Personnel are never permitted to use Technology Assets for any inappropriate or unlawful purpose. Unacceptable activities constituting misuse include but are not limited to the following:

- Engage in illegal, fraudulent or malicious conduct
- Possess, store, display, or transmit any material that may be offensive because of their sexual, racist or religious content including material that is in violation of any harassment or workplace laws
- Access systems or software that are restricted to IT/OT personnel
- Intentionally tamper with or otherwise interfere with the normal operation of the IT environment, including the propagation of computer viruses or other malware
- Intentionally alter the configuration of Technology Assets, bypass access restrictions, acquire or install software (where controls are in place to prevent this) without specific authorization from the IT/OT personnel
- Use of Technology Assets for personal gain or for prolonged non-business related activities
- Conduct non-business related activities that may impact the performance of the organization's IT environment such as streaming audio/video, online video gaming, etc., or which may negatively affect the organization's reputation
- Conduct any activity that may impact the organization's security posture without specific authorization from IT/OT personnel. This includes establishing wireless networks or other multi-user systems for communicating information, acquiring, possessing or using hardware or software tools that could be employed to evaluate or compromise security
- Infringe upon others' intellectual property or privacy rights

- Share personal account and password information or use of someone else's account
- Leave Technology Assets unprotected from opportunistic theft outside of BEP facilities
- Open unsolicited email, attachments, or links in email from unknown parties
- Generate or forward non-business chain email
- Provision cloud services to store, process, share, or manage BEP information without specific authorization from the IT/OT personnel. This includes forwarding messages to a non-BEP personal email account for convenience.

5.2 Computer Security and Sensitive Information

If you have been assigned a BEP computer or mobile device, you are considered to be the custodian of that asset. You should exercise care in the handling and safe-keeping of assets in your possession, especially outside of BEP facilities. If an asset has been damaged, lost, stolen, or is otherwise unavailable for business activities, you must promptly inform your manager as well as the IT Service Desk. Computer equipment, with the exception of personally-assigned laptops or mobile devices, must not be moved or relocated without the express approval of BEP IT.

It is your responsibility to ensure that all data, including sensitive, valuable, or critical information is appropriately stored on the BEP network or within an approved system or repository.

You must keep account information such as login IDs and passwords secure. You are also responsible for activities undertaken in the context of accounts that are assigned you. When creating passwords, you should employ best practices in creating complex passwords that include a combination of upper and lower case letters, numbers and special symbols. Passwords should not be written down.

All laptops and workstations are secured with a password-protected screensaver with an automatic activation feature and you must lock or log off any computer that is left unattended for any period of time.

The BEP technology environment contains information that is sensitive and confidential. You are expected to take all necessary steps to prevent unauthorized access to or disclosure of this information in accordance with The Code of Business Conduct and Ethics and The Disclosure Policy. Removable media containing sensitive information must be handled with care, as described below.

5.3 Removable Media

Removable media, including CD/DVD, USB drives, and portable storage drives are frequent sources of security incidents, such as malware infections and data breaches. Accordingly, you must not:

- Connect removable media from an unknown source to a BEP computer. Although BEP computers are protected with antivirus software, this is not always effective against malware embedded in removable media.
- Store sensitive or confidential information in clear text (unencrypted) on removable media, as loss could result in an information breach. Sensitive or confidential information that needs to be exchanged through removable media must be encrypted using a BEP IT approved tool.
- Removable media containing sensitive information must not be left out in the open or allowed to be vulnerable to opportunistic theft.

6. MONITORING & PRIVACY

All information contained within the BEP IT environment is BEP property. All information stored within BEP Technology Assets is not private or confidential even when passwords or other security restrictions are in place. BEP maintains access to, and reserves the right to access and monitor content on or within any BEP Technology Asset at any time, and can retrieve, review, audit, intercept, disclose or restrict any information on such systems, including, but not limited to, email, instant messages, files, and Internet usage logs, without the permission of the account holder.

The reasons for which BEP or others authorized by BEP may access data or systems include, but are not limited to: determining whether a violation of this policy or other BEP policy has occurred; investigating a failure or error in a system; monitoring system or network utilization, obtaining information requested by a third party in litigation, or in response to a government investigation, and in the normal course of business.

7. REPORTING

We all have an obligation to adhere to this Policy. If you witness behavior on the part of the Organization's personnel or any Third Party that you believe may represent a violation of this Policy you must promptly report it. Internal reporting is important to the Organization and it is both expected and valued.

The Organization takes all reports seriously, and every report received will be assessed and, where necessary, appropriate investigation will be undertaken. The confidentiality of reported violations will be maintained where possible, consistent with the need to conduct an adequate review and subject to applicable law.

Reports should in the first instance be made to the IT senior managers listed in Appendix "A", or other senior manager, who will ensure that the information is properly handled and escalated as necessary. In the event that this does not appear to be an appropriate avenue because of the nature or the content of the report, it should be made to the Ethics Reporting Line or Ethics Reporting Website. The Ethics Reporting Line/Website is managed by an independent third party and allows for anonymous reporting. Reports can be made in English, French and Portuguese, along with other languages, and is available toll-free, 24 hours a day, 7 days a week. Please see Appendix "A" for the ways in which you can reach the Ethics Reporting Line/Website.

No retribution or retaliation will be taken against any person who has made a report based on the reasonable good faith belief that a violation of this Policy has occurred.

8. ENFORCEMENT AND DISCIPLINARY ACTION

Any violation of this policy is grounds for BEP to:

- Revoke and/or restrict access to BEP Technology Assets
- Take disciplinary action including termination of employment or contract
- Initiate legal action against the individual and/or other persons who may be involved

APPENDIX A
CONTACT INFORMATION FOR POLICY

Steve Little	(819) 561-2722 ext. 6661	steve.little@brookfieldrenewable.com
Yanic Croteau	+55 (21) 2439-5154	yanic.croteau@brookfieldenergia.com
Michelle McClafferty	+353 (21) 422-3637	michelle.mcclafferty@brookfieldrenewable.com
Peter Pilgrim	(819) 561-8636	peter.pilgrim@brookfieldrenewable.com

ETHICS REPORTING LINE

The Network, a NAVEX Global Company

North America:	1-800-665-0831
Brazil:	0800-777-0772
UK:	0-808-234-2210
Ireland:	1-800-94-6551
Portugal:	800-78-4717
Worldwide:	770-613-6339

ETHICS REPORTING WEBSITE

https://brookfieldrenewable.tnwreports.com/

POLÍTICA DE **USO ACEITÁVEL PARA ATIVOS DE TECNOLOGIA**

Brookfield

SUMÁRIO

1. DEFINIÇÕES

TERMO	DEFINIÇÕES
Brookfield Renewable Partners (BEP)	Brookfield Renewable Partners L.P. refere-se à BEP e suas subsidiárias, inclusive à Brookfield Energia Renovavel (BER), BEP Corporate, as Plataformas BEP, e a Brookfield Energy Marketing L.P. ("BEM").
Ativo de Tecnologia	Inclui, mas não se restringe a todos os equipamentos/sistemas e softwares de Tecnologia da Informação (TI) e de Tecnologia Operacional (TO) de propriedade da BEP ou fornecidos por terceiro (como um Software como Serviço, Plataforma como Serviço, Infraestrutura como Serviço) para uso por parte da BEP e aplicativos de software hospedados; redes, inclusive local, , *Internet, wireless* e móvel; dispositivos de rede, sistemas de telefonia, impressoras, sistemas de servidores e armazenagem, *PCs, laptops*, *smartphones, tablets* e outros dispositivos móveis; e ferramentas de colaboração, inclusive e-mail e mensagem instantânea. Todos os ativos de TI nos ambientes de controle/operação da fábrica estão incluídos nesta definição.
Malware	Software destinado a explorar, infiltrar ou danificar Ativos de Tecnologia sem o consentimento do Usuário. Inclui também vírus e worms de computador, cavalos de Tróia *(Trojan horses*), *rootkits*, *spyware, dishonest adware* e outros softwares indesejados.
Colaboradores	Qualquer funcionário, pessoa contratada, indivíduo ou prestador de serviço autorizado a ter acesso a, ou a usar Ativo de Tecnologia da BEP

2. OBJETIVO

O objetivo desta política consiste na definição do uso aceitável de Ativos de Tecnologia da BEP. Estas normas existem para proteger os colaboradores, clientes, sócios, parceiros e contrapartes da BEP de eventual dano causado por uso indevido de Ativos de Tecnologia.

As Plataformas Operacionais também poderão definir políticas e diretrizes suplementares específicas às suas necessidades, que devem ser lidas em conjunto com esta política. Na hipótese de eventual conflito entre esta Política e a política de TI/TO suplementar de uma plataforma, esta política prevalecerá.

3. ESCOPO

Esta política se aplica a todos os colaboradores e a todos os Ativos de Tecnologia da BEP.

4. RESPONSABILIDADES

O Diretor de Tecnologia da Informação (*Chief Information Officer* - "CIO") do Grupo Corporativo é responsável pelo conteúdo e manutenção desta política.

Os CIOs (Corporativo e de Plataforma) são responsáveis pela disseminação, treinamento, monitoramento e aplicação desta política dentro de suas áreas de responsabilidade. Os CIOs (Corporativo e de Plataforma) comunicarão o conteúdo desta política às suas respectivas equipes de gestão e coordenarão a divulgação da política.

5. POLÍTICA

5.1 Uso de Ativos de Tecnologia

Os Ativos de Tecnologia são fornecidos como instrumentos que permitem aos colaboradores dar apoio às metas e objetivos da empresa. Portanto, os Ativos de Tecnologia devem ser usados no desempenho das atribuições e responsabilidades de modo compatível com esta e outras políticas da BEP; inclusive o Código de Ética e Conduta Corporativa, a Política de Ambiente de Trabalho Positivo, e a Política de Segurança de TI Corporativa.

Admite-se o eventual uso pessoal de Ativos de TI para fins não corporativos desde que tal uso não implique em quaisquer das seguintes consequências:

- Consumo de quantidade de recursos de rede ou computador maior que o trivial
- Interfira na produtividade de outros
- Tenha prioridade sobre as atividades da empresa
- Provoque problemas jurídicos, morais ou desconforto a outros colaboradores ou à própria BEP

Não se tolera o uso indevido de Ativos de Tecnologia da BEP. Não se admite que o colaborador use Ativos de Tecnologia para qualquer finalidade inadequada ou ilegal. Atividades inaceitáveis consideradas como uso indevido incluem, dentre outros, as seguintes:

- A prática de conduta ilegal, fraudulenta ou dolosa
- A posse, armazenagem, exibição ou transmissão de qualquer material que possa ser ofensivo em virtude de seu conteúdo sexual, racista ou religioso, incluindo-se material que infrinja quaisquer leis contra assédio ou disciplinadoras do ambiente de trabalho
- O acesso a sistemas ou software que sejam restritos à equipe de TI/TO
- A alteração ou interferência intencional nas operações normais do ambiente de TI, inclusive a propagação de vírus ou outros *malwares*
- A alteração intencional da configuração dos Ativos de Tecnologia, o desvio de restrições de acesso, a aquisição ou instalação de software (onde haja controles destinados a evitar tais práticas) sem autorização específica da equipe de TI/TO
- Uso de Ativos de Tecnologia em benefício pessoal ou para atividades de longo prazo não relacionadas à empresa
- A realização de atividades não relacionadas à empresa que possam interferir no desempenho do ambiente de TI da empresa, como o uso de áudio/vídeo em streaming, uso de vídeo game online, etc., ou que possa prejudicar a reputação da empresa

- A prática de qualquer atividade que possa comprometer a postura da segurança da empresa sem autorização específica da equipe de TI/TO, que inclui o estabelecimento de redes sem fio ou outros sistemas de usuários múltiplos de comunicação de informação, aquisição, posse ou uso de ferramentas de hardware ou software que poderiam ser usadas para avaliar ou prejudicar a segurança
- A violação de direitos de propriedade intelectual ou de privacidade de outrem
- O compartilhamento de informações sobre contas e senhas pessoais, ou o uso de conta de outrem
- A falta de zelo para com os Ativos Tecnológicos, deixando-os sujeitos a furto fora das dependências da BEP
- A Abertura de e-mails, anexos ou links não solicitados em mensagens eletrônicas de pessoas desconhecidas
- A geração ou o encaminhamento de cadeia de e-mail não corporativo
- A prestação de serviços de armazenagem de dados em nuvem para guardar, processar, compartilhar ou gerenciar informações da BEP sem autorização específica da equipe de TI/TO, inclusive o encaminhamento de mensagens a contas pessoais de e-mail de que não seja da BEP por conveniência.

5.2 Segurança de Computador e Informações Sensíveis

Quem recebe um computador ou dispositivo móvel da BEP é considerado responsável por tal ativo e deve ter cuidado no manuseio e na guarda de tais ativos em sua posse, especialmente fora das instalações da BEP. Em caso de dano, perda, roubo ou outra hipótese de indisponibilidade de tal ativo para uso corporativo, o responsável deverá prontamente informar à sua gerência, bem como à Central de Serviço de TI. Os computadores, com exceção dos laptops ou dispositivos móveis entregues pessoalmente para uso do funcionário, não devem ser transportados ou deslocados sem autorização expressa do TI da BEP.

É de responsabilidade do colaborador garantir que todos os dados, inclusive informações sensíveis, valiosas ou críticas sejam adequadamente armazenadas na rede da BEP ou em sistema ou repositório autorizado.

O responsável deve manter as informações de conta, tais como nomes de usuário (login IDs) e senhas em segurança. Ele é também responsável pelas atividades realizadas no âmbito das contas entregues a eles. Ao criarem senhas, os responsáveis devem envidar seus melhores esforços para gerarem senhas complexas que incluam a combinação de maiúsculas e minúsculas, números e símbolos. As senhas não devem ser registradas por escrito.

Todos os laptops e estações de trabalho contam com protetor de tela protegido por senha e de ativação automática, e sempre deve ser desligado ou travado quando ficar sem uso por qualquer período de tempo.

O ambiente de tecnologia da BEP contém informações sensíveis e confidenciais. Todas as medidas necessárias devem ser tomadas para evitar o acesso não autorizado ou a revelação dessas informações, de acordo com o Código de Ética e Conduta Corporativa e com a Política de Divulgação de Informações. Mídias removíveis que contenham informações sensíveis devem ser manuseadas com cuidado, conforme descrito abaixo.

5.3 Mídias Removíveis

As mídias removíveis, inclusive CD/DVD, drives de USB, e drives de armazenamento portáteis são frequentemente fontes de incidentes de segurança, como infecções por *malware* e vazamento de dados. Portanto, não se deve:

- Conectar mídias removíveis de uma fonte desconhecida a um computador da BEP. Embora os computadores da BEP estejam protegidos com software de antivírus, eles nem sempre são eficientes contra malwares embutidos em mídias removíveis.

- Armazenar informações sensíveis ou confidenciais em textos abertos (sem criptografia) em mídias removíveis, já que sua perda poderia resultar em acesso não-autorizado a informações. As informações sensíveis ou confidenciais que precisarem ser trocadas por meio de mídia removível devem ser criptografadas utilizando-se ferramenta aprovada pelo TI da BEP.

- As mídias removíveis que contiverem informações sensíveisou confidenciais não devem ser deixadas abertas ou vulneráveis a furto.

6. MONITORAMENTO & PRIVACIDADE

Todas as informações contidas no ambiente de TI da BEP constituem propriedade da BEP. Nenhuma informação armazenada nos Ativos de Tecnologia da BEP é considerada particular nem confidencial, mesmo quando protegida por senha ou outros meios de segurança. A BEP mantém seu acesso, e reserva a si o direito de acessar e monitorar conteúdo que esteja em qualquer Ativo de Tecnologia da BEP a qualquer tempo, podendo resgatar, revisar, auditar, interceptar, revelar ou restringir qualquer informação contida nesses sistemas, inclusive, dentre outros, em e-mails, mensagens instantâneas, arquivos e registros de uso de internet, sem a permissão do titular da conta

Os motivos pelos quais a BEP ou outros autorizados pela BEP podem acessar dados ou sistemas incluem, dentre outros: determinar se houve violação desta política ou de outra política da BEP; investigar falha ou erro em um sistema; monitorar o uso de sistema ou de rede, obtendo informações solicitadas por terceiro em litígio, ou em resposta a investigação governamental, e no curso regular das atividade

7. DENÚNCIA

Todos temos o dever de aderir a esta Política. Quem testemunhar qualquer comportamento por parte dos colaboradores da Empresa, ou por qualquer Terceiro que se acredite que possa representar uma violação desta Política, tem o dever de denunciá-lo imediatamente. A denúncia interna é importante para a Empresa e é não apenas esperada como também valorizada.

A Empresa leva seriamente em consideração todas as denúncias, sendo cada uma delas avaliada e, se necessário, encaminhada à investigação. A confidencialidade das violações denunciadas será mantida sempre que possível, e de modo compatível com a necessidade de realizar sua devida revisão e sujeição à legislação aplicável.

As denúncias devem primeiramente ser feitas aos gerentes sêniores de TI relacionados no Apêndice “A”, ou a outro gerente sênior, que garantirá que a informação seja devidamente examinada e encaminhada, se necessário. Na hipótese de não ser este o caminho adequado, em virtude da natureza ou do conteúdo da denúncia, ela deverá ser feita ao Canal Confidencial O Canal Confidencial é administrado por uma empresa terceira independente e permite a denúncia anônima. As denúncias podem ser feitas em inglês, francês e português, em conjunto com outras línguas, e são disponibilizadas por ligação gratuita, 24 hours por dia, 7 dias por semana. Consulte o Apêndice “A” para saber como contatar o Canal Confidencial.

Não haverá punição ou retaliação contra quem fizer uma denúncia, considerando-se a boa-fé que se acredita existir da parte da pessoa que denuncia uma violação desta Política.

8. APLICAÇÃO E MEDIDAS DISCIPLINARES

Qualquer violação desta política constitui base para que a BEP:

- Revogue e/ou restrinja o acesso a Ativos de Tecnologia da BEP
- Tome medidas disciplinares, incluindo-se a rescisão da relação de emprego ou do contrato
- Ajuíze demanda contra a pessoa e/ou outras pessoas que estejam envolvidas

APÊNDICE A
INFORMAÇÕES DE CONTATO PARA A POLÍTICA

Steve Little	(819) 561-2722 ext. 6661	steve.little@brookfieldrenewable.com
Yanic Croteau	+55 (21) 2439-5154	yanic.croteau@brookfieldenergia.com
Michelle McClafferty	+353 (21) 422-3637	michelle.mcclafferty@brookfieldrenewable.com
Peter Pilgrim	(819) 561-8636	peter.pilgrim@brookfieldrenewable.com

CANAL CONFIDENCIAL

A Network, uma Empresa da NAVEX Global

North America:	1-800-665-0831
Brazil:	0800-777-0772
UK:	0-808-234-2210
Irlanda:	1-800-94-6551
Portugal:	800-78-4717
No mundo:	770-613-6339

WEBSITE DO CANAL CONFIDENCIAL

https://brookfieldrenewable.tnwreports.com/