Logo and name for employer/assignor			

Confidentiality declaration for sensitive power system information

Personal data and identification		
National ID number	Surnavn (Capital letters)	First name (Capital letters)
Type of ID document	Controlled, place and date	Controlled by (first- and surname)
For external personell		
Enterprise/Institution/Company	Assignment	

Declaration

I understand that

- my assignment/duties involve access and/or exposure to sensitive power system information
- handling and storage of sensitive power system information is accompanied by a duty of confidentiality
- adherence to confidentiality principles requires a sense of responsibility and loyalty

I have read and know the provisions of

- The Norwegian Energy Act Section 9-3 (see attachment)
- The Power Contingency Regulation Section 6-2, 6-3 and 6-4 (see attachment)
- [Information Security Agreement [*document references*]]
- Security directive for [*document references*]

I commit myself to

- comply with said regulations and agreements for the handling, storage and protection of confidential information and documents
- handle all confidential documents carefully and prevent them from falling into the hands of unauthorized persons
- not publish or disclose confidential information to unauthorized persons
- not utilize confidential information for unjustified gain to myself or others

I am aware that

- breach of confidentiality may have consequences for the employment or contractual relationship
- breach of confidentiality may result in criminal liability
- the duty of confidentiality also applies after the employment or contractual relationship has ended

Place and date	Signature
I confirm that this declaration has been rightfully signed, and I have controlled the ID document.	Witness/ID document control signature

Excerpts from the most relevant provisions of law and regulations

The Norwegian Energy Act *(unofficial translation)*
Section 9-3 (Information Security)

All entities in PSPO *[The Norwegian Power Supply Preparedness Organization]* must assess the security of all processing of information on the power supply. The entities must identify which information is sensitive, where it is located and who has access to it. Effective shielding and protection of sensitive information must be established.

Everyone is obliged to prevent other than legitimate users from accessing or knowing sensitive information about the power supply.

The Ministry may issue further regulations on information security in the power supply and on the duty of confidentiality.

The Power System Contingency Regulations *(unofficial translation)*
Section 6-2. Sensitive power system information

Sensitive power system information is subject to confidentiality according to section 9-3 in the Norwegian Energy Act.

Sensitive power system information refers to specific and detailed information on power supply that can be used to harm power plants, systems or facilities, or in other ways affect functions important to power supply, including:

a. Any system that ensures important power system operational control, including necessary ancillary equipment like electronic communications.
b. Detailed information on the power system, including single-line diagrams, with the exception of single-line diagrams for less important power plants.
c. Detailed information on classified transformer substations and associated switchgear, including configuration and operation.
d. Overview of power distribution networks for socially critical functions. Overview of district heating networks for socially critical functions.
e. Accurate mapping of underground power cables. Accurate mapping of district heating networks with class 2 heating plants.
f. Preventive security measures against deliberate vandalism.
g. Localisation of reserve operation centers and other special contingency facilities for management and operation.
h. Detailed analyses of vulnerabilities that may be exploited for deliberate vandalism.
i. Contingency plans to handle deliberate vandalism.
j. General overview of spare parts, backup solutions or contingency repair capabilities significant to handle deliberate vandalism.

Section 6-3. Protection, Shielding and Access Control

Organizations that possess or process sensitive power system information must establish, maintain and develop systems and procedures for efficient shielding, protection and access control of sensitive power system information. Protection must include measures against surveillance and manipulation by unauthorised persons.

System and procedures must include labelling, storage, use and distribution, destruction and measures for internal and external reporting of events that may jeopardize information security.

Special rules and safeguards must be established for use of mobile devices that can receive, send and read sensitive power system information.

Section 6-4. Security Directive

Organizations that possess or process sensitive power system information must establish and put into practice a security directive to ensure that requirements for information security are fulfilled. The security directive must describe which systems, routines and measures are established to comply with the requirements of information security, including requirements for protection, shielding and access control.

The security directive must include information to employees and other legitimate users regarding the duty of confidentiality, according to the Energy Act, section 9-3, second paragraph, and set requirements for signature of a confidentiality declaration. The security directive shall also include information that the confidentiality of the sensitive power system information is not to be disclosed.

Guidance for using and completing the confidentiality declaration

Sensitive power system information is subject to confidentiality. A confidentiality declaration is personal and must be filled out correctly, signed and kept by the employer and/or assignor. A valid confidentiality declaration must be present before accessing systems or documents containing sensitive power system information, or in other ways acquiring knowledge of sensitive power system information, e.g. by surveys or briefings.

The template is primarily designed for entities that **own** sensitive power system information, but can also be used by entities that **produce** or **process** such information. The template can be adapted to local or temporary needs, including other confidential information categories.

When a valid confidentiality declaration already exists, a new declaration completion is not necessary. For external personnel (e.g. installers, project managers or consultants) belonging to companies or institutions with significant ties to the power supply sector, it would be appropriate to sign a confidentiality declaration under the auspices of the employer. In such cases, the client or assignor should require a copy of the confidentiality declaration. For persons who process sensitive power system information only sporadically, a case-by-case declaration may be preferred.

Logo and name of employer/assignor: Enter name of employer. Enter the name of the assignor/client when the company uses external personnel (who have not already submitted a valid confidentiality declaration under the auspices of their own employer).

National ID number: Enter the national identification number for unambiguous identification of the person.

Surname (Block letters): Enter the last name as specified in the ID document.

First name (Block letters): Enter first name as specified in ID document.

Type of ID document: Specify if valid document for identification is passport, driver's license with photo, or bank card with photo.

Controlled, place and date: Enter the place and date for ID document verification.

Controlled by (first and last name): Enter the name of the responsible person who checks the ID document.

For external personnel: Fill out the following two fields when appropriate (i.e. valid confidentiality declaration not present):

> **Enterprise/institution/company:** Enter the name of your home enterprise/institution/company.
>
> **Assignment:** Provide a description or reference to the specific need for confidentiality.

Declaration: Enter and correct the list of provisions. When applicable, provide references to the information security agreement and security directive.

Place and Date: Enter the place and date of signing the confidentiality declaration.

Signature: Sign the confidentiality declaration.

Witness/ID document control signature: Provide a witness and ID control signature (same person as the **Controlled by (first and last name)** field.