ICS 35.040
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术
政府网站云计算服务安全指南

Information security techniques -

Security guide of government website cloud computing services

（征求意见稿）

（本稿完成日期：2017 年 8 月 21 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：西安未来国际信息股份有限公司、阿里云计算有限公司、中国电子技术标准化研究院、北京信息安全测评中心、华为技术有限公司、杭州安恒信息技术有限公司、北京安信天行科技有限公司、北京京东尚科信息技术有限公司、国家信息技术安全研究中心、深信服科技股份有限公司、北京时代远景信息技术研究院、中国电信集团公司、烽火科技集团有限公司、杭州迪普科技股份有限公司、广州赛宝认证中心服务有限公司、首都之窗、西北大学。

本标准主要起草人：叶润国、张磊、张辉、冯超、杨潇、王丽、陈雪秀、周俊、刘俊河、钟金鑫、李媛、耿涛、周立勇、刘国伟、江舟、孙骞。

引　言

在大力推动政府网站选择云服务的背景下，云计算受到广泛的关注。在云计算环境下，传统的信息安全问题大多依然存在，同时还出现了一些新的安全风险。为了管控政府部门采用云计算的安全风险，国家出台了相关的政策和标准，但是尚未制定一个标准从云服务客户的角度来指导规范政府网站采用云计算服务的工作流程，并规范相应的安全职责和管理措施。

本标准清晰地描述了政府网站采用云计算服务中各种参与角色的安全职责，重点描述了云服务客户的安全职责，可用于指导政府机构采用云计算服务保障其网站的安全。

信息安全技术　政府网站云计算服务安全指南

1　范围

本标准规定了政府网站采用云计算服务过程中涉及到的云服务客户、云服务商、云客户供应链服务商和第三方评估机构四个角色及其安全职责，并明确了政府网站在采用云计算服务时，在规划准备、部署迁移、运行管理、退出服务等阶段应采取的安全技术和管理措施，为政府网站采用云计算服务提供指导。

本标准适用于建成的政府网站采用云计算服务，对于新建政府网站采用云计算服务可参照使用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/Z 20985-2007　信息安全技术　信息安全事件管理指南

GB/Z 20986-2007　信息安全技术　信息安全事件分类分级指南

GB/T 22240-2008　信息安全技术　信息系统安全等级保护定级指南

GB/T 25069-2010　信息安全技术　术语

GB/T 31167-2014　信息安全技术　云计算服务安全指南

GB/T 31168-2014　信息安全技术　云计算服务安全能力要求

GB/T 31506-2015　信息安全技术　政府门户网站系统安全技术指南

GB/T 32400-2015　信息安全技术　云计算概览与词汇

3　术语和定义

GB/T 31167-2014、GB/T 25069-2010 界定的及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 31167—2014 中的某些术语和定义。

3.1

云服务客户 cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31167—2014，定义 3.4]

3.2

云服务商　cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的基础设施及软件，通过网络交付云计算的资源。

[GB/T 31167—2014，定义 3.3]

3.3

云计算环境 cloud computing environment

云服务商提供的云计算平台及客户在云计算平台之上部署的软件及相关组件的集合。

[GB/T 31167－2014，定义 3.8]

3.4

云客户供应链服务商 cloud customer supply chain service provider

独立于云服务商为云服务客户提供服务的服务提供商。

注：包括网站开发商、系统集成商、安全服务商等。

3.5

政府网站 government website

政府机构对外发布政务信息、提供在线服务、开展互动交流等而建立的网站，包括为用户提供展示和交互功能的页面及生成和处理页面的应用程序、中间件等。

3.6

第三方评估机构 Third Party Assessment Organizations（3PAO）

独立于云计算服务相关方的专业评估机构。

[GB/T 31167—2014，定义 3.5]

4 缩略语

下列缩略语适用于本文件。

3PAO	Third Party Assessment Organization
APT	Advanced Persistent Threat
SQL	Structured Query Language
DDoS	Distributed Denial of Service

5 概述

5.1 安全风险

5.1.1 采用云计算服务面临的安全风险

a) 客户对数据控制管理能力减弱。在云计算环境里，政府客户将自己的网站系统迁移到云服务商的云计算平台上，失去了对这些数据和业务系统的直接控制能力，增加了客户数据和业务的风险。

b) 安全责任难以界定。在云计算模式下，云计算平台的管理和运行主体与数据安全的责任主体不同，相互之间的责任如何界定，缺乏明确的规定。服务模式和部署模式的多样性、云计算环境的复杂性也增加了划分云服务商与客户之间责任的难度。

c) 可能产生司法管辖问题。在云计算环境里，数据的实际存储位置往往不受客户控制，客户的数据可能存储在境外数据中心，改变了数据和业务的司法管辖关系。

d) 数据保护更加困难。云服务商可能会使用其他云服务商的服务，使云计算平台复杂且动态变化。随着复杂性的增加，云计算平台实施有效的数据保护措施更加困难，客户数据被未授权访问、

篡改、泄露和丢失的风险增大。

e) 容易产生对云服务商的过度依赖。云计算平台间的互操作和移植比较困难，客户数据和业务迁移到云计算平台后容易形成对云服务商的过度依赖。

f) 可管理性较弱。云服务商可能未能提供与云服务客户预期一致的管理能力，对于按需供给的服务能力的监管较弱。

5.1.2 迁移过程中的安全风险

a) 系统不一致。网站系统作为一套信息系统，由很多软硬件组成，且各组件之间关系复杂，迁移过程中存在漏迁、错迁的风险。

b) 数据不一致。网站系统作为在线系统，包含大量业务数据并动态增加，迁移过程中存在数据迁移不完整、错误等风险。

c) 配置不一致。政府网站系统的管理及安全配置在迁移过程中存在配置意外变更、配置错误等风险。

d) 软件不兼容。网站系统在原有环境下运行正常，迁移到新的云环境下，系统原有的组成软件在云环境下存在无法安装使用或运行不稳定的风险。

e) 安全防护能力被削弱。云环境下安全防护体系发生变化，有的安全措施无法在云环境下实施，存在迁移后安全防护能力被削弱的风险。

f) 回退机制失效。政府网站系统在迁移前制定的回退机制可能存在错误、遗漏等问题，导致迁移过程中回退时失败的风险。

g) 网站切换失败。政府网站迁移至云平台后，在新旧网站进行业务切换时，存在因域名切换失败、系统异常等问题，导致切换失败的风险。

5.2 安全目的

政府网站采用云计算服务，可根据自身网站的实际安全需求采用不同的服务模式，并且在云服务商提供的基础安全保障上，结合云客户供应链服务商提供的安全服务，来有效降低网站面临的安全风险，实现以下安全目的：

a) 提升政府网站的管理能力，降低管理不当造成的安全风险；

b) 强化安全管控措施，提升政府网站安全保障能力；

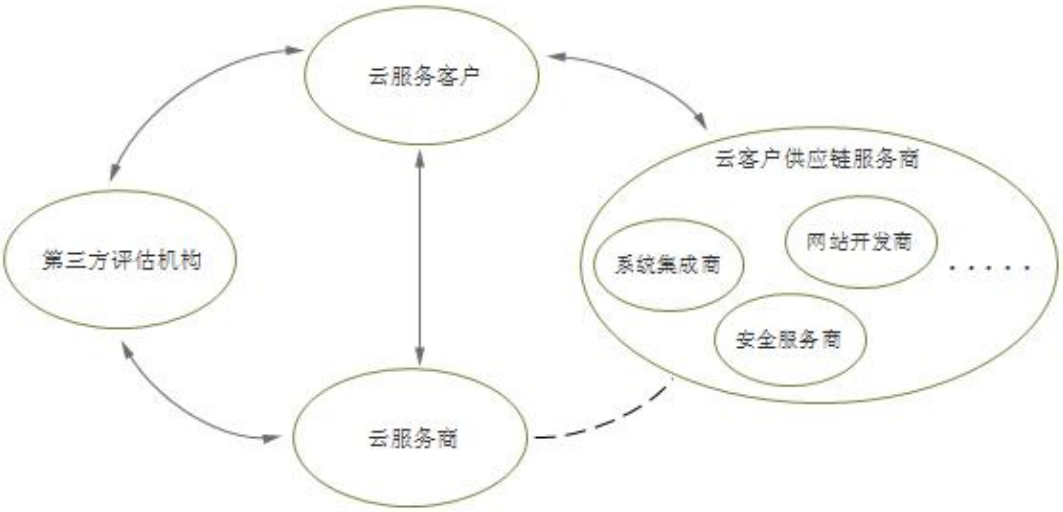
c) 具备对安全事件的预判和感知能力；

d) 具备对较为充足的服务资源能够快速响应服务需求的能力；

e) 具备识别黑客渗透/社会工程/APT 攻击，并具备快速应急响应的能力。

5.3 安全角色

云服务客户采购和使用云计算服务的过程可分为规划准备、部署迁移、运行管理、退出服务四个阶段，参与这四个阶段的云计算服务的主要角色及关系如下：



图例	
⬭	安全角色
↔	直接关系
----	间接关系

图1：角色与关系

云服务客户在本指南中即政府网站的所属方或运营单位。

云服务商是为云服务客户提供云计算产品与服务的专业机构，通常为法人企业或企业联合，并具备系统服务相关资质。在云服务客户采用云计算服务时，云服务商亦可承担云客户供应链服务商的角色和职责。

云客户供应链服务商是对云服务客户提供有偿服务的服务提供商，可提供但不限于网站开发、网站迁移、网站部署、安全保障等服务，具体可分为网站开发商、系统集成商、安全服务商等。

a） 网站开发商是对云服务客户提供入云网站开发的服务提供商，负责网站的系统架构、web 安全功能设计、代码实现及源代码安全、软件部署安全等。

b） 系统集成商指为云服务客户提供系统集成，可对入云的政府网站提供网站建设、迁移、运维服务等。

c） 安全服务商为政府网站提供安全保障的服务提供商，可提供安全咨询、网站安全建设规划、网站安全优化、网站安全监测防护、应急响应等服务。

第三方评估机构是对云服务商与云服务客户开展独立的安全评估，具备国家授予的相应资格的企业法人或组织。

6 规划准备

6.1 概述

规划准备阶段，云服务客户应对政府网站进行安全需求分析，明确采用的云服务模式和部署模式；提出各项功能、性能及安全要求；明确参与各方的角色与安全职责，根据云计算服务和政府网站的特点进行安全需求分析，形成入云方案。

6.2 安全职责

6.2.1 云服务客户

云服务客户是其信息安全的责任主体，云服务客户在规划准备阶段的安全职责如下：

a) 应针对网站采用云计算服务的过程制定相应的管理制度，并指定安全负责人；
b) 应参照GB/T 31167—2014《信息安全技术 云计算服务安全指南》等国家标准，对数据的敏感程度、业务的重要性进行分类；
c) 应组织本单位人员开展安全培训，明示使用云计算服务带来的安全风险；
d) 应就其网站内容、单位信息向监管部门进行报备并进行网站定级工作；
e) 应配合监管部门对入云网站系统的安全检查，并对发现的安全问题进行整改；
f) 应根据政府网站的功能、性能及安全指标对政府网站采用云计算服务的需求进行分析，确定采用云计算服务的数据、业务范围；
g) 应根据信息的敏感程度、人员技能、业务需求的动态性等来选择应用的部署模式。

6.2.2 云服务商

云服务商在规划准备阶段的安全职责如下：

a) 保证提供的云计算服务符合国家法律法规要求且安全可靠；
b) 应遵守云计算服务相关标准及安全要求提供服务，并具备相关服务资质；
c) 应参照有关信息安全国家标准逐步通过政务云审查；
d) 保证提供服务的云计算平台、数据中心等设在境内；
e) 应遵守党政信息系统的信息安全政策规定、信息安全等级保护要求、技术标准，落实安全管理和防护措施；
f) 应及时响应客户的服务需求。

6.2.3 云客户供应链服务商

云客户供应链服务商在规划准备阶段的安全职责如下:

a) 应向云服务客户详细介绍服务内容、服务流程、安全责任等；
b) 应根据云服务客户的要求，对云服务客户采用云服务模式的需求进行分析，梳理入云网站系统架构、功能、性能等安全方面的要求；
c) 应在云服务客户的协调下，与云服务商对提供的服务内容进行功能和责任区分，并通过服务协议或者合同等进行约束；
d) 在云服务客户的统筹协调下，供应链服务商之间应该进行边界梳理，能够达成兼容协同的综合服务。

6.2.4 第三方评估机构

第三方评估机构在规划准备阶段的安全职责如下：

a）第三方评估机构应在开展安全评估工作前，与云服务客户签订服务协议、保密协议；
b）第三方评估机构可根据云服务客户委托对政府网站进行安全测评。

6.3 需求分析

6.3.1 网站状况梳理

在网站采用云计算服务之前，需要对网站现有系统进行梳理，确定迁移的系统边界，形成网站现状梳理报告，梳理内容包括：

a) 网站系统的网络拓扑结构，网络边界，包含的网络设备型号、配置、使用情况、运维情况等；

b) 网站包含的应用系统，以及各应用系统的计算资源、存储资源、网络情况、基础软件配置情况、应用系统部署架构、高峰时段资源使用情况、系统运维情况、技术支撑情况等；
c) 本单位业务系统内部、业务系统之间以及与其他单位业务系统之间的网络连通关系及关联程度；
d) 原有的业务安全要求，已部署的安全软件、网络安全策略和安全服务需求等；
e) 系统数据备份及灾备系统情况，包括备份机制、备份策略等，进行数据备份恢复演练，确保数据备份的有效性、完备性；
f) 有无特殊设备如加密卡、网闸、视频卡等。

6.3.2 上云决策

云服务客户应参照国家有关信息安全的法律、法规和相关标准，根据安全风险分析情况与现状梳理情况，做好上云决策分析：

a) 云服务客户应参照《中华人民共和国保守国家秘密法》、《中华人民共和国政府信息公开条例》等相关法律、法规，建立保密审查制度对计划迁移到云平台上的数据、业务进行综合分析与保密审查，对于涉及国家秘密、工作秘密的数据和业务，不应采用社会化云计算服务；
b) 云服务客户应参照《信息安全技术 信息系统安全等级保护定级指南》等国家标准对政府网站及数据重要性进行分类定级，全面系统评估所采用云计算服务的安全风险，等级保护定级为四级及以上的政府网站不宜采用社会化云计算服务；
c) 对于包含大量敏感信息和公民隐私信息、直接影响党政机关运转和公众生活工作的关键业务，或者云服务客户核心业务，不宜采用社会化云计算服务；
d) 云服务客户可根据业务及数据需要，重点评估云计算服务的安全性、可控性，明确云计算服务的数据、业务范围、安全责任、工作进度等，为后续进行云服务采购和迁移工作做好决策支持分析；
e) 云服务客户可向政府网站数据所涉及的相关部门征求业务及安全性方面的建议，作为入云决策的重要参考依据。

6.3.3 资源需求

云服务客户应明确入云网站的资源需求，包括计算资源、存储资源、网络资源等，合理申请网站系统资源。有些政府网站业务具有临时、周期性特点，可能会出现访问和请求的突发高峰，可要求云服务商根据访问需求动态分配资源，并按照实际占用的资源支付使用费用。

6.3.4 安全要求

6.3.4.1 安全部署与隔离

云服务客户应明确政府网站的信息安全等级保护定级情况，明确相关技术和管理要求；明确外部和内部用户访问政府网站的访问控制策略，网站系统设备之间的访问策略，与政务外网和互联网间的数据共享交换策略。应调查了解云服务商为满足客户网站系统合规及安全控制策略提供的基础安全措施，包括自身物理、网络、主机、应用、数据和虚拟化等方面的安全措施，做好安全部署规划。

若云服务客户采用社会化公有云计算服务，应要求云服务商做好系统边界的隔离，包括与其他租户业务系统、虚拟机、虚拟网络、虚拟存储之间的安全隔离。

根据网站现有安全防护措施和水平，结合云计算特点形成安全防护需求，迁移后的防护水平应不低于现有防护水平。

6.3.4.2 Web 应用安全

入云政府网站应具有以下基本安全能力：

a) 具有身份鉴别机制，支持多种身份认证方式；
b) 具有权限设置和访问控制功能，可根据不同的网站访问者角色设置不同的权限，限制其可操作的权限；
c) 具备网站安全审计能力，针对前台用户的注册、登录、关键业务操作等行为进行日志记录；针对网站编辑人员的登录、网站内容编辑、审核及发布等行为进行日志记录；针对系统管理用户的登录、账号及权限管理等系统管理操作进行日志记录；
d) 具备网页防篡改的能力；
e) 具备主流 Web 应用漏洞的发现与修复能力；
f) 具备抵御应用层各类攻击防御的能力，包括但不限于 SQL 注入攻击、跨站脚本攻击、拒绝服务攻击等。

6.3.4.3 外部入侵防御

政府网站应具有以下抵御外部攻击者恶意入侵的安全能力：

a) DDoS 攻击防御；
b) 密码暴力破解防御；
c) 网站后门检测和处理；
d) 异地登陆告警；
e) Web 攻击防御；
f) 抵御云上其他客户系统的攻击。

6.3.4.4 域名安全

政府网站的域名安全包括：

a) 应选择主管部门批准的域名注册服务机构进行域名注册和域名托管，并进行域名信息报备；
b) 应遵循国家有关监督审批流程开展域名变更、解析地址变更等工作；
c) 应使用“.gov.cn”、“.政务.cn”或“.政务”等域名；
d) 应加强域名管理账号的管理，防止域名被恶意篡改。

6.3.4.5 内容安全

政府网站上发布的信息属于对外公开信息，云服务客户应做好网站内容发布的审核和审批，确保发布的内容均属于可对外公开信息。应加强网站内容发布后台的管理，做好访问控制，防止非法的后台访问；做好后台发布用户的鉴别和权限管理，防止后台用户账户被恶意破解使用。

6.3.4.6 安全监测与告警

云计算服务模式在一定程度上减弱了云服务客户对自身网站的控制能力，云服务客户需要通过监管了解和掌握自身网站在云计算平台上的运行情况，并通过自动化手段实现对网站系统的安全监测与告警，安全监测内容包括：

a) 对网站虚拟机、数据库、网络运行情况进行实时监测，发现异常时进行告警；
b) 对网站关键运行指标进行监控的能力，当指标达到阈值时进行告警；
c) 对网站安全漏洞监测的能力；
d) 对网站服务质量监测的能力；
e) 对网站数据完整性的监测，当发现网站数据被篡改时及时告警；
f) 对网站系统被攻击及入侵的监测，并在发现网站系统被恶意攻击时进行及时告警；

g) 对云计算平台漏洞的监测和发现能力；
h) 对网站系统日志备份，并进行常态化安全审计。

6.3.5 需求报告

云服务客户根据以上分析形成需求报告，需求报告应包括：
a) 政务网站的安全保护等级要求、网站系统特定的安全要求；
b) 需要采取或需要改造的安全技术措施需求；
c) 需要云服务商提供的技术接口支持需求；
d) 对云服务商提出的需求；
e) 对云客户供应链服务商提供的服务及产品需求；
f) 需要采取的安全管理措施需求。

6.3.6 资源和模式选择

云计算有SaaS、PaaS和IaaS三种主要服务模式，客户应参照GB/T 31167—2014《信息安全技术 云计算服务安全指南》相关要求，根据当地政策要求、不同服务模式的特点和自身网站系统的安全管理要求，结合自身技术能力、市场和技术成熟度等因素选择服务模式。

6.4 入云方案

云服务客户应主导规划设计网站的入云方案，入云方案应包含安全方案与工作方案，可委托云客户供应链服务商提供入云方案。云服务客户在安全需求分析的基础上，咨询云服务商、云客户供应链服务商，设计完善政府网站入云方案，并进行论证，入云方案包括：
a) 各服务商根据安全责任的划分，做好操作系统、数据库、中间件、应用系统和数据等方面的安全保障，采取安全措施，包括漏洞扫描、脆弱性检查和安全加固方案等；
b) 待迁移的政府网站迁移前应通过代码审计、渗透测试等安全检查，重点加强对迁移时的访问安全、部署安全、账号安全以及数据安全的检查，避免迁移入云的政府网站存在安全隐患；
c) 云服务客户应协调各相关服务商，做好敏感信息保护和备份、恢复等工作；
d) 明确云服务商应提供的保障内容和必要的安全支持服务，如应急演练工作的配合、安全测评和安全检查期间的技术支持等。

6.5 服务商选择

云服务客户应根据网站定级情况、云服务商提供的标准安全服务、增值安全服务、接入方式等对云服务商进行选择，根据云客户供应链服务商提供的安全保障服务对云客户供应链服务商进行选择，选择时应进行如下考虑：
a) 云服务商选择
   1) 当地信息化主管部门推荐或选定的云服务商；
   2) 按照国家或监管部门的要求选择通过党政部门网络安全审查的云服务商；
   3) 等级保护定级为三级及以上的政府网站优先选择通过增强级政务云审查的云服务商；
   4) 云服务商应提供标准化安全服务保障自身云平台安全，包括物理、网络、主机、应用、虚拟化等方面的安全；
   5) 若云服务商提供云服务客户供应链服务，云服务商应承担相应的责任，并取得相应的资质；
   6) 云服务商应提供符合云服务客户要求的安全监管接口。
b) 云客户供应链服务商选择
   1) 系统集成商：根据政府网站建设、维护的安全需求选择有相应资质的服务商；

2) 网站开发商：网站开发商应取得软件安全开发类的相关资质认证；
3) 安全服务商：进行风险评估的安全服务商应至少具备风险评估类的服务资质；进行应急响应的安全服务商应具备安全应急响应类服务资质；提供安全产品的服务商所提供的安全产品应具备相关的安全产品销售许可证。

6.6 合同签订

6.6.1 服务合同

服务合同是明确云服务客户与各服务商之间责任义务的基本手段，能够保护云服务客户和各服务商的合法利益。合同内容应包括（参见附录 A）：

a) 云服务客户与云服务商签订合同，合同中明确服务部署模式，划分双方安全责任边界，制定服务水平协议，规范双方的安全权利义务以及安全保密协议等内容；
b) 云服务客户应与云客户供应链服务商签订合同，在合同内容中要明确各服务商的安全责任边界、安全保密条款以及双方的安全权利义务等；
c) 云服务客户应要求云服务商与云客户供应链服务商在合同中声明不使用有恶意代码产品或假冒产品；
d) 云服务客户与云服务商应在合同中明确资产的所有权，资产包括云服务客户的业务系统在云平台上运行过程中产生的数据和文档；
e) 云服务客户应要求云服务商保障云服务客户运行在云平台的数据的保密性、完整性和可用性；
f) 云服务客户与云服务商应在合同中约定云计算服务退出条件及双方在退出阶段的责任；
g) 云服务客户与云客户供应链服务商应在合同中明确不得窃取修改云服务客户数据资料。

6.6.2 服务水平协议

服务水平协议（简称 SLA）是约定云服务商向云服务客户提供的云计算服务的各项具体技术和管理指标，是合同的重要组成部分。云服务客户应与云服务商协商服务水平协议，并作为合同附件，服务水平协议应包含的内容如下（参见附录 A 中附件 2）：

a) 服务水平协议应与服务需求对应，针对需求分析中给出的范围或指标，在服务水平协议中要给出明确参数；
b) 服务水平协议中应对涉及到的术语、指标等明确定义，防止因二义性或理解差异造成违约纠纷或客户损失。

6.6.3 保密协议

可访问云服务客户信息或掌握云服务客户业务运行信息的服务商应与云服务客户签订保密协议；能够接触云服务客户信息或掌握业务运行信息的服务商内部员工，应签订保密协议，并作为合同附件，参见附录A中附件3。

7 部署迁移

7.1 概述

部署迁移阶段，云服务客户应协调云服务商、云客户供应链服务商做好相关准备工作，根据需求分析形成迁移部署方案，其中包括安全方案。明确相关人员、服务、设备、相关资源等，并且各方要明确自身的安全职责，云服务客户应协调各服务商做好部署和实施工作。

7.2 安全职责

7.2.1 云服务客户

云服务客户在部署迁移阶段的安全职责如下：

a) 应配合云服务商或云客户供应链服务商进行云计算服务实施；
b) 应组织协调云服务商、云客户供应链服务商进行政府网站的部署迁移；
c) 应按照云服务商或云客户供应链服务商的要求提供相应的支持；
d) 应根据自身需求来自由选择云服务商和云客户供应链服务商提供的服务内容。

7.2.2 云服务商

云服务商在部署迁移阶段的安全职责如下：

a) 应配合云服务客户完成对网站的部署迁移；
b) 负责云计算平台的安全，提供安全基础防护措施；
c) 应在云计算平台的外部边界和内部关键边界上监视、控制和保护网络通信；
d) 应根据云服务客户的要求，制定可审计事件清单，明确审计记录内容；
e) 应根据云服务客户的要求制定相应的应急预案；
f) 应建立完善的维护云计算平台设施和软件系统的相关规范制度，定期维护云计算平台设施和软件系统；
g) 应对维护所使用的工具、技术、机制以及维护人员采取有效的控制措施；
h) 应对云计算平台进行配置管理，在系统生命周期内建立和维护云计算平台（包括硬件、软件、文档等）的基线配置和详细清单，设计和实现云计算平台中各类产品的安全配置参数。

7.2.3 云客户供应链服务商

云客户供应链服务商在部署迁移阶段的安全职责如下:

a) 应与云服务商就服务内容、边界、交互等进行确认，确保云客户供应链服务商不影响云服务商及其他云服务客户的正常使用；
b) 系统集成商负责政府网站的迁移及安全部署，负责安全配置、整体安全功能联调等网站建设安全；
c) 网站开发商应根据云服务客户的需求完成网站的安全功能开发，并协助系统集成商完成相关部署工作；
d) 安全服务商应提供整个部署过程中的安全保障和网站安全建设，提供相关的安全产品及服务，并协助云服务客户与云服务商共同建立政府网站云计算服务安全保障体系。

7.2.4 第三方评估机构

第三方评估机构根据云服务客户委托，配合政府网站的部署迁移工作，第三方评估机构安全职责如下：

a) 配合云服务客户进行安全合规验收；
b) 在部署迁移完成后，对政府网站进行风险评估；
c) 在部署迁移完成后，对政府网站进行等级保护定级。

7.3 入云迁移

7.3.1 迁移准备

入云实施工作开展前，云服务客户应协调各服务商做好相关准备，主要包括责任人和联系人、工具、产品、服务及相关资源，云服务客户的安全职责如下：

a) 云服务客户应通知相关业务部门迁移的时间计划及对业务的影响；
b) 云服务客户应组织云客户供应链服务商与云服务商之间的对接工作；
c) 云服务客户应对政府网站进行敏感数据的加密存储和数据的加密传输；
d) 云服务客户应对政府网站进行数据备份，包括数据库、应用程序、重要配置以及操作系统等；
e) 云服务客户应组织相关服务商提供责任人和联系人，并对相关人员进行培训；
f) 云服务客户应对云服务商的安全防护措施进行调研，并结合现有安全防护措施，形成云上的防火措施；
g) 云服务客户应对云服务商提供的主机、应用等进行安全检查，确保云服务资源的安全性；
h) 云服务客户应协同系统集成商做好入云政府网站建设及迁移的准备工作，包括实施组织、实施方案、实施计划、实施工具及沟通协调等具体工作；
i) 云服务客户应协同网站开发商做好政府网站软件功能实现的安全需求调研及确认工作，包括但不限于安全认证、用户授权、密码策略、安全审计、细粒度访问控制等安全功能；
j) 云服务客户应委托安全服务商提供所需的安全能力组件（产品或服务），同时在云服务客户的授权下做好同云服务商及其他云客户供应链服务商的协同工作；
k) 云服务客户应要求云服务商为云服务客户划分独立的安全域，并在网络边界处部署安全措施；
l) 云服务客户应要求云服务商准备网站入云后所需的资源。

7.3.2 应用迁移

云服务客户应牵头负责政府网站的迁移工作，各个服务提供商配合并对迁移工作进行指导协助。云服务客户安全职责如下：

a) 云服务客户应授权并配合系统集成商进行政府网站迁移实施的具体工作，包括进行政府网站在云平台的部署、调试、测试及验证等工作；
b) 云服务客户应授权并配合安全服务商在应用迁移过程中提供的安全保障服务；
c) 云服务客户应确保政府网站迁移完成后，网站能正常访问；
d) 云服务客户应协同云服务商、安全服务商对发现的安全隐患(如存在)进行整改，并对整改的结果进行复核确认；
e) 云服务客户应对政府网站迁移后的变更进行严格监督和审核，以确认变更操作不会影响或降低政府网站的安全性；
f) 云服务客户应对政府网站进行安全检测，并根据检测结果出具检测报告。

7.3.3 应用切换

完成政府网站迁移后，云服务客户需对应用进行切换，应制定切换方案明确切换顺序，云服务商、云客户供应链服务商应协助云服务客户做好切换测试、数据同步等安全保障工作。

7.3.4 应用回退

云服务客户应制定政府网站迁移失败的回退方案，以确保在迁移、部署、切换等阶段造成的业务中断或数据丢失等风险时能快速进行回退工作。云服务客户的安全职责如下：

a) 在云服务客户的统一协调下，若发生政府网站迁移失败事件，云服务商与系统集成商应协助云服务客户将网站恢复至初始状态；
b) 若无法回退至初始状态，云服务客户应要求云服务商与系统集成商应配合使用备份数据进行相应的恢复工作。

7.3.5 安全优化

政府网站在云计算环境部署完成后，需要对网站进行进一步的优化，云服务客户或委托具有相关资质的云客户供应链服务商进行安全优化，云服务客户的安全职责如下：

a) 安全评估。在进行安全优化之前，云服务客户应评估政府网站的安全状况，包括但不限于安全功能、安全配置、源代码安全、应急处置等。

b) 安全测试。在安全加固之前，云服务客户应对政府网站进行安全测试，测试内容包含但不限于配置核查、漏洞扫描、渗透测试等。

c) 安全加固

1) 云服务客户应对政府网站进行安全优化，包含但不限于软件平台安全、应用安全、数据安全及备份恢复安全等；

2) 云服务客户应对政府网站的数据进行备份，进而进行安全加固操作，安全加固应不能影响政府网站的安全运行，应具有故障情况下的数据恢复和应急处置措施，加固过程中涉及的安全工具、安全策略及安全补丁应先在测试环境进行安全性验证；

3) 安全加固后，云服务客户应对变更进行测试，确认其不会影响政府网站的功能及运行。

7.3.6 制度建设

根据入云后服务商的变化，云服务客户应对原有安全管理制度进行修订，明确相关人员的职责和权限，明确在具体运维中各方的具体工作。

云服务客户应组织相关服务商制定相应的安全管理制度，并对能够接触业务信息的各类人员进行职责划分及权限管理，为政府网站安全迁移提供管理依据。

7.3.7 安全预案

云服务客户应组织相关服务商共同制定安全预案，预案应按照：统一领导、规范管理、明确责任、分级负责、预防为主、加强监控几个原则进行制定。云服务客户的安全职责如下：

a) 保障措施

1) 应建立健全网络与信息安全管理预案，加强对网站网络信息的日常监测、监控，强化安全管理，对可能引发网络与信息安全事件的有关信息，要认真收集、分析判断，发现有异常情况时，及时处理并逐级报告。

2) 应当备份网站文件和数据库。备份采用完全备份策略与部分备份策略相结合，云客户负责每天对网站数据库进行一次完整备份，每季度对网站文件进行一次完整备份，备份数据应短时间可恢复至政府网站正常运行。定期进行网站文件和数据库备份恢复演练，确保备份数据的有效性。

3) 特殊时期应启动网站信息安全应急值班制度。在特殊时期进行 24 小时应急值班，对网站信息数据加强保护，进行不间断监控，一旦发生安全事件，立即启动应急预案，判定事件危害程度，采取应急处置措施，并立即将情况报告有关领导。在处置过程中，及时报告处置工作进展情况，直至处置工作结束。属于重大事件或存在非法犯罪行为的，及时向公安机关报告。

4) 应保持与相关服务商沟通渠道的畅通，确保在应急处理过程中遇到困难或问题时能及时获得相关服务商的技术支援。

b) 应急措施

1) 发现网站出现非法信息或内容被篡改，应立即通知云服务商和上级领导，保存非法信息或篡改页面，启动备份系统。情况严重的，立即向公安机关报警。

2) 系统软件遭到破坏性攻击，网站瘫痪，应立即向云服务商和上级领导报告，停止系统运行，

启用备份系统，情况严重的，立即向公安机关报警。

7.4 入云交付

入云交付是政府网站入云过程的最后环节，分为网站试运行、安全合规验收和安全交付三个阶段。

7.4.1 网站试运行

在该阶段，云服务客户的安全职责如下：

a) 云服务客户应根据政府网站运行情况，制定相应的试运行方案，并明确试运行时间(通常建议为 3 个月)，确保政府网站入云后的安全、可靠、稳定的运行；
b) 云服务客户应对网站系统的功能进行一致性测试，确保迁移后的网站功能正常。
c) 云服务客户或委托第三方评估机构应模拟实际运行情况对政府网站进行全面的安全测试；
d) 云服务客户应加强试运行期间的安全监测，全面查看各种日志信息，以便能及时发现问题并进行整改；
e) 云服务客户应提高试运行期间的数据备份频率，以便出现问题时能尽可能的恢复丢失的数据。

7.4.2 安全合规验收

云服务客户或委托第三方评估机构进行安全合规验收测评，根据验收目标和范围，结合安全建设方案对实施情况进行安全评估，云服务客户的安全职责如下：

a) 云服务客户应对安全架构合理性分析、脆弱性评估以及安全配置检测等；
b) 云服务客户应明确提出安全验收测试的要求，云服务商应协助云服务客户进行安全验收测试等工作；
c) 安全验收测试通过后，云服务客户在确认安全风险和隐患均得到有效控制后，方可正式开展政府网站的相关服务；
d) 安全测试通过后，云服务客户需重新确定信息系统安全保护等级，形成信息系统安全保护等级定级报告并向相关监管部门进行报备。

7.4.3 安全交付

完成政府网站的迁移，并通过安全验收测试后，各相关服务商应提交给云服务客户相应的实施成果文档，包括但不限于如下成果文档：

a) 源代码；
b) 实施方案；
c) 资源清单；
d) 配置清单；
e) 使用手册；
f) 安全预案。

各相关服务商在完成相应的实施工作后，云服务客户应要求开展相关实施后培训，确保所有交付成果有效开展。

8 运行管理

8.1 概述

此阶段云服务客户应监督云服务商履行合同规定的责任义务，云服务客户遵守政府信息安全的有关政策规定和标准。共同维护数据、业务及云计算环境的安全。在采用云计算服务时，虽然云服务商承担了部分控制和管理任务，但云服务客户依然是安全责任的最终责任人，云服务客户应采取有效的措施加强对云服务商的运行监管以及自身云计算服务使用、管理和技术措施的运行监管。

8.2 安全职责

8.2.1 云服务客户

云服务客户在运行管理阶段的安全职责如下：

a) 应建立云计算服务保密审查制度，指定机构和人员定期负责对迁移到云计算平台上的数据、业务进行保密审查，确保数据和业务不涉及国家秘密；
b) 应持续监督各服务商，并要求各服务商严格履行安全责任和义务；
c) 应在云服务商、云客户供应链服务商处理信息安全事件过程中提供协助；
d) 应定期对其网站应用开展安全自查，并及时将自查结果汇报至监管部门；
e) 应为安全事件的处理提供必需的支持；
f) 应遵从政府网站云计算服务相关标准及要求对云上政府网站进行管理。

8.2.2 云服务商

云服务商在运行管理阶段的安全职责如下：

a) 云服务商有重大调整变更时，例如收购与被收购、重大技术措施调整、重大组织机构人员调整及其他可能对客户服务造成影响的，应向云服务客户提前通知，并获得监管部门审核；
b) 在进行重大变更前，应提前通知云服务客户，评估可能对云服务客户造成的影响；
c) 发生重大变更后，应组织进行安全评估，并形成评估报告；
d) 严格履行合同规定中的责任和义务，遵守相关的安全管理政策和标准；
e) 周期性地进行风险评估，对目标进行持续监控，对于异常情况及时告警；
f) 应接受监管部门组织的信息安全检查，包括必要的渗透测试、风险评估、安全审计等；
g) 对云计算环境的维护进行规划、实施、记录，并定期对维护记录进行归档；
h) 在系统、组件或服务的运行过程中实施配置管理，保证记录、管理和控制变更的完整性；
i) 保障云服务客户的数据和业务的机密性、完整性、可用性，以及互操作性、可移植性；
j) 持续开展对员工的安全和保密教育，自觉维护云服务客户的云计算服务安全；
k) 应根据监测情况定期向云服务客户提供云服务客户网站安全运行报告；
l) 制定应急预案及安全事件处置响应计划，出现重大信息安全事件时，及时向云服务客户和监管部门报告事件及处置情况。

8.2.3 云客户供应链服务商

云客户供应链服务商在运行管理阶段的安全职责如下:

a) 应接受云服务客户对其提供的服务的持续监管；
b) 应配合云服务客户、云服务商进行相应的业务服务，如：等级保护测评、云计算安全审查、基础设施安全检查等；
c) 应根据与云服务客户签订的服务协议、合同，向云服务客户提供安全服务，并定期向云服务客户提供服务报告；
d) 在为云服务客户提供服务过程中，涉及云服务商的基础设施、网络等时，应提前向云服务商及云服务客户说明，在遵守云服务商的相关规定下进行；

e) 应确保在向云服务客户提供服务时，不影响云服务的运行及其他云服务客户的使用。

8.2.4 第三方评估机构

第三方评估机构的安全职责如下：

a) 第三方评估机构应在云计算服务运行过程中配合监管部门或云服务客户，对云计算平台或政府网站进行安全评估；

8.3 安全防范

云服务客户应对入云政府网站采取安全防范措施，云服务客户的安全职责如下：

a) 云服务客户应建立安全事件处理计划，包括对事件的预防、检测、分析、控制、恢复等，对事件进行跟踪、记录；
b) 云服务客户应对网站访问行为进行监测，对攻击行为进行实时告警；
c) 云服务客户应删除或者修改密码默认演示用户；
d) 云服务客户应采取安全措施保障网页篡改、Web漏洞扫描、SQL注入、跨站脚本攻击、DDoS攻击等攻击的安全防护能力，并记录相关日志；
e) 云服务客户应采取安全措施进行病毒防御，并及时升级病毒库。

8.4 安全监测

8.4.1 对网站的监测

8.4.1.1 对网站的监管

云服务客户对网站的监管应包括以下内容：

a) 应对业务系统使用者进行监管，要求其遵守国家有关信息安全的法律法规、标准及合同，不得对信息系统进行网络攻击、恶意程序传送、窃取或篡改资料数据、传播非法信息等违规违约的恶意行为；
b) 应对系统中的账号进行监管，发现任何非法使用的情况，应在权限范围内处置，必要时通知云服务商；
c) 应监管使用者在不同模式下部署的应用及业务系统的安全措施；
d) 应通过自查或委托第三方测评机构对使用者负责实施的安全措施进行安全测评和检查。

8.4.1.2 可用性监测

云服务客户对网站的可用性监测应包括以下内容：

a) 应对网站虚拟层资源状态进行监测，涉及计算资源、存储资源、网络资源，监测项包括但不限于虚拟CPU使用率、虚拟CPU平均负载、虚拟内存使用率、磁盘利用率等；
b) 实时监测网站业务的可用性，并对异常情况进行报警和处置；
c) 应对网站运行状态进行监测，包括提供网站服务的相关系统、中间件等；
d) 实时监测网站云计算平台的可用性，并对异常情况进行报警和处置；
e) 应定期进行网站的域名及IP合规性检测，检测内容包含域名对应关系、是否存在非法解析、域名劫持等情况。

8.4.1.3 网页内容监测

云服务客户对对网页内容监测应包括以下内容：

a) 实时监测网站发布内容,发现有害信息进行告警和处置；

b) 利用网页防篡改系统并结合人工自检方式或采用专业安全服务等方式，对网页内容篡改情况进行实时监测和处置。

8.4.1.4 网站业务安全监测

云服务客户对网站业务安全监测应包括以下内容：

a) 利用网站木马、后门检测监控系统或采用安全服务等方式对网站系统可能存在的挂马、后门情况进行实时监测和处置；
b) 定期对网站服务器的对外服务端口情况进行检测，及时关闭高风险的服务端口；
c) 定期对网站应用程序、操作系统及数据库进行脆弱性扫描，发现可能存在的安全漏洞并定期修复，对 SQL 注入、跨站脚本攻击漏洞、表单破解、信息泄露等高危漏洞应及时修复；
d) 具备信息交换与情报共享机制，及时获知 0Day 漏洞等未知威胁对网站可能造成的侵害，及时做好防护工作；
e) 对网站业务安全防护措施进行测评和检查。

8.4.1.5 网站环境安全监测

云服务客户对网站环境安全监测应包括以下内容：

a) 实时监测网站业务状态，并对异常情况进行报警和处置；
b) 实时监测网站网络状态，并对异常情况进行报警和处置；
c) 实时监测网站所在的云计算平台状态，并对异常情况进行报警和处置；
d) 对网站环境安全防护措施进行定期测评和检查。

8.4.2 对服务商的监管

8.4.2.1 对云服务商的监管

云服务客户应对云服务商进行监管，监管包括以下内容：

a) 云服务商应能够将安全策略进行集中呈现，对不同云服务客户的策略能够独立监控；
b) 云服务商应实时监控策略的有效性，保证虚拟机迁移时，相关安全策略能够随其迁移；
c) 云服务商应该严格履行合同中的责任和义务，遵守政府信息系统安全管理相关政策及标准；
d) 云服务商应开展周期性的风险评估和监测，保证安全能力持续符合GB/T 31168—2014《云计算服务安全能力要求》相关要求，若云服务商不能保证其安全能力，云客户有权更换或要求云服务商提升其安全服务能力；
e) 云服务商应满足不同客户或同一客户不同业务的信息系统之间隔离的需求。

8.4.2.2 对云客户供应链服务商的监管

云服务客户应对云客户供应链服务商采取监管，监管包括以下内容：

a) 如果感知到云服务商还未上报的安全事件，及时通知云服务商和云服务客户；
b) 应提供急联络方式给云服务商，以便云服务商记录在其应急响应计划中；
c) 协助云服务商处理安全事件；
d) 监控自身负责的安全控制措施。

8.5 应急响应

云服务客户应为入云的政府网站制定应急响应预案，并定期演练，确保在紧急情况下重要信息资源的可用性。云服务客户的安全职责如下：

a) 云服务客户应根据其网站系统的具体特点，并按照《国家突发公共事件总体应急预案》、《国家网络与信息安全事件应急预案》等文件要求，制定应急响应预案。应急响应预案应包含总则、角色及职责、预防和预警机制、响应分级、处置流程、保障措施等内容；
b) 云服务客户应综合分析各类安全事件可能造成的影响，破坏程度和恢复周期等多方面因素，有针对性地制定、维护网站不同事件的应急预案，每两年至少开展各典型类别安全事件的应急演练一次；
c) 云服务客户应建立应急值班制度，8h 工作时间以外，安排专人通过电话、邮件等方式进行监控。遇到重大节日或敏感时期，应安排 24h 值班，并定期进行信息报送；
d) 信息安全事件发生时，云服务客户应按照应急预案的要求及时组织应急处置并记录，涉及到云计算平台的应要求云服务商配合处置。

8.6 评估改进

云服务客户应定期对入云政府网站进行安全检查和评估，并根据检查结果进行安全改进。云服务客户的安全职责如下：

a) 云服务客户应制定安全检查工作计划和安全检查方案，说明安全检查的范围、对象、工作方法等，明确安全检查需要的各类表单和工具；
b) 云服务客户应对检查结果进行汇总、分析，编制安全检查报告，并将安全检查过程的各类文档、资料归档保存；
c) 云服务客户应根据安全检查结果，确定安全改进方案，包含改进方法、改进内容、时间计划等，并提交监管部门对安全改进方案进行评审；
d) 云服务客户应制定业务连续性计划，包含业务影响分析、业务连续性风险评估、明确业务连续性团队、业务连续性测试与演练、业务连续性计划步骤；
e) 云服务客户应定期或者在入云政府网站发生重大变更后进行风险评估，并要求云服务商为风险评估活动提供必要的接口和材料，配合云服务客户进行风险评估；
f) 云服务客户可根据评估结果要求云服务商对涉及云平台的问题进行整改。

9 退出服务

9.1 概述

在退出云计算服务时，云服务客户应要求云服务商履行相关责任和义务，确保退出云计算服务阶段数据、业务的安全，如安全返还云服务客户数据、彻底清除数据等。

9.2 安全职责

9.2.1 云服务客户

云服务客户在退出服务阶段的安全职责如下：

a) 云服务客户应对云服务商在退出服务阶段提供的各种文档资料进行校验，确定其完整性和准确性；
b) 云服务客户应对云服务商返还的数据完整性进行验证，如将数据、程序放在新的平台上运行验证；
c) 云服务客户应监督云服务商返还数据的过程，并对数据进行测试；
d) 变更云服务商时，云服务客户应按要求选择新的云服务商，重点关注云计算服务迁移过程的数据和业务安全。

9.2.2 云服务商

云服务商在退出服务阶段的安全职责如下：

a) 应制定详细的移交清单，移交清单不仅包含云计算服务过程中提供给云服务商的各种文档资料，还包括云服务客户业务系统在云计算平台上运行期间产生、收集的数据以及相关文档资料；
b) 应彻底删除云服务客户数据信息及所有备份，对云服务客户的数据存储介质应彻底清理，云服务客户的数据存储介质重用之前应进行清理或进行物理销毁；
c) 云服务客户的数据存储介质清理后，不应存放公开信息；
d) 应根据移交清单返还云服务客户数据信息（包括历史数据和归档数据）。

9.2.3 云客户供应链服务商

云客户供应链服务商在退出服务阶段的安全职责如下：

a) 应协助云服务客户进行政府网站的服务退出；
b) 应根据与云服务客户签订的服务协议、合同，向云服务客户交付相应的程序、数据、文档等；
c) 应确保在服务退出后，彻底销毁云服务客户信息。

9.2.4 第三方评估机构

在退出服务阶段，云服务客户可委托第三方评估机构对退出过程进行监督审计，第三方评估机构的安全职责如下：

a) 第三方评估机构配合云服务客户对云服务商及云客户供应链服务商的退出环节进行审计。

9.3 服务安全退出

9.3.1 退出需求

退出云计算服务是一个复杂的过程，合同到期或其他原因都可能导致云服务客户退出云计算服务，或将数据和业务转移到其他云计算平台上。云服务客户的安全职责如下：

a) 云服务客户在与云服务商签订合同时提前约定退出条件，以及退出时云服务客户、云服务商的责任义务；
b) 云服务客户应要求云服务商应完整返还云服务客户数据；
c) 在将数据和业务退出后，云服务客户应满足业务的可用性和持续性要求；
d) 云服务客户应及时取消云服务商对云服务客户资源的物理和电子访问权限；
e) 云服务客户提醒云服务商在云服务客户退出云计算服务后仍应承担的责任及义务，如保密要求等；
f) 云服务客户应要求云服务商应对数据进行彻底清除。

9.3.2 退出方案

云服务客户应在退出需求的基础上主导制定退出方案，明确退出过程中的各角色职责分工，做好网站退出的各项保障工作。根据退出后网站的处理情况做好相应的衔接工作，如网站迁移至其他云上，应同步制定迁移的方案，如网站废弃，应按照相关规定做好网站的注销和数据留存工作。

9.3.3 数据移交

从云计算平台迁移出的数据，不仅包括云服务客户移交给云服务商的数据和资料，还应包括政府网站在云计算平台上运行期间产生、收集的数据以及相关文档资料，如数据文件、程序代码、说明书、技术资料、运行日志等，云服务客户应要求云服务商应制订详细的移交清单，包括但不限于以下内容：

a) 数据文件。每个数据文件都应标明：文件名称、文件数据内容的描述、存储格式、文件大小、校验值、类型（敏感或公开）等。
b) 程序代码。针对云服务客户定制的功能或业务系统，在合同或其他协议中明确是否移交可执行程序、源代码及技术资料。可能涉及的内容包括：可执行程序、源代码、功能描述、设计文档、开发及运行环境描述、维护手册、用户使用手册等。
c) 文档资料。云服务客户使用云计算服务过程中提供给云服务商的各种文档资料，及双方共同完成的涉及云服务客户的相关资料。
d) 其他数据。根据事先的约定和双方协商，确定应移交的其他数据，包括云服务客户业务运行期间收集、统计的相关数据，如用户使用云计算服务的行为习惯统计资料、网络流量及分布规律等。

9.3.4 数据的完整性

云服务客户应对云服务商返还的数据完整性进行验证，云服务客户的安全职责如下：

a) 云服务客户与云服务商的合同中应就退出服务阶段移交数据清单进行约定，并对移交数据的类型、有效期进行明确；
b) 云服务客户应要求云服务商根据移交数据清单完整返还云服务客户数据信息，特别注意历史数据和归档数据；
c) 云服务客户或委托第三方评估机构应对云服务商返还云服务客户数据信息的过程进行监督；
d) 云服务客户或委托第三方评估机构应监督云服务商返还云服务客户数据信息过程的安全性，对数据信息移交过程中采取的安全措施进行安全检查，确保数据信息不被泄露；
e) 云服务客户应通过业务系统验证数据信息的有效性和完整性，如将数据、程序放在新的平台上运行验证。

9.3.5 安全删除数据

云服务客户退出云计算服务后，仍应要求云服务商安全处理云服务客户数据，承担相关的责任义务，云服务客户或委托第三方评估机构应当对数据删除过程进行监督。云服务客户的安全职责如下：

a) 云服务客户可要求云服务商应按照合同安全要求保留云服务客户数据信息一段时间，收到云服务客户的书面授权后才能删除云服务客户数据信息；
b) 云服务客户应要求云服务商制定数据信息删除计划，监督数据信息删除过程，并对数据信息删除情况进行验证；
c) 云服务客户应要求云服务商对存放云服务客户数据的存储介质进行清理，并对过程进行监督。

附 录 A
（资料性附录）
合同模板

编号：

XX
服务合同

客户名称_____

业务名称_____

签订日期　　年　　月　　日

本合同由甲乙双方于【　】年【　】月【　】日在【】省【】市签署：

甲方：_____

单位地址：_____

单位负责人：_____

邮政编码：_____

业务部门名称：_____

业务部门负责人：_____**办公电话：**_____**手机：**_____

经办人：_____**办公电话：**_____**手机：**_____

乙方：_____

单位地址：_____

单位负责人：_____

邮政编码：_____

业务部门名称：_____

业务部门负责人：_____**办公电话：**_____**手机：**_____

经办人：_____**办公电话：**_____**手机：**_____

本合同甲方委托乙方就_____项目进行的_____技术服务，并支付相应的服务报酬。双方经平等协商，在真实、充分地表述各自意愿的基础上，根据《中华人民共和国合同法》的规定，达成如下协议，并由双方共同恪守。

1　甲方委托乙方进行技术服务的内容

1.1　甲方将自有业务部署在乙方云计算平台，由乙方提供相关服务（详见附件一）。

1.2　甲方部署的业务系统清单及乙方为该系统运行提供支撑环境和相关服务的期限如下表：

序号	业务系统名称	主要用途及应用对象	服务期限
1			_____年____月____日至 _____年____月____日
2			_____年____月____日至 _____年____月____日

3			_____年____月____日至 _____年____月____日
4			

2　合同金额及付款方式

2.1　甲方在合同签订后【】个工作日内支付乙方服务总款项的【】%，在【】支付剩余【】%。

2.2　甲方已经充分了解并同意乙方所计算的、本合同所涉及的费用，并保证已经采用了正确的付款方式。

2.3　因甲方没有及时支付服务费的，视为本合同的相关权利、义务自动终止。乙方将停止甲方所使用的服务。

2.4　服务到期日后【】天，甲方仍未续费的，乙方将有权不保留甲方云计算平台的数据，由此带来的一切损失由甲方自行负责。

3　乙方云计算平台提供的有关服务标准

3.1　机房环境：

（1）标准机架、UPS 电源、照明、消防、机房专用空调；

（2）7×24 小时机房环境管理和人工值守。

3.2　安全措施：

（1）防病毒：平台提供统一的主机病毒防护软件；

（2）防火墙：平台边界区域及应用区、数据区、互联网接入区统一配备防火墙；

（3）漏洞扫描：平台在安全管理区配备漏洞扫描系统；

（4）入侵检测：平台网络接入区、数据区、应用区统一部署入侵检测系统；

（5）上网行为审计：平台互联网接入区部署上网行为审计系统；

（6）防病毒网关：平台互联网接入域配备防病毒网关；

（7）WEB 应用安全网关:平台在 WEB 服务器接入域前端部署 WEB 应用安全网关(布署在互联网应用区)；

（8）安全管理中心(soc)：平台安全管理区部署有安全管理中心(soc)。

3.3　其他：_____

4　甲方的权利、义务和责任

4.1　甲方承诺在签订合同前已阅读并遵守《中华人民共和国网络安全法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》《互联网站管理工作细则》等相关法律。

4.2　甲方有权按本协议规定获得乙方提供的服务。

4.3　甲方应配合乙方进行云计算服务实施，按要求提供相应的支持。

4.4　甲方应组织协调乙方和其他服务商进行网站的部署迁移。

4.5　甲方应确保业务系统迁入云计算平台前的安全。

4.6　甲方人员进入乙方云计算平台服务中心进行联网调测、现场系统维护等工作必须遵守乙方的相关规定，否则乙方有权拒绝甲方人员进入。

4.7　甲方负责对其在云计算平台部署的相关软件进行维护管理，负责进行病毒检测和系统升级等，并负责自身的信息安全及安全事件处理。

4.8　对于甲方自行安装软件或自行操作引发的任何故障、问题以及因甲方发布信息所产生的一切影响，均由甲方自行负责，乙方不承担任何责任，若甲方行为给乙方造成损失的，甲方应负责赔偿。

4.9 甲方负责自身业务系统及其生产数据的安全管理和运行维护。要定期清理不必要的业务数据，及时释放存储资源，对因管理不当造成业务数据恶性膨胀的，乙方可强制甲方释放相关资源。

4.10 甲方业务系统所生产数据由乙方负责提供存储环境的，乙方要按照公示的备份策略或经甲乙双方约定的策略进行备份。甲方负责备份数据的验证工作。

4.11 甲方应对自身业务系统中的账号进行监管，发现任何非法使用的情况，应在权限范围内处置，必要时通知乙方。

4.12 甲方有义务维护自己的数据、口令或密码的完整性和保密性，非因乙方原因造成外泄或遗失，所产生的一切后果由甲方自行负责。

4.13 甲方应向乙方提供甲方执行本合同的联系人和所有管理甲方采用云计算服务的人员名单、联系方式及权限，并在上述信息发生变化时及时通知乙方。因上述人员名单及相关信息提交不及时、不准确而引起的任何损失及因甲方以上人员（包括已经离职的原甲方雇员）的行为而引起的任何责任与损失均由甲方自行承担。

4.14 甲方及其业务使用者应遵守国家有关信息安全的法律法规、标准及合同，不得通过甲方业务系统对云计算平台和平台内其他云服务客户进行网络攻击、恶意程序传送、窃取或篡改资料数据、传播非法信息等违规违约的恶意行为。

4.15 甲方及其客户在使用乙方提供的产品时，必须遵守有关法律法规、行政规章及国家政策。甲方不得利用乙方提供的服务进行任何违法经营活动，或任何违反法律或违背社会公德的行为（包括但不限于：黑客行为，侵权行为）；不得进行其它超出乙方提供的范围，以及一切可能给乙方带来任何不利影响的行为；甲方对其经营信息引起的一切后果承担全部责任。甲方违反本款义务的，乙方有权停止甲方的云计算服务，并且不退还甲方已支付的协议金额，直至甲方采取措施消除影响。甲方因上述行为给乙方或其他第三方造成损失（尤其包括由于司法介入而给乙方造成的经济损失与名誉损失）的应予以赔偿。

4.16 甲方必须事先为其云服务器上运行的所有网站办理 ICP 报批报备、变更、注销等手续（如果网站有绑定多个域名，则必须为所有绑定域名申请备案审批）；否则因此而导致的云服务器被关闭或网络被切断，以及其它的任何政治责任及法律后果均由甲方自行承担。如果因为甲方违反本条款规定导致乙方被上级主管部门处罚，则此处罚金额及其它相关责任必须全部由甲方承担。

4.17 甲方必须依照《互联网信息服务管理办法》的规定保留自己网站的访问日志记录【 】日，包括发布的信息内容及其发布时间、互联网地址（IP）或者域名等，该记录在国家有关机关依法查询时必须提供。甲方自行承担由于其未按规定保留相关记录而引起的全部责任。

4.18 甲方务必不要直接将账号密码告知乙方工作人员，若因处理业务问题需要将账号密码转交乙方工作人员，甲方需在转交密码的当日或业务处理完毕的当日内自行在线修改账号密码并再次确认修改信息，否则将视为甲方自愿将账号管理及操作权限转交与乙方无关的第三方。由此产生任何后果由甲方自行承担，乙方不负任何法律责任。

4.19 甲方需要获得乙方的售后服务时，需提供详尽信息，若因甲方提供的信息不详而乙方不能确认身份且不能提供相应服务，由此带来的一切后果由甲方自行承担。

4.20 甲方应在乙方处理信息安全事件过程中提供协助。

4.21 乙方不能保证其安全能力或不能满足甲方需求时，甲方有权更换或要求乙方提升其安全服务能力。

5 乙方的权利、义务和责任

5.1 乙方应保证提供的云计算服务符合国家法律法规要求且安全可靠。

5.2 乙方对承载甲方网站的云计算平台的管理应按照政府信息系统进行管理，乙方须遵守有关政府信息安全的政策规定、国家标准，以及甲方网站所属部门的信息安全管理要求。

5.3 乙方负责云计算平台互联网接入，平台网络设备的维护，保证公共网络的正常运行。

5.4 甲方提供给乙方的数据、文档等资源，以及云计算平台上甲方系统运行过程中收集、产生、存储的数据和文档等都属甲方所有,乙方应保证甲方对这些资源的访问、利用、支配等权利。

5.5 乙方保留根据公安部门及其它相关管理部门的授权查看甲方存储在乙方云计算平台数据的权利。

5.6 乙方不得依据外国的法律和司法要求将甲方数据及相关信息提供给外国政府。

5.7 未经甲方授权，乙方不得访问、修改、披露、利用、转让、销毁甲方数据。

5.8 乙方应采取有效管理、技术措施确保甲方的数据和业务的保密性、完整性和可用性，以及互操作性、可移植性。

5.9 乙方不以持有甲方数据相要挟，配合做好甲方数据和业务的迁移和退出。

5.10 发生纠纷时，在双方约定期限内乙方仍应保证甲方数据安全。

5.11 若乙方因基础设施扩容或其他国家工程建设方面因素而无法为甲方提供正常服务，应提前【 】个工作日以书面、电话或 E-Mail 等形式通知甲方。在此情况下甲方同意不视为乙方违约。除了提前通知外，乙方应提供临时方案以保障甲方业务不中断。

5.12 由于乙方原因，造成服务中断，乙方以【】为单位，以月费【】为基数，按平均每【】费用的【 】倍向甲方赔偿。但每月累计赔偿以当月乙方实际收取的月服务费为最高限。

5.13 由于电信运营商的原因造成甲方业务的故障，将由乙方负责与运营商交涉，并及时排除故障。

5.14 乙方有重大调整变更时，例如收购与被收购、重大技术措施调整、重大组织机构人员调整及其他可能对客户服务造成影响的，应向甲方提前通知，评估可能对甲方造成的影响并告知甲方。

5.15 乙方因为非不可抗力原因而中断为甲方提供服务，应于【 】小时前通知甲方。在此情况下甲方同意不视为乙方违约,电信运营商原因不属于不可抗力，非不可抗力造成服务中断视为乙方违约。

5.16 乙方应接受甲方或甲方相关职能部门的信息安全监管。

5.17 乙方应接受甲方组织的信息安全检查。

5.18 当发生安全事件并造成损失时按照双方的约定进行赔偿。

5.19 乙方应根据监测情况定期向甲方提供甲方网站安全运行报告。

5.20 乙方应满足甲方不同业务的信息系统或与其他云服务客户之间隔离的需求。

5.21 乙方应制定应急预案及安全事件处置响应计划，出现重大信息安全事件时，及时向甲方报告事件及处置情况。

5.22 乙方负责运行维护云计算相关服务器及存储设备。

5.23 在甲方退出云计算服务阶段，乙方应制定详细的移交清单（移交清单不仅包含云计算服务过程中提供给乙方的各种文档资料，还包括甲方业务系统在云计算平台上运行期间产生、收集的数据以及相关文档资料），并根据移交清单返还甲方的数据信息（历史数据和归档数据）。

5.24 乙方在甲方退出云计算服务后，应彻底删除甲方数据信息及所有备份，对甲方的数据存储介质应彻底清理，甲方的数据存储介质重用之前应进行清理或进行物理销毁。

5.25 乙方应承担法律法规明确或双方约定的其他责任义务。

6 特别声明

因 Internet 上的通路偶然阻塞、突然中断、第三方原因、国与国之间问题等不可预知的因素以外的原因导致的云服务器无法访问，双方将进行协商解决，由乙方在协议范围内尽可能满足甲方的合理要求。若出现故障，双方技术人员应共同分析故障的原因。

7 不可抗力

7.1 合同签订后，合同双方中任何一方，由于火灾、旱灾、台风、大雪、地震、战争和双方认同的其他不可抗力的事故而影响本协议履行时，可根据情况部分或全部免予承担违约责任。

7.2　受事故影响的合同一方应尽快将所发生的不可抗力事故情况以传真通知合同另一方。

7.3　当不可抗力事故停止或消除后，受事故影响的合同一方应尽快通知合同另一方。

7.4　因不可抗力导致本合同不能履行或不能继续履行而造成的损失，由甲、乙双方自行承担。

8　适用法律及争议的解决

8.1　本合同所有条款均适用于中华人民共和国相关法律。

8.2　本合同执行过程中如发生争议，甲、乙双方应协商解决。如协商不成，甲、乙双方一致同意提交XX机构，依据其仲裁规则进行裁决。双方一致同意仲裁结果是最终的，并对双方均有约束力，并遵照执行。

9　本合同经双方签字盖章后生效

甲方：_____（盖章）

法定代表人/委托代理人：_____（签名）

年　月　日

乙方：_____（盖章）

法定代表人/委托代理人：_____（签名）

年　月　日

附件 1 服务项目表

序号	服务名称	型号及配置描述	数量	服务期限	服务费用
总计					

附件 2 服务水平协议

服务水平协议

甲方：

乙方：

1.目的

为规范乙方所提供的云计算服务及相关客户服务的品质，保障甲方享有的服务品质，甲乙双方本着友好协商，互相理解，互相促进的原则签订此协议。本协议仅对甲方所获得的产品保障和服务品质做出相关约定。

2.服务指标

序号	服务质量指标	参数值
1	电力的持续供应	≥【】%
2	网络联通性	≥【】%
3	服务器无故障率	≥【】%
4	一级故障解决率	≥【】%
5	二级故障解决率	≥【】%
6	客服服务时间	7×24 小时
7	服务响应时间	响应时间≤【】分钟
8	数据备份频率	每【】（周/天/月）【】次
9	备份数据保留时间	【】个（周/天/月）
10	日志保留时间	【】个（周/天/月）
11	紧急情况报告保证	【】分钟之内通知甲方
12	免费培训保障	每年≥【】次

2.1 电力的持续供应：乙方云计算平台向甲方提供的市电或 UPS 电源具有电力。

2.2 网络联通性：是指乙方云计算平台的网络设备同甲方网站是否联通。

2.3 系统无故障率：指甲方系统无故障时间与系统进行时间的比率。

2.4 一级故障：甲方整个系统不能使用的故障。

2.5 一级故障解决率：解决时间≤【】小时的次数与所有一级故障次数的比率。

2.6 二级故障：甲方系统主要模块和功能不可用。

2.7 二级故障解决率：解决时间≤【】小时的次数与所有二级级故障次数的比率。

2.8 服务响应时间：指在服务时间（7×24）内，甲方客户提出服务请求后，乙方响应请求的时间。

2.9 数据备份频率：乙方提供每【】周一次邮件内容的数据备份，备份数据保留时间为【】周。

2.10 免费培训保障：乙方为甲方提供每年不低于【】次的免费产品培训服务。

2.11 紧急情况报告保证：发生安全事故及乙方监测到甲方网站的非正常运行情况报告。

3.违约责任

3.1 当乙方提供服务品质无法满足服务项目中约定的指标而造成服务中断时，乙方赔偿甲方【】。

3.2 因不可抗力原因造成的无法满足约定指标或者造成损失时，乙方不承担赔偿责任。

3.3 当影响到服务品质的指标不在约定范围内时，乙方不承担赔偿责任，甲乙双方可以通过充分沟通重新调整服务项目和品质要求。

4.不可抗力

因不可抗力而造成无法履行保证时，乙方将不承担违约责任。本协议中规定的不可抗力包括：

地震、台风、洪水等自然灾害；

战争、罢工、停电、政府行为等；

政府电力部门或电信部门的行为；

外部人为破坏因素引起的，超过安全设备的承载能力。

5.本协议一式两份，双方各执一份。

6.本协议自双方签字盖章之日起生效，于甲方停止采用乙方云计算服务时终止。

甲方：（盖章） 乙方：（盖章）

甲方代表（签字）： 乙方代表（签字）：

日期： 日期：

附件 3 保密协议

保密协议

鉴于：

甲乙双方（以下简称“双方”）正在进行_____项目（以下简称“项目”）；双方就该项目的实施以及合作过程中，甲方向乙方提供有关保密信息，且该保密信息属甲方合法所有；甲乙双方均希望对本协议所述保密信息予以有效保护。经双方协商，达成本协议。

一、本协议所指保密范围：

甲方提供给乙方的数据和资料，以及云计算平台上甲方系统运行过程中收集、产生、存储的数据和文档等，包括数据文件、程序代码、说明书、技术资料、运行日志等。

二、双方权利与义务

（1）甲乙双方应遵守相关法律、法规、政策、规章、制度和协议，乙方在基于甲方授权的前提下合理使用甲方信息，不得以任何手段获取、使用协议规定以外的甲方信息。

（2）未经授权，乙方不应在工作职责授权范围以外使用、分享甲方信息。

（3）未经授权，乙方不得泄露、披露、转让以下信息：

a）技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；

b）业务信息：同甲方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；

c）安全信息：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限信息，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息。

（4）第三方要求披露（3）中信息或甲方敏感信息时，乙方不应响应，并立刻报告。

（5）对违反协议或可能导致违反协议、规定、规程、法律的活动、策略或实践，乙方一经发现，应立即向甲方报告。

（6）上述限制条款不适用于以下情况：

乙方应法院或其它法律、行政管理部门要求披露的信息（通过口头提问、询问、要求资料或文件、传唤、民事或刑事调查或其他程序）因而透露保密信息，在该种情况发生时，乙方应立即向甲方发出通知，并作出必要说明。

三、违约责任

乙方未履行本协议项下的条款均被视为违约。乙方应承担因自己的违约行为而给甲方造成的损

失。

四、免责条款

由于地震、水灾、火灾或政策变化等人力不能预见、不能避免、不能抗拒的原因，导致乙方不能履行或不能完全履行本协议项下的有关义务时，乙方可不承担违约责任；在不可抗力影响消除后的合理时间内，乙方应当继续履行本协议。

五、本协议有效期自【】年【】月【】日至【】年【】月【】日。

六、争议的解决

本协议受中华人民共和国（以下简称“中国”）的法律管辖并按照中国的法律进行解释。由于本协议的履行或解释而产生的或与之有关的任何争议，如双方无法协商解决，应提交【】仲裁机构并按照其当时有效的仲裁规则和仲裁程序进行最终裁决。

七、经双方书面确认，任何一方不得变更或修改本协议，国家另有规定的除外。

八、本协议未尽事宜，双方可签订补充协议。本协议的补充协议为其不可分割的一部分，与本协议具有同等法律效力。

九、本协议一式两份，双方各执一份。

十、本协议自双方签字盖章之日起生效。

甲方：　　乙方：

授权代表：　　授权代表：

日期：　　日期：

参 考 文 献

[1] 《国务院办公厅关于印发政府网站发展指引的通知》.
[2] 《关于加强党政部门云计算服务网络安全管理的意见》.
[3] 《国家电子政务“十二五”规划》.
[4] 《国外政府云计算安全标准建设及启示》.
[5] 《基于云计算的电子政务公共平台顶层设计指南》.
[6] 《欧洲政府云计算与发展研究》.
[7] 《信息安全等级保护管理办法》.
[8] GB/T 29245-2012 信息安全技术 政府部门信息安全管理基本要求.
[9] NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, May 2012.
[10] AGIMO, Australia. A Guide to Implementing Cloud Services. September 2012.
[11] NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations. September 2011.
[12] NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap. June 2013.
[13] 《Federal Cloud Computing Strategy》,February 2011
[14] NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011.