通用采购条件

1.适用范围；合同之缔结

1.1 除非另行约定，本采购条件适用于供应方的货物及服务。其它通用标准条款与条件，特别是供应方的标准条款与条件，将不在此适用，即使在个别情况下采购方未明确反对或采购方已无保留地接受所订货物/服务。

1.2 采购订单及订单的接受（以下简称"订单确认函"）及采购方和供应方为履行合同目而订立的所有协议，只有以书面形式订立方对双方有效力。书面形式包含以数据传输、传真、使用电子签名程序如 DocuSign，AdobeSign，e 签宝或电子邮件等方式发送或订立的文件。

1.3 供应方承诺应当在收到采购订单后两周内以订单确认函的方式确认接受采购订单，如供应方未按照此处约定时间及方式确认的，采购方有权利撤销采购订单。如果订单确认函与采购订单有任何偏离（即使该等偏离不是实质性的），该等偏离只有在采购方明确同意的情况下方可生效。

2.交货；交货地点；未能按时交货；业务中断

2.1 双方约定的交货期有约束力。如因任何情况导致无法按时交货或迟延交货的，供应方应立即通知采购方。应依据在采购方场地或订单指定的交货/履行地点（"履行地"）收到货物的时间或完成服务的时间来判断供应方是否按时交货。

2.2 分批交货需获得采购方的同意。

2.3 如果供应方逾期交货或提供服务的，每逾期一（1）周，采购方可要求供应方按照延迟提供货物或服务所涉金额的 1%支付迟延履行违约金，但该金额累计不得超过合同中货物或服务总金额的 10%。采购方的其他法律权利（合同终止权，解除权和要求赔偿损失的权利）不受影响。如果采购方的实际损失高于此处迟延履行的违约金，采购方有权利举证和主张相应赔偿（不受此处限额限制），供应方有权利证明相关损失较低或没有损失。

2.4 采购方无条件接受逾期交付的货物或服务，并不意味着采购方放弃要求供应方承担迟逾期交付货物或服务的赔偿责任。

2.5 如遇短时工作、业务中断和其他停工情况，导致采购方因不可归咎于自身的原因无法在受影响地区接受交付的，双方应尽可能商定一个合适的替代日期。在商定出合适的替代日期之前，双方的合同义务应在事件持续期间暂停。如果可能，采购方应尽早与供应方联系。

3.备用零件的提供

供应方应当确保，在采购方所购型号产品停产后十年内，采购方能够获得充足的备用零件。在上述期间内，对于用于生产备用零件的资料和图纸，供应方亦应当一并保存。供应方的上述义务在该期间到期且经过采购方书面同意后方可解除。除非有合适且正当的原因，否则供应方不得拒绝履行此处的义务。

4.价格；风险转移及付款条件

4.1 订单所规定的价格应具约束力。订单价格均为按照国际贸易术语解释通则 2020 版（Incoterms 2020）规定的目的地交货（DAP）的价格（包括包装费）。该价格不包含法定增值税。货物毁损灭失的风险在本采购订单约定的交货时转移。

4.2 供应方应当将发票寄送至采购订单中约定的地址并且在发票中注明采购订单号码。如果采购订单丢失，采购方将不予支付对应发票的款项并会将发票退还供应方，采购方不承担任何因此导致的迟延责任。针对每个采购订单，供应方应当开具对应的发票，发票应当按照采购订单的要求开具。不管是预付款、部分付款还是尾款的发票，都应当按照此处要求注明清楚。如果货物或服务已经交付或履行，那么采购方和供应方签署的交接工作表（报告）应当附在发票后。

4.3 在供应方交付货物或提供服务后且采购方收到发票后九十（90）日内付款。

5.验收测试

如果供应方需要交付货物或提供服务，必须要经过采购方的正式验收。采购方有权选择在供应方工厂或合同履行地进行验收。采购方的无条件付款不得视为其验收和认可了供应方提供的货物或服务，亦不得视为其放弃针对产品或服务缺陷的索赔。

6.货物运输

6.1 货物装运通知最迟应在货物离开供应方工厂时发出。

6.2 供应方同意将采购订单号及采购方的准确交货地址标注在所有的货运单据和提货单上。如供应方未按照此要求履行的，供应方应当承担由此导致的所有迟延交付责任。

6.3 如约定采购方承担全部或部分运费的，供应方应采用最划算的方式进行货物运输，并且应当遵守采购方的运输规范。

6.4 关于货物运输的指示和要求具体在采购订单中约定。

7. 包装

7.1 供应方承诺会根据采购订单及采购方相应规范的要求包装需要运输的货物，以确保货物在正常的运输过程中不受到损害。

7.2 供应方应根据采购方的要求免费回收使用后的包装，并将其进行再利用或循环使用。如果采购方要求回收包装，则包装回收的地点应为采购方的厂区门口。

8. 缺陷通知

在不影响正常经营的情况下，采购方应检查所收货物的数量是否正确、运输中是否造成损伤以及是否有明显缺陷。采购方将在发现缺陷后五（5）日内通知供应方。供应方就此放弃对采购方迟延履行缺陷告知义务的抗辩权。采购方保留后续对货物进行更为详细检查的权利。

9. 缺陷责任

9.1 供应方向采购方保证，所订购的货物或服务在风险转移时符合合同约定和通常所预期的属性（即符合适用于交付货物或提供服务的合同约定和法律规定、适用的技术指南和标准以及现有技术水平）且无缺陷，且权属上无法律瑕疵。

9.2 如采购方告知供应方所供货物和服务的用途和使用地，供应方应保证其所供货物和服务适于此用途和使用地。

9.3 如存在缺陷或权属瑕疵的，采购方有权根据法定的权利索要全额赔偿。

9.4 原则上，采购方有权选择补救方式。采购方提出补救要求后，如果供应方未能按照合同约定随即开展补救措施（例如改正缺陷或交付替代品），在此情况下，以及为了防止危险或避免/控制损失，采购方有权按其选定的方式自行或由第三方进行补救，所发生之费用由供应方承担。供应方未能改正缺陷或未能发送替代品的，或其改正或替代品不被接受的，采购方享有上述同样的权利。

9.5 供应方需承担所有与缺陷有关的或在缺陷纠正工作期间所产生的所有费用，特别是安装和拆除的费用、往返最终目的地的运输费用以及其他所有损失（例如由于缺陷导致的采购方的客户提出的索赔），无论供应方是否对缺陷负责。

9.6 如因供应方提供的货物/服务导致采购方遭受第三方的侵权索赔，供应方应在收到初次书面要求后立即对采购方遭受的索赔予以赔偿。供应方对采购方的赔偿应包含采购方因第三方索赔所产生或相关的一切必要费用。

9.7 除非供应方有意欺诈，否则产品缺陷索赔权在法定时效届满后失效，时效应从采购方知道或应当知道缺陷之时开始计算。如供应方以提供替代品的方式履行了补救缺陷的义务，对该替代品的诉讼时效自其交付后重新开始计算。

10.信息技术
10.1 对于非代采购方开发的软件/硬件和/或运营技术和电气和电子系统解决方案（包括作为供应方货物和服务组成部分的文件），应适用本采购条件**附件 1** 所列的条款条件。
10.2 对于供应方代采购方开发或改造的在信息技术/运营技术/电气和电子系统领域的所有货物和服务，或涉及第 10.1 节未涵盖的信息技术服务或信息技术的采购，应适用本采购条件**附件 2** 所列的条款条件。

11.质量保证
11.1 供应方承诺，通过适当的质量保证体系——如 DIN EN ISO 9001 ff 或类似体系来持续监督其产品质量，并且根据采购方要求的或其他适当的质量检测方法，对生产过程中和生产完成后的产品进行检查。供应方应当记录所有检查内容并保留相关文件十年。

11.2 购方或采购方聘用的人员有权要求供应方提供能够证明其交付的产品及其所使用的质量保证体系与合同约定质量标准相符合的证据，以保证产品不存在质量问题并确保在供应方或供应方分包商工厂所进行的产品检测方法是充分有效的。供应方承诺在供应方或供应方分包商的工厂开展检验和审计活动并自行承担相关费用。

11.3 供应方所加工材料的成分或者其货物或服务在设计上发生变更的，供应方应立即按照第 1.3 条款规定的书面形式及时告知采购方，即便采购方未对此做出要求。任何变更均需获得采购方的书面许可。

11.4 如供应方拟将货物或服务的全部或主要部分分包给分包商，其应事先通知采购方并需经过采购方的书面批准。

11.5 采购方告知供应方的质量保证政策，以及采购方与供应方所订立的质量保证协议，均为合同的组成部分。

12.营销产品和产品责任
12.1 供应方承诺遵守其注册地址所在地及合同履行地的相关法律规定。

12.2 若供应方供应货物属于欧盟针对首次上市产品的法规指令的适用范围之内，例如《欧盟机械指令》、《欧洲压力设备指令》、《电磁兼容指令》等，供应方承诺符合此类法规规定的相关健康和安全要求和流程，并出具其中规定的文件。如有《欧盟机械指导法令》No. 2006/42/EC 版规定的机械半成品的，供应方应按照采购方要求的形式，向采购方提供《欧盟机械指导法令》附录 II B 项规定的符合性申明（扩展的符合性申明），并提供符合《欧盟机械指导法令》附录 I 第 1.7.4 部分规定的使用说明。如采购方要求，供应方应根据采购方的选择，或允许采购方检查其做的风险评估，或向采购方提供该风险评估。

12.3 如果供应方对所供货物以外的损害负有责任，且第三方根据产品责任相关的法律向采购方提出索赔，则如果损害的原因属于供应方的责任范围，且供应方本身应对第三方负责，则供应方有义务在采购方提出请求的第一时间就第三方提出的损害索赔向采购方作出赔偿。责任还包括：供应方必须补偿采购方因发布产品警告或召回产品所产生的一切费用。采购方应尽可能并合理地将预备采取的措施的内容与范围告知供应方，并就其与供应方进行协调。产品责任有关的法律规定的其它权利不受影响。

12.4 供应方承诺购买产品责任险，覆盖单个索赔的保险金额应不低于一（1）百万元欧元。上述保险不妨碍采购方要求供应方赔偿更多额外损失的权利。

13.安全生产，环境保护及冲突矿产
13.1 供应方应当确保，其交付的货物和服务符合在采购方场地或其他履行地所生效和适用的有关环保、事故预防和劳动安全的条例，通过熟悉上述与安全相关的规定，避免或减少对人员和环境造成的负面影响。为此，供应方应当为此目的建立管理体系，如遵守 DIN EN ISO14001 环境管理体系或其他类似体系。采购方有权要求供应方提供其采取了管理体系的证据或在供应方场所对其进行审查。

13.2 供应方承诺遵守欧盟和中国关于化学品和危险品管理的法律法规，以及遵守欧盟和中国有关化学品管理的 REACH 规定（欧盟第 1907/2016 号规定）的要求，尤其是要遵守化学品注册登记流程。采购方没有义务为供应方交付的货物获取符合欧盟 REACH 规定的批准。供应方进一步承诺，根据其自身产品性质，对于包含下列规定明令禁止危险物质的货物不得交付给采购方：欧盟 REACH 规定的附件 1 至附件 9；欧盟委员会决定 2006/507/EC（包含斯德哥尔摩公约；消耗臭氧层物质的法规(EC) No1005/2009；全球汽车申报物质清单 GADSL；RoHS 指令 2002/95/EC 等）。上述规定以其最新版本为准。如果供应方交付的货物包含 REACH 规定的 SVHC 清单（需要引起高度关注的物质清单）中的物质，供应方承诺将立即告知采购方。这也适用于某些物质之前没有列入该清单，而在交货时被列入清单的情形。除此之外，供应方交付的货物禁止包含石棉、抗菌剂或放射性材料。如果供应方交付的货物包含相应物质，供应方应当在发货前以书面形式告知采购方，详细说明物质名称、识别号（比如 CAS 化学品登记号）及最新的安全数据表。含有上述物质货物的供货需要经过采购方单独批准。

13.3 供应方承诺，通过在其机构内部采取正确的方式，并参照其自身的交付链，确保交付给采购方的产品不包含美利坚合众国《Dodd Frank 法案》第 1502 和 1504 款规定的冲突矿产（包括但不限于产于刚果民主共和国及其邻国的钶钽铁矿、锡矿、钨矿、金矿及相关衍生品）。

13.4 供应方有义务确保采购方免于承担因供应方不遵守本条款约定而引起的一切责任，并应当赔偿采购方因此遭受的所有损失。

13.5 供应方应当遵守有关废弃物和剩余材料处置的规定，并且告知采购方所有关于产品处理、储藏和废弃处置的相应要求。

14.所有权保留；模具和工具；保密
14.1 供应方承诺不对交付采购方的货物保留所有权。

14.2 对于采购方提供给供应方的所有材料、部件、集装箱等一切物品，采购方拥有上述物品的所有权。供应方只能代表采购方对上述物品开展加工或改造。如果采购方所有的物品与不属于采购方所有的部件经过加工形成新产品的，采购方将根据双方部分的价值按比例与他方共享新产品的所有权。

14.3 任何由供应方生产的、采购方承担费用的模具和工具在采购方付款时即成为采购方财产。供应方应细心处理，只能将其用于生产采购方订单约定的货物，供应方应将其标记为采购方的财产，如条件允许，将其和供应方的其他产品分开存放。供应方应自付费用对该模具和工具投保火灾、水灾、盗窃、遗失或其它毁损险。供应方承诺会根据实际情况及时对该模具和工具进行保养和维护，并自行承担相关的维保费用。未经采购方书面允许，不得转售经用该模具和工具生产的产品。

14.4 为了生产订购的货物和/或提供服务之需要，采购方以任何形式向供应方提供的任何文件、绘图、计划和草图以及其它专有技术都应视为采购方财产。以上内容均属采购方的商业秘密并应严格保密。供应方承诺将谨慎处理上述文件，确保只有为执行合同所需的员工才能获知其内容，确保该等员工也应对该内容保密，不得让第三方获取该文件，并仅为执行订单之目的而进行复制。在供货和服务完成后，供应方应将所有文件及复印件交还采购方，或者应采购方的要求，将其全部销毁。

15. 数据保护
15.1 供应方可能会向采购方提供其参与合同谈判和履行的人员的个人信息（“供应方个人信息”）。供应方保证其已就收集和向采购方提供供应方个人信息的事宜征得相关人员的明确同意，据此，采购方有权出于履行本合同、内部管理和业务合作伙伴管理的目的，在中国大陆境内和/或境外收集、存储、使用、处理、披露、提供和传输供应方个人信息。采购方对供应方个人信息的保存期限为履行合同所必需的期限、根据合同可提出法律索赔的期限、法定保存期限以及需要（可能需要）该数据的正式诉讼程序所需的期限。如果任何相关人士就供应方个人信息提出获取信息或行使进一步权利的要求，供应方应在国家法律框架内立即通知采购方。

15.2 供应方保证其在履行本合同时遵守所有适用的个人信息保护法律，该等法律适用于供应方在合同谈判和履行过程中对其获得的所有个人信息（“个人信息”）的处理。

15.3 供应方进一步保证：(i) 供应方应采取一切合理且必要的措施保护其所拥有的个人信息，包括采取适当的技术和组织措施，并制定适当的安全程序，以防止未经授权的访问、披露、销毁、丢失或篡改个人信息；(ii) 供应方处理个人信息的目的仅限于谈判或履行合同，除非其有适当的合法依据用于其他目的；(iii) 供应方应确保其工作人员或其他第三方在需要知情的基础上接收此类个人信息，并应确保他们能够与供应方保持同等水平的个人信息保密性和安全性； (iv) 供应方应在发生任何信息安全事故或存在此类威胁时及时通知采购方，并按照采购方的指示采取补救措施；以及 (iv) 供应方

应在采购方提出要求或合同到期、解除或终止时及时归还或删除所有个人信息。

15.4 对于因供应方不遵守或违反个人信息保护义务而直接或间接导致的任何索赔、损害赔偿、费用和责任，供应方应向采购方和采购方的关联方、员工、董事或代理人作出赔偿、为其辩护并使其免受损害。供应方应赔偿采购方因此造成的所有损失，包括但不限于向第三方作出的任何赔偿、执法机关处以的任何罚款，以及处理该事件和追究供应方责任的费用，如调查费、诉讼费、律师费等。如果采购方自行决定认为供应方的违规行为严重并构成实质性违约，采购方有权终止合同。

16.原产地和出口控制

16.1 根据采购方的要求，供应方承诺按照法律规定的要求免费提供产品原产地证明给采购方。如采用供应方的长期声明，供应方应在接受订单时，无需提示，即告知采购方原产地状态的变更。在任何情况下，产品的实际原产地应当注明在交易文件中，即使不存在任何优惠关税待遇。

16.2 若根据德国、欧洲、中国和美国的法律以及其他适用的出口和海关的要求，供应方产品出口（再出口）应获得相关许可，则供应商有义务及时向采购方给出指示。 为此，除非供应方报价中已提供该信息，否则供应方应在订单确认函和每份发票中提供相关信息：商品代码、 EC 两用品法规当前版本或出口清单第一部分（德国外贸和支付法规附件“AL”）的 AL 号（出口清单号）以及根据美国出口法规规定的 ECCN （出口控制分类号）。

16.3 经采购方要求，供应方应书面告知产品和零件方面的所有外贸数据，如第 16.1 至 16.2 部分数据有任何变化，应立即书面通知采购方。

16.4 根据 2014 年 7 月 31 日欧盟理事会第 833/2014 号法规，关于针对俄罗斯破坏乌克兰局势稳定的行动所采取的限制性措施，以及该法规不时修订的内容（以下简称“欧盟第 833/2014 号条例”）。供应方声明、陈述并保证，根据欧盟第 833/2014 号法规附件 XVII 所列、由供应方销售或交付给采购方或其任何关联公司的钢铁产品不包含欧盟第 833/2014 号法规附件 XVII 所列的原产于俄罗斯的钢铁产品。

16.5 如上述部分信息未被提供或提供有误，采购方有权在不影响其进一步向供应方索赔的权利的条件下解除合同。

17.合同解除和终止权利

17.1 采购方可在任何时候提前四周书面通知供应方终止采购订单，无需任何理由。在此情况下，供应方有权根据相应的证据获得截至终止之日按照合同提供的服务的价格，由此节省的费用必须扣除。

17.2 除了法律规定的采购方的合同解除或终止权外，如果供应方的财务状态发生或可能发生重大恶化，并因此危及到供应货物和服务的义务，则采购方有权利解除或终止合同。如果供应方被采购方的竞争对手控制的，采购方亦有权利解除或终止合同。

17.3 双方根据中国法律终止合同的权利不受影响。特别是，如果供应方、其高级职员、员工、代理人或受供应方委托营销或经销其产品的人员违反了第 16 条、18.1 条、第 18.2 条、第 18.3 条规定的人权和环境要求，或至少存在相应的、有事实依据的怀疑，则采购方有权立即终止合同，除非该违反行为可忽略不计且供应方已立即并永久性地进行了补救。

18.企业责任

18.1 供应方应承诺履行其企业责任，以确保其遵守法律规定（包括环 保、劳动和员工健康安全方面的法律法规）；在生产、销售以及服务过程中，不聘用童工，不强迫劳动。自接受订单之日起，供应方应当进一步保证不从事且不容忍任何形式的贿赂、腐败行为。采购方在此方面遵守“德瑞泰克集团的行为准则”，行为准则在德瑞泰克的网站 http://www.Driventic.com 可以查到。采购方希望供应方遵守该准则所含的规则和原则，并为确保其能够得到遵守提供支持。

18.2 供应方承诺其支付给自己员工的工资不得低于法律规定的最低工资标准，并且要求其分包商亦遵守此义务。此外，供应方有义务遵守适用于德国、欧盟和中国的出口法律规定。如果采购方提出要求，供应方应当提供其已经遵守此处义务的证据给采购方。如果因供应方未能遵守此处的义务，导致采购方因第三方索赔而承担赔偿责任或遭受罚款的，供应方应当赔偿采购方因此遭受一切损失和费用。

18.3 供应方特别承诺遵守下列人权和环境要求：

- 禁止使用童工，包括遵守国际劳工组织第 138 号公约规定的最低就业年龄，以及根据国际劳工组织第 182 号公约第 3 条禁止并立即采取行动消除最恶劣形式的童工劳动；
- 根据国际劳工组织第 29 号公约，禁止雇用人员从事强迫劳动；
- 禁止工作场所一切形式的奴役、类似奴役的做法、劳役或压迫；
- 在工作地点依法履行适用的职业健康和安全义务；
- 禁止无视结社自由；
- 禁止基于民族、人种、种族、健康状况、残疾、性取向、年龄、性别、政治观点、宗教、信仰的就业不平等待遇，除非有就业要求的正当理由；
- 禁止克扣合理工资；
- 禁止污染土壤、水、空气、有害噪音或过度用水；
- 禁止非法驱逐，禁止非法剥夺土地、森林和水域以购置、建设或其他方式使用可保障人的生计的土地、森林和水域；
- 禁止雇用或使用私人或公共安全部队保护企业项目，在此过程中使用酷刑和残忍、不人道或有辱人格的待遇，伤害生命或肢体，或无视结社和工会自由；
- 禁止上述侵权行为之外的违反义务的作为或不作为，这种作为或不作为直接能够以特别严重的方式损害受保护的法律地位，其违法性显而易见；
- 根据《水俣公约》（第 4 条第一款和附件 A 第 1 部分第 5 条第 2 款和附件 B 第 1 部分第 11 条第 3 款）的规定，禁止生产和使用汞和汞化合物以及处理汞废物；
- 根据《关于持久性有机污染物的斯德哥尔摩公约》（23.05.2001，06.05.2005）和欧盟《关于持久性有机污染物的 2021/277 号条例》（第 3 条第 1a 款和附件 A 第 6 条第 1d(i)，(ii)款）适用法律制度的规定，禁止生产和使用化学品，禁止以非无害环境的方式处理、收集、储存和处置废物；
- 《控制危险废物越境转移及其处置巴塞尔公约》（22.03.1989 和 06.05.2014）规定的以下禁令:根据第 1013/2006 号法规（EC）第 1（1）条、2 条、第 4 （1 b）、（1 c）、（5）和（8） p.1、第 4A 条和第 36 条禁止出口危险废物和其他废物；禁止从非《巴塞尔公约》缔约方进口危险废物和其他废物（第 4(5)条）。

如果采购方的人权和环境相关要求发生变化，供应方应同意对本第 18.3 条进行调整，以落实人权和环境相关要求的变化。采购方应及时以书面或文本形式将人权和环境相关要求的变更通知供应方。

供应方应当以适当的方式针对自己的分包商以及进一步在其整个供应链中落实本第 18.3 条中提及的人权和环境要求，特别是确保自己的分包商遵守这些要求，或者在存在违反人权或环境义务的情况下，通过适当的合同条款终止分包商。这还应包括，在法律允许和合理的范围内，认真努力签订协议，确保将此义务传递给其自身的供应方。

供应方进一步承诺谨慎选择其供应方，尤其是根据本第 18.3 条规定的人权和环境要求谨慎选择其供应方，并应充分调查任何违反人权和环境要求的迹象，并在选择供应方时将其考虑在内。

18.4 采购方有权通过对供应方的场地或其生产场地进行现场检查（审计权），核实第 18.3 条所述人权和环境要求的遵守情况。采购方可通过其员工、采购方委托的第三方（如律师或审计师）或使用公认的认证或审计系统行使审计权。除非存在迫在眉睫的危险，或者提前书面通知会危及、显著降低或消除审计的有效性，否则采购方应合理提前书面通知供应方进行审计。审计权原则上应在正常营业时间内在供应方的营业或生产场所行使。供应方承诺在适当的时间内，但至少在 [10] 个工作日内（“审核期”），提供采购方要求的文件、记录、供应链内的分包商名称和已知的分包商名称（“供应链文件”）供德瑞泰克检查。应采购方要求，供应方还应在审计期内自费在符合当前 IT 安全标准的合适的在线数据室中提供供应链文件，并允许采购方从其自身的营业场所进行访问。此外，供应方还将允许采购方访问其员工和管理人员，例如进行访谈以行使审计权。在采购方行使审计权时，必须遵守数据保护要求，并且在不与采购方履行法律义务相冲突的情况下，考虑保护供应方的商业秘密。

18.5 应采购方的要求，供应方应支持并促成采购方为遵守第 18.3 条中规定的人权和环境要求而进行的培训和进修，并应在法律允许的范围内指定自己的相关员工并确保其参与培训和进修。根据本第 18.5 条组织和实施培训和进修的细节应由采购方和供应方根据具体情况商定。在此过程中，应适当考虑供应方在培训课程的类型和持续时间、频率和参与者群体方面的利益，以避免给供应方造成过重的负担。培训课程的形式可以是网络培训、在线形式或面对面活动。

19. 一般条款- 一般责任

19.1 除非合同或本采购条件中另有明确约定，双方应根据适用法律的规定对对方承担责任。

19.2 供应方在采购方场所或采购方关联公司场所履行合同义务的人员，必须要遵守各场所的工作准则。针对上述人员在上述场所发生的伤亡事故，采购方无需承担责任，应由供应方自行承担全部责任。除非证明是采购方的人员或代理人故意或重大过失导致的。

19.3 供应方不得将双方的询价、订单及相关往来函件用于广告宣传的目的。只有经过采购方事先书面允许，供应方才可被允许宣传与采购方的商业关系或公开引用采购方的名称。

19.4 采购方书面同意，供应方不得将合同下的任何权利和债权转让给任何第三方。

19.5 供应方或采购方仅在其反诉合法成立或无争议时才享有抵销权和保留权。

19.6 本采购条件适用中华人民共和国法律，但不适用其法律冲突原则，《联合国国际货物销售合同公约》也不适用。

19.7 因合同和本采购条件引起的或与之相关的任何争议均应提交法院进行诉讼。双方的诉讼管辖地为采购方注册地址的管辖法院。

19.8 若本采购条件中某条款完全或部分失效时，不影响其余条款效力。合同双方应商定一个能兼顾双方利益的条款。

附件 1: 软件/硬件和/或运营技术及电气与电子系统(包括文件)的供应条件

附件 2: 在信息技术和运营技术和电气与电子系统(包括文件)范围内供货、提供服务与开发软件/硬件的条件

附件一：软件/硬件和/或运营技术及电气与电子系统（包括文件）的供应条件

德瑞泰克通用采购条件现行版本经下列条款和条件补充，适用于所有软件/硬件和/或运营技术和电气与电子系统解决方案供应，包括与信息技术/运营技术相关的文件。

本条款和条件补充适用，如有不一致，本条款和条件优先于德瑞泰克通用采购条件适用。

定义

信息技术 (IT)	信息技术包括用于处理和分发数据的计算机系统、软件和网络的开发、维护和使用；
运营技术 (OT)	运营技术包括通过对工业设备、机器、资产、流程和事件的直接监控和/或控制来检测或导致发生变化的硬件和软件；
E/E 系统	电气与电子系统
采购方数据	系指供应方或其任何分包商根据本条款和条件或与本条款和条件相关而生成、向供应方或其任何分包商提供或以其他方式被供应方或其任何分包商保留的，由采购方集团和/或其任何代表拥有、被授予许可（供应方授予许可的除外）或与之相关的所有信息和数据（包括文本、文件、图纸、图表、图像或声音），无论是人工可读形式还是机器可读形式；
安全事件	涉及与本条款和条件有关的实际或企图未经授权地访问和/或使用包含采购方数据的系统和/或未经授权地访问、使用、销毁、丢失或修改采购方数据的事件；该等事件可被归类为严重安全事件、重大安全事件或低优先级安全事件。
严重安全事件	指导致交付工作严重中断的安全事件；
重大安全事件	指导致交付工作性能下降或可能导致采购方数据或采购方或供应方使用的与本条款和条件有关的任何数据在公共领域泄露的安全事件；
低优先级安全事件	对交付工作的可用性或性能没有重大影响的安全事件；
信息资产	存有属于某一组织的信息的任何信息系统/信息技术系统
信息系统/信息技术系统	信息系统是支持某一组织运作的信息技术、流程、数字信息和用户活动的任何组合；
安全威胁	是指可能利用安全漏洞引发安全事件并可能造成危害的潜在威胁;
安全漏洞	是指可以被一个或多个安全威胁利用的信息系统的弱点；
风险评估	风险评估是指：(a) 识别与信息资产和已确认的安全威胁有关的风险，以及(b) 评估风险发生的可能性和风险发生后的影响的总体效果的过程。
安全风险	安全风险是指发生坏事对信息资产造成损害的可能性；
安全风险评估	确定与具体情况和采购方数据和/或系统安全面临的已确认的威胁有关的风险的定量或定性值；
漏洞评估	一种对计算机系统，包括相关网络、数据库和软件应用程序中的漏洞进行识别、量化和优先排序（或分级）的
	安全风险评估；
关联公司	任何控制采购方、受采购方控制或与采购方处于共同控制之下的实体。此外，采购方可在修订协议中将更多实体定义为采购方的关联公司； 控制系指公司或个人，或公司和/或个人团体，联合或一致行动，事实上或基于任何类型的协议、有表决权的证券、其他权利或其他方式，直接和/或间接地，就受控制的一家或多家实体而言： (i) 拥有其 50%或以上的注册资本或股本； (ii) 拥有其 50%或以上的表决权； (iii) 有能力任免其 50%或以上的董事（和/或管理/执行机构成员）； (iv) 实际任命了其 50%或以上的董事（和/或管理/执行机构成员）；和/或 (v) 有能力决定和/或否决其主要决定，包括管理和政策方向。
采购方集团	是指采购方及其关联公司；

1 开源软件

开源软件（"OSS"）是通常免费提供的开放源码软件，可在不限制软件再分发的许可证下使用，允许修改和衍生作品，并必须允许根据与原始软件许可证相同的条款下进行再分发（“OSS 许可证”）。OSS 许可证包括但不限于 “BSD 许可协议”（BSD）、“GNU 通用公共许可证”（GPL）和 “GNU 宽通用公共许可证”（LGPL）。著佐权许可（"著佐权"）是要求任何衍生作品或基于程序的作品只能根据原始许可证条款进行分发或传递的许可。

1.1 要求

OSS 可能被包含在供应方提供的软件中。供应方将向采购方提供关于在软件中使用 OSS 的所有信息和资料。这包括：
(i) 根据 OSS 许可证授权的所有组件的公开完整清单,
(ii) 每个 OSS 许可证的许可文本,
(iii) 版权声明,
(iv) 对所有使用的开源代码进行最先进的安全和漏洞监测的结果，以及
(v) 关于所有使用 OSS 组件的明确说明和文件。

采购方将自行决定是否给予批准。如果所提供的信息或材料虚假或不完整，所授予的批准将被撤销。
OSS 许可证文本和相应的源代码必须单独提供。在适用许可要求的范围内，供应方将提供所有开放源代码。
供应方应使采购方始终完全符合适用的 OSS 许可证的所有要求。
这些要求也适用于软件的任何更新、补丁、升级或新版本。

1.2 责任

供应方知悉其负有特殊责任，即保护采购方免受因 OSS 集成到供应方供应的软件中及采购方使用该等软件而造成的损害。 有鉴于此，供应方应特别注意确保第三方的所有权利得到证明和保证。

1.3 赔偿

对于供应方违反上述任何义务或要求而直接或间接导致的任何权利主张、损失、费用和责任，无论基于何种法理，供应方应对采购方及其关联方、雇员、董事或代理予以赔偿，为其进行抗辩，并使其免受损害。

2 软件开发生命周期

对于包含软件开发的供应，供应方应建立安全软件开发流程
(i) 采用根据公知标准（例如 IEC 62443 4-1）的安全软件开发生命周期方法。 需要认证。
(ii) 提供证据证明已确定的安全要求和相应的安全控制已设计并实施到软件中。

(iii) 确保在开发和集成过程中进行适当的安全测试，包括但不限于静态和 动态代码检查和持续漏洞评估，并在软件发布之前对发现的任何问题进行补救；以及
(iv) 允许采购方和/或其代理对开发的软件进行漏洞评估。如果采购方发现任何风险分值为“高”或“关键”的漏洞，供应方应在软件发布前采取措施降低风险。

3 漏洞管理
(i) 在漏洞评估的过程中，供应方应聘用独立和可信的漏洞评估服务，和/或配合并协助由采购方指定的独立第三方开展漏洞评估。
(ii) 供应方应每月审查供应方威胁和漏洞信息来源，以了解与供应方管理的系统相关的最新漏洞、威胁和补救措施。
(iii) 一旦发现漏洞或为防止漏洞产生，供应方应实施消除漏洞活动补救计划，并对该计划的进展进行优先排序、跟踪和监控。所有补救计划都应存档备查。对安全性有重大影响的漏洞应在可行的情况下尽快补救。对于较低和中等风险，补救的时间范围应考虑降低风险所需的成本、时间和工作。
(iv) 如果供应方未能补救任何严重或高危漏洞，应立即通知采购方，并向采购方提出必要的安全控制措施。
(v) 供应方应确保所有定制产品均包含安全参数化文件。
(vi) 作为供应方漏洞管理一部分的活动，如漏洞评估，无论其类型或目标如何，就开展补救活动所需的所有工作和时间，都将由供应方承担费用，而不会向采购方收取费用。

4 安全管理
(i) 供应方将任命一名人员（"供应方安全经理"），负责:
- 根据协议规定协调和管理安全的所有方面；以及
- 在发生安全事件时，作为代表供应方及其分包商的唯一联系人。

(ii) 如果供应方希望更换供应方安全经理，其将以书面形式通知采购方，并提供替换人员的联系方式。

附件二: 在信息技术和运营技术和电气与电子系统（包括文件）范围内供货、提供服务与开发软件/硬件的条件

德瑞泰克通用采购条款现行版本经下列条款和条件补充，适用于与信息技术 (IT) / 运营技术 (OT)（A 部分）以及软件的创建或改编或相关服务的提供（B 部分）相关所有的供货和服务。

本条款和条件补充适用，如有不一致，本条款和条件优先于德瑞泰克通用采购条件适用。

定义

信息技术 (IT)	信息技术包括用于处理和分发数据的计算机系统、软件和网络的开发、维护和使用；
运营技术 (OT)	运营技术包括通过对工业设备、机器、资产、流程和事件的直接监控和/或控制来检测或导致发生变化的硬件和软件；
E/E 系统	电气与电子系统
采购方数据	系指供应方或其任何分包商根据本条款和条件或与本条款和条件相关而生成、向供应方或其任何分包商提供或以其他方式被供应方或其任何分包商保留的，由采购方集团和/或其任何代表拥有、被授予许可（供应方授予许可的除外）或与之相关的所有信息和数据（包括文本、文件、图纸、图表、图像或声音），无论是人工可读形式还是机器可读形式；
安全事件	涉及与本条款和条件有关的实际或企图未经授权地访问和/或使用包含采购方数据的系统和/或未经授权地访问、使用、销毁、丢失或修改采购方数据的事件；该等事件可被归类为严重安全事件、重大安全事件或低优先级安全事件。
严重安全事件	指导致交付工作严重中断的安全事件；
重大安全事件	指导致交付工作性能下降或可能导致采购方数据或采购方或供应方使用的与本条款和条件有关的任何数据在公共领域泄露的安全事件；
低优先级安全事件	对交付工作的可用性或性能没有重大影响的安全事件；
个人数据	与中国《个人信息保护法》及其他相关法律法规中规定的 "个人信息 "含义相同;
信息资产	存有属于某一组织的信息的任何信息系统/信息技术系统
信息系统/信息技术系统	信息系统是支持某一组织运作的信息技术、流程、数字信息和用户活动的任何组合；
安全威胁	是指可能利用安全漏洞引发安全事件并可能造成危害的潜在威胁;
安全漏洞	是指可以被一个或多个安全威胁利用的信息系统的弱点；
风险评估	风险评估是指：(a) 识别与信息资产和已确认的安全威胁有关的风险，以及(b) 评估风险发生的可能性和风险发生后的影响的总体效果的过程；
安全风险	安全风险是指发生坏事对信息资产造成损害的可能性；
安全风险评估	确定与具体情况和采购方数据和/或系统安全面临的已确认的威胁有关的风险的定量或定性值；
漏洞评估	一种对计算机系统，包括相关网络、数据库和软件应用程序中的漏洞进行识别、量化和优先排序（或分级）的安全风险评估；
关联公司	任何控制采购方、受采购方控制或与采购方处于共同控制之下的实体。此外，采购方可在修订协议中将更多实体定义为采购方的关联公司； 控制系指公司或个人，或公司和/或个人团体，联合或一致行动，事实上或基于任何类型的协议、有表决权的证券、其他权利或其他方式，直接和/或间接地，就受控制的一家或多家实体而言： (i) 拥有其 50%或以上的注册资本或股本； (ii) 拥有其 50%或以上的表决权； (iii) 有能力任免其 50%或以上的董事（和/或管理/执行机构成员）； (iv) 实际任命了其 50%或以上的董事（和/或管理/执行机构成员）；和/或 (v) 有能力决定和/或否决其主要决定，包括管理和政策方向。
采购方集团	是指采购方及其关联公司

A 部分—对于供应方在信息技术/运营技术和电气与电子系统范围内的供货和提供服务的条件

1. 合规性和基本技术要求

供应方应按照适当数据处理的原则提供服务。这些原则包括但不限于遵守法定的数据保护和网络安全的法规，特别是中国的《个人信息保护法》、《数据安全法》和《网络安全法》，以及实施所有公认的最先进的预防措施和办法。

供应方应采取适当的技术和组织措施，确保其服务及其为提供该等服务所要求的信息技术系统的高度信息技术安全。在适用于服务和供应商提供该等服务所使用的信息技术系统的范围内，供应方应确保符合 ISO/IEC 27001：2013 的最低标准（或以后出现的该等标准的任何后续版本），或其他类似但更高安全标准的最新适用版本，如 BSI (Bundesamt für Sicherheit in der Informationstechnik) IT-Grundschutz 。如采购方要求，供应方应详细披露该等措施以及相应的概念、证书和审计报告。

2. 信息安全的培训和意识提升

供应方应定期向其雇员和受委托提供服务的第三方提供有关信息安全主题的信息，包括他们在提供服务时应承担的保证信息安全的义务。

3. 保护采购方数据免遭滥用和丢失

供应方在此承诺，将立即、有效地、符合最新技术标准地保护其接收或生成的所有采购方数据，防止未经授权的访问、修改、销毁或丢失、禁止的传输、其他禁止的处理和任何其他滥用。在保护采购方数据的过程中，供应方必须采取所有最先进的预防措施和办法，以确保数据可随时存档和修复而不会丢失。如果在持续提供服务期间，有关安全措施的最新技术标准发生变化，供应方应根据新的最新技术标准采取一切措施，保护所有采购方数据。

4. 采购方数据的所有权

采购方及其关联公司拥有并保留对其数据的所有权利、所有权和利益，供应方仅代表采购方和/或采购方的关联公司持有该等数据。

5. 信息发送时的保护

在供货和提供服务过程中，任何以实物或电子形式发送的数据，都应采用与其敏感程度相适应的方式（如挂号信、快递、电子邮件加密等）进行传输。

6. 防范恶意软件

供应方应使用最先进的测试和分析程序检查所有服务和数据载体或以电子方式（如通过电子邮件或数据传输）传输的服务，以确保该等服务在提供

或使用之前不受恶意软件（如木马、病毒、间谍软件）的危害。不得使用检测到恶意软件的数据载体，如发现采购方受到恶意软件的危害，供应方应立即通知采购方。同样的义务适用于所有形式的电子通信。

7. 服务与流程的透明度

服务不得包含任何可能危及其安全性的无书面证明支持的机制或功能。数据仅可在采购方明确书面同意的情况下自动传输给供应方或第三方。

8. 服务出现缺陷或错误时的沟通

如果供应方发现向采购方提供的服务存在可能危及采购方运行或安全的缺陷或错误，供应方应立即通知采购方。

9. 向供应方提供的硬件、软件、访问方式和访问数据的处理

采购方向供应方提供的所有硬件、软件、访问方式和访问数据的使用，供应方均应遵守采购方的使用条款。供应方应对向其提供的所有访问数据和访问方式保密，并采取最先进的措施防止第三方未经授权的访问和使用。如果为供应商提供服务之目的而向其提供的硬件、软件、访问方式和访问数据不再需要，供应商应立即将该等硬件、软件、访问方式和访问数据归还采购方。如果所提供的软件、访问方式和访问数据不可能返还，供应方应删除或卸载向其提供的软件、访问数据和访问方式，但在未联系采购方并征求其对删除/卸载的批准的情况下不得删除或卸载。此后，供应方应以书面形式向采购方确认该删除/卸载。只有在采购方事先允许的情况下，供应方才可在与提供服务有关的采购方系统和网络中使用自己的硬件和软件。

B 部分 - 提供开发的软件/硬件和/或 运营技术和电气和电子系统解决方案（包括文件）的条款和条件

1. 供应方的主要义务

供应方的主要义务是，作为服务合同的一部分，根据所提供软件说明书、相应文档（例如用户手册）和源代码（如不存在其它合同约定）所规定的规格和功能提供随时可用的软件，在每种情况下均按照当前的程序和更新状态，（下称“**合同服务**”）。

供应方应根据双方另行达成的或作为软件支持和/或软件维护协议一部分的服务标准协议，维持和保障软件的正常运行。

供应方应亲自履行合同。除非采购方事先书面通知同意第三方参与，否则不得允许第三方提供服务。

一旦合同服务完成，供应方应以书面或文本形式通知采购方，并商定一个提交工作成果的日期。供应方应给予采购方在合同服务验收前进行功能测试的机会。双方应就测试的具体细节达成一致意见。

验收工作应遵循正式程序。验收工作应出具一份双方都签字的报告。如果合同服务尚未具备验收条件，供应方保证立即纠正缺陷，并再次将服务提交采购方验收。

2. 使用权

2.1 所有权和采购方的独家使用权

供应方就作为合同一部分的软件/硬件和/或运营技术和电气和电子系统的开发所提供的服务的所有成果和中间成果的所有权，如性能说明、规格、研究、概念、文件，包括安装、使用和操作手册及维护方面的文件、源代码和进一步开发、报告、咨询文件、图表、图表、图像和预定软件、程序、改编软件（定制）和参数化，以及在此过程中产生的所有中间成果、帮助和/或其他性能成果（合称“工作成果”），若为实物，均应在上述项目交付时转移给采购方。

在其他方面，供应方在工作成果创建时，但最迟在工作成果交付时，授予采购方对工作成果的独占的、永久的、不可撤销的、可转许可的和可转让的权利。软件的运行可由采购方及其关联公司中的任何一家进行。

采购方除自己使用外，还可根据所订立的协议规定将软件提供给其关联公司供其使用，也可为这些公司使用软件。这种使用权是临时的，它应在采购方和使用软件的公司不再有任何关联关系的六个日历月后终止。

采购方可将软件的运行交由第三方公司进行（如外包或托管）。采购方应事先将此情况书面通知供应方，并应供应方要求，向其提交第三方声明，声明软件将予以保密，并仅为采购方及其关联公司之目的使用。

在保证的权利范围之外，采购方有权将软件交给第三方，以纠正错误。其有权将软件，包括书面文件，提供给第三方，用于培训采购方及其关联公司的雇员。

这些权利应不受地理区域、时间和内容的限制，对其使用和开发也不受任何限制。

这些使用权应包括所有类型的使用，特别是数据的存储、加载、执行和处理，以任何方式进行的处理，包括修正错误，也包括由第三方进行的处理，包括与供应方服务的永久组合，复制和传播的权利，表演和演示的权利，包括公开表演的权利，以及营销、修改、转换、翻译、补充和进一步开发的权利。这种使用权还应包括将来出现的新型使用形式。关于新型的使用形式，供应方应根据中国有关法律规定，就作者的任何索赔向采购方作出赔偿。

采购方可根据各自的使用情况，根据最新技术，制作备份拷贝。

采购方可打印和复印用户手册和其它信息，并将其提供给关联公司。

采购方有权对这些使用权授予免费和收费的分许可和进一步使用权，并有权将这些使用权转让给第三方，而无需获得供应方的进一步许可。

供应方应确保为其履行合同的人员将放弃下列权利：作为作者署名的权利，以及获得任何软件或其它作品（如文件、图纸和其它受知识产权保护的工作成果）原始副本的权利。

2.2 采购方的非独占使用权

供应方在此授予采购方及其关联公司一项非独占的、不可撤销的、永久性的权利，允许其使用供应方在合同开始前已经开发或使用的作品、其它受版权保护的资料和其它不受保护的技术知识（“专有技术”），以及供应方及其代理人在提供服务的过程中获得的专有技术、标准软件和开发工具（合称“**供应方的知识产权**”），与合同服务无关。这些权利不受特定地理区域的限制，是可转让的、可分许可的使用权，并应包含在约定的补偿范围内，只要是采购方及其关联公司使用供应方提供的工作成果所必要的，则无需获得供应方的进一步同意。这也包括采购方及其关联公司或第三方都有权复制、编辑和修改供应方的知识产权，但前提是上述行为是出于使用工作成果的需要。

关联公司的此项使用权为临时使用权，在采购方与使用该使用权的公司不再存在任何关联关系的六个日历月后终止。

2.3 定制服务的使用权

在供应方为采购方定制其自己的软件或第三方软件的情况下，供应方应根据第 2.1 条的规定授予采购方及其关联公司对该软件的使用权。

2.4 通知义务

在合同结束前，供应方应将工作成果开发过程中将使用的所有第三方软件、标准软件、开发工具和其他作品（如进一步开发和处理供应方的工作成果所需的所有文件），包括供应方经许可使用的材料书面通知采购方。这些，包括供应方的权利，均应在合同中列明。除非合同中另有约定，否则供应方应根据第 2.2 条的规定授予采购方对第三方软件、标准软件、开发工具和其他作品的使用权。

2.5 共同作者

在供应方的雇员或其委托代理人为共同作者的情况下，供应方保证其已从他们处获得上述第 2.1 条和第 2.2 条规定的使用权和开发权的授予权。

2.6 发明权

在工作成果包含发明性成果的情况下，如发明系由雇员完成，供应方承诺及时提出权利主张并将该发明转让给采购方。采购方有权自行决定是否以自己的名义或以其指定的第三方的名义为世界范围内的知识产权注册该等发明。供应方承诺作出任何声明并提供签名以获得、维护和保护发明，但供应方不得因此而获得任何特殊报酬。

2.7 授予更新和补充履行的权利

供应方向采购方提供的更新、升级、补充、新版本和类似以及经更新的文件（统称为“更新”）也应遵守本协议的规定。

2.8 继续使用

如果永久获得使用权，且支付了所有约定的报酬的情况下，则已授予的使用权不应因合同撤销、合同的解除、终止或以任何其他方式终止而受到影响。

3. 缺陷和性能的中断

供应方应特别注意确保合同服务不受第三方权利的限制或排除合同规定范围内的使用，并避免第三方声称授予采购方的使用权侵犯了该第三方的权利。供应方应最准确地记录其采购过程，通过与其雇员起草合同确保权利的安全转让，最大限度地谨慎地选择次级供应方，立即、深入地跟踪任何权利瑕疵的可疑情况。如果第三方提出上述索赔，一经采购方使用权受到第三方侵害的通知，供应方即应不受限制地向采购方提供相关信息和专业知识，以便澄清事实并对索赔进行抗辩。如有可能，供应方应与其次级供

应方签订能够全面履行上述义务的协议。在与第三方发生法律纠纷时，供应方应根据相应的法律程序的类型提供正确形式的证据（如以确认声明代替宣誓或提供原始文件）。

供应方还应特别注意确保合同服务符合采购方的特殊要求、规定的或约定的技术规格或其他规格，并且适合与约定的性能要求一致的计划用途。

合同服务与约定质量的任何偏差均应视为质量缺陷。如果合同服务不适用于合同中规定的用途，则上述规定同样适用。

如果一个具有使用软件通常知识水平的有知识的用户，在文档的帮助下尽合理努力仍不能操作个别功能或解决出现的问题，则该文档应被视为存在缺陷。

供应方确认，为确保采购方业务运营的正常运行，合同服务与现行程序（但至少是合同目的所需的程序）之间的顺利互动对采购方而言是最重要的。采购方已委托供应方提供合同服务，因此供应方应尽其所能确保合同服务能够在行业标准的基础上无故障地运行。供应方进一步确认，合同服务在验收时符合现行的法律要求对采购方而言是最重要的，其应特别注意确保合同服务符合要求。

质量缺陷的诉讼时效应在现行法律规定的期限内，从采购方知道或应当知道缺陷时起算。采购方发出的缺陷通知中断诉讼时效。在诉讼时效期间发生的任何缺陷，采购方应立即通知供应方。如有必要，在与采购方协商后，采购方应按要求参与分析和纠正缺陷。

3.1 补充履行

在质保期内，供应方应立即并在适当期限内纠正缺陷，同时考虑采购方的利益，并提供合同服务的改进版本，或从新提供合同服务。如果按照合同规定使用合同服务会损害第三方的权利，供应方应修改合同服务使其不侵犯受保护的权利，或获得授权使合同服务能够不受任何限制地按照合同使用，且采购方无需支付额外的费用。提供替代方案或变通方案可作为提供临时解决方案或绕过缺陷影响的短期措施。在合理的时间内完全解决缺陷之前，缺陷不被视为得到纠正。

如果供应方未能立即纠正缺陷，且由于未能立即纠正缺陷而使采购方遭受了不合理的较大的不利影响，则采购方应有权自己纠正缺陷、要求第三方纠正缺陷或采购替代品，费用由供应方承担。供应方所补偿的费用不应不成比例，且应限于供应方在其有权纠正缺陷的期限内自行纠正缺陷所应承担的金额。采购方保留法律或合同项下进一步索赔的权利。

3.2 折价，撤销

如果供应方拒绝纠正缺陷或未能成功地纠正缺陷，或允许供应方延长的期限届满后仍未找到解决缺陷的方法，则采购方有权选择减少其报酬或全部或部分撤销合同，除非其已按照第 3.1 条的规定自行纠正了缺陷。

3.3 付款的扣留与抵销

如果供应方未能履行其义务，则采购方有权扣留对合同服务的付款，直至供应方完全履行了其义务。由于供应方未能遵守其义务，采购方可从应付供应方的报酬中扣除其对供应方的索赔。

3.4 费用的补偿；赔偿

更广泛的索赔，包括有关赔偿和费用补偿的索赔，不应受到影响。

4. 开源软件

开源软件（“OSS”）是通常免费提供的开放源码软件，可在不限制软件再分发的许可证下使用，允许修改和衍生作品，并必须允许根据与原始软件许可证相同的条款下进行再分发（“OSS 许可证”）。OSS 许可证包括但不限于 “BSD 许可协议”（BSD）、“GNU 通用公共许可证（GPL）”和 “GNU 宽通用公共许可证”（LGPL）。著佐权许可（"著佐权"）是要求任何衍生作品或基于程序的作品只能根据原始许可证条款进行分发或传递的许可。

4.1 要求

只有采购方事先书面批准的情况下，OSS 才能包含在供应方提供的软件中。供应方应向采购方提供决定在软件中使用 OSS 所需的所有信息和资料。这包括：

(i) 根据 OSS 许可证授权的所有组件的公开完整清单,
(ii) 每个 OSS 许可证的许可文本,
(iii) 版权声明,
(iv) 对所有使用的开源代码进行最先进的安全和漏洞监测的结果，以及
(v) 关于 OSS 组件技术集成的明确说明和文件。

采购方将自行决定是否给予批准。如果所提供的信息或材料虚假或不完整，所授予的批准将被撤销。

OSS 许可证文本和相应的源代码必须单独提供。在适用许可要求的范围内，供应方将提供所有开放源代码。

供应方应使采购方始终完全符合适用的 OSS 许可证的所有要求。

这些要求也适用于软件的任何更新、补丁、升级或新版本。

4.2 责任

供应方知悉其负有特殊责任，即保护采购方免受因 OSS 集成到供应方供应的软件中及采购方使用该等软件而造成的损害。 有鉴于此，供应方应特别注意：

(i) 始终遵守适用的 OSS 许可证要求，并确保采购方已从集成到软件中的 OSS 的作者处获得所有必要的许可，
(ii) 具有符合行业最佳实践的开放源码合规系统，
(iii) 仅使用在兼容的开源软件许可证项下获得许可的 OSS 组件，
(iv) 未在软件中纳入任何著佐权许可，
(v) 对软件中使用的所有开放源码进行了安全风险扫描。

4.3 赔偿

对于供应方违反上述任何义务或要求而直接或间接导致的任何权利主张、损失、费用和责任，无论基于何种法理，供应方应对采购方及其关联方、雇员、董事或代理予以赔偿，为其进行抗辩，并使其免受损害。

5. 软件开发生命周期

对于包括软件开发在内的工作，供应方应：

(i) 采用根据公知标准（例如 IEC 624434-1）的安全软件开发生命周期方法。 需要认证。
(ii) 提供证据证明已确定的安全要求和相应的安全控制已设计并实施到软件中。
(iii) 确保在开发和集成过程中进行适当的安全测试，包括但不限于静态和动态代码检查和持续漏洞评估，并在软件发布之前对发现的任何问题进行补救；以及
(iv) 允许采购方和/或其代理对开发的软件进行漏洞评估。如果采购方发现任何风险分值为 “高”或 “关键”的漏洞，供应方应在软件发布前采取措施降低风险。

6. 漏洞管理

(i) 在漏洞评估的过程中，供应方应聘用独立和可信的漏洞评估服务，和/或配合并协助由采购方指定的独立第三方开展漏洞评估。
(ii) 供应方应每月审查供应方威胁和漏洞信息来源，以了解与供应方管理的系统相关的最新漏洞、威胁和补救措施。
(iv) 供应方应进行网络级和应用级漏洞评估，以确定可能缺失或无法有效保护目标免受潜在威胁的控制措施。
(v) 一旦发现漏洞或为防止漏洞产生，供应方应实施消除漏洞活动补救计划，并对该计划的进展进行优先排序、跟踪和监控。所有补救计划都应存档备查。对安全性有重大影响的漏洞应经采购方同意在可行的情况下尽快补救。对于较低和中等风险，补救的时间范围应考虑降低风险所需的成本、时间和工作。
(vi) 供应方应对补救工作完成后的所有漏洞进行再次测试，以确认风险已降低到采购方确定的可接受水平。
(vii) 供应方应及时向采购方提供以下信息：
- 由独立漏洞评估服务提供商提供的漏洞评估结果和建议的报告（原始格式）；以及
- 供应方对已识别漏洞的补救计划。

(viii) 如果供应方未能补救任何严重或高危漏洞，应立即通知采购方，并建议必要的安全控制措施，并与采购方商定必要的安全控制措施。
(ix) 供应方应确保所有应用程序、中间件、后端软件、系统和网络均以默认方式安全构建和配置。作为标准构建部署的一部分，技术组件将根据权威安全建议的来源进行配置设置，如由产品供应方（如西门子、微软）或行业组织（如 ISO、IEC、CIS、NIST、SANS、OWASP）提供的建议。
(x) 漏洞评估，无论其类型或目标如何，就开展补救活动所需的所有工作和时间，都将由供应方承担费用，而不会向采购方收取费用。

7. 安全管理

(i) 供应方将任命一名人员（"供应方安全经理"），负责：
- 根据协议规定协调和管理安全的所有方面；以及
- 在发生安全事件时，作为代表供应方及其分包商的唯一联系人。

(ii) 如果供应方希望更换供应方安全经理，其将以书面形式通知采购方，并提供替换人员的联系方式。
(iii) 如果供应方对信息技术安全的任何方面或本附件要求的执行有任何疑问，应与采购方协商。

8. 风险管理

(i) 经采购方合理要求，对于供应方与采购方的信息技术系统发生交互的情况，供应方将协助采购方进行工作的安全风险评估，该等评估可在正常工作时间的任何时间进行。

(ii) 如果安全风险评估中发现的任何问题被评为“高”或“严重”，供应方将向采购方提供一切合理的协助，以分析风险，并确定需由供应方实施的适当控制措施，以保护供应方根据本文件中详述的要求所管理或占有的采购方数据或服务。
(iii) 如果供应方拟对其提供的工作进行任何重大变更，或采购方要求对工作进行任何重大变更，供应方将进行安全风险评估。
(iv) 供应方应确保对安全风险评估中发现的任何风险进行及时补救、监控和管理，直至风险消除。供应方应随时向采购方通报安全风险评估中发现的所有风险的补救活动。

9. 人员安全

(i) 供应方应确保任何能够访问采购方数据的供应方或供应方人员已根据本协议和/或采购方的指示进行了审查和筛选。
(ii) 供应方及其分包商应确保所有供应方人员接受任何必要的培训，并知晓其在本协议安全规定方面的责任。
(iii) 供应方应实施并保持适当的控制措施，以降低供应方人员人为错误、盗窃、欺诈或滥用设施的风险。

10. 数据中心安全

(i) 供应方应实施并维护适当的物理和环境安全控制，以防止对包含采购方数据或工作提供过程中使用的任何信息的任何数据中心进行未经授权的访问、损坏和干扰。
(ii) 供应方应确保所有数据中心均通过 ISO 27001（或替代或补充 ISO 27001 的任何标准）认证。
(iii) 如果供应方拟变更适用于数据中心的任何程序或政策，而该变更可能会合理地增加任何采购方数据的安全性和完整性风险，则供应方应合理地事先向采购方发出书面通知。

11. 访问控制

(i) 供应方应确保采用适当的访问控制机制，在允许访问工作之前对所有用户（或实体）进行验证和认证，无论是来自供应方、第三方还是采购方的用户 （或实体）。
(ii) 所有访问或请求访问工作的用户（或实体）均应作为规定的访问管理 流程的一部分进行供应、管理和授权。
(iii) 供应方应使用至少支持用户名和密码组合的认证方法，其中用户名和密码是唯一的，不得重新分配，也不得由一组用户共享。如果是管理账户，供应方应要求提供额外的验证因素。
(iv) 供应方应要求所有从较低权限级别过渡到较高或敏感权限级别的用户重新进行身份验证。
(v) 供应方应使用适当的控制措施，在存储和传输过程中保护密码和其他访问凭证。供应方不得以明文形式传输或存储密码，登录时也不得在系统上明显地显示密码。
(vi) 供应方不得在脚本或明文文件（如 shell 脚本、批量配置文件和连接字符串）中硬编码用户名和密码。

12. 网络安全

(i) 供应方应在供应方（或分包商）直接控制的网络环境中管理采购方数据的传输。应管理和保护网络免受外部威胁，包括但不限于在物理、网络和应用层面进行访问控制，仅允许供应方合法授权的人员访问采购方数据。网络应予以隔离，拒绝来自公共或不受信任的网络的访问，包括属于第三方的网络，供应方未与该等第三方签订与本条款和条件中的条款等同的合同，也未与该等第三方签订单独的数据处理协议（DPA）。
(ii) 供应方应确保系统定期及时更新最新的相关安全软件，以及来自其他供应方提供系统的预先测试和授权的安全软件补丁和修补程序。供应方应每月进行漏洞评估，以评估系统的配置和软件补丁状态。
(iii) 供应方应确保所有采购方网络与供应方网络连接，在通过不信任网络（如互联网）传输任何被列为 “机密” 的采购方数据时，都是通过符合采购方安全政策或 ISO 或 NIST 等已公布标准的加密网络链接进行的。
(iv) 供应方应确保生成可审计事件，包括但不限于安全特定事件、所有成功和失败的网络访问尝试，并保存网络安全配置所有变更的日志。
(v) 供应方应建立、实施和管理程序以及安全信息和事件管理 (SIEM) 系统，以监控网络安全，防止可疑入侵或未经授权访问。
(vi) 供应方应确保用于执行安全监控的流程和控制措施的实施方式能够维护所收集的安全监控相关事件的完整性、保密性和可用性。
(vii) 供应方应保持任何开发和测试环境与生产环境的隔离。任何包含个人数据的实时采购方数据在用于测试前均应匿名化（即转换为无法识别个人身份或无法重建数据以方便识别的形式），并获得采购方的明确书面批准。
(viii) 如果供应方的系统或网络与采购方网络连接，供应方的系统或网络必须遵守采购方的安全政策。

13. 分包商和第三方

(i) 在雇用分包商时，供应方应促使分包商同意本文件中包含的有关信息技术/运营技术和电气和电子系统安全的相同条款和条件，以直接惠及采购方，并在必要时签订单独的数据处理协议 (DPA)，如果采购方和供应方已签订数据处理协议 (DPA)，则其主要认为有必要。
(ii) 应采购方要求，供应方应核实并提供书面报告，详细说明其分包商遵守本条款和条件文件规定的分包商安全义务的情况。
(iii) 如果供应方为向采购方交付工作而雇佣第三方，供应方应

a) 利用技术和流程对所有第三方系统进行验证，以确保不可抵赖性；
b) 实施控制措施，保护供应方的网络，防止：
    1) 第三方网络和供应方网络之间未经授权的访问；
    2) 第三方网络和任何互联网接入点之间未经授权的访问；以及
    3) 第三方网络和与供应方网络连接的其他第三方网络之间未经授权的访问；
c) 将与第三方网络的所有入站和出站连接限制在特定主机和端口上，并将在这些主机上的工作限制在满足采购方需求所需的最低限度；
d) 如果采购方提出要求，将工作范围的所有变更（包括防火墙规则变更）告知采购方;
e) 保留一份可访问供应方网络的所有人员的名单，并每月审查该名单；
f) 记录所有成功和失败的第三方访问，并在需要时提供给采购方审查；
g) 立即通知采购方任何安全漏洞，包括实际或怀疑未经授权访问或破坏任何系统，并根据本条款和条件采取补救措施；以及
h) 每年或在连接和访问控制要求发生变化时审查所有第三方网络连接，并终止任何过时或不需要的第三方连接。

(iv) 供应方应对其分包商的任何失职行为负责，其责任范围与供应方对其自身失职行为负责的范围相同。

14. 安全事故管理

(i) 供应方应始终监控和验证对采购方数据的所有访问均已获得授权，并检查任何安全事件。
(ii) 如果发生采购方认定的严重安全事件或重大安全事件，供应方应

a) 在安全事件发生后四小时内通知采购方（包括在必要时升级通知）；
b) 根据安全服务级别和安全事件响应计划中规定的程序，立即以适当方式对此类事件做出响应；以及
c) 立即协助采购方和/或采购方代表进行调查，并保留与任何此类调查有关的所有文件。

(iii) 未经采购方书面授权，供应方不得向第三方披露安全事件或弱点的细节。
(iv) 供应方应在调查安全事件时使用取证程序收集和保护证据，确保监管链，并在必要时遵守监管要求。
(v) 供应方应根据《采购方数据分类政策》将所有安全事故报告归类为 "机密"， 并确保采取适当控制措施保护该信息。
(vi) 发生安全事故时，供应方应提供安全事故报告。此类报告应包括但不限于：

a) 事件的来源和目的地，以及事件的时间、日期和类型；
b) 严重程度加权（低优先级、重大或严重安全事件）；
c) 每起安全事件的根源分析报告；以及
d) 用于追踪的单独参考编号。

(vii) 发生安全事件后，或应采购方要求，供应方应启动纠正措施，以尽量减少和 防止今后发生与工作范围有关的安全事件。
(viii) 供应方应针对导致信息丢失或损坏的安全事件启动备份和恢复程序。

15. 安全审计

(i) 供应方应允许采购方和/或采购方指定的任何外部审计人员（在供应方正常工 作时间内）进入和访问供应方的办公场所和/或记录，以进行以下工作：

a) 审查采购方数据和/或工作范围的完整性、保密性和安全性；
b) 确保供应方遵守本条款和条件；或
c) 对包含采购方数据的任何系统进行漏洞评估。

(ii) 在本协议有效期内，采购方有权在任何日历年根据第(i)款进行一次审计，但如果采购方有理由怀疑供应方严重违反本条款和条件，则采购方有权随时进行审计。
(iii) 如果对与 IT/OT & E/E 系统安全和/或供应方或其任何分包商提供的工 作有关的涉嫌欺诈或犯罪活动进行调查，供应方应允许采购方、采购方的任何法定或监管审计人员及其各自授权的代理人迅速进入和访问供应方的场所和记录以进行审计，且供应方应在协议期间或其后任何时间为进行该等调查提供一切必要协助。
(iv) 各方应自行承担因行使其权利或履行其义务而产生的成本和费用。
(v) 供应方应并将促使其分包商向采购方（和/或其代理人或代表）提供以下内容：

a) 采购方在任何审计的许可范围内要求的所有信息；
b) 为审计之目的，进入由供应方控制的任何地点或数据中心，且采购方拥有的任何设备将被用于执行工作；
c) 审计之目的访问供应方信息系统中保存的记录；以及
d) 为审计之目的接触供应方和供应方人员。