山东省计算中心（国家超级计算济南中心）

云平台使用网络安全责任承诺书

为贯彻落实《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》以及网络安全等级保护要求等相关法律法规、文件规定的要求，进一步加强和优化山河平台网络安全防护工作，山东省计算中心（国家超级计算济南中心）（以下简称“中心”） 按照 “谁使用谁负责”的原则，制定网络安全责任承诺书，提高网络安全责任意识，推进安全问题整改进度，强化业务应用运行环境安全。

**一、 网络安全责任主体**

对于部署在中心的对外应用或使用中心的资源，包含但不限于服务器、虚拟机、网络设备、公网IP、端口服务、网络链路等，均需明确网络安全责任人，如不明确，中心有权调整业务应用的保障级别或停止相关服务。

（1）本次网络安全责任承诺主体为：XXXXX

（2）涉及项目或应用为：XXXXX

（3）涉及资源：见附件一

**二．工作要求**

网络安全负责人需明确并承诺以下网络安全工作要求涉及的内容：

1.业务应用自身安全防护措施参照网络安全法、个人信息保护法、数据安全法以及网络安全等级保护要求等相关法律法规、文件规定的要求，在前期建设时完成底层代码、业务逻辑、数据交互等与业务密切相关模块安全防护措施。

2.业务应用在正式上线前按照“先检测，后上线，有漏洞，先修复”的原则开展工作。开展上线前安全检测的业务应用或信息系统为当前交付进度下的最终交付版，非临时测试或应付上线检测的版本。原则上提供用户名密码用于深度测试，且在测试过程中不采用针对性拦截措施。

3.业务应用在正式上线后如存在架构或模块的调整、优化、更新等变更操作，及时告知服务对接人，上报变更内容，并进入变更后安全检测环节。变更后安全检测环节与上线前安全检测环节要求一致。

4.业务应用如进入废弃消亡阶段，及时告知服务对接人，提交与业务应用或信息系统相关资产的明确废弃范围，同时确认废弃时间以及废弃处理方式。

**三.责任承诺**

对于可能存在的网络安全隐患，已经发生的网络安全事件，或者是已被主管单位下发的安全通报，网络安全负责人须需明确并承诺以下内容：

1.业务应用系统在正式上线前，须完成上线前检测工作已发现安全问题的整改处置，否则中心有权限暂缓或拒绝上线工作流程的推进。

2.对于因本应用已发现但未整改的安全问题所造成的安全事件或负面影响，以及相关的业务损失，均由网络安全负责人承担。

3.业务应用的安全隐患或安全问题，由网络安全负责人协调相关人员进行整改处置，中心仅提供整改建议，协助配合整改。

4.如未及时告知业务应用系统的变更而引发的安全漏洞、安全事件、安全通报，均由网络安全负责人负责，包括安全问题处置、应对监管单位、面向领导汇报等内容。

5.对于中心监测检测发现的安全问题，网络安全负责人须协调相关人员在期限内完成整改处置。如未完成整改，中心有权关闭业务对外开放的访问策略，并且不再承担其他业务支持。

附件一：

XXX VPC 相关信息如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | VPC IP | 公网 IP | VPC承载或开放服务 |
| 1 |  |  |  |

XXX服务器相关信息如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务器IP | 公网 IP | 服务器承载或开放服务 |
| 1 |  |  |  |

对于以上安全责任问题，我（我单位）充分理解并承诺遵守中心网络安全工作要求，及时整改处置已存在的网络安全问题，积极践行“积极防御、综合防范、强化管理、安全第一”的工作原则。

承诺人/承诺单位（章）：

联系方式：

年 月 日