This SharePoint site is the property of ENTSO-E. It is for authorised users only. If you are not an authorised user then do not attempt to access this site. **[Click Here]** I have read and understand the ENTSO-E Extranet Acceptable Usage Policy (AUP) and agree to abide by these rules and practices.

ENTSO-E Extranet Acceptable Usage Policy (AUP)

The ENTSO-E Extranet (https://extranet.entsoe.eu) is a valuable and strategic asset designed to facilitate and foster information exchange and collaboration between members of the ENTSO-E Secretariat and the TSO community only. The purpose of this Acceptable Usage Policy (AUP) is to establish rules and practices regarding the use of and interaction of SharePoint resources, and to ensure compliance with applicable legal, regulatory and contractual obligations. ENTSO-E management reserves the right to revise, amend or modify this AUP at any time. Usage of the ENTSO-E SharePoint Extranet is for authorized business purposes only. Before you are granted access to any part of the ENTSO-E Extranet, you must read and agree to follow the rules contained in the Acceptable Usage Policy (AUP). Failure to comply may result in the suspension or termination of some or all of the access and privilege rights granted.

A prerequisite for accessing the ENTSO-E SharePoint Extranet is a valid identity in the ENTSO-E Active Directory. Users must take appropriate precautions to protect their account credentials at all times. The ENTSO-E service desk must be informed immediately if you suspect your password has been compromised. Extranet users must report any suspected or confirmed security incidents, issues or bad practices (via the “Report an Incident” form on the Information Security SharePoint site). Users must not attempt to access information in the ENTSO-E SharePoint Extranet for which they do not have authorization or explicit consent, and must not purposely engage in any activity that may degrade the performance of SharePoint, deprive an authorized user access to a SharePoint resource, or obtain extra resources or privileges beyond those allocated.

ENTSO-E Secretariat users and TSO members must abide by the Confidentiality clause (Article 35) of the ENTSO-E Internal Regulations. Although the ENTSO-E D&I team manage the SharePoint environment and controls, site owners are responsible and accountable for configuring their sites and sub-sites, and for managing and preserving the security and confidentiality of the information contained in these sites appropriately. SharePoint users must not intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene. There is also no guarantee of personal privacy, since the use of electronic communication tools and SharePoint services may be monitored and audited.

All electronic files created, sent, received and stored in the ENTSO-E SharePoint Extranet must be labelled with metadata. “Data Classification” and “Document Type” are mandatory metadata requirements for all files. All users are expected to know and understand the ENTSO-E Data Classification labels (Public, Protect, Confidential and Restricted) and apply the correct label to all files. The Document Type metadata label ensures that the correct archive and retention period can be applied to all files. Details of all ENTSO-E Information Security policies and standards can be found on the Information Security SharePoint site.

Public: Information/Data that can be released to anyone.

Protect: ENTSO-E Information/Data which must not be disclosed outside of the ENTSO-E Secretariat, for example, Personally Identifiable Information (PII), Commercial-In-Confidence information, HR Records etc.

Confidential: Confidential ENTSO-E or TSO Information/Data that can be provided by the Secretariat to external third party requests, subject to authorization (currently Confidential Category 2 and Confidential Category 3).

Restricted: Confidential ENTSO-E or TSO Information/Data that cannot be provided by the Secretariat to external third party requests (currently Confidential Category 1).

Article 35:

ENTSO-E Internal Regulations (28 June 2011). Article 35. – Confidentiality

1. In accordance with the principles set forth in Article 12 of Directive 2003/54/EC (and, as from their entry into force, in the Articles 16 and 21 (9) of Directive 2009/72/EC), national legislation implementing the abovementioned provisions and/or other national or international legislation imposing specific confidentiality and non-disclosure obligations, no Member or Observer (or its (substitute) Representative) of the Association will use any confidential information obtained by it (the "Recipient") through membership or observership of the Association for any purpose save as strictly required by its obligations set forth in Article 9d of Directive 2003/54/EC (and, as from its entry into force, in Article 12 (e) of Directive 2009/72/EC), or disclose any such information to any third party other than the Recipient's directors, employees, professional advisers and representatives who strictly need to know such information for the proper performance of their professional activities and who are correspondingly bound in writing by the same strict obligations of confidentiality.
All Members and Observers of the Association will organise their data handling in such a way as to minimise the risks of misuse or unauthorised access or disclosure of Confidential Information.
Confidential information includes:
1. all information relating to users of the electricity network systems, which is commercial in nature and, if disclosed, is likely to influence market conditions;
2. all information clearly marked as "confidential" provided that the person conveying the information can validly justify in writing on request by the other party the reasons why the information must be treated as confidential; and excludes information which:
1. is the public domain other than by reason of breach of this clause;
2. is already lawfully in the possession of the Recipient prior to its receipt from the disclosing party; or
3. the Recipient is required to disclose under any Law, court order or order of authorities.
Any Member or Observer, who is deemed by the Assembly to be in breach of this Article, may be excluded by the Assembly from exercising its rights as a Member or Observer of the Association as appropriate.

2. In case third persons are invited to participate in a meeting of a body of the Association, the body concerned may decide to require the signing of a confidentiality agreement by the persons concerned.