1. Purpose

The purpose of this document is to provide guidelines for access to Third party users to use Brookfield Renewable (Operating) India Private Limited's resources. The data must be protected from unauthorized access, alteration, deletion, or destruction. This policy is applicable to Brookfield Renewable (Operating) India Private Limited and all the entities of Brookfield Renewable in India hereinafter collectively referred to as 'BRIPL'.

2. Scope

This policy applies to all outsourced parties who need access to information resources and IT infrastructure. The information resources covered under this policy includes software, applications, databases, servers and desktops, laptops, standalone devices, networking/security components, etc.

The tools and technologies mentioned in the policy will be deployed as per the Information Security roadmap.

3. Roles & Responsibilities

Role	Responsibility
IT Head	• Responsible for creation and implementation of this guideline • Responsible for approving access requests in consultation with the respective business unit heads/ and system/ application owners. • Responsible for documenting and retaining a record of user access rights for auditing purposes.
System Administrator of respective system	• Responsible for the protection of administrator account details and must not share credentials with unauthorized users. • Will only use administrator accounts for performing administration related activities.
Business Manager	• Supervise user access requests and rights for the Business Team • Are responsible for ensuring third-party service providers of services and systems comply with User Access Management policy.
Cyber Security Specialist	• Monitor and inspect all user access activity related to network access, remote access, privileged access, etc. • Responsible to conduct periodic user access reviews and other compliance checks to ensure security is not compromised. • Report any cyber risks or unauthorized user activities identified to the IT Head and further suggest ways to mitigate the risks.
Third Party Users	• Responsible to comply with BRIPL policies • Immediately alert Business Unit Head or IT team if any information is disclosed or breach occurs.

4. User Access Management Policy

Identity Access Management

User Access Management

- A formal user registration and de-registration process shall be followed to create and assign user accounts to any new contract user
- All requests for access or privileges to information systems must be approved by the system or information owner or appropriate delegate (IT Head). Only access that is required by the individual or entity to perform his/ her responsibilities will be granted, using the "need to know" and "least privilege" principles.
- Unique user-IDs shall be assigned to personnel on enrollment and registration. Whenever possible, a standardized user-ID naming convention will be utilized to maintain consistency across systems.
- Access privileges shall be assigned to a unique user-ID that is mapped to an employee/contractor based on individual's subscribed role, business need and security requirements.
- Generic user-IDs shall not be created unless required by technology limitations or under business needs. An owner shall be identified and documented for every generic user-ID created and the owner shall be accountable for all actions associated with the generic user-ID.
- Contractors and third-party vendors shall not be granted access to BRIPL information and information systems unless there is a contractual agreement and Non-Disclosure Agreement (NDA) in place.
- The BRIPL employee coordinating with the respective third-party contractors and vendors are responsible for justifying and authorizing the access rights granted to third-party vendors.
- The access to specific functionalities in information systems and level of access required at the granular level of read, modify & update, deletion shall be identified and documented as a part of role-based access control framework. These requirements shall be translated into system profiles for the different classes of business users.
- The use of group or shared IDs shall be restricted unless required by technology limitations or business needs. Furthermore, mechanisms shall be established to record and monitor all shared ID activity to ensure traceability/audit trails of usage to individual users.

Review of Users and Access Rights

- All the users will be reviewed periodically, to validate that the access provisioned to users are relevant and required. This includes ensuring that inactive accounts are disabled, and personnel do not have excessive privileges.
-

Removal or Adjustment of Access Rights

- Offboarding process shall be followed
- Logical access to information systems and assets must be revoked or disabled under following cases but not limited to:
    - To which users no longer require access
    - Termination of employment or agreement/contract
    - User account was found inactive for more than 60 days
- The revocation process should be done within the timeframes, service providers SLAs, and other processes as defined on an asset-by-asset basis.
- Upon receiving formal offboarding request from HR, the user's account should be disabled within **5 working days**. All group memberships, licenses assigned to the user should be removed.

Laptop and Desktop

- The third-party users can use their laptop
- Guest Wifi access will be provided while the users are in BRIPL office
- The laptop must be configured with
    - Antivirus, up to date
    - USB protection
    - Fully Patched
    - Using Licensed products

BRIPL Services

AD account

- User account will be created in BRIPL environment
- It will be done through the onboarding process
- The IDs will be reviewed periodically
- In case any user is separated from BRIPL, it should be informed to Business Manager, who will inturn raise an offboarding request

Access to email

- Mailbox services will be provided to the contract users for their official communications
- Incoming and outgoing emails to external domains will be blocked. Exception for specified domains will be provided based on the approval of Business Manager and IT head

OneDrive

- OneDrive will be provided to the users to store the data
- The users laptop must be configured with the BRIPL OneDrive to backup My Documents and Desktop on the BRIPL OneDrive

D365

- Access to D365 will be provided strictly on need basis
- It will be provided only through Onboarding process, with due approval from Business Manager