# Terms Of Use
# for remote access to the IT network of MAN EnergySolutions SE, or any of its subsidiaries ('MAN-ES'), and the computer systems linked to the network

The service provider intends to use remote access to obtain access to IT systems within the MAN-ES internal network for the purposes of fulfilling its contractual obligations from its agreement with MAN-ES ('Main Contract'). MAN-ES shall grant remote access to their IT network in accordance with the following provisions. The service provider hereby agrees and commits to comply with these regulations.

1. Access to the MAN-ES IT network must only be used for the purposes of fulfilling the Main Contract. Access to the MAN-ES network and the software that may be required for this must only be activated when needed.

2. MAN-ES is logging any remote access, including the time, name of the person accessing the network and the target systems.

3. The computer from which the MAN-ES network is accessed must have up-to-date protection against malicious software and must be configured in such a way that MAN-ES is protected against any unauthorized access, e.g. by disconnecting the network cable or using a suitable configured firewall.

4. The permission to remotely access the MAN-ES IT network is specific to each person and is non-transferable.

    a. MAN-ES must be informed immediately of any changes, particularly if the service provider's participating employee changes. MAN-ES must be informed immediately if the access is no longer required.

    b. In exceptional cases, it is possible to deviate from the above regulations under section 4 for maintenance agreements in the production environment if it is not possible, at reasonable cost or effort, to register and maintain a separate userID for each individual affected employee of the service provider.

In this exceptional case, the following provisions shall apply:

i. For the abovementioned Main Contract, only one single personalized user ID is created in the MAN-ES Active Directory (AD), and this may be used by several of the service provider's employees for remote access.

ii. The service provider shall name an internal employee from their company (hereinafter referred to as the 'Responsible Employee'), in whose name the user ID and remote access is registered; this is usually the head of support or a person in a similar position.

iii. The Responsible Employee is the only contact partner for technical operation and the Service Desk of MAN-ES. For example, this is the only person who can report incidents to the MAN-ES Service Desk – the Service Desk will not accept reports from other persons.

iv. The Responsible Employee must ensure that the remote access is properly used and in line with this regulations. In particular, they

1. must ensure that the user ID is only known to the relevant group of persons.

2. must personally ensure that, once an employee who knows the access information leaves the company, the password is changed in order to prevent unauthorized access.

v. Before each use of the remote access, the name of the person who will use this access must be provided to MAN-ES in writing, e.g. via e-mail.

vi. Immediately after any remote access, the responsible operator of the system must be informed in writing (e.g. by e-mail) about the activities that were carried out so that the system can be set to normal operation again in a controlled fashion.

5. The right of use for the remote access shall apply only for remote access using the channels that have already been established. It does not, under any circumstances, represent permission to operate an external company's computer within the MAN-ES internal network.

6. The current valid version of the MAN-ES Information Security Guidelines for Suppliers must be applied and complied with by the service provider.

7. The Service Provider shall be liable for damages resulting from improper use of the remote access in accordance with the statutory provisions unless the Main Contract provides otherwise.

8. The service provider shall keep strictly confidential the business relationship with MAN-ES along with all information that is exchanged as part of this business relationship and, in particular, information that is exchanged via remote access. The confidentiality

obligation shall continue to apply for a period of nine (9) years after the relevant assignment has ended or has been completed. If a confidentiality agreement has been concluded as part of the Main Contract, this shall also apply for the use of the remote access and, therefore, for any information obtained using this method, and shall replace the rules in this section for the duration of its applicability.

9. The right of use for the remote access shall end automatically once the Main Contract ends. The right ofuse for the remote access can be withdrawn by MAN-ES with immediate effect if these provisions are violated or if an infringement is suspected.

10. In cases where there is a reasonable suspicion of infringement, MAN-ES reserves the right to carry out a security audit of the service provider, which shall include consulting the relevant documents and IT systems.

11. MAN-ES does not guarantee the continuous availability of the remote access. For technical maintenance reasons in particular, the access may be interrupted.

12. Should individual provisions be or become invalid or unenforceable, this shall not affect the effectiveness of the remaining provisions. The invalid or unenforceable provision must be replaced by a provision whose objective comes as close as possible to the objective of the invalid or unenforceable provision.