**服务等级协议（SLA）**

**数据存储持久性**

数据可靠性应不低于 99.99999%,云平台应按照等保三级标准建设并通过测评。

**数据可销毁性**

确保系统在新环境运行稳定后，关停原服务，并对原有系统数据进行安全擦除。采用反复填零的方式多次写入数据到磁盘上，以覆盖原始数据，通常使用随机数据或固定数据模式进行多次覆盖，在完成擦除后，进行数据恢复测试，以确保之前的数据不可恢复。

**数据可迁移性**

在信息系统迁移和交接工作中，乙方应在甲方提出系统迁出需求后 45 天内配合甲方完成信息系统迁移的相关工作，包含梳理迁出系统的云资源、安全策略配置等。

**数据私密性**

因承接本协议约定项目所知悉的该项目信息或甲方信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为甲方的保密信息，乙方应按 照《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施 办法》及甲方关于保密工作的相关要求，对上述保密信息承担保密义务。未经甲方书面同意，乙方不得将甲方保密信息透露给任何第三方。并通过访问控制、身份验证、数据隔离、安全审计和监控保障用户数据隐私。

访问控制：根据用户角色和权限限制用户对数据和服务的访问权限，确保只有授权用户能够访问敏感数据。

身份验证：通过多种方式确认用户身份，增加安全性。

数据隔离：虚拟化和容器化技术：使用虚拟机或容器来隔离不同用户的应用和数据，防止跨用户数据泄露。专用虚机和专用主机：为某些用户提供专门的虚机或主机，确保数据在物理层面上得到隔离。

安全审计：记录用户操作和系统事件，以便发现异常行为或安全威胁。

实时监控：对系统和网络进行实时监控，及时发现潜在的安全问题并进行响应。

任何时间内，一经甲方提出要求，乙方应按照甲方指示在收到甲方书面 通知后5日内将含有保密信息的所有文件或其他资料归还甲方，且不得擅自复制留存。

**数据知情权**

用户数据存储于北京市政务云数据中心，数据备份情况、数据中心符合当地法律、除政府监管部门监管审计需要外，未经客户同意，用户所有数据不会提供给任意第三方。用户所有数据不会存在国外数据中心或用于国外业务以及数据分析。用户数据所在的数据中心均遵守当地数据中心相关的法律。

**数据可审查性**

按照《关于加强党政部门云计算服务网络安全管理的意见》(中网办发文[2015]14号)的要求和有关网络安全标准，落实并通过所建设的云平台的第三方网络安全审查。

为甲方提供的服务质量应符合国家有关质量法规、质量标准的规定及相关行业的标准。

**服务功能**

为甲方提供本协议约定的全部服务，协助甲方开展信息系统部署迁移工作，做好云主机等云资源或云服务的运维工作。

包括计算服务、存储服务、网络服务、云主机深度监控服务、基础软件支撑服务、安全服务、安全检测监测审计服务、其他。

**服务可用性**

提供的云平台整体可用性应不低于99.99%。

**服务资源调配能力**

提供的云平台应具备资源动态调整机制，根据甲方信息系统运行情况进行资源的动态调整。如遇信息系统使用高峰期，经双方协商可短期内提供免费的云资源扩容服务，如需要长期使用扩容服务，以北京市级政务云基础服务目录价格为准双方协商费用，并签订补充协议

**故障恢复能力**

具备故障快速定位和恢复能力，故障定位排除时限不超过30分钟，重要信息系统故障定位排除时限不超过10分钟。

**网络接入性能**

负责管理客户申请的IP地址，为甲方提供IP地址分配和管理服务。

**服务计量准确性**

按照北京市级政务云服务目录收取服务费，按照市级政务云要求及标准提供政务云服务。

**服务变更、中止条款**

1、在运营期间，如发生附件1中所列A 级事件1 次，甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

2、在运营期间，如发生附件1所列B 级事件2次，甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

3、乙方提供服务过程中可能发生的违约行为及相应应承担的违约金详见附件2、3，违约金的支付从尾款中抵扣，如尾款不足支付则由乙方另行支付甲方。 系同一事件或原因导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，经甲乙双方协商，择其重者确定乙方支付违约金的办法。

4、在运营期间出现下列情况，甲方向乙方提出整改要求和期限，且乙方在规定期限内未能履行甲方正当要求的，甲方有权与乙方终止协议：

(1)多次在云综合监管服务商已发出整改通知后未正确处置，出现问题并造成B级及以上事故；

(2)重大活动期间所承诺的骨干人员和管理人员未到场；

(3)连续2个月所承诺的运维服务人员人数未达到协议要求。

**服务赔偿条款**

1、在运营期间，如发生附件1中所列A 级事件1 次，甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

2、在运营期间，如发生附件1所列B 级事件2次，甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

3、乙方提供服务过程中可能发生的违约行为及相应应承担的违约金详见附件

2、3 规定，违约金的支付从尾款中抵扣，如尾款不足支付则由乙方另行支付甲方。系同一事件或原因导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，经甲乙双方协商，择其重者确定乙方支付违约金的办法。

4、在运营期间出现下列情况，甲方向乙方提出整改要求和期限，且乙方在规 定期限内未能履行甲方正当要求的，甲方有权与乙方终止协议：

(1)多次在云综合监管服务商已发出整改通知后未正确处置，出现问题并造 成B 级及以上事故；

(2)重大活动期间所承诺的骨干人员和管理人员未到场；

(3)连续2个月所承诺的运维服务人员人数未达到协议要求。

**用户约束条款**

1、甲方有权对乙方提供的各项服务进行监督、检查和评价。

2、甲方应提出有关管理、技术需求和要求，协调乙方与信息系统服务商的关 系，协调信息系统服务商配合调研、迁移、运维、安全和应急演练等过程的工作。

3、甲方需按照《北京市市级政务云管理办法》的要求申请、变更、退出云服 务；在系统入云、上线、服务变更、退出等关键节点，甲方应提前提交《北京市市 级政务云服务统一工单》相应部分内容至政务云管理单位进行备案作为工作依据。甲 方应按本协议约定使用乙方提供的云资源，做到资源专用，协议未约定或未提交《北京市市级政务云服务统一工单》至政务云管理单位备案的信息系统不得部署入云。

4、甲方如需对已上线信息系统进行维护升级、渗透测试、安全加固等操作，应 提前告知乙方。

6、甲方有权要求乙方现场技术指导、处理故障及其他服务。

7、乙方须按照协议所约定的服务内容标准向甲方提供相关资源和服务。

8、乙方应协助甲方建立健全信息系统管理配套制度，包括：运维制度、应急 预案、安全保障制度、运行监管办法等。

9、乙方负责云平台基础安全保障和运维工作。

10、乙方应负责本单位人员的安全培训、技术培训，确保工作人员符合岗位要 求。

11、乙方需按照有关规定进行操作，确保各系统不被人为损坏。

12、乙方负责提供资源调度管理和维护，提供云主机状态监控，对甲方所购买 使用的资源提供运维服务，未经授权不得擅自修改信息系统数据或发布信息等。

13、乙方负责管理甲方申请的 IP地址，为甲方提供IP地址分配和管理服务。

14、信息系统正式上线后，乙方需定期向甲方提供政务云服务报告，以便甲 方及时获取政务云资源或服务的使用情况。

15、甲方如需乙方提供重启服务器操作时，乙方有权要求甲方提供书面申请。除 本款约定外，乙方原则上不接受甲方提出的其他可能对甲方服务器造成损坏的任何操作要求。

16、乙方应提供技术支持服务，以维护甲方系统的正常运行。

17、重大活动期间，乙方应配合甲方制定重保方案并提供云平台的现场值守等 服务。

18、乙方应配合甲方制定信息系统应急预案，并配合开展信息系统应急演练工 作，做好日常应急响应工作。

19、乙方接到甲方故障报告后，应及时做好相关信息的登记工作，并进行故 障排查。乙方应定时向甲方反馈检查进度及结果，故障排除后，乙方应将结果及时 反馈甲方并做好书面报告和故障记录。

20、由于甲方指定的其他技术服务提供商提供的软件或产品的缺陷，造成的 信息系统运行故障、安全漏洞、信息泄露等事故，乙方需要配合甲方进行整改。

21、当甲方入云信息系统出现严重影响政务云平台安全稳定运行的事件时，乙方有权暂时中断甲方的云服务并书面通知甲方，事件处理完毕后恢复服务。

22、乙方应保证为甲方提供具备本合同项下服务所需的相应资质和许可。乙 方应保证技术服务人员在甲方工作过程中人员相对稳定。

23、乙方工作人员未经甲方授权，擅自篡改甲方业务数据，或利用甲方现有 业务应用系统、网络平台或者冒用甲方身份获取非法利益，造成甲方或任何第三 方损失的，由乙方承担法律责任并负责赔偿相应损失。

24、乙方保证其向甲方提供的服务不存在任何侵犯第三方著作权、商标权、 专利权等合法权益的情形，否则乙方应赔偿因此给甲方造成的全部损失。

25、未经甲方同意，乙方不得擅自部分或全部转委托。

**服务商免责条款**

1、协议中不可抗力指地震、台风、火灾、水灾、战争、罢工以及其他双 方共同认同的不能预见、不能避免并不能克服的客观情况。

2、由于网络运营商的核心设备故障造成的网络中断、阻塞，从而影响到系 统的正常访问或响应速率降低，属于不可控事件和不可抗力，甲方应对此表示认同。

3、由于不可抗力致使协议无法履行的，受不可抗力影响一方应立即将不能 履行本协议的事实书面通知对方，并在不可抗力发生之日起15天内提供相关政 府部门或公证机关出具的证明文件。

4、由于不可抗力致使协议无法履行的，本协议在不可抗力影响范围及其持 续期间内将中止履行，本协议执行时间可根据中止的时间相应顺延，双方无须承 担违约责任。不可抗力事件消除后，双方应就协议的履行及后续问题进行协商， 按照该事件对协议履行的影响程度，决定继续履行协议或终止协议。

**附件1**

**重大违约行为表**

违约金=合同金额\*100%

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **类别** | | **范围** | **影响** | **影响时间** | **事件** **级别** | **次数** |
| 重 大  安 全  事 故 (云服 务商主责) | 服务中断 | 云平台整体 | 因非不可抗力造成重要信息 系统中断或影响人数5万以上或导致50万元以上经济损失。 | 2小时以上 | A级 | 1次 |
| 重大篡  改事件 | 信息系统 | 在重大或特别重大保障期间， 因云服务商的安全隐患原因 造成的系统被恶意篡改事件。  事件发生后云服务商未及时 进行处置，造成信息安全事件 处置延误。 | 3 0 分 钟 以上 |
| 数据丢失 | 等保三级或  重要信息系统的核心业务数据 | 因非不可抗力造成重要信息 系统丢失数据，且确认无法恢 复。 | —— |
| 恶意入  侵攻击 | 等保三级或  重要信息系统 | 被第三方安全机构通报云平  台存在安全隐患，云服务商未  在4小时内做有效处置或应急防护措施，造成信息系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。 | —— |
| 服务中 断 | 云平台整体 | 因非不可抗力造成信息系统 中断或影响人数1万以上或 导致10万元以上经济损失。 | 2小时以上 | B级 | 2 次  2次 |
| 重大篡  改事件 | 信息系统 | 因云服务商的安全隐患原因 造成的系统被恶意篡改事件，  事件发生后云服务商未及时 进行处置，造成信息安全事件 处置延误。 | 30分钟以上 |
| 数据丢失 | 信息系统核  心业务数据 | 因非不可抗力造成信息系统 丢失数据，且确认无法恢复。 | —— |
|  | 恶意入侵攻击 | 信息系统 | 被第三方安全机构通报云平台存在安全隐患，云服务商未在24小时内做有效处置或应急防护措施，造成信息系统被恶意篡改或敏感信息泄露事件。 | —— |  |  |

**附件2**

**严重违约行为表**

违约金=信息系统云服务费/服务月数\*系数

|  |  |  |
| --- | --- | --- |
| **序号** | **问题描述** | **惩罚系数** |
| 1 | 所提供的云服务可用性低于99.99%,或数据可用性低于99.9999%, 出现问题并造成重大损失的 | 200% |
| 2 | 因未做好系统和数据互备，由于另一家云服务商服务中断，而导致系统和数据无法正常应用的，但影响未达到B级及以上事故影响的 | 200% |
| 3 | 因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响 | 600% |
| 4 | 因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响 | 600% |
| 5 | 因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响 | 600% |
| 6 | 在云安全监管服务商已发出整改通知后未正确处置，出现问题并造成 重大事故 | 200% |
| 7 | 平均响应时间大于15分钟且小于30分钟，造成重大事故 | 200% |
| 8 | 运维需求平均响应时间大于30分钟且小于60分钟，造成重大事故 | 200% |
| 9 | 运维需求平均故障恢复时间大于30分钟且小于60分钟，造成重大影响 | 100% |
| 10 | 运维需求平均故障恢复时间大于60分钟且小于120分钟，造成重大影响 | 200% |
| 11 | 现场无人值守超过大于1小时且小于2小时，造成重大事故 | 100% |
| 12 | 现场无人值守超过大于2小时且小于4小时，造成重大事故 | 200% |

**附件3**

**一般违约行为表**

违约金=信息系统云服务费/服务月数\*系数

|  |  |  |
| --- | --- | --- |
| **序号** | **问题描述** | **惩罚系数** |
| 1 | 所提供的云服务可用性达不到99.99%,或数据可用性低于99.9999%, 出现问题但未造成重大损失的 | 50% |
| 2 | 所提供的云服务可用性达不到99.99%,或数据可用性低于99.9999%, 且在服务期内接到用户投诉此类情况3次以上的 | 20% |
| 3 | 在运营期间，甲方对乙方实施月度考核，如乙方连续3次未能通过考核，经限期整改后仍不能达到甲方要求的 | 20% |
| 4 | 在运营期内，如乙方未能按照用户方的扩容需求，在7个自然日内完 成云平台的资源扩容，且经管理单位书面通知仍未能限期满足用户需求 的 | 20% |
| 5 | 因所提供的云服务或安全服务出现故障，造成某系统宕机2小时以上 | 30% |
| 6 | 因所提供的云服务或安全服务出现故障，造成某系统连续宕机3次以上或累计8小时以上 | 60% |
| 7 | 在云安全监管服务商已发出整改通知后未正确处置，出现问题的，未造 成重大影响 | 50% |
| 8 | 运维需求平均响应时间大于15分钟且小于30分钟，出现问题但未造成重大影响 | 30% |
| 9 | 运维需求平均响应时间大于30分钟且小于60分钟，出现问题但未造成重大影响 | 50% |
| 10 | 运维需求平均故障恢复时间大于30分钟且小于60分钟，出现问题但未造成重大影响 | 30% |
| 11 | 运维需求平均故障恢复时间大于60分钟且小于120分钟，出现问题但未造成重大影响 | 50% |
| 12 | 现场无人值守超过大于1小时且小于2小时，出现问题但未造成重大影响 | 30% |
| 13 | 现场无人值守超过大于2小时且小于4小时，出现问题但米造成重大影响 | 50% |