Guideline for external service providers for access to TRILUX IT systems

1. Scope of application

The companies of the TRILUX Group (see list of companies at www.trilux.com or made available upon request) contract external IT service providers for the provision of IT services (consulting, application development, and operation), among others also by means of external communications connections ("remote access"). The utilisation of the IT system by external uses required in this case shall be subject to the following regulations as minimum requirements for a provision of service and shall – upon execution/acknowledgement – become a component of the existing contract / business relationship with the service provider.

2. General regulations on data access, IT security

2.1. The service provider shall, at any time, ensure that the service provider's action not negatively affect the confidentiality, integrity or availability of IT systems. Service provider shall exclusively perform those activities required for the fulfilment of the services ordered. Service provider shall perform these exclusively within the framework of the agreements entered into and as directed by client. Modifications of the area of activity and procedural changes must be agreed upon in writing. A processing shall only take place to the extent it has been agreed upon in the underlying service contract.

2.2. Information, data, and programs may only be transmitted from client's infrastructure and/or installed in the context of the fulfilment of agreed upon activities and subject to prior approval by client.

2.3. Access may only take place from systems the security level of which corresponds to the information security requirements at client's.

2.4. Service provider shall warrant that the data processed is kept strictly separate from other data volumes.

2.5. Service provider shall participate in a suitable manner in the development of process descriptions if this is stipulated in the contractual provision of services are requested by client.

2.6. Service provider shall adhere to the principles of proper data processing. Service provider shall ensure compliance with the statutorily required data security measures.

2.7. If the security measures taken by contractor are not sufficient to meet client's requirements, contractor shall notify client of this immediately. The same shall apply to disruptions, violations of the service provider or of persons employed there against provisions of data protection / privacy law, or against the specifications stipulated in the order as well as in case of suspicion of violations of data protection / privacy, or in case of irregularities in the processing of personal data.

2.8. Service provider shall immediately bring to client's attention if an instruction issued by client is, in service provider's opinion, violating statutory provisions.

2.9. Contractor shall communicate to client which employees contractor will be using for the fulfilment of the activities and how these will identify themselves. For this, sufficiently secure identification processes shall be utilised which shall be protected

accordingly. If the identifying characteristics are disclosed, client shall be notified of this immediately.

2.10. Service provider shall ensure that the infrastructure at client's is not negatively impacted by service provider's activities. Negatively impacted shall mean irregular, abnormal behaviour of the infrastructure that leads to failure of individual components or of the whole system and is service provider's fault.

2.11. Subsequent to conclusion of the contractual work, service provider shall hand over any and all documents service provider obtained possession of and processing and usage results created that are related to the contractual relationship. Thereafter service provider's data carrier media shall be physically deleted. Test and scrap material shall be destroyed immediately or handed over of client. The deletion and/or destruction shall be confirmed to client in writing, including specification of the date.

2.12. Service provider has named an employee who is responsible for all IT security aspects of the provision of service.

3. Access, right to audit

3.1. Client will provide service provider only with those access rights necessary for carrying out the agreed upon activities, and will regularly check their topicality and apply corrections, where applicable. Service provider may only utilise the access rights granted to service provider to the extent indispensably necessary for performing the activities.

3.2. Client shall have the right to disrupt contractor's access to client's IT systems.

3.3. Client shall be entitled to inspect or have somebody inspect compliance with the provisions arising from this agreement at the required scope. To do so, service provider shall – subsequent to prior coordination – grant unhindered access to the site, access to the facilities, and access to the information-processing systems, programmes, files and information related to the carrying out of the activities. Contractor shall provide client with any and all information necessary for fulfilling the inspection function.

3.4. Client shall be authorised to log and analyse any and all actions of service provider within its infrastructure.

4. Employees and sub-contractors of service provider

4.1. Service provider may only utilise sub-contractors in the context of the fulfilment of the contractually agreed upon activities subject to prior written approval by client. Service provider shall be responsible for the actions or omissions of its sub-contractors in the same manner as service provider is responsible for actions or omissions of its own.

4.2. Service provider warrants that the contents of this guideline are known to any and all employees and sub-contractors approved in accordance with Article 4.1 who received access to client's information and will enter into the work instruction listed in ANLAGE 1 with each and every employee/sub-contractor receiving access to client's IT systems.

5. Confidentiality

5.1. Service provider shall be required to treat as confidential any and all knowledge of trade secret and data security measures of client obtained in the context of the

contractual relationship, even beyond the end of the contract. Any general or further obligations arising from the contractual relationship, where applicable, shall not be affected by this declaration.

5.2. Upon written request by client, service provider shall mmediately, return to client and/or traceably destroy any and all confidential information and other documents created based on said information that service provider is in possession of.

6. Data Protection

6.1. While maintaining appropriateness, service provider shall ensure all organisational and technical measures for the protection of personal data in accordance with Art. 32 GDPR.

6.2. At client's, the duly appointed Data Protection Officer can be reached at privacy@trilux.com. To the extent that the service provider is legally obligated to do so, the service provider has appointed a Data Protection Officer and shall on request declare the contact data without delay. The parties shall notify each other immediately of any change of the Data Protection Officer.

6.3. Service provider shall inform client immediately and in writing of any incidents relevant to data protection / privacy and any violations of contractual provisions.

6.4. Data transmissions necessary for access purposes shall take place in sufficiently encrypted form; exceptions shall be subject to specific justification.

6.5. The processing and storage of data shall take place exclusively within the territory of the European Union. Any relocation to a third country shall require client's prior approval and may only take place if the special requirements of Art. 44-49 GDPR are fulfilled. If a subcontractor is to be contracted, these requirements shall apply in addition to the provisions of Par. 13 of this agreement.

7. IT-supported communication and exchange of data

7.1. To ease order-related communication and the exchange of data, accesses and shares within the TRILUX domain may be set up.

7.2. The utilisation of the platforms shall be permitted only in connection with the order. Private utilisation is not permitted.

7.3. The passing on of data to third parties or to private storage locations is not permitted. Exceptions shall be subject to express approval.

ANLAGE 1 Work instruction remote maintenance/utilisation of TRILUX IT systems

– Subsequent to prior order placement, service provider's employee shall receive a personal access authorisation to the data processing system if this is necessary in the context of task fulfilment. The access authorisation is not transferable to a third party.

– For task fulfilment, service provider's employee receives an access authorisation to the data processing systems. Said access authorisation consists of a unique personal user identification and a password. Additionally, service provider's employee receives an access authorisation for remote login.

– The following complexity requirements apply to the password and also have to be taken into consideration in case of a password change. The initial password must be change upon the first login and every 90 days thereafter. The password

  – must not contain a logical sequence of characters (e. g. a sequence of characters directly next to each other on the keyboard),

  – must not be easy to guess or derive (e. g. groceries, music, dictionary terms),

  – must utilise upper- and lower-case characters,

  – must have a minimum length of 12 characters,

  – must utilise numerals (0–9),

  – must utilise special characters (e. g. &, §, >, #).

– Client's helpdesk must be notified of this immediately if problems or aberrant technical behaviours occur. The helpdesk assists in the solution and is available for questions regarding the login. The helpdesk can be reached at the following contact data: **+49(0)2932/301-444** / helpdesk@helpdesk.trilux.de

– Access to company resources shall take place only in the context of the contract. The corresponding access rights are assigned by client. Access to information that is not needed is prohibited. If service provider's employee notices that the access authorisation were assigned incorrectly, this shall be communicated to client immediately. The latter shall immediately initiate an adjustment of the access authorisations. It is prohibited to take advantage of incorrect access authorisations.

– If the access verification is not performed in another manner (e. g. Active Directory, Single Sign-On), different passwords shall be used for different applications. Passwords that are used for login at service providers on the Internet must not be used to log on to client's network. Passwords shall be entered unobserved. Publication, passing-on or misuse is expressly prohibited for these identifying characteristics. Password storage functions available in applications must not be used. Similarly, it is prohibited to write down the user ID and password. If it is necessary to store passwords, a password safe can be used.