

Conditions for Access to CLAAS IT Systems

between

CLAAS Kommanditgesellschaft auf Aktien mbH
Muehlenwinkel 1, 33428 Harsewinkel, Germany
- hereinafter referred to as **CLAAS** -

and

Supplier
- hereinafter referred to as **Contract Partner** -

CLAAS will possibly enable the Contract Partner to use IT systems. CLAAS will decide to grant access in its free discretion. In this context CLAAS will grant the necessary access rights to certain employees of the Contract Partner in accordance with the following provisions.

1. Entrance and Access

- 1.1. The possibility of access is given from own or CLAAS' owned computer to CLAAS IT Systems as well as the CLAAS network. CLAAS makes the relevant accounts available to the Contract Partner itself or for the purpose of passing them on to its staff members authorized by CLAAS. For the purpose of authentication, the Contract Partner receives a personal user name and an individual password for each authorised employee (hereinafter referred to as Access Data). For various security-critical accesses, a further third factor is additionally required in the authentication process via multi-factor authentication (hereinafter referred to as MFA). The use of MFA requires separate registration by the user prior to first use.
- 1.2. The Access Data is confidential information of CLAAS and therefore must be treated confidentially. Any passing on to third parties is prohibited.
The Contract Partner will only pass on the Access Data provided by CLAAS to the employees to whom the Access Data are assigned. The Contract Partner will give CLAAS in writing first names and last names of its employees who must have access to the CLAAS systems due to their participation in the cooperation with CLAAS for the purpose of setting up the accounts. CLAAS points out that any access to CLAAS systems is logged.
- 1.3. When providing Access Data, the Contract Partner is obliged to expressly inform its employees about the careful handling of the Access Data and their safe custody, the prohibition on disclosure and/or use of the Access Data by third parties, as well as the handling of confidential information (in particular according to a confidentiality agreement (NDA) with CLAAS¹) and to oblige the employees accordingly.

¹ An existing non-disclosure agreement is the contractual prerequisite for the agreement on access to IT systems

The Contract Partner must oblige its employees to report the loss of Access Data to it without delay. The Contract Partner is then obliged to notify CLAAS immediately of the loss.

(for information: +49 5247 12 2000 or e-mail: it-support@claas.com).

- 1.4. In the event of a breach of one of the obligations in sections 1.2 and 1.3, CLAAS shall be entitled to deactivate all accounts of employees of the Contract Partner.

2. Deactivation of Access ID

CLAAS is entitled to block the Access Data of individual or all employees of the Contract Partner if this is reasonable from the point of view of CLAAS for the security of the CLAAS IT Systems.

In order to allow CLAAS to block access, the Contract Partner will immediately notify CLAAS when its employee no longer needs access. This is particularly the case when the employment relationship between the Contract Partner and one of its employees with Access Data ends, or the employee no longer participates in the cooperation with CLAAS in such a way that access is required.

The authorisation to use is limited to the duration of the cooperation with CLAAS (in particular the duration of the order or project). CLAAS will suspend or delete the accounts upon expiration of the cooperation with CLAAS.

3. Obligations of the Contract Partner

- 3.1 The Contract Partner must ensure that the hardware (personal computers, servers, gateways) used and provided by the Contract Partner has the most up-to-date version of client security software with a regularly updated virus and attack signature database, which provides protection against attacks by viruses, worms, exploit kits and other attack variants, in particular via email, web, USB sticks or other media, by controlling file access and scanning at least the web (http, https, ftp, etc.) and mail traffic (smtp, pop3, etc.).
- 3.2 The Contract Partner provides its employees with the necessary systems (smartphone with current Android or Apple iOS operating system) for secure multi-factor authentication.
- 3.3 When connecting to the CLAAS network, the Contract Partner must ensure that its own network does not allow uncontrolled third-party access to the CLAAS IT Systems. Any initial implementations and any changes to network configuration (hardware/software) affecting the security of connectivity to the CLAAS IT Systems must be agreed with CLAAS in advance.

4. Obligation of Data Secrecy

Should the Contract Partner come into contact with personal data within the CLAAS IT Systems within the scope of his duties, a corresponding data processing agreement must be concluded.

In any case, the employees of the Contract Partner are prohibited from collecting, processing, disclosing, making accessible to it or others personal data for a purpose other than the purpose of fulfilling the respective tasks.

5. Liability of Contract Partner

The Contract Partner shall be liable for any damage CLAAS suffered caused or attributable to Contract Partner as a result of the unauthorised disclosure or use of Access Data provided to the Contract Partner, the loss of such Access Data or the non-immediate notification of the removal of the necessity for the use of the CLAAS IT Systems or network access.

6. Term of Agreement

This Agreement shall enter into force upon signature. It may be terminated at any time with a notice period of 14 days to the end of a month by notice to the other party. The right to terminate for cause remains unaffected. The termination must be made in writing (e.g. e-mail). Upon termination of the Agreement, the right to of access ceases.

7. Data Storage

Contract Partner informs its employees that their personal data can be collected, stored, transmitted, blocked and deleted, as far as this is necessary within the scope of cooperation with CLAAS and its affiliated companies within the meaning of the term. § 15 AktG.