AGREEMENT ON MANAGEMENT AND PROTECTION OF SENSITIVE POWER SYSTEM INFORMATION

In accordance with regulations on preventative security and emergency preparedness in the energy supply

between

[Business name]

VAT registration number and tax ID no.: 000 000 000

Information Owner

and

[Business name]

VAT registration number and tax ID no.: 000 000 000

Information Processor

Date: 20xx-xx-xx

1. Introduction

This agreement modulates rights and obligations between Information Owner and Information Processor (hereafter referred to as 'parties') according to:

- The Act on production, conversion, transmission, trading, distribution and use of energy of 29 June 1990 no. 50 (The Norwegian Energy Act) § 9-3
- The Regulation on security and preparedness in the energy supply of 7 July 2012 no. 1157, latest version from 1 January 2019, chapter 6

2. Definitions

Sensitive Power System Information refers to specific information received regarding electrical installations, functions, systems, etc. that may be used with the intent to harm or interrupt the supply of energy, in the event of information loss or disclosure to unauthorized persons.

Formatert: Skrift: Fet

Processing of Sensitive Power System Information comprises presentation, collection, registration, compilation, processing, use, storage, administration, exchange, sharing, disposal, **management and protection**. Certain of the aforementioned tasks overlap.

Information Owner – an operator within energy supply that lawfully controls Sensitive Power System Information through strict routines and directives for management, protection and processing.

Information Processor – an operator that within the scope of this agreement manages Sensitive Power System Information on behalf of the Information Owner as part of providing services or goods, or due to legitimate needs.

3. Purpose

The agreement aims to ensure that the Information Processor complies with the demands for confidentiality and security when managing and protecting sensitive information.

4. Framework and scope

This agreement comprises all management and protection of sensitive information that the Information Processor carries out in relation to [*name of service/assignment/need*]

The services/requirement comprise(s)/consists of:

- [service #1]

Sensitive Power System Information comprises:

- [list]

Any sensitive information shared with the Information Processor in accordance with this agreement is at the Information Owner's disposal at all times. The Information Owner is entitled to control how sensitive information available to the Information Processor is administered and processed.

Sensitive information must only be used for the purposes described or derived from this agreement, or any future written agreements between the parties. All other intentions or

types of communication may only take place in accordance with the Information Owner's written consent.

5. The Information Owner's rights and obligations

The Information Owner shall

- comply with obligations stated in the Norwegian Energy Act, the regulations on preventative safety and emergency preparedness in the energy supply and other legal decisions thereunder
- inform Information Processor of any amendments to requirements and regulations in writing
- hand over or share any sensitive information specified in this agreement when the job/assignment commences
- in the event of handover to / sharing with a third party, provide written confirmation or a refusal with an explanation in line with legitimate needs
- be given the opportunity to audit the Information Processor, providing any necessary documentation proving compliance with this agreement

6. The Information Processor's rights and obligations

The Information Processor shall

- manage sensitive information within the framework of this agreement, always ensuring that the Information Owner is protected from violating any current rules and regulations through any actions or oversights
- carry out necessary technical and organisational measures, ensuring that sensitive information is always handled according to information security requirements
- establish or update internal security measures for management and protection of sensitive information to avoid loss of or dissemination of sensitive information, publication, unauthorised access or any use in conflict with the Information Owner's intentions
- establish a system and routines for managing sensitive information in accordance with internal safety instructions and the demands for information security laid down in this agreement
- establish or update an internal control system for handling security breaches or other nonconformities associated with processing of sensitive information
- maintain the appropriate confidentiality by ensuring that staff with access to sensitive information sign a non-disclosure agreement, as well as be familiarised with the internal safety instructions and this agreement's demands towards information security
- store, administer and process any sensitive information on the businesses own equipment, and prevent that sensitive information is stored and processed on privately owned storage media and equipment
- be wary of storing sensitive information on mobile devices (mobile phone, camera, tablets and PCs), encrypt data if possible and delete after use
- ensure that electronic documents are stored on a server with access control, or encrypted and password protected, as well as implement logging if at all possible

- ensure that external connection to a network or other solutions for storing sensitive information is made using secure VPN access
- encrypt sensitive information when sharing or sending, as well as use acknowledged encryption algorithms with sufficient cryptographic keys and password strengths
- ensure that all physical or electronic documents containing sensitive information are labelled, as far as possible, with a clearly visible identification, such as part of the file or object name, or both
- ensure that all physical documents with sensitive information are locked away in a cabinet or room when not in use
- apply screen lock when not at workstation
- obtain written confirmation from Information Owner before any sensitive information is passed on or shared, as well as ensure that any third parties adhere to the same obligations as the Information Processor is committed to according to this agreement
- ensure that all sensitive information, including backup, is permanently deleted through acknowledged routines at the end of an assignment or termination of this agreement
- warn Information Owner of any possible or evident security breaches, nonconformity, or other events or situations that may threat information security
- inform Information Owner of renaming, Management changes, change of address, restructuring and acquisitions, debt settlement negotiations and bankruptcy, or any other changes that might affect the fulfilment of this agreement
- facilitate efficient audits and document handover when Information Owner requests to check the Information Processor ‘s compliance to this agreement

7. Confidentiality

The Information Processor must make all staff and third parties handling sensitive information within this agreement aware of the contents of the non-disclosure agreement. Sensitive information must not on any account be made public. The non-disclosure agreement applies even after termination if this agreement, cf. The Norwegian Energy Act § 9-3.

8. Audit and inspection

The Information Owner may at any time undertake audits and inspections of systems, routines and documentation used for the administration and processing of sensitive information covered by this agreement. The Information Processor must rectify any deviations without undue delay.

Upon request, the Information Processor must also produce background material associated with any exception handling as a result of other Information Owner’s audits.

Audits and inspections must be notified well in advance so that the Information Processor is able to make time for the activity in his/her work plan.

9. Duration, notice and termination

This agreement comes into force on the date on which both parties sign. It applies until terminated, or other connected agreements that have been entered into between the parties are discontinued, as mentioned in item 3. Both parties can at any time terminate the agreement with 30 day's written notice.

In the event of the agreement being terminated or discontinued, all parties must agree on how to delete and/or return electronic and physical documents and the Information Processor provide a final written confirmation on what is agreed.

If there is a breach of contract, the Information Owner may demand changes to the Information Processor's routines, or immediately impose that the Information Processor stops any future processing of sensitive information.

Amendments and/or appendices to this agreement must be in writing and signed by both parties.

10. Information

Information, notifications or other communication between Information Owner and Information Processor must be in writing or confirmed in writing to:

Information Owner	Information Processor
[Business name] [Address]	**[Business name]** [Address]
Name: Role: E-mail: Mobile no.:	Name: Role: E-mail: Mobile no.:

11. Signing process

This agreement has been signed in two original copies, where each party receives a copy.

City/town and date:

[*City/town*], 20xx-xx-xx

Information Owner	Information Processor
Name:	Name: