

Agreement on access to the company network of Franz Kessler GmbH

between

Franz Kessler GmbH
Franz-Kessler-Straße 2
88422 Bad Buchau

hereinafter referred to as "client"

and

all external partners of the Kessler Group,
with technical access to the company network
hereinafter referred to as 'Contractors'

1. Purpose and scope

- 1.1 The contractor is obliged to perform specific services for KESSLER as outlined in the assignment issued by KESSLER. To perform these services for KESSLER, it is agreed that the contractor shall be granted access to the company network of KESSLER.

- 1.2 This agreement governs, among other things, granting of access by KESSLER to the KESSLER network and the obligations of the contractor as a user. It specifies that the contractor may use the granted access solely for its own use and access data and information in the KESSLER network exclusively for fulfilling the assignment within the agreed contractual scope. It includes minimising potential misuse by the personnel of the contractor, as well as addressing technical and IT security risks such as vulnerability to viruses, worms and hackers.
- 1.3 This agreement covers all connections of any IT components and devices (including PCs, tablets, smartphones, notebooks or other "systems") used by the contractor, its personnel or third parties acting on behalf of the contractor to access the KESSLER network and its applications, as well as the management of information and data within the KESSLER network.
- 1.4 Since the network connections to and within the KESSLER network are provided exclusively to support the internal functions and processes at KESSLER, and not for independent business purposes or unrestricted use outside of the KESSLER domain, KESSLER cannot be considered as a "service provider" to the contractor.

2. Granting access, access authorisation, rules and obligations

- 2.1 Access to the KESSLER network is granted for supporting process activities and developing and designing production machines or their components and is subject to these terms and conditions. Network access is activated technically only when all the contractual requirements have been fulfilled and is reviewed internally every three months.
- 2.2 Access authorisations are restricted in scope and duration and are intended solely for providing the commissioned services as outlined in the agreement. Access authorisations are valid until the end of the contractor's assignment, at the latest. KESSLER reserves the right to periodically review the eligibility of network access. The contractor will respond to such requests without delay. KESSLER may block access whenever there are any uncertainties regarding the necessity of access or the continuation of the assignment. Access may also be blocked temporarily during periods of inactivity.
- 2.3 It is strictly forbidden to access the KESSLER network and the data, information and functions accessible via it beyond what is required for provision of the agreed service, even if this is technically feasible. In particular, the contractor is prohibited from gathering or analysing information (such as evaluating the Intranet or scanning the network), engaging in advertising and other acquisition activities or using KESSLER's systems and networks for its own purposes. Any information that is obtained inadvertently must be kept strictly confidential.
- 2.4 The contractor shall ensure that its employees utilise the access granted to the KESSLER network solely for the purpose of the commissioned services and within the parameters set for KESSLER. It is strictly forbidden to utilise access for other or private purposes.
- 2.5 The number of people with access authorisation must be kept to a minimum. They must be registered by name with KESSLER by the contractor and be agreed with KESSLER. Each authorised person shall receive personal access data from KESSLER. The contractor shall inform KESSLER promptly of any changes in this regard, especially if an individual from the contractor's group who is authorised to access the system is no longer working on the KESSLER assignment. In this case, the contractor shall ensure that this individual no longer has access to the KESSLER network as soon as they are no longer working on the KESSLER assignment. The access data of employees who have been transferred or left the company or of subcontractors who no longer work for the contractor

must be delisted immediately with KESSLER. Upon completion of the assignment, access to the KESSLER network is deactivated. The contractor will inform KESSLER of this without delay.

The prerequisite for applying for access to the KESSLER network is always a valid "Agreement on access to the company network of Franz Kessler GmbH" signed by both parties, which can also be effectively concluded as an annex to another agreement.

- 2.6 The contractor undertakes to keep all access data provided confidential and to change access passwords immediately at the start of the first session, insofar as this is technically feasible.
- 2.7 If unauthorised third parties gain knowledge of the access data, the contractor must change the relevant passwords immediately and inform the KESSLER IT Service Desk accordingly on +49 7582 809 4444.
- 2.8 The access data (especially passwords) must be protected securely to prevent unauthorised access by third parties. Under no circumstances should this data be stored unprotected or easily accessible on the contractor's computers, in particular not through the "Save password" option provided by Windows. The access data must be entered manually each time a connection is established or a login is attempted.
- 2.9 It is strictly forbidden to temporarily transfer or disclose access data to third parties, e.g. to subcontractors or freelancers of the contractor.

In any instance where confidential information, such as access data, processed data or information related to the contractual relationship, is shared (even temporarily), the contractual partner agrees to establish an agreement with subcontractors, freelancers or other third parties containing the same provisions before disclosing or utilising the data or information. The necessary documentation must be provided if requested by KESSLER.

- 2.10 The contractor must inform all individuals working on its behalf to fulfil the contractual obligations regarding KESSLER and who receive access to the KESSLER network for this purpose, including both its own employees and those of subcontractors, about this agreement and require them to comply fully with its terms and conditions. In addition to this agreement, everyone must comply fully with all guidelines issued by KESSLER that govern IT operations and IT security.
- 2.11 Alongside the terms and conditions of this agreement, the contractor and its employees, as well as any individuals assigned to carry out the assignment, are required to adhere to the user guidelines provided by KESSLER, insofar as they have been communicated to the contractor and are applicable to their activities within the KESSLER network.
- 2.12 External registrations are only possible via MFA.
- 2.13 The contractor shall strive at all times to maintain its security level to standard ISO 27001 and must provide the client with confirmation of this if requested to do so. It should be explicitly noted, however, that certification to the relevant ISO standard is not mandatory.

3. Technical network access

- 3.1 A Citrix access point is usually used to establish the network connection between the contractor and the KESSLER network. Alternatively, it is possible to set up an online connection via a VPN tunnel

(VPN = virtual private network), if required. In this case, it is crucial to ensure that login is established via multi-factor authentication (MFA).

The personalised access granted by KESSLER is generally permanently operational (24/7), although periods of unavailability due to maintenance measures or malfunctions are conceivable.

A network connection between the contractor and the KESSLER network can also be established using remote maintenance software online, e.g. TeamViewer or comparable products.

- 3.2 The contractor shall procure and install all the access components it requires. In doing so, the contractor must adhere to the current KESSLER standards, as long as these standards have been communicated to the contractor. It is essential for the contractor to observe the KESSLER IT security guidelines (see annex). KESSLER will assist the contractor during installation by offering phone support and error analysis if requested to do so. KESSLER reserves the right to update access technology at reasonable intervals to align with advancements in technology and shifts in communication needs. KESSLER shall inform the contractor of these activities in advance.
- 3.3 Only temporary network connections are generally permitted between the contractor and KESSLER. These connections are set up and taken down by the contractor. Connection periods must be limited to what is strictly necessary. Network connections must be disconnected during work breaks and outside the normal working hours of the contractor. Access to the KESSLER network must not be used to interlink the KESSLER network and the contractor's network.

Only one computer of the contractor may be connected to the KESSLER network at any given time when using a single access point. Connections must terminate on this computer. It is strictly forbidden to forward (route) data traffic. When connected directly to the KESSLER network (e.g. via VPN), no other network connections may be active at the same time. This does not apply to indirect network connections, e.g. via Citrix.

Multiple contractors can access the network simultaneously, each using a different identity.

- 3.4 If a permanent network connection (e.g. site-to-site VPN) is necessary (contrary to point 3.3.), the technical conditions and security precautions (e.g. firewalls or gateways) must be agreed separately between the contractor and the person responsible for the network at KESSLER.
- 3.5 To coordinate and address technical questions and issues, both contracting parties shall designate technically competent contacts.
- 3.6 If KESSLER has outsourced management of the KESSLER network and other IT systems to an external IT service provider, this provider shall be responsible for carrying out any services, coordination and organisational tasks arising from this agreement on behalf of KESSLER. The point of contact for the contractor may also include employees of the external IT service provider whose names and details have been disclosed to the contractor by KESSLER. Matters relating to the actual assignment must be clarified with KESSLER and not be disclosed to KESSLER's external IT service provider.

4. Other boundary conditions

The contractor must ensure that all resources and any access provided by KESSLER are protected against access by third parties. The confidentiality, integrity and availability of KESSLER's systems and data must be maintained at all times.

All information and data that can be accessed by the contractor must be treated as confidential trade secrets and must not be disclosed, shared or made accessible to third parties.

The contractor must implement adequate measures to ensure compliance with IT security when using devices that are not supplied and managed by KESSLER. This includes, as a minimum, maintaining up-to-date antivirus software, promptly installing operating system and application patches, utilising firewalls with regular rule checks and routinely verifying authorisation and network settings, among various other security practices. Additionally, the devices used by the contractor must be secured to prevent unauthorised access and misuse under standard business conditions (i.e. room protection, password protection with periodic changes, boot protection, hard disk protection, etc.). For particularly sensitive areas, KESSLER may require additional protective measures that must be agreed with the contractor.

Services or software that could disrupt IT operations at KESSLER and that have absolutely nothing to do with an assignment or collaboration must not be utilised. This must be ensured, for example, by means of an appropriate firewall setting and hardening of the firewall. KESSLER or a third party appointed by KESSLER has the right to terminate the connection without prior notice if the contractor causes a disruption to IT operations or is responsible for an IT security incident. Saving or further processing information or data provided by KESSLER is only permitted if this has been agreed in writing with KESSLER in advance.

Upon the termination of the business relationship, all data belonging to KESSLER or processed on behalf of KESSLER must be securely deleted from all computers and storage media of the contractor, unless otherwise agreed. The deletion of data must be confirmed to KESSLER in writing upon request.

5. Malfunctions, data backup and security

- 5.1 Malfunctioning systems and networks at KESSLER of which the contractor becomes aware must be reported immediately to the KESSLER Service Desk at hotline@kessler-group.biz or alternatively on +49 7582 809 4444 with a clear description of the problem.
- 5.2 In the event of technical issues that are within KESSLER's area of responsibility, fault elimination shall commence within a reasonable time. In the event of faults that are the responsibility of external network operators, KESSLER will actively support these companies within its capabilities and resources.
- 5.3 If the issue cannot be resolved promptly, the contractor shall utilise the local access options to the KESSLER network on KESSLER's premises to fulfil its contractual obligations to the best of its ability. If it is possible to bridge a disruption by exchanging data via e-mail, KESSLER shall support the contractor within its technical and personnel capabilities and resources. The prerequisite is, however, that confidential or personal data is transmitted in encrypted form.
- 5.4 Either of the contracting parties may disconnect the network connection without prior notice if IT security attacks, such as viruses, worms or other malware, are detected. Furthermore, KESSLER reserves the right to delete and remove infected files (e.g. e-mails, programs or other data files) from KESSLER's systems, even without a data backup or informing the data owner.
- 5.5 To prevent any loss of data, the contractor is responsible for backing up all the data and programs necessary for fulfilling the purpose of the assignment, provided that such actions are technically and

economically feasible and unless the contractor has a written statement from KESSLER indicating that KESSLER will handle the data backup.

- 5.6 KESSLER periodically uses monitoring systems to check that the security of its systems and networks is intact. The contractor is obliged to rectify any security deficiencies in its devices within a reasonable period of time or to disconnect them from the KESSLER network. Only IP addresses provided by KESSLER, (dynamic DHCP addresses and, in some cases, also static addresses) may be utilised for accurate identification. It is strictly forbidden to use self-selected static IP addresses.

6. Logging of connection data, monitoring, obligation to give information

- 6.1 KESSLER logs all the contractor's dial-up connections. If any abnormalities are detected, KESSLER may block the corresponding access to the KESSLER network along with the consequences described under point 7.1.
- 6.2 KESSLER reserves the right to store all connection data and activities related to this connection, to evaluate them either electronically or manually and to question the contractor about such data and activities. The contractor is obliged to answer these questions promptly, truthfully and fully. In doing so, KESSLER will comply with all applicable data protection laws.
- 6.3 KESSLER reserves the right to check the validity of user accounts periodically (e.g. every 30 days) and to block them, if necessary. Measures that are necessary for the contractor to implement this process must be fully supported by the contractor.
- 6.4 KESSLER reserves the right to authorise partners to perform these tasks and to uphold KESSLER's security interests.

7. Suspicion of misuse, misuse

- 7.1 KESSLER may block the contractor's access to the KESSLER network without prior notice if there is a mere suspicion of misuse or other violations of this agreement. Access may be blocked until the situation is clarified, and KESSLER may unilaterally suspend the underlying assignment without being considered in default of any cooperation service or obligation under this agreement or any other assignment.
- 7.2 In the event of misuse or other serious violations of this agreement by the contractor or its employees or by the persons employed to fulfil the assignment, KESSLER may terminate the assignment without prior notice and block access accordingly.

Alternatively, KESSLER may also terminate this agreement. In this case, the contractor is not relieved of its obligation to perform services under the assignment and must continue to fulfil its contractual duties in coordination with KESSLER as part of the assignment. As such, any additional expenses shall be borne by the contractor.

8. Liability

- 8.1 KESSLER shall not be held liable for any damages or claims resulting from operational disruptions caused by external network operators or providers that negatively impact the contractor.
- 8.2 Claims for damages or defaults by the contractor against KESSLER arising from justified access blockages, technical malfunctions, malware-related PC infections or loss of data are excluded.

- 8.3 The contractor shall indemnify KESSLER against any third-party claims resulting from infringements of third-party rights for which the contractor is responsible.
- 8.4 The contractor shall be liable for any damages and claims from KESSLER or third parties that arise from the use or misuse of the access authorisation to the extent that the contractor is responsible for such incidents. Damage resulting from use may occur, e.g., if safety regulations or other stipulations of this agreement are not followed fully.

9. Right to information and obligation to notify

- 9.1 The contractor must provide the client with all information that is relevant to the execution of the commissioned service. This includes notification of significant circumstances that could impact provision of the service.
- 9.2 The client has the right to request information from the contractor about the status of the service. The contractor must provide this information immediately and truthfully.
- 9.3 The contractor shall notify the client immediately of any changes that impact the service, especially those related to scheduling, costs or quality.
- 9.4 The obligation of the contractor to give information applies even without an explicit request from the client, as long as the information is absolutely necessary to fulfil the agreement.

10. Costs

Unless otherwise specified in the actual agreement, no costs related to access to the KESSLER network or the use of KESSLER's IT systems shall be borne by the contractor. Any expenses and costs incurred by the contractor to gain access to the KESSLER network shall be borne by the contractor.

Excluded from this are the equipment, licenses, etc. that are required by the contractor for functional operation of the assignment. Unless otherwise agreed, these expenses shall be incurred by the contractor.

11. Duration and termination

11.1 Duration of the agreement

This agreement is concluded for an indefinite period and shall come into force upon being signed by both contracting parties.

11.2 Termination

11.2.1 Ordinary termination

The contractual relationship is generally terminated at the end of the period for which it was entered into. If the duration of the contractual relationship is neither determined nor can it be inferred from the nature or purpose of the services, either party may terminate the service relationship in accordance with statutory provisions.

The agreement may be terminated ordinarily by either contracting party upon 14 days notice to the end of the month. Ordinary termination is excluded if the validity of the agreement is limited in time.

11.2.2 Extraordinary termination

Either party may terminate the contractual relationship without notice for good cause if, considering all the circumstances and the interests of both contracting parties, it would be unreasonable to expect the terminating party to continue the service relationship.

11.2.3 Termination due to position of trust

In the case of agreements with a special position of trust, the service relationship may be terminated without notice if trust in the fulfilment of the agreement is permanently impaired.

11.2.4 Obligation upon termination

Upon termination, both contracting parties are obliged to fully dismantle any technical measures established or provided for the fulfilment of the agreement. All data, documents and access information must be either handed over to the client or destroyed, with confirmation of such action provided by the contractor.

12. Final provisions

- 12.1 No verbal collateral agreements have been made. The parties specifically agree that any changes and supplements to this agreement will not become effective unless confirmed in writing. This also applies to any changes to this written form clause.
- 12.2 This agreement shall be subject exclusively to the substantive law of the Federal Republic of Germany, excluding its conflict of laws provisions.
- 12.3 If the contractor is a merchant, the sole jurisdiction for all disputes arising from this contractual relationship shall be the court with appropriate local and subject matter jurisdiction over the issue at KESSLER's principal place of business. However, KESSLER also has the right to sue the contractor at the location of its registered office.
- 12.4 If any provision of this agreement is found to be invalid or unenforceable, such invalidity or unenforceability shall not affect the other provisions of this agreement.