# Annex 1: Conditions for Supplies of Software/ Hardware and/or OT & E/E Systems incl. documentation

Voith General Purchase Conditions, in their current version, are supplemented by the following terms and conditions, which apply to all supplies of Software/Hardware and/or OT & E/E systems solutions including documentation relating to information technology (IT)/operational technology (OT).

These terms and conditions apply additionally and, in the event of contradictions, shall take precedence over the Voith General Purchase Conditions.

DEFINITIONS

| | |
|---|---|
| Information Technology (IT) | Information technology (IT) involves the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data; |
| Operational Technology (OT) | Operational Technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, machinery, assets, processes and events; |
| E/E Systems | Electrical and Electronic Systems |
| Customer Data | means all information and data (including texts, documents drawings, diagrams, images or sounds) owned by, licensed to (other than by Supplier) or relating to the Customer and/or any of its representatives whether in a human form or machine readable form, which is in each case generated by, supplied to, or is otherwise retained by, Supplier or any of its sub-contractors pursuant to or in connection with this terms and conditions; |
| Security Incident | an event involving the actual or attempted unauthorised access to and/or use of the Systems containing the Customer Data and/or the unauthorised access to, use of, destruction, loss or alteration of the Customer Data in connection with this terms and conditions; such incidents may be categorised as a Critical Security Incident, Major Security Incident or Low Priority Security Incident. |
| Critical Security Incident | a Security Incident that results in a severe disruption to the work delivered; |
| Major Security Incident | a Security Incident that results in a reduction in the performance of the delivered work or may lead to a disclosure of the Customer Data or any data used by the Customer or the Supplier in connection with this terms and conditions in the public domain; |
| Low Priority Security Incident | a Security Incident that has no significant impact on the availability or performance of the delivered work; |
| Information Asset | any Information System/IT System that holds information belonging to an organisation |
| Information System / IT System | an Information System is any combination of information technology, processes, digital information and user activities that support the operations of an organisation; |
| Security Threat | is a possible danger that might exploit a Security Vulnerability to cause a Security Incident that may result in harm; |
| Security Vulnerability | is a weakness of an Information System that can be exploited by one or more Security Threats; |
| Risk Assessment | a Risk Assessment is the process of (a) identifying the risks related to an Information Asset and recognised Security Threats, and (b) evaluating the overall effect of the likelihood that the risks will occur and the impact if they should occur; |
| Security Risk | A Security Risk is the likelihood that something bad will happen that causes harm to an Information Asset; |
| Security Risk Assessment | a determination of quantitative or qualitative value of risk related to a concrete situation and a recognised threat to the security of the Customer Data and/or the systems; |
| Vulnerability Assessment | a Security Risk Assessment that leads to the identification, quantification and prioritisation (or ranking) of the vulnerabilities in a computer system, including the associated networks, databases and software applications; |
| Affiliated Companies | any entity that is to be considered as affiliate of the Customer within the terms of sections 15 et seq AktG (the German Act on Corporations). Further, Customer can define further entities as being Affiliated Companies of Customer in an amendment agreement; |
| Customer Group | shall mean Customer together with its Affiliated Companies; |

## 1 Open-Source-Software

Open Source Software ("OSS") is software, which is generally provided free of charge and open source and can be used under a license, which does not restrict redistribution of the software, allows modifications and derived works and must allow redistribution thereof under the same terms as the license of the original software ("OSS-License"). OSS-Licenses include without limitation "Berkeley Software Distribution License" (BSD), "GNU General Public License" (GPL), and the "GNU Lesser General Public License" (LGPL). Copyleft Licenses are licenses that require that any derivative work or work based on the program is distributed or conveyed only under the original license terms ("Copyleft License").

### 1.1 Requirements

OSS may be included in the software provided by the Supplier. The Supplier will provide to the Customer all information and materials on the use of OSS in the software. This includes:
(i) a transparent and complete list of all components licensed under an OSS-License,
(ii) the license text of each OSS-License,
(iii) copyright notices,
(iv) the results of a state of the art security and vulnerability monitoring of all open source code used, and
(v) A clear description and documentation regarding the used OSS components.

The Customer will grant the approval in its sole discretion. A granted approval is to be revoked, if the provided information or materials are false or incomplete.
OSS-License texts and the respective source code must be provided separately. The Supplier will provide all open source code to the extent that this is required by applicable licenses.
The Supplier will put the Customer in a position to completely comply with all requirements under the applicable OSS-Licenses at all times.
These requirements also apply to any updates, patches, upgrades or new versions of the software.

### 1.2 Responsibility

The Supplier is aware of its special responsibility to protect the Customer from damage caused by the integration of OSS software in the software supplied by the Supplier and the use of such software by the Customer. In view of this, the Supplier shall take special care that all rights of 3rd parties are proven and guaranteed.

### 1.3 Indemnification

The Supplier shall indemnify, defend, and hold harmless the Customer and Customer's affiliates, employees, directors or agents of any claims, damages, expenses and liability which arise in direct or indirect connection of Supplier's breach of one of the foregoing requirements of obligations, irrespective under what legal theory.

## 2 Software Development Lifecycle

For supplies that includes software development, the Supplier shall establish a Secure Software Development process.
(i) adopt a Secure Software Development Lifecycle approach according to well known standards, such as IEC 62443 4-1. A certification is expected.

(ii) provide evidence that identified security requirements and corresponding security controls are designed and implemented into the software.
(iii) ensure that appropriate security tests including but not limited to static and dynamic code checks and continuous vulnerability assessment are applied in the development and integration pipelines and any issues uncovered are remediated before software release; and
(iv) allow Customer and/or its agents to carry out Vulnerability Assessments of the developed software. If any vulnerability with a risk score of "high" or "critical" is found by the Customer, the Supplier shall take action to mitigate the risks before the software release.

### 3 Vulnerability Management

(i) The Supplier will engage an independent and trusted Vulnerability Assessment service and/or cooperate and assist an independent third party appointed by the Customer in the conduct of Vulnerability Assessments.
(ii) The Supplier shall on a monthly basis, review the Supplier's sources of threat and vulnerability information for the latest vulnerabilities, threats and remediation relevant to the systems under the Supplier's management.
(iii) The Supplier shall implement a remediation plan of mitigation activities once a vulnerability is identified or to prevent a vulnerability from arising, and for prioritising, tracking and monitoring the plan's progress. All remediation plans shall be documented for future reference. Vulnerabilities with a significant security impact shall be remedied as soon as practicably possible. For lower and medium risks, the timescale for remediation shall take into account the cost, time and effort required to mitigate the risks.
(iv) The Supplier shall notify the Customer immediately if it fails to remedy any Critical or High rated Vulnerability and shall propose the Customer necessary security controls.
(v) The Supplier shall ensure that all customizable products contain a documentation for secure parametrization.
(vi) Activities as part of the Suppliers Vulnerability Management, like Vulnerability Assessments, regardless of type or target, and all work and time required to carry out remediation activities, will be at the cost of the Supplier and will not be charged to the Customer.

### 4 Security Governance

(i) The Supplier will appoint an individual (the "Supplier Security Manager"), to:

- coordinate and manage all aspects of security in accordance with the Agreement; and
- act as the single point of contact on behalf of the Supplier and its Subcontractors in the event of a Security Incident.

(ii) In the event that the Supplier wishes to change the Supplier Security Manager it will notify the Customer in writing, providing contact details for the replacement individual.

# Annex 2: Conditions for Supplies, Services, Development of Software/Hardware in the Context of IT & OT & E/E Systems incl. Documentation

Voith General Purchase Conditions, in their current version, are supplemented by the following terms and conditions, which apply to all supplies and services relating to information technology (IT)/operational technology (OT) (Part A) and the creation or adaptation of software or the rendering of associated services (Part B).

These terms and conditions apply additionally and, in the event of contradictions, shall take precedence over the Voith General Purchase Conditions.

DEFINITIONS

| | |
|---|---|
| Information Technology (IT) | Information technology (IT) involves the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data; |
| Operational Technology (OT) | Operational Technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, machinery, assets, processes and events; |
| E/E Systems | Electrical and Electronic Systems |
| Customer Data | means all information and data (including texts, documents drawings, diagrams, images or sounds) owned by, licensed to (other than by Supplier) or relating to the Customer and/or any of its representatives whether in a human form or machine readable form, which is in each case generated by, supplied to, or is otherwise retained by, Supplier or any of its sub-contractors pursuant to or in connection with this terms and conditions; |
| Security Incident | an event involving the actual or attempted unauthorised access to and/or use of the Systems containing the Customer Data and/or the unauthorised access to, use of, destruction, loss or alteration of the Customer Data in connection with this terms and conditions; such incidents may be categorised as a Critical Security Incident, Major Security Incident or Low Priority Security Incident. |
| Critical Security Incident | a Security Incident that results in a severe disruption to the work delivered; |
| Major Security Incident | a Security Incident that results in a reduction in the performance of the delivered work or may lead to a disclosure of the Customer Data or any data used by the Customer or the Supplier in connection with this terms and conditions in the public domain; |
| Low Priority Security Incident | a Security Incident that has no significant impact on the availability or performance of the delivered work; |
| Personal Data | shall have the same meaning as set out in the General Data Protection Regulation 2016/679; |
| Information Asset | any Information System/IT System that holds information belonging to an organisation |
| Information System / IT System | an Information System is any combination of information technology, processes, digital information and user activities that support the operations of an organisation; |
| Security Threat | is a possible danger that might exploit a Security Vulnerability to cause a Security Incident that may result in harm; |
| Security Vulnerability | is a weakness of an Information System that can be exploited by one or more Security Threats; |
| Risk Assessment | a Risk Assessment is the process of (a) identifying the risks related to an Information Asset and recognised Security Threats, and (b) evaluating the overall effect of the likelihood that the risks will occur and the impact if they should occur; |
| Security Risk | A Security Risk is the likelihood that something bad will happen that causes harm to an Information Asset; |
| Security Risk Assessment | a determination of quantitative or qualitative value of risk related to a concrete situation and a recognised threat to the security of the Customer Data and/or the systems; |
| Vulnerability Assessment | a Security Risk Assessment that leads to the identification, quantification and prioritisation (or ranking) of the vulnerabilities in a computer system, including the associated networks, databases and software applications; |
| Affiliated Companies | any entity that is to be considered as affiliate of the Customer within the terms of sections 15 et seq AktG (the German Act on Corporations). Further, Customer can define further entities as being Affiliated Companies of Customer in an amendment agreement; |
| Customer Group | shall mean Customer together with its Affiliated Companies; |

## Part A - Conditions for Supplies and Services in the Context of IT/OT & E/E Systems at the Supplier

### 1. Compliance and basic technical requirements

The Supplier shall render the service in compliance with the principles of proper data processing. These include but are not limited to observance of statutory data protection regulations and implementation of all recognized state-of-the-art precautions and measures.

The Supplier shall take appropriate technical and organizational measures to guarantee a high level of IT security with regard to the services and the IT systems required by the Supplier for the purpose of rendering such services. Insofar as they are applicable to the services and the IT Systems used by the Supplier to provide such services, the Supplier shall ensure compliance with the minimum standards of ISO/IEC 27001:2013 (or any subsequent version of such standards which may have appeared at a later time) or the latest applicable versions of other similar but higher standards of security, such as BSI (Bundesamt für Sicherheit in der Informationstechnik) IT-Grundschutz. The Supplier shall disclose such measures in detail with the corresponding concepts, certificates and audit reports at the request of the Customer.

### 2. Training and awareness raising in the context of information security

The Supplier shall regularly inform their employees and third parties entrusted with the rendering of the services about relevant information security topics, including the duties which are incumbent on them in connection with the rendering of the services to guarantee information security.

### 3. Protection of the Customer's data against misuse and loss

The Supplier hereby undertakes to secure all the Customer's information and data received or generated by it immediately, effectively and in compliance with the state-of-the-art against unauthorized access, modification, destruction or loss, prohibited transmission, other prohibited processing and any other misuse. In securing the Customer's data, the Supplier must take all state-of-the-art precautions and measures to ensure that data can be archived and restored at any time without loss. If during the continued performance of the provision of Services the state of the art with regard to security measures changes, Supplier shall undertake to all measures to secure all Customer Group's information and data according to the new state of the art.

### 4. Ownership of Customer's data

Customer and its Affiliated Companies possess and retain all right, title and interest in and to their data and Supplier's possession thereof is solely on Customer's and/or Customers Affiliate's behalf.

5. Protection when sending information
Any data which is sent, either physically or electronically, in the context of the supplies and services must be transmitted by means (e.g. registered post, courier, email encryption) which are appropriate to the degree of sensitivity of such data.

6. Protection against malware
The Supplier shall use state-of-the-art test and analysis procedures to examine all services and data carriers or electronically (e.g. via email or data transfer) transmitted services to ensure that they are not compromised by malware (e.g. trojans, viruses, spyware) before such services are provided or used. Data carriers on which malware is detected may not be used. The Supplier shall inform the Customer immediately if it discovers that the Customer is compromised by malware. The same obligations apply to all forms of electronic communication.

7. Transparency in services and processes
Services may not contain any undocumented mechanisms or functions which may compromise their security. Data may only be transmitted automatically to the Supplier or to third parties with the Customer's explicit written consent.

8. Communication in the event of defects or errors in the services provided
The Supplier shall inform the Customer immediately if it discovers defects or errors in the services provided to the Customer which may compromise the Customer's operations or security.

9. Handling of hardware, software, means of access and access data provided to the Supplier
All hardware, software, means of access and access data which the Customer provides to the Supplier shall be used in compliance with the Customer's terms of use. The Supplier shall keep all access data and means of access provided to it secret and take state-of-the-art measures to protect them against unauthorized access and use by third parties. If hardware, software, means of access and access data provided to the Supplier for the purpose of rendering the services are no longer required, they shall be promptly returned to the Customer. If the return of the software, means of access and access data provided is not possible, the Supplier shall delete or uninstall the software, access data and means of access provided to it but not without having contacted Customer and asking for approval of deletion/unistallment. Afterwards, Supplier shall confirm deletion / uninstallment to Customer in writing. The Supplier may only use its own hardware and software with or on the Customer's systems and networks in connection with the rendering of a service if this has been permitted in advance by the Customer.

Part B - Terms and Conditions for the Provision of Developed Software/Hardware and/or OT & E/E Systems solutions including Documentation

1. Principle obligation of the Supplier
The Supplier's principal obligation is to provide as part of the service contract software that is ready to use in accordance with the specifications and functions set out in the software specifications provided, the corresponding documentation (such as the user manual) and, if no other contractual agreement is made, the source code, in each case in accordance with the current program and update status (hereinafter called the "Contractual Service").

The Supplier shall maintain and safeguard the operational readiness of the software, where this is agreed in accordance with a service level agreement that is to be agreed separately or as part of the agreement on software support and/or software maintenance.

The Supplier shall fulfill the contract in person. Performance of the service by a third party shall be excluded, unless the Customer agrees to the involvement of a third party in the course of prior written notification.

Once the Contractual Service has been completed, the Supplier shall notify the Customer of this in writing or text form and agree a date on which to present the results of the work. The Supplier shall give the Customer an opportunity to carry out functional tests before acceptance of the Contractual Service. The parties shall reach a mutual agreement on the details of these tests.

All acceptances must follow a formal procedure. A report to be signed by both parties shall be produced for the acceptance. If the Contractual Service is not ready for acceptance, the Supplier undertakes to rectify the defects immediately and present the service to the Customer again for acceptance.

2. Rights of use
2.1 Ownership and the Customer's exclusive rights of use
Ownership of all results and interim results of services provided by the Supplier with regard to the development of software/hardware and/or OT & E/E Systems as part of the contract, e.g. performance descriptions, specifications, studies, concepts, documentation, including installation, usage and operating manuals as well as documentation on maintenance, the source code and further development, reports, consultancy documents, charts, diagrams, images and bespoke software, programs, adapted software (customizing) and parameterization as well as all interim results, aids and/or other performance results produced in the course of this (together: "Work Results") shall pass to the Customer when these objects are handed over, providing they are physical objects.

In other respects, the Supplier grants the Customer exclusive, permanent, irrevocable, sub-licensable and transferrable rights to the Work Results when these are created but at the latest when they are handed over. The operation of the software may be carried out for the Customer and its Affiliated Companies by one of these companies.

The Customer may - in addition to its own use - provide the software to its Affiliated Companies for their own use in accordance with the provisions of the agreements entered into and may use the software for these companies. This right of use is temporary; it ends six calendar months after the point in time at which the Customer and the using company are no longer affiliated with each other.

The Customer may have the operation of the software carried out by a third company (e.g. as outsourcing or hosting). The Customer shall inform the Supplier of this in writing in advance and shall submit the third party's declaration to the Supplier at the latter's request that the software will be kept secret and used exclusively for the purposes of the Customer and its Affiliated Companies.

Outside the scope of warranty rights, the Customer may hand over the software to third parties for the purpose of rectifying errors. It may provide the software, including the written documents, to third parties for the training of the employees of the Customer and its Affiliated Companies.

These rights shall be unlimited in respect of the geographical area, time and content and have no limitation in respect of the use and exploitation.

These usage rights shall include all types of use, in particular the storage, loading, execution and processing of data, processing in any way, including error correction, also by third parties, including permanent combination with the Supplier's services, the right to reproduce and disseminate, the right of performance and presentation, including in public, the right to market, make changes, convert, translate, make additions to and develop further. The usage right shall also include future novel usage forms. With regard to novel usage forms, the Supplier shall indemnify the Customer against any claims of the authors pursuant to Sections 31a (2), 32a UrhG (German Copyright Act).

The Customer may make backup copies in accordance with a use in accordance with the respective state-of-the-art.

The Customer may print out and copy the user manual and other information and also make them available to the Affiliated Companies.

The Customer shall be entitled to grant both free-of-charge and paid-for sublicenses and further usage rights to these usage rights and to transfer usage rights to third parties, without requiring further permission from the Supplier.

The Supplier shall ensure that those he brings in to fulfill the contract for him will waive the following rights: to be named as authors, and to have access to any original copies of software or other work such as documentation, drawings and other Work Results that may be protected by copyright.

2.2 The Customer's non-exclusive usage rights
The Supplier hereby grants the Customer and its Affiliated Companies a non-exclusive, irrevocable, permanent right to use works, other copyright material and other un-protected technical knowledge ("Know-how") that the Supplier had already developed or used before the start of the contract and Know-

how, standard software and development tools (together called "**the Supplier's Intellectual Property**") acquired by the Supplier and his vicarious agents the course of providing the service, independently of the Contractual Service. These rights shall not be limited to a specific geographical area, they shall be transferable, sub-licensable usage rights that are covered by the agreed compensation, providing this is necessary for the Customer and its Affiliated Companies to use the Work Results provided by the Supplier, without further consent being required on the part of the Supplier. This also includes the reproduction, editing and modification of the Supplier's Intellectual Property by the Customer and its Affiliated Companies or third parties, providing that this is required to use the Work Results.

This right of use of the Affiliated Companies is temporary; it ends six calendar months after the point in time at which the Customer and the using company are no longer affiliated with each other.

2.3 Usage rights for customizing services
Where the Supplier has customized his own software or the software of third parties for the Customer, he shall grant the Customer and its Affiliated Companies usage rights to this in accordance with item 2.1.

2.4 Duty to notify
Before the end of the contract the Supplier shall give the Customer written notification of all third-party software, standard software, development tools and other works (such as all documentation required for the further development and processing of the Supplier's performance results) to be used in the context of developing the Work Results, including materials that the Supplier uses under license. These, including the Supplier's rights, are to be listed in the contract. Unless agreed to the contrary in the contract, the Supplier shall grant the Customer the usage rights to third-party software, standard software, development tools and other works in accordance with Item 2.2.

2.5 Coauthors
Where the Supplier's employees or vicarious agents are coauthors, the Supplier warrants that he has acquired from them the right to grant usage and exploitation rights set out in Items 2.1 and 2.2 above.

2.6 Rights to inventions
Where Work Results contain inventive achievements, if the invention has been made by an employee, the Supplier undertakes to claim it in good time and transfer the invention to the Customer. The Customer is free to make the decision whether to register inventions for worldwide intellectual property rights in his name or the name of a third party designated by him. The Supplier undertakes to make any declarations and provide signatures to obtain, maintain and defend inventions. No special remuneration shall be provided for this.

2.7 Granting of rights for updates and supplementary performance
Updates, upgrades, additions, new versions and similar as well as the updated documentation in each case (together called "Updates") provided to the Customer by the Supplier shall also be subject to the provisions of this agreement.

2.8 Continued application
In case usage rights are permanently acquired and provided all agreed remuneration has been paid, the usage rights granted shall not be affected by withdrawal from the contract, its termination or ending in any other way.

## 3. Defects and performance disruptions

The Supplier shall take special care to ensure that the Contractual Service is free from third party rights that limit or exclude the use in accordance with the contractually defined scope and that claims by third parties that the rights of use to be granted to the Customer infringe the rights of this third party can be warded off. They shall document their own procurement processes with the greatest accuracy, ensure a secure transfer of rights by drafting contracts with their employees, select sub-suppliers with the greatest possible care, follow up any suspicion of a defect of title immediately and intensively. Should a third party assert such claims, the Supplier shall, upon notification of the Customer that their rights of use are being attacked by a third party, make this information and their expertise available to the Customer without restriction in order to clarify the facts and defend against the alleged claims. If possible, the Supplier shall conclude agreements with its sub-suppliers which enable and ensure comprehensive fulfilment of these obligations. In the event of a legal dispute with the third party, the Supplier shall provide evidence in the correct form according to the respective type of proceedings (e.g. as an affirmation in lieu of an oath or as original documents).

The Supplier also shall take special care to ensure that the Contractual Service meets the Customer´s special requirements, the specified or agreed technical or other specifications and is suitable for the planned use that is consistent with the agreed performance requirements.

Any deviation of the Contractual Service from the agreed quality shall always be deemed to be a quality defect. The same shall apply if the Contractual Service is not suitable for the use set out in the contract.

The documentation is deemed to be defective if a knowledgeable user with the level of knowledge usually expected to use the software cannot, by applying reasonable effort with the help of the documentation, operate individual functions or resolve the problems that occur.

The Supplier acknowledges that the smooth interaction between the Contractual Services and the current programs but at least those intended for the purpose of the contract is of utmost importance for the Customer in order to ensure the functioning of Customer's business operations and that Customer has commissioned the Supplier with the provision of Contractual Services and thus does everything they can to ensure that the Contractual Services can be operated free of malfunctions using the Contractual Service on the basis of industrial standards. The Supplier furthermore acknowledges that compliance of the Contractual Service with the current statutory requirements at the time of acceptance is of utmost importance to the Customer and shall take special care to ensure that such compliance is given.

The limitation period for quality defects shall be two years from acceptance of the Contractual Service. The statute of limitations for defects of title shall be two years and commence at the end of the calendar year in which the claim arises and the Customer became aware of the defect of title (in particular infringement of an intellectual property right) and the entitled party received the information or should have done so unless gross negligence was involved. A defect notification by the Customer suspends the statute of limitations. The Customer shall inform the Supplier without delay of any defects that occur up to the time the statute of limitation applies. If required and after consultation, the Customer shall be involved as required in analyzing and rectifying the defect.

3.1 Supplementary performance
The Supplier shall rectify defects immediately and within an appropriate period during the warranty period, taking account of the Customer's interests, and either deliver an improved version of the Contractual Service or provide the Contractual Service from new. If use in accordance with the contract causes an impairment of the rights of third parties, the Supplier shall either modify the Contractual Service so that it does not infringe the protected rights or obtain authorization so that the Contractual Service can be used in accordance with the contract without any limitation and without additional cost for the Customer. The provision of a replacement solution or a workaround can be used as a short-term measure to provide a temporary solution or to bypass the effects of a defect. The defect is not deemed to be rectified until it has been fully resolved within a reasonable period of time.

If the Supplier fails to rectify the defect immediately and if the Customer suffers an unreasonably high disadvantage in relation to the Supplier's disadvantage due to the failure to remedy the defect immediately, the Customer shall be entitled to remedy the defect himself, to have it remedied or to procure a replacement at the Supplier's expense. The costs to be reimbursed by the Supplier shall not be disproportionate and shall be limited to the amount which the Supplier would have incurred if it had rectified the defect itself within the rectification period to which it is entitled. Further legal or contractual claims remain reserved.

3.2 Reduction in the price, withdrawal
If the Supplier refuses to rectify the defect or is unsuccessful in doing so or if the additional period allowed to the Supplier passes without a resolution being found, the Customer may choose whether to reduce the remuneration or withdraw from the contract in full or in part unless it has remedied the defect himself subject to Item 3.1.

3.3 Withholding of payment and offsetting payments
If the Supplier does not meet his obligations, the Customer may hold back payment for the Contractual Services until the Supplier has fulfilled his obligations in full. The Customer may deduct his claims against the Supplier from

remuneration due to the Supplier on account of the Supplier's failure to comply with his obligations.

3.4 Reimbursement of expenses, compensation
More extensive claims, including in relation to compensation and re-imbursement of expenses, shall not be affected.

## 4. Open-Source-Software

Open Source Software ("OSS") is software, which is generally provided free of charge and open source and can be used under a license, which does not restrict redistribution of the software, allows modifications and derived works and must allow redistribution thereof under the same terms as the license of the original software ("OSS-License"). OSS-Licenses include without limitation "Berkeley Software Distribution License" (BSD), "GNU General Public License" (GPL), and the "GNU Lesser General Public License" (LGPL). Copyleft Licenses are licenses that require that any derivative work or work based on the program is distributed or conveyed only under the original license terms ("Copyleft License").

4.1 Requirements
OSS may only be included in the software provided by the Supplier with prior written approval by the Customer. The Supplier will provide to the Customer all information and materials necessary for deciding on the use of OSS in the software. This includes:
(i) a transparent and complete list of all components licensed under an OSS-License,
(ii) the license text of each OSS-License,
(iii) copyright notices,
(iv) the results of a state of the art security and vulnerability scan of all open source code used, and
(v) A clear description and documentation regarding the technical integration of the OSS components.

The Customer will grant the approval in its sole discretion. A granted approval is to be revoked, if the provided information or materials are false or incomplete.
OSS-License texts and the respective source code must be provided separately. The Supplier will provide all open source code to the extent that this is required by applicable licenses.
The Supplier will put the Customer in a position to completely comply with all requirements under the applicable OSS-Licenses at all times.
This requirements also apply to any updates, patches, upgrades or new versions of the software.

4.2 Responsibility
The Supplier is aware of its special responsibility to protect the Customer from damage caused by the integration of OSS software in the software supplied by the Supplier and the use of such software by the Customer. In view of this, the Supplier shall take special care that it:
(i) complies at all times with the license requirements of applicable OSS-Licenses and that the Customer has received all necessary licenses from the authors of the OSS incorporated in the software,
(ii) has an Open Source Compliance System in place that is an accordance with best practices of the industry,
(iii) uses only OSS components that are licensed under compatible OSS-Licenses,
(iv) has not incorporated any Copyleft License in the software,
(v) has scanned all open source code used in the software for security risks.

4.3 Indemnification
The Supplier shall indemnify, defend, and hold harmless the Customer and Customer's affiliates, employees, directors or agents of any claims, damages, expenses and liability which arise in direct or indirect connection of Supplier's breach of one of the foregoing requirements of obligations, irrespective under what legal theory.

## 5. Software Development Lifecycle

For work that includes software development, the Supplier shall:
(i) adopt a Secure Software Development Lifecycle approach according to well known standards, such as IEC 62443 4-1. A certification is expected.
(ii) provide evidence that identified security requirements and corresponding security controls are designed and implemented into the software.
(iii) ensure that appropriate security tests including but not limited to static and dynamic code checks and continuous vulnerability assessment are applied in the development and integration pipelines and any issues uncovered are remediated before software release; and
(iv) allow Customer and/or its agents to carry out Vulnerability Assessments of the developed software. If any vulnerability with a risk score of "high" or "critical" is found by the Customer, the Supplier shall take action to mitigate the risks before the software release.

## 6. Vulnerability Management

(i) The Supplier will engage an independent and trusted Vulnerability Assessment service and/or cooperate and assist an independent third party appointed by the Customer in the conduct of Vulnerability Assessments.
(ii) The Supplier shall on a monthly basis, review the Supplier's sources of threat and vulnerability information for the latest vulnerabilities, threats and remediation relevant to the systems under the Supplier's management.
(iv) The Supplier shall conduct both network level and application level Vulnerability Assessments to identify controls that may be missing or not effective to protect a target from potential threats.
(v) The Supplier shall implement a remediation plan of mitigation activities once a vulnerability is identified or to prevent a vulnerability from arising, and for prioritising, tracking and monitoring the plan's progress. All remediation plans shall be documented for future reference. Vulnerabilities with a significant security impact shall be remedied as soon as practicably possible in agreement with the Customer. For lower and medium risks, the timescale for remediation shall take into account the cost, time and effort required to mitigate the risks.
(vi) The Supplier shall retest all vulnerabilities post remediation activities, to confirm that the risks have been mitigated to acceptable levels as defined by the Customer.
(vii) The Supplier shall promptly provide the Customer with the following:

- the reports (in original format) of the results and recommendations of the Vulnerability Assessments provided by the independent Vulnerability Assessment service providers; and
- the Supplier's remediation plans to remediate identified vulnerabilities.

(viii) The Supplier shall notify the Customer immediately if it fails to remedy any Critical or High rated Vulnerability and shall propose and agree with the Customer necessary security controls.
(ix) The Supplier shall ensure that all applications, middleware, back-end software, Systems and networks are built and configured securely by default. As part of standard build deployment, technology components will have configuration settings used in accordance with sources of authoritative security recommendations such as those provided by product Suppliers (e.g. Siemens, Microsoft) or industry groups (e.g. ISO, IEC, CIS, NIST, SANS, OWASP).
(x) Vulnerability Assessments, regardless of type or target, and all work and time required to carry out remediation activities, will be at the cost of the Supplier and will not be charged to the Customer.

## 7. Security Governance

(i) The Supplier will appoint an individual (the "Supplier Security Manager"), to:

- coordinate and manage all aspects of security in accordance with the Agreement; and
- act as the single point of contact on behalf of the Supplier and its Subcontractors in the event of a Security Incident.

(ii) In the event that the Supplier wishes to change the Supplier Security Manager it will notify the Customer in writing, providing contact details for the replacement individual.
(iii) If the Supplier has any questions in relation to any aspect of IT Security or the implementation of the requirements in this Schedule, it will consult with the Customer.

## 8. Risk Management

(i) Upon reasonable request of the Customer, for the cases when the Supplier has interaction with the Customer's IT system, the Supplier will assist the Customer with a Security Risk Assessment of the work, which may be carried out at any time during common business hours.
(ii) In the event that any issues identified from a Security Risk Assessment are rated High or Critical, the Supplier will provide all reasonable assistance to the Customer in the analysis of the risks and identification of appropriate controls to be implemented by Supplier to protect the Customer's Data or Service managed or possessed by the Suppler in accordance with the requirements detailed in this document.
(iii) In the event that the Supplier intends to make any material change to its provision of work, or the Customer requests any material change to the work, the Supplier will perform a Security Risk Assessment.
(iv) The Supplier will ensure that any risks identified in a Security Risk Assessment are promptly remediated, monitored and managed until their closure.

The Supplier shall keep the Customer informed of remediation activities for all risks identified during the Security Risk Assessment.

### 9. Personnel Security

(i) The Supplier will ensure that any Supplier or Supplier Personnel with access to the Customer Data have been vetted and screened in accordance with this agreement and/or as directed by the Customer.
(ii) The Supplier and its Subcontractors shall ensure that all Supplier Personnel receive any required training and are aware of their responsibilities regarding the security provisions in this agreement.
(iii) The Supplier shall implement and maintain appropriate controls to reduce the risks of human error, theft, fraud or misuse of facilities by the Supplier Personnel.

### 10. Data Center Security

(i) The Supplier shall implement and maintain appropriate physical and environmental security controls to prevent unauthorised access, damage and interference to any Data Centres containing Customer Data or any information utilised in the provision of the work.
(ii) The Supplier shall ensure that all Data Centres are certified to ISO 27001 (or any standard which replaces or supplements ISO 27001).
(iii) The Supplier shall give the Customer reasonable prior written notice of any proposed change by Supplier of any procedures or policies applicable to a Data Centre which might reasonably be expected to increase the risk to the security and Integrity of any Customer Data.

### 11. Access Control

(i) The Supplier shall ensure appropriate access control mechanisms are employed to verify and authenticate all users (or entities), whether from the Supplier, a third party or the Customer, before access is granted to the work.
(ii) All users (or entities) which access or request access to the work will be provisioned, managed and authorised as part of a defined access management process.
(iii) The Supplier shall use an authentication method supporting a minimum of a user ID and password combination, where the user IDs and passwords are unique, not reassigned and not shared by a group of users. In the case of administrative accounts, the supplier shall require an additional factor for authentication.
(iv) The Supplier shall require all users transitioning from a lower to a higher privilege or sensitive level of access to re-authenticate.
(v) The Supplier shall use appropriate controls to protect passwords and other access credentials in storage and when transmitted. The Supplier shall not transmit or store passwords in clear text and not visibly display passwords on the Systems when logging in.
(vi) The Supplier shall not hard code user IDs and passwords in scripts or clear text files such as in shell scripts, batch configuration files and connection strings.

### 12. Network Security

(i) The Supplier shall manage the transmission of the Customer Data in a network environment under the direct control of the Supplier (or a Subcontractor). The network shall be managed and protected from external threats, including but not limited to access control at the physical, network and application levels to allow only those who have legitimately been authorised by the Supplier to have access to the Customer Data. The network shall be segregated to deny access from public or untrusted networks, including networks belonging to third parties with whom the Supplier have not agreed a contract with clauses equivalent to the clauses in this terms and conditions and a separate data processing agreement (DPA).
(ii) The Supplier shall ensure the Systems are updated with the latest and relevant security software and pre-tested and authorised security software patches and fixes from other Supplier-provided Systems regularly and in a timely manner. The Supplier shall conduct Vulnerability Assessments to assess the configuration and software patch status of the systems on a monthly basis.
(iii) The Supplier shall ensure that all Customer network connections to the Supplier's network transporting any Customer Data classified "CONFIDENTIAL" over an untrusted network, such as the internet, is via an encrypted network link in compliance with the Customer Security Policies or published standards such as ISO or NIST.
(iv) The Supplier shall ensure auditable events are generated, including but not limited to security specific events, all successful and failed access attempts on the network, and will maintain a log of all changes to the security configurations of the network.
(v) The Supplier shall establish, implement and manage procedures and a Security Information and Event Management (SIEM) system to monitor the security of the network for suspected intrusion or unauthorised access.
(vi) The Supplier shall ensure that the process and controls used to perform security monitoring will be implemented in such a manner as to maintain the Integrity, confidentiality and availability of collected security monitoring related events.
(vii) The Supplier shall maintain segregation of any development and test environments from production environments. Any live Customer Data containing Personal Data shall be made anonymous (i.e. converted into a form which does not identify individuals or enable data to be rebuilt to facilitate identification) before they are used for testing and have explicit written approval from the Customer.
(viii) Where a Supplier's system or network is connecting to the Customer network, the Supplier system or network must comply with Customer Security Policies.

### 13. Subcontractors and Third parties

(i) When engaging a Subcontractor, the Supplier shall procure that the Subcontractor agrees to the same terms and conditions as contained in this document in respect of IT/OT & E/E Systems Security for the direct benefit of the Customer and enter into a separate data processing agreement (DPA), if necessary, whereas it principally deems necessary, if Customer and Supplier have entered into a data processing agreement (DPA).
(ii) Upon request from the Customer, the Supplier shall verify and provide a written report in detail on its Subcontractors' compliance with the security obligations required of the Subcontractors in accordance with this terms and conditions document.
(iii) Where the Supplier engages a third party for the purposes of delivering the work to the Customer, the Supplier will:

a) authenticate all third party systems using technology and processes to enforce non-repudiation;
b) implement controls to protect the Supplier's network from unauthorised access between:
    1) the third party network and the Supplier's network;
    2) the third party network and any internet access points; and
    3) the third party network and other third party networks connected to the Supplier's network;
c) restrict all inbound and outbound connections to or from third party networks to specific hosts, ports and work on these hosts to the minimum required to meet the needs of the Customer;
d) communicate all changes to the scope of work, including firewall rule changes, to the Customer if requested;
e) maintain a list of all individuals who have access to the Supplier's network and review the list on a monthly basis;
f) log all successful and failed third party access and make them available for review by the Customer when required;
g) immediately notify the Customer of any security breaches, including actual or suspected unauthorised access to or compromise of any system, and take such remedial actions in accordance with this terms and conditions; and
h) review all third party network connections on an annual basis or when there is a change to the connections and access control requirements and terminate any obsolete or un-required third party connections.

(iv) The Supplier shall be responsible for any breach of duty on the part of its subcontractors to the same extent as it is responsible for its own breach of duty.

### 14. Security Incident Management

(i) The Supplier shall at all times monitor and verify that all access to the Customer Data is authorised and to check for any Security Incidents.
(ii) In the event of a Critical Security Incident or Major Security Incident, as determined by the Customer, the Supplier shall:

a) notify the Customer no later than four hours after the Security Incident (including, where necessary, escalating such notification);
b) respond immediately and in an appropriate manner to such incident in accordance with the Security Service Levels and the procedure set out in the Security Incident Response Plan; and
c) provide immediate assistance to the Customer and/or Customer's representatives into the investigation and retain all documentation relating to any such investigations.

(iii) The Supplier shall not disclose the details of a Security Incident or weakness to third parties without written authorisation from the Customer.

(iv) The Supplier shall collect and secure evidence in the investigation of a Security Incident using forensics procedures, ensuring a chain of custody and, where necessary, compliance to regulatory requirements.
(v) The Supplier shall classify all reports of Security Incidents as "CONFIDENTIAL" in accordance with the Customer Data Classification Policy and ensure that appropriate controls are applied to protect this information.
(vi) The Supplier shall, in the event of a Security Incident, provide reports on Security Incidents. Such reports shall include, but shall not be limited to:

a) the source and destination of the event as well as the time, date and type of event;
b) a weighting of criticality (Low Priority, Major or Critical Security Incident);
c) a Root Cause Analysis report in respect of each security incident; and
d) an individual reference number to be tracked.

(vii) Following a Security Incident, or as requested by the Customer, the Supplier shall initiate corrective action to minimise and prevent future Security Incidents relating to the scope of work.
(viii) The Supplier shall invoke backup and recovery procedures in response to Security Incidents that result in lost or damaged information.

## 15. Security Audits

(i) Supplier shall grant access (during Supplier's regular working hours) to the Customer and/or any external auditors appointed by the Customer, to the premises and/or records of the Supplier for the purposes of:

a) reviewing the Integrity, confidentiality and security of the Customer Data and/or the scope of work;
b) ensuring that the Supplier is complying with this terms and conditions; or
c) carrying out a Vulnerability Assessment of any of the systems containing Customer Data.

(ii) Customer shall be entitled to conduct an audit in accordance with paragraph (i) once in any calendar year during the term of the Agreement, provided that the Customer shall be entitled to conduct an audit at any time if it reasonably suspects Supplier to be in material breach of this terms and conditions.
(iii) In the event of an investigation into suspected fraudulent or criminal activity relating to IT/OT & E/E Systems Security and/or the provision of the work by the Supplier or any of its Subcontractors, the Supplier shall provide to the Customer, any statutory or regulatory auditors of the Customer, and their respective authorised agents, prompt access to the premises and records of the Supplier for the purposes of conducting an audit and Supplier shall render all necessary assistance to the conduct of such investigation at all times during the period of the Agreement or any time thereafter.
(iv) Each party shall bear its own costs and expenses incurred in exercising its rights or complying with its obligations.
(v) The Supplier shall, and will procure that its Subcontractors shall, provide the Customer (and/or its agents or representatives) with the following:

a) all information requested by the Customer within the permitted scope of any audit;
b) access to any sites or Data Centres controlled by the Supplier in which any equipment owned by the Customer is used in the performance of the work for the purposes of an audit;
c) access to records held in the Supplier information systems for the purposes of an audit; and
d) access to Supplier and Supplier Personnel for the purposes of an audit.