SharePoint for Extranet

Policy Statement

Including
Standard Operational Procedures
1 Extranet Policy Statement

1.1 Introduction
This document describes the SharePoint policy guidelines and procedures, on which the use of Extranet SharePoint Environment is based on, including the Standard Operating Procedures (SOP’s) that are to be followed when managing and working with the SharePoint Extranet.

The procedures do not give a detailed work instruction on HOW to perform all the activities. These work instructions can be found in the user guide related to the use of SharePoint within ENTSO-E. The ownership of the document lies within SharePoint Business Adviser.

- The Extranet is an environment for collaboration between TSO members and the Secretariat.
- It designed as a working environment for all TSO members.

1.1.1 Audience/users
The intended audience for this document is:

Persons of the SharePoint team to manage this environment.
- All secretariat persons working with the SharePoint Extranet environment
- The Secretariat Communication section to use this document for their communication to TSO members.

1.2 The Extranet Principles
The ENTSO-E Extranet (https://extra.entsoe.eu) is a valuable and strategic asset designed to facilitate and foster information exchange and collaboration between ENTSO-E and its members.

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 requirements of Article 45 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, Open within ENTSO-E, Confidential, Restricted, and Protect) and apply the correct label to all files. “Open within ENTSO-E” is the classification that must apply to documents such as session files, decisions and minutes. It is the label that applies to all files by default.
- The business record metadata label (Document Type) ensures that the correct archive and retention period can be applied to all files. “Indefinite” is the labelling by default.

1.3 Management of Sites on Extranet

- There are different levels of sites defined within Extranet and each of these sites is managed by a site owner, and a back-up site owner.
- The Level 1 site owner is Secretariat Corporate Affairs; Level 2 sites are managed by the secretariat and Level 3 sites are mainly owned by TSO members and by the secretariat.

1.3.1 Management of the Level 1 site

- Modifications to the level 1 site are allowed with their approval.
- All modifications to existing L1 site are directly managed by Corporate Affairs (as is for any other site).
- Any other user who wants to suggest a change on the L1 site should contact Corporate Affairs Section.

1.3.2 Management of the L2, L3 or L4 Sites

1.3.2.1 New sites

- New Level 2 and 3 sites can be proposed by the TSO-members and the secretariat, but new Level 2 or 3 sites can only be added after approval from Corporate Affairs.
- Requesting the creation of a new sub site should only be considered when:
  - A new ENTSO-E body is formed
  - the community that needs to work in a site is separate from the parent body and is not a subset
  - otherwise use alternative means of achieving the objective such as: adding additional libraries calendars, create another page for the work, etc.
- Level 2 and 3 sites are based on a predefined template. Corporate Affairs owns the lay-out templates of the sites.
- The requests for the creation of a new L2, L3 or L4 sites are managed by the SharePoint Change Request procedure (this is a “standard” change), and will only be allowed after approval of Corporate Affairs. The request can be launched on the related CR-page.
- All New Site requests either successful or unsuccessful are archived and retained.
1.3.2.2 Modifications to existing L2, L3 or L4 sites

- Any user who wants to suggest a change on an existing site can contact the site owner. This role is clearly indicated on each site.
- It is the responsibility of the site owner to accept the proposal for change and to realise the change, after acceptance.

1.3.3 Management of Site templates

- ENTSO-E Corporate Affairs manager owns the site templates.
- Modifications to the template are managed by the Change Request procedure (this is a “normal” change), and will only be allowed after approval of Corporate Affairs.
- The steps to follow are documented in the SharePoint Change Request procedure. The request can be launched on the related CR-page.
- Site owners, and their back-up owners, are indicated on each Extranet site.
  - Each site owner has the ability to control which user have access to that sites’ content.
  - The site owner can also change the structure and setup of their site.
- SharePoint security guidelines are owned by the Secretariat Information Security Officer and are published here.

1.4 Access & Security Principle

1.4.1 The principle of least privilege
Give users the lowest permission levels they need to perform their assigned tasks

1.4.2 Work with security groups
There are 3 levels of access-rights:

- **Owners** are responsible for their site/s. They can change the structure of their site, and can add pages, change the site settings and appearance. Owners also have Contributor rights. **Owner access** is assigned by the Extranet Administrator (this is the Service Desk at ENTSO-E).
- **Contributors** can manage documents and other items in the sites. Contributors can upload and edit documents and items, create tasks and calendar events but cannot change the site structure or appearance. **Contributor access** is assigned by the Site Owner.
- **Visitors** can read all information (documents and other items). This is the **default access right**, given at the creation of each Extranet user profile. Visitors have read-only permission for all sites, therefore they can view pages and items, open items and documents, and download documents. They cannot add nor modify any items or documents.

1.4.3 Limit the number of users in the Owners group
Only site owners can change the structure, settings, or appearance of the site. Therefore only users who are trusted for this responsibility and trained should be in the Owners group.
1.4.4 The importance of ownership
When creating a new site, there must always be a user and backup user who will be the Owner and thus responsible for that site and its contents. These are called the site owners and their back-up owners.

1.4.5 Ability to encrypt sensitive documents
File Encryption functionality is provided to allow SharePoint users to encrypt and decrypt Restricted and Confidential documents. Hashing type functionality is provided to allow SharePoint users to ensure the integrity of key documents.

1.5 Operational Reporting
It is possible to produce a report from each of the workspaces (Sites) periodically or ad-hoc, detailing the status of each of the documents within that workspace. This is available at committee level and for each of the user groups, so that working groups can see what documents they need to input to, review etc. at any given time to enable them to drive workload and get the correct people talking.

There is one global Acceptable Usage Policy (AUP) defined covering all SharePoint policies and procedures (user access management, back-up, data retentions/version control,...). This policy is available on the extranet.

All SharePoint Users will be required to agree to this SharePoint Acceptable Use Policy (AUP) before being allowed access to this platform.

2 Specific functionalities

2.1 Manage the access to the Extranet
ENTSO-E manages security of the Extranet environment by limiting the creation of new accounts to pre-defined, approved email domains.

In order to correctly manage the user access, with the objective to protect data and ensure business security, all users need to have a unique user-id and password for receiving access to the extranet. If a member forgets the username and/or password, they have to use the portal on https://contacts.entsoe.eu and retrieve their username and/or password.

The following rules apply:

- Only employees of member-TSO’s and people working at the secretariat have access to the extranet.
- The Secretariat Legal section owns the list of the member-TSO domain names list
  - All TSO’s have a predefined list of e-mail domains which is accepted and approved by Legal
  - For a new TSO domain name to be added – Legal Section will approve this, and communicate the information to D&I for implementation in the system.
- Since only TSO-related domains are allowed, contractors working for TSOs will need to use a TSO e-mail address
- All registered member-TSOs have by default the Visitor access to all sites.
2.2 Granting access to Extranet

To correctly manage the user access, with the objective of protecting data and ensuring business security, all users need to have a unique user-id and password to be able to access the extranet.

There is a clear distinction between internal secretariat users, members and public (external visitors).

- Granting access to SharePoint for TSO members
  - Adding a new TSO-Member
    - Any TSO-employee can ask access through the advisor in charge of the group or the coordinator of the section
    - The request is sent to the SharePoint Adviser, who evaluates the request with the respective coordinator (if the request is not coming from the coordinator) to ensure that the request for TSO-member access is from a validated TSO.
    - After approval, the request is transferred to the ENTSO-E Service Desk for creation.
    - For each new user, the name, organisation and e-mail address is needed to create the user account for Extranet. Before creating the new user, a check is performed on the completion of mandatory login-details and whether the e-mail address belongs to a pre-defined TSO domain name.
    - This means that if the user is a contractor, working for a TSO, a TSO e-mail address needs to be given, by the TSO, to the user.
    - If access is required for non-members (e.g. the Turkish TSO) this request must be approved via a special process. These access rights will always be time-bound accounts with a period agreed when the account is set up (normally 1 year).

- If a new domain has to be added belonging to a TSO; Legal Section has to be informed and to approve this, and communicate to D&I this new information in order to keep a smooth communication on the allowed TSO-domain lists.

- Removing TSO-members
  - In order to manage the TSO-members who left the TSO or are not active anymore, the following procedure should be followed:
    - ENTSO-E secretariat staff SPOC for that person/TSO, should be informed together with relevant coordinator of the section and/or the SharePoint Adviser.

2.3 Granting access to a specific site

All identified SharePoint users have by default a read access right to the Extranet. However, some parts of sites can be secured.

The identified Site Owner and Backup Owner are responsible for granting and revoking all user access to their site.

In a site all contributors and owners have access to all libraries (including restricted).

When a user wants to visit a secure area they receive an access request pop-up, asking the reason for accessing this area.
The user fills in that pop-up window.

Site Owner and Backup Owner will receive this request from the SharePoint system.

Site Owner or Backup Owner may
- grant users access - either Contributor access OR Read-Only access
- reject the request (adding a justification text for the rejection).

SharePoint users will be automatically notified by the SharePoint system of:
- Contributor Access granted
- Read-Only Access granted
- Request rejected (a justification text for the rejection).

The SharePoint system event log will automatically record all user access permissions. Event logs must be archived and retained.

2.4 Meta Data

2.4.1 GENERAL RULE

Each new document is assigned a series of metadata (descriptions/properties) at the time of the creation, and all edits and changes are recorded, which then allows efficient search, retrieval and modifiable display of all documents.

Meta data “Data Classification” and “Document Type” are mandatory metadata requirements for all files. All contributors are expected to know and understand the ENTSO-E Data Classification labels (Public, Open within ENTSO-E, Confidential and Restricted and Protect), and apply the correct label to all files. The “Open within ENTSO-E” label is the label that must be used for all session files, decisions and minutes and is the applicable label by default for all files.

The Records Management metadata label ensures that the correct archive and retention period is applied to all files. This will be set on “Indefinite” for all files.

2.4.2 Metadata Types

There are 5 types of metadata, you must assign to each document you upload.

- **Work Area** :
  - Is based on the name of the site, where you upload the document

- **Document Classification** defines the security level of the document
  - There are 5 levels of classifications, based on the data classification levels defined in the ENTSO-E security policy
    - **Public**: Information/Data that is freely available on the Internet (e.g. European legislation, reports published by the European Commission, etc.), or that has been communicated by ENTSO-E to other entities in a way which does not restrict them from publishing it.
- **Open within ENTSO-E**: ENTSO-E or TSO Information/Data, which is available to all extranet Users but can generally not be disclosed to third parties. This and the following categories’ definitions will be adjusted once the ENTSO-E Secretariat Procedure for Handling External Requests for Confidential Data has been updated according to the new ENTSO-E Articles of Associations and Internal Regulations with respect to data transparency and confidentiality.

- **Confidential**: Confidential ENTSO-E or TSO Information/Data that can be provided only by the Secretariat to external third party requests, subject to authorization (as foreseen currently under Confidential Category 2 and Confidential Category 3 of the ENTSO-E Secretariat Procedure for Handling External Requests for Confidential Data).

- **Restricted**: Confidential ENTSO-E or TSO Information/Data that cannot be provided to external third party requests, (as foreseen currently under Confidential Category 1 of the ENTSO-E Secretariat Procedure for Handling External Requests for Confidential Data).

- **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.

  - All documents are “Open within ENTSO-E” by default
  - A higher security level can be assigned, if the document cannot be read by everybody, who has access to the site.

- **Business record** defined how long a document (as a record) should be safeguarded
  - By default the Business record is “Indefinite”
  - At a later phase, (in the near future) other business record types will be defined.

- **Document type**
  - There are a number of pre-defined document types
  - You can choose anything (relevant) from the drop list
  - When you do not find the document type you would like to add, you need to launch a Change Request to the Application Lead, who will accept your request and create the new document type or advise you to use another existing document type.

- **Approval level**
  - Assembly and Board will only approve documents that are on the Board & Assembly site
  - For the other sites, the functions can be chosen from the list

There is another kind of metadata, named DOCUMENT TAGS, which is optional and is free text that help the search engine among others.

- This are functionalities that might help you when searching to find a document in the future
- You might add the date of an event as tag, so that it can be easily found while searching by date.
2.4.3 Metadata Addition.

Currently the ownership of the Metadata resides with the S-G, and his executive assistant, for maintaining all Metadata definitions and lists. When someone needs to add a different metadata the SharePoint adviser together with the SharePoint administrator can add new Metadata definitions or add values to existing metadata.

The values of metadata can NEVER be changed, nor can a metadata be deleted!

SharePoint users may request new Metadata definitions, or additions of values to existing metadata.

- Requestor completes The CR form in the appropriate SharePoint site, which launches an automatic sending of the request to the Application lead.
- The application lead makes a first assessment and notifies the SharePoint adviser and the executive assistant of the S-G.
  - If the proposal is considered valid
    - the SharePoint administrator creates new definition OR adds the value to the existing Metadata
    - the SharePoint adviser will inform the requestor about the creation and informs all site owners & contributors about the new metadata or the new metadata value.
  - If the proposal is rejected, the requestor is informed by email of the rejection (a justification text for the rejection).
- All Metadata addition requests either successful or unsuccessful are archived and retained.

2.5 Naming conventions

Naming conventions are to be respected for all secretariat related documents, referring to meetings, decisions and session files.

For other documents, the naming conventions should be respected as far as this has an added value, as it provides some more information about the context of the document.

The name of the document should define clearly and briefly what the document is about. There should be no date, no version, no names or any other information that is managed by SharePoint in the properties of the document.

2.5.1 GENERAL RULE

- The name consists of 3 parts:
  - Date (ymmdd)
  - Work Area (abbreviation)
  - Title (free text)

Between the parts “underscore” should be used; i.e: 140919_BD_text text text text
2.5.2 MORE SPECIFIC

- **Exception**: for meetings, the name only consists of 2 parts: the date & work area (no title required)
  - the date is the date of the related meeting
  - the value you fill in the metadata field “Meeting” is the same as the date in the name document!

- For Minutes, Decisions, Session Files related to AS, BD, SOC, SDC, MC, RDC, LRG:
  o yymmdd_area_name of the document (i.e. 140821_BD_Decisions) / name of the document = title
  o if the meeting is for two days, date is set up as follows: 140821-22_BD_Decisions
  o if the document is FINAL is recommended to use: (i.e. 140821_BD_Decisions_vFINAL)

- For documents related to the meetings or any other documents with special title of the document:
  o yymmdd_area_name of the document (i.e. 140821_BD_Cover note on Network Codes summary)
  o the date is the date of creation of the file, when the document is final, a new document is created (uploaded) with the date of finalisation
  o Please don’t use the numbering of the meetings => it is no more 1st, 2nd, 15th meeting, but please say 140901_Staff Meeting

- For letters:
  o yymmdd_LT_from to_title of the letter the date is the date of letter coming to ENTSO-E or being sent or for incoming the date of the arrival (i.e. 140821_LT_ENTSO-E to ACER_HVDC network code)