**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

*The client*

and

**[Business name]**

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

*The supplier*

Date: 20xx-xx-xx

1. Introduction

This agreement modulates rights and obligations regarding sensitive power system information between the client and the supplier (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
1. Definitions

**Sensitive power system information** refers to specific information 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.

**Processing** of sensitive power system information comprises presentation, collection, registration, compilation, processing, use, storage, administration, exchange, sharing, disposal, **management and protection**. Certain of the listed activities overlap.

**The client** isa company within energy supply that lawfully controls sensitive power system information through strict routines and directives for management, protection and processing.

**The supplier** is a company or an entity which, within the scope of this agreement, manages sensitive power system information on behalf of the client as part of providing services or goods, or due to otherwise legitimate needs.

1. Definitions

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

The service(s) comprise(s)/consist(s) of:

* [service #1]

Sensitive power system information comprises:

* [list]

The client has at all times full disposal of the sensitive power system information that has been handed over or communicated to the supplier in accordance with this agreement.

The supplier retains copyright and property rights to its own manufactured information, but is obliged to protect sensitive power system information and documentation in accordance with this agreement.

The supplier may store sensitive information beyond the assignment when there are justifiable reasons, e.g. in connection to declarations of conformity or repeated assignments. This agreement is not intended to conflict with such obligations or needs.

The client has the right to control the management and processing of sensitive power system information at the supplier.

Sensitive information must only be used in accordance with 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 client’s written consent.

1. The client’s rights and obligations

The client must

* 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 or sharing with a third party, provide written confirmation or a refusal with an explanation
* be given the opportunity to audit the supplier and request documentation proving compliance with this agreement
1. The supplier’s rights and obligations

The supplier must

* manage sensitive information within the framework of this agreement, always ensuring that the client 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 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
* store, administer and process any sensitive information on the business’ 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 files after use
* ensure that electronic documents are stored on a server with access control, or encrypted and password protected, and implement logging wherever applicable
* 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, and 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 leaving workstations
* obtain written confirmation from the client before any sensitive information is passed on or shared, as well as ensure that any third parties adhere to the same obligations as the supplier is committed to, according to this agreement
* ensure that all sensitive information, including backup, is permanently deleted through acknowledged routines upon termination of this agreement, when the client makes a legitimate claim for deletion, or the justifiable basis for continued retention lapses
* warn the client of any possible or evident security breaches, nonconformity, or other events or situations that may threat information security
* inform the client 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 the client requests to check the supplier’s compliance to this agreement
1. Confidentiality

The supplier 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 of this agreement, cf. The Norwegian Energy Act § 9-3.

1. Audit and inspection

The client 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 supplier must rectify any deviations without undue delay.

Upon request, the supplier must also provide background material associated with any exception handling as a result of other clients audits.

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

1. Duration, notice and termination

This agreement comes into force on the date on which both parties sign. It applies until terminated, or the associated agreements between the parties, as mentioned in section 4, terminate. 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 supplier provide a final written confirmation on what is agreed.

If there is a breach of contract, the client may demand changes to the supplier’s routines, or immediately impose that the supplier stops any future processing of sensitive information.

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

1. Information

Information, notifications or other communication between client and supplier must be in writing or confirmed in writing to:

|  |  |
| --- | --- |
| The client | The supplier |
| **[Business name]**[Address] | **[Business name]**[Address] |
| Name:Role:E-mail:Mobile no.:  | Name:Role:E-mail:Mobile no.: |

1. 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

|  |  |
| --- | --- |
| The client | The supplier |
|  |  |
| Name: | Name: |