

ICS ××.×××.××  
B××

DB13

河北省地方标准

DB 13/ T ×××—××××

信息安全技术  
电子政务云安全保护管理与技术规范

Information security technology

E-government cloud security protection management and technical specification

(征求意见稿)

××××-××-××发布

××××-××-××实施

河北省技术质量监督局

发布

目 次

前 言..... IV

引 言..... V

信息安全技术 电子政务云安全保护管理与技术规范..... 1

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

3.1 安全保护能力..... 1

4 电子政务云保护概述..... 1

4.1 电子政务云..... 1

4.2 电子政务云安全保护能力..... 1

5 电子政务云安全保护技术基本要求..... 1

5.1 物理安全..... 1

5.1.1 物理位置的选择..... 1

5.1.2 物理访问控制..... 1

5.1.3 防盗窃和防破坏..... 2

5.1.4 防雷击..... 2

5.1.5 防火..... 2

5.1.6 防水和防潮..... 2

5.1.7 防静电..... 2

5.1.8 温湿度控制..... 2

5.1.9 电力供应..... 2

5.1.10 设备运送和移除..... 3

5.1.11 电磁防护..... 3

5.2 网络安全..... 3

5.2.1 结构安全..... 3

5.2.2 访问控制..... 3

5.2.3 安全审计..... 4

5.2.4 边界完整性检查..... 4

5.2.5 入侵防范..... 4

5.2.6 恶意代码防范..... 4

5.2.7 网络设备防护..... 4

5.3 主机安全..... 5

5.3.1 身份鉴别..... 5

5.3.2 访问控制..... 5

5.3.3 安全审计..... 5

5.3.4 剩余信息保护..... 6

5.3.5 入侵防范..... 6

5.3.6 恶意代码防范..... 6

5.3.7 镜像和快照保护..... 6

5.3.8 资源控制..... 6

5.4 应用安全..... 7

5.4.1 身份鉴别..... 7

5.4.2 访问控制..... 7

5.4.3 安全审计..... 7

5.4.4 剩余信息保护..... 7

5.4.5 通信完整性..... 7

5.4.6 通信保密性..... 8

5.4.7 抗抵赖..... 8

5.4.8 软件容错..... 8

5.4.9 资源控制..... 8

5.5 数据安全及备份恢复.....8

5.5.1 数据完整性.....8

5.5.2 数据保密性.....8

5.5.3 数据迁移.....8

5.5.4 备份和恢复.....8

6 电子政务云安全保护管理基本要求.....9

6.1 安全管理制度.....9

6.1.1 管理制度.....9

6.1.2 系统文档.....9

6.1.3 制定和发布.....9

6.1.4 评审和修订.....9

6.2 安全管理机构.....10

6.2.1 岗位设置.....10

6.2.2 人员配备.....10

6.2.3 授权和审批.....10

6.2.4 沟通和合作.....10

6.2.5 审核和检查.....10

6.3 人员安全管理.....11

6.3.1 人员录用.....11

6.3.2 人员离岗.....11

6.3.3 人员考核.....11

6.3.4 安全意识教育和培训.....11

6.3.5 外部人员访问管理.....11

6.4 系统建设管理.....11

6.4.1 资源分配.....11

6.4.2 系统生命周期.....11

6.4.3 配置管理计划.....12

6.4.4 系统定级.....12

6.4.5 安全方案设计.....12

6.4.6 开发过程、标准和工具.....12

6.4.7 开发商配置管理.....13

6.4.8 产品采购和使用.....13

6.4.9 自行软件开发.....13

6.4.10 外包软件开发.....13

6.4.11 工程实施.....13

6.4.12 测试验收.....13

6.4.13 开发商安全测试和评估.....14

6.4.14 系统交付.....14

6.4.15 系统备案.....14

6.4.16 等级测评.....14

6.4.17 安全服务商选择.....14

6.4.18 外部信息系统服务及相关服务.....15

6.5 系统运维管理.....15

6.5.1 环境管理.....15

6.5.2 资产管理.....15

6.5.3 安全资源.....15

6.5.4 介质管理.....15

6.5.5 设备管理.....16

6.5.6 受控维护.....16

6.5.7 维护工具.....16

6.5.8 维护人员.....16

6.5.9 监控管理和安全管理中心.....16

6.5.10 网络安全管理.....16

6.5.11 外部信息系统的使用.....17

6.5.12 系统安全管理.....17

6.5.13 恶意代码防范管理.....17

6.5.14 密码管理.....17

6.5.15 变更管理.....17

6.5.16 变更控制.....18

6.5.17 备份与恢复管理.....18

6.5.18 安全事件处置.....18

6.5.19 应急预案管理.....18

6.5.20 支撑客户的业务连续性计划.....19

参考文献.....20

## 前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由河北省工业和信息化厅提出并归口。

本标准起草单位：河北省信息安全测评中心、杭州华三通信技术有限公司、华为技术有限公司、中国联合网络通信有限公司河北省分公司。

本标准主要起草人：陶卫江、张凤臣、闫利平、黄亮、王辙、刘艳、蒋啸龙、吴书林、胡金岭、梁志、孟宪辉、崔健、李鹏、王淑婧、李娜、高凡、李陶钧、李韦、王子强、张鹏、张振博、陈永军、姚会亭、苏桂敏、郑丹、重健。

## 引 言

云计算是一种提供信息技术服务的模式。随着云计算在政府部门的广泛应用，政务云的安全需求成为个政府部门关注的焦点。为了规范云服务商、云租户和监管部门的行为，减少安全威胁，依据《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〔2014〕14号）、《国务院关于促进云计算创新发展培育信息产业新业态的意见》（国发〔2015〕5号），制定本标准。

电子政务云的安全管理要求分为技术和管理。本标准在 GB/T 22239—2008 等技术类标准的基础上，根据现有技术的发展水平，提出和规定了电子政务云的最低安全技术和管理要求，即技术安全要求。本标准即适用于电子政务云的安全测评，又适用于指导电子政务云的安全建设和管理，以及电子政务云安全主管部门的监督检查。

# 信息安全技术

## 电子政务云安全保护管理与技术规范

### 1 范围

本标准规定了电子政务云安全保护物理安全、网络安全、主机安全、应用安全、数据安全五个方面的技术要求。

本标准适用于指导政府机关等行使公共管理职责的机构的各类组织和机构建立电子政务云安全保护的管理指导和评估。

### 2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

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 22239-2008 信息安全技术 信息系统安全等级保护基本要求

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〔2014〕14号

国务院关于促进云计算创新发展培育信息产业新业态的意见国发〔2015〕5号

### 3 术语和定义

GB/T 31167-2014、GB/T 31168-2014和GB/T 22239-2008中界定的以及下术语和定义适用于本标准。

#### 3.1 安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

### 4 电子政务云保护概述

#### 4.1 电子政务云

电子政务云（E-government cloud）属于政府云，结合了云计算技术的特点，对政府管理和服务职能进行精简、优化、整合，并通过信息化手段在政务上实现各种业务流程办理和职能服务，为政府各级部门提供可靠的基础IT服务平台。。

#### 4.2 电子政务云安全保护能力

电子政务云应具备的基本安全保护能力如下：

应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

### 5 电子政务云安全保护技术基本要求

#### 5.1 物理安全

##### 5.1.1 物理位置的选择

本项目包括但不限于：

- a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
- c) 确保机房位于中国境内。
- d) 确保云计算服务器及运行关键业务和数据的物理设备位于中国境内。

##### 5.1.2 物理访问控制

本项目包括但不限于：

- a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员；
- b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；
- c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
- d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。
- e) 制定和维护具有机房访问权限的人员名单。
- f) 及时从授权访问名单中删除不再需要访问机房的人员。
- g) 根据职位、角色以及访问的必要性对机房进行细粒度的物理访问授权。
- h) 除对机房出入口实施访问控制外，云服务商还应严格限制对云计算平台设备的物理接触。

### 5.1.3 防盗窃和防破坏

本项目包括但不限于：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 应利用光、电等技术设置机房防盗报警系统；
- f) 应对机房设置监控报警系统。

### 5.1.4 防雷击

本项目包括但不限于：

- a) 机房建筑应设置避雷装置；
- b) 应设置防雷保安器，防止感应雷；
- c) 机房应设置交流电源地线。

### 5.1.5 防火

本项目包括但不限于：

- a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
- b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

### 5.1.6 防水和防潮

本项目包括但不限于：

- a) 水管安装，不得穿过机房屋顶和活动地板下；
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- d) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

### 5.1.7 防静电

本项目包括但不限于：

- a) 主要设备应采用必要的接地防静电措施；
- b) 机房应采用防静电地板。

### 5.1.8 温湿度控制

本项目包括但不限于：

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

### 5.1.9 电力供应

本项目包括但不限于：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求；
- c) 应设置冗余或并行的电力电缆线路为计算机系统供电；



d)应建立备用供电系统。

e)为云计算平台配备应急照明设备并进行维护，并可在断电的情况下触发，应急照明包括机房内的紧急通道和疏散通道指示牌。

#### 5.1.10 设备运送和移除

本项目包括但不限于：

a)建立重要设备台帐，明确设备所有权，并确定责任人；

#### 5.1.11 电磁防护

本项目包括但不限于：

a)应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b)电源线和通信线缆应隔离铺设，避免互相干扰；

c)应对关键设备和磁介质实施电磁屏蔽。

### 5.2 网络安全

#### 5.2.1 结构安全

本项目包括但不限于：

a)应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；

b)应保证网络各个部分的带宽满足业务高峰期需要；

c)应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

d)应绘制与当前运行情况相符的网络拓扑结构图；

e)应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f)应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

g)应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

h)应实现不同云租户之间网络资源的隔离，并避免网络资源的过量占用；

i)应绘制与当前运行情况相符的虚拟网络拓扑结构图，并能对虚拟网络资源、网络拓扑进行实时更新和集中监控；

j)应保证虚拟机只能接收到目的地址包括自己地址的报文；

k)应保证云平台管理流量与云租户业务流量分离；

l)应能识别、监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量；

m)应提供开放接口，允许接入第三方安全产品，实现云租户的网络之间、安全区域之间、虚拟机之间的网络安全防护；

n)应根据云租户的业务需求定义安全访问路径。

#### 5.2.2 访问控制

本项目包括但不限于：

a)应在网络边界部署访问控制设备，启用访问控制功能；

b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

c)应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；

d)应在会话处于非活跃一定时间或会话结束后终止网络连接；

e)应限制网络最大流量数及网络连接数；

f)重要网段应采取技术手段防止地址欺骗；

g)应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统资源访问，控制粒度为单个用户；

- h) 应限制具有拨号访问权限的用户数量。
- i) 应在虚拟网络边界部署访问控制设备，并设置访问控制规则；
- j) 应依据安全策略控制虚拟机间的访问；
- k) 应实时监视云服务远程连接，并在发现未授权连接时，采取恰当的应对措施；
- l) 应对远程执行特权命令进行限制，采取严格的保护措施并进行审计；
- m) 当进行远程管理时，管理终端和云平台边界设备之间应建立双向身份验证机制。

### 5.2.3 安全审计

本项目包括但不限于：

- a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；
- b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- c) 应能够根据记录数据进行分析，并生成审计报表；
- d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。
- e) 应根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
- f) 应为安全审计数据的汇集提供接口，并可供第三方审计；
- g) 应能够根据记录数据进行分析，并生成审计报表；
- h) 应根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

### 5.2.4 边界完整性检查

本项目包括但不限于：

- a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确确定出位置，并对其进行有效阻断；
- b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确确定出位置，并对其进行有效阻断。
- c) 将允许外部公开直接访问的组件、服务等，划分在一个与内部网络逻辑隔离的子网络上。并确保允许外部人员访问的组件与允许客户访问的组件在逻辑层面实现严格的网络隔离；
- d) 应支持对虚拟机的DHCP隔离，防止该虚拟机通过安装的DHCP软件，为其他虚拟机分配IP地址，影响其他虚拟机的正常运行。

### 5.2.5 入侵防范

本项目包括但不限于：

- a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；
- b) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
- c) 应能检测到云租户对外的攻击行为，并能记录攻击类型、攻击时间、攻击流量；
- d) 应具备对异常流量的识别、监控和处理能力；
- e) 应对发布到互联网的有害信息进行实时监测和告警。

### 5.2.6 恶意代码防范

本项目包括但不限于：

- a) 应在网络边界处对恶意代码进行检测和清除；
- b) 应维护恶意代码库的升级和检测系统的更新。

### 5.2.7 网络设备防护

本项目包括但不限于：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备用户的标识应唯一；
- d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
- e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

h)应实现设备特权用户的权限分离。

i)应在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制；

j)应采取必要措施防止网络策略控制器和网络设备（或设备代理）之间的网络通信被窃听和嗅探。

## 5.3 主机安全

### 5.3.1 身份鉴别

本项目包括但不限于：

a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

### 5.3.2 访问控制

本项目包括但不限于：

a)应启用访问控制功能，依据安全策略控制用户对资源的访问；

b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c)应实现操作系统和数据库系统特权用户的权限分离；

d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

e)应及时删除多余的、过期的帐户，避免共享帐户的存在。

f)应对重要信息资源设置敏感标记；

g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

h)应保证虚拟机之间、虚拟机与宿主机之间的安全隔离；

i)当进行远程管理时，防止远程管理设备同时直接连接其他网络资源；

j)应确保云平台运维管理员和云服务管理员的权限分离；

k)应保证虚拟机仅能迁移至相同安全保护等级的资源池；

l)应确保仅云租户拥有其数据库的最高管理权限；

m)应提供云平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限。

### 5.3.3 安全审计

本项目包括但不限于：

a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d)应能够根据记录数据进行分析，并生成审计报表；

e)应保护审计进程，避免受到未预期的中断；

f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。

g)应根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；

h)应保证云服务方对云租户系统和数据的操作可被云租户审计；

i)应保证审计数据的真实性和完整性；

- j) 应为安全审计数据的汇集提供接口，并可供第三方审计；
- k) 应根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

#### 5.3.4 剩余信息保护

本项目包括但不限于：

- a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。
- c) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

#### 5.3.5 入侵防范

本项目包括但不限于：

- a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
- b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；
- c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。
- d) 应能够检测虚拟机对宿主机资源的异常访问，并进行告警；
- e) 应能够检测虚拟机之间的资源隔离失效，并进行告警；
- f) 应能检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。

#### 5.3.6 恶意代码防范

本项目包括但不限于：

- a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
- b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；
- c) 应支持防恶意代码的统一管理。
- d) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并提出告警。

#### 5.3.7 镜像和快照保护

本项目包括但不限于：

- a) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- b) 应采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
- c) 应针对重要业务系统提供加固的操作系统镜像。

#### 5.3.8 资源控制

本项目包括但不限于：

- a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
- b) 应根据安全策略设置登录终端的操作超时锁定；
- c) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；
- d) 应限制单个用户对系统资源的最大或最小使用限度；
- e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。
- f) 应提供自动保护功能，当故障发生时自动保护所有状态，保证系统能够进行恢复；
- g) 应屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；
- h) 应对物理资源和虚拟资源按照策略做统一管理调度与分配；
- i) 应保证虚拟资源的业务处理能力具备冗余空间，满足业务高峰期需要；
- j) 应保证分配给虚拟机的内存空间仅供其独占访问；
- k) 应根据业务服务的重要性来分配虚拟资源的优先级别，保证在资源紧张的时候优先保护重要业务服务所占用资源；

- l) 应对虚拟机的网络接口的带宽进行设置，并进行监控；
- m) 应为监控信息的汇集提供接口，并实现集中监控；
- n) 确保虚拟镜像模板的配置正确性，并明确模板的谱系来源。

## 5.4 应用安全

### 5.4.1 身份鉴别

本项目包括但不限于：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
- c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
- d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

### 5.4.2 访问控制

本项目包括但不限于：

- a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
- d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
- e) 应具有对重要信息资源设置敏感标记的功能；
- f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；
- g) 应保证云计算服务对外接口的安全性。

### 5.4.3 安全审计

本项目包括但不限于：

- a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
- b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
- e) 应根据云服务方和云租户的职责划分，收集各自控制的部分的审计数据；
- f) 应保证云服务方对云租户系统和数据的操作可被云租户审计；
- h) 应保证审计数据的真实性和完整性；
- i) 应为安全审计数据的汇集提供接口，并可供第三方审计；
- j) 系统日志应区分操作日志和运行日志；
- k) 应支持系统每天自动进行定时备份；
- l) 有查询权限的人才能导出日志，应设置日志独有的导出格式；
- m) 云计算平台内部有唯一确定的系统时钟，且所有设备根据唯一确定时钟统一时间。

### 5.4.4 剩余信息保护

本项目包括但不限于：

- a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

### 5.4.5 通信完整性

本项目包括但不限于：

应采用密码技术保证通信过程中数据的完整性。

#### 5.4.6 通信保密性

本项目包括但不限于：

- a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
- b) 应对通信过程中的整个报文或会话过程进行加密。

#### 5.4.7 抗抵赖

本项目包括但不限于：

- a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
- b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

#### 5.4.8 软件容错

本项目包括但不限于：

- a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

#### 5.4.9 资源控制

本项目包括但不限于：

- a) 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
- b) 应能够对系统的最大并发会话连接数进行限制；
- c) 应能够对单个帐户的多重并发会话进行限制；
- d) 应能够对一个时间段内可能的并发会话连接数进行限制；
- e) 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；
- f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；
- g) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。
- h) 应能够对应用系统的运行状况进行监测，并在发现异常时进行告警。

### 5.5 数据安全及备份恢复

#### 5.5.1 数据完整性

本项目包括但不限于：

- a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
- b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
- c) 应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

#### 5.5.2 数据保密性

本项目包括但不限于：

- a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；
- b) 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。
- c) 应确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露。

#### 5.5.3 数据迁移

本项目包括但不限于：

- a) 数据迁移过程中应部署监控机制；
- b) 应保证数据迁移过程中，平台的业务操作能连续运行且不中断；
- c) 迁移后的数据自动恢复后，系统应能够正常使用。

#### 5.5.4 备份和恢复

本项目包括但不限于：

- a) 应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；
- b) 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；
- c) 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；
- d) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。
- e) 云租户应在本地保存其业务数据的备份；
- f) 应提供查询云租户数据及备份存储位置的方式；
- g) 应保证云租户业务及数据能移植到其他云平台或者迁移到本地信息系统；
- h) 应具备系统级备份能力，按照一定的时间频率，对信息系统中的系统级信息进行备份，如系统状态、操作系统及应用软件；
- i) 应防止通过备份过程访问客户的明文数据。

## 6 电子政务云安全保护管理基本要求

### 6.1 安全管理制度

#### 6.1.1 管理制度

本项目包括但不限于：

- a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 应对安全管理活动中的各类管理内容建立安全管理制度；
- c) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
- d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

#### 6.1.2 系统文档

本项目包括但不限于：

- a) 要求信息系统、组件或服务的开发商制定管理员文档，且涵盖以下信息：
  - 1) 信息系统、组件或服务的安全配置，以及安装和运行说明。
  - 2) 安全特性或功能的使用和维护说明。
  - 3) 与管理功能有关的配置和使用方面的注意事项。
- b) 要求信息系统、组件或服务的开发商制定用户文档，且涵盖以下信息：
  - 1) 用户可使用的安全功能或机制，以及对如何有效使用这些安全功能或机制的说明。
  - 2) 有助于用户更安全地使用信息系统、组件或服务的方法或说明。
  - 3) 对用户安全责任和注意事项的说明。

#### 6.1.3 制定和发布

本项目包括但不限于：

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 安全管理制度应具有统一的格式，并进行版本控制；
- c) 应组织相关人员对制定的安全管理制度进行论证和审定；
- d) 安全管理制度应通过正式、有效的方式发布；
- e) 安全管理制度应注明发布范围，并对收发文进行登记。

#### 6.1.4 评审和修订

本项目包括但不限于：

- a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；

b) 应定期或不定期对安全管理制度进行检查和审定,对存在不足或需要改进的安全管理制度进行修订。

## 6.2 安全管理机构

### 6.2.1 岗位设置

本项目包括但不限于:

a) 应设立信息安全管理工作的职能部门,设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责;

b) 应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责;

c) 应成立指导和管理信息安全工作的委员会或领导小组,其最高领导由单位主管领导委任或授权;

d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

### 6.2.2 人员配备

本项目包括但不限于:

a) 应配备一定数量的系统管理员、网络管理员、安全管理员等;

b) 应配备专职安全管理员,不可兼任;

c) 关键事务岗位应配备多人共同管理。

### 6.2.3 授权和审批

本项目包括但不限于:

a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等;

b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序,按照审批程序执行审批过程,对重要活动建立逐级审批制度;

c) 应定期审查审批事项,及时更新需授权和审批的项目、审批部门和审批人等信息;

d) 应记录审批过程并保存审批文档。

### 6.2.4 沟通和合作

本项目包括但不限于:

a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通,定期或不定期召开协调会议,共同协作处理信息安全问题;

b) 应加强与兄弟单位、公安机关、电信公司的合作与沟通;

c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通;

d) 应建立外联单位联系列表,包括外联单位名称、合作内容、联系人和联系方式等信息;

e) 应聘请信息安全专家作为常年的安全顾问,指导信息安全建设,参与安全规划和安全评审等。

### 6.2.5 审核和检查

本项目包括但不限于:

a) 安全管理员应负责定期进行安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况;

b) 应由内部人员或上级单位定期进行全面安全检查,检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等;

c) 应制定安全检查表格实施安全检查,汇总安全检查数据,形成安全检查报告,并对安全检查结果进行通报;

d) 应制定安全审核和安全检查制度规范安全审核和安全检查工作,定期按照程序进行安全审核和安全检查活动。



## 6.3 人员安全管理

### 6.3.1 人员录用

本项目包括但不限于：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- c) 应签署保密协议；
- d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

### 6.3.2 人员离岗

本项目包括但不限于：

- a) 应严格规范人员离岗过程，及时终止离岗员工的所有访问权限；
- b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- c) 应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

### 6.3.3 人员考核

本项目包括但不限于：

- a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
- b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
- c) 应对考核结果进行记录并保存。

### 6.3.4 安全意识教育和培训

本项目包括但不限于：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
- c) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
- d) 应对安全教育和培训的情况和结果进行记录并归档保存。

### 6.3.5 外部人员访问管理

本项目包括但不限于：

- a) 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；
- b) 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

## 6.4 系统建设管理

### 6.4.1 资源分配

本项目包括但不限于：

- a) 在规划系统建设时考虑系统的安全需求。
- b) 在工作计划和预算文件中，将信息安全作为单列项予以说明。

### 6.4.2 系统生命周期

本项目包括但不限于：

- a) 将信息安全纳入云平台系统的整个生命周期，确保信息安全措施同步规划、同步建设、同步运行。
- b) 确定整个信息系统生命周期内的信息安全角色和责任。

- c) 将信息安全角色明确至相应责任人。
- d) 将信息安全风险管理过程集成到系统生命周期活动中。

#### 6.4.3 配置管理计划

本项目包括但不限于：

- a) 制定并实施云计算平台的配置管理计划。
- b) 在配置管理计划中，规定配置管理相关人员的角色和职责，并详细规定配置管理的流程。
- c) 在系统生命周期内，建立配置项标识和管理流程。
- d) 定义信息系统的配置项并将其纳入配置管理计划。
- e) 保护配置管理计划，以防非授权的泄露和变更。

#### 6.4.4 系统定级

本项目包括但不限于：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；
- c) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；
- d) 应确保信息系统的定级结果经过相关部门的批准。

#### 6.4.5 安全方案设计

本项目包括但不限于：

- a) 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；
- b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
- c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
- d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
- e) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

#### 6.4.6 开发过程、标准和工具

本项目包括但不限于：

- a) 要求信息系统、组件或服务的开发商制定明确的开发规范，在规范中明确以下事项：
  - 1) 所开发系统的安全需求。
  - 2) 开发过程中使用的标准和工具。
  - 3) 开发过程中使用的特定工具选项和工具配置。
- b) 要求信息系统、组件或服务的开发商在开发过程的初始阶段定义质量度量标准，并以定期检查质量度量标准的落实情况。
- c) 要求信息系统、组件或服务的开发商对信息系统进行威胁和脆弱性分析。
- d) 要求信息系统、组件或服务的开发商通过清晰的流程来持续改进开发过程，以满足质量要求，适应威胁环境的变化。
- e) 要求信息系统、组件或服务的开发商使用[赋值：自行定义或云服务商定义的工具]执行漏洞分析，明确漏洞利用的可能性，确定漏洞消减措施，并将工具的输出和分析结果提交给 相关人员。
- f) 要求信息系统、组件或服务的开发商即使在交付信息系统、组件或服务后，也应跟踪漏洞情况，在发布漏洞补丁前便应通知云服务商，且应将漏洞补丁交由云服务商审查、验证并允许云服务商自行安装。

- h) 在信息系统、组件或服务的开发和测试环境使用生产数据时，应先行批准、记录并进行保护。
- i) 要求信息系统、组件或服务的开发商制定应急预案，并将应急预案纳入云服务商的事件响应计划中。

#### 6.4.7 开发商配置管理

本项目包括但不限于：

- a) 在信息系统、组件或服务的设计、开发、运行过程中实施配置管理。
- b) 记录、管理和控制的变更的完整性。根据实际情况，配置项可包括但不限于：形式化模型、功能、高层设计说明书、低层设计说明书、其他设计数据、实施文档、源代码和硬件原理图、目标代码的运行版本、版本对比工具、测试设备和文档。
- c) 得到批准后，才能对所提供的信息系统、组件或服务进行变更。
- d) 记录对信息系统、组件或服务的变更及其所产生的安全影响。
- e) 跟踪信息系统、组件或服务中的安全缺陷和解决方案。
- f) 要求信息系统、组件或服务的开发商提供能够验证软件和固件组件完整性的方法。
- g) 在没有专用的开发商配置团队支持的情况下，由本组织的人员建立相应的配置管理流程。
- h) 要求信息系统、组件或服务的开发商提供对硬件组件进行完整性验证的方法，如防伪标签、可核查序列号、防篡改技术等。
- i) 要求信息系统、组件或服务的开发商，在开发过程中使用工具验证软件或固件源代码及目标代码的当前版本与以往版本异同，以防止非授权更改。

#### 6.4.8 产品采购和使用

本项目包括但不限于：

- a) 应确保安全产品采购和使用符合国家的有关规定；
- b) 应确保密码产品采购和使用符合国家密码主管部门的要求；
- c) 应指定或授权专门的部门负责产品的采购；
- d) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

#### 6.4.9 自行软件开发

本项目包括但不限于：

- a) 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；
- b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
- d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；
- e) 应确保对程序资源库的修改、更新、发布进行授权和批准。

#### 6.4.10 外包软件开发

本项目包括但不限于：

- a) 应根据开发需求检测软件质量；
- b) 应在软件安装之前检测软件包中可能存在的恶意代码；
- c) 应要求开发单位提供软件设计的相关文档和使用指南；
- d) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

#### 6.4.11 工程实施

本项目包括但不限于：

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
- c) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

#### 6.4.12 测试验收

本项目包括但不限于：

- a) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- c) 应对系统测试验收的控制方法和人员行为准则进行书面规定；

- d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
- e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

#### 6.4.13 开发商安全测试和评估

本项目包括但不限于：

- a) 制定并实施安全评估计划。
- b) 对信息系统、组件或服务进行安全性测试或评估。
- c) 提供安全评估计划的实施证明材料，并提供安全评估结果。
- d) 实施可验证的缺陷修复过程。
- e) 更正在安全评估过程中发现的脆弱性和不足。
- f) 要求信息系统、组件或服务的开发商在开发阶段使用静态代码分析工具识别常见缺陷，并记录分析结果。
- g) 要求信息系统、组件或服务的开发商实施威胁和脆弱性分析，并测试或评估已开发完成的信息系统、组件或服务。
- h) 在对信息系统、组件或服务的开发商进行评估时，应：
  - 1) 选择满足具有资质的第三方，验证开发商实施安全评估计划的正确性以及在安全测试或评估过程中产生的证据。
  - 2) 确保独立第三方能够获得足够的资料来完成验证过程，或已被授予获得此类信息的访问权限。
- i) 要求信息系统、组件或服务的开发商对特定代码实施人工代码审查，审查结果应易于理解且向云服务商提供，并确保云服务商可重构系统。
- e) 要求信息系统、组件或服务的开发商按照合同要求进行渗透性测试。
- f) 要求信息系统、组件或服务的开发商分析所提供的硬件、软件和固件容易受到攻击的脆弱点。
- g) 要求信息系统、组件或服务的开发商验证安全措施测试或评估过程满足合同要求。

#### 6.4.14 系统交付

本项目包括但不限于：

- a) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责系统运行维护的技术人员进行相应的技能培训；
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
- d) 应对系统交付的控制方法和人员行为准则进行书面规定；
- e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

#### 6.4.15 系统备案

本项目包括但不限于：

- a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
- b) 应将系统等级及相关材料报系统主管部门备案；
- c) 应将系统等级及其他要求的备案材料报相应公安机关备案。

#### 6.4.16 等级测评

本项目包括但不限于：

- a) 在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- c) 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；
- d) 应指定或授权专门的部门或人员负责等级测评的管理。

#### 6.4.17 安全服务商选择

本项目包括但不限于：

- a) 应确保安全服务商的选择符合国家的有关规定；
- b) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
- c) 应确保选定的安全服务商提供技术培训和承诺，必要的与其签订服务合同。

#### 6.4.18 外部信息系统服务及相关服务

本项目包括但不限于：

- a) 要求外部服务提供商遵从并实施云服务商的安全要求。
- b) 明确外部服务提供商的安全分工与责任，同时要求外部服务提供商接受相关客户监督。
- c) 在采购或外包之前进行风险评估。
- d) 确保采购或外包得到批准。
- e) 要求采购或外包的服务提供商明确说明该服务涉及的功能、端口、协议和其他服务。
- f) 建立并保持与外部服务提供商的信任关系。
- g) 制定全面的采购或外包安全控制措施，确保采购或外包提供商不损害本组织的利益。根据实际情况，安全防护措施可以是：

- 1) 对外部服务提供商进行人员背景审查，或要求外部服务提供商提供可信的人员背景审查结果。
- 2) 检查外部服务提供商资本变更记录。
- 3) 选择可信赖的外部服务提供商，如有过良好合作的提供商。
- 4) 定期或不定期检查外部服务提供商的设施。
- h) 基于采购或外包的安全要求，确定信息处理、信息或数据、信息系统服务的地点。

#### 6.5 系统运维管理

##### 6.5.1 环境管理

本项目包括但不限于：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- b) 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- d) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。

##### 6.5.2 资产管理

本项目包括但不限于：

- a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
- c) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- d) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

##### 6.5.3 安全资源

本项目包括但不限于：

- a) 对信息安全资源需求进行详细分析，并确保这些资源的可用性。
- b) 建立和维护信息系统的资产清单，该清单涵盖但不限于资产管理中a)条所规定的信息系统组件清单。

##### 6.5.4 介质管理

本项目包括但不限于：

- a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
- b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
- c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；
- d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；
- e) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

f) 应对重要介质中的数据和软件采取加密存储, 并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

#### 6.5.5 设备管理

本项目包括但不限于:

- a) 应对信息系统相关的各种设备 (包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理;
- b) 应建立基于申报、审批和专人负责的设备安全管理制度, 对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理;
- c) 应建立配套设施、软硬件维护方面的管理制度, 对其维护进行有效的管理, 包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等;
- d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理, 按操作规程实现主要设备 (包括备份和冗余设备) 的启动/停止、加电/断电等操作;
- e) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

#### 6.5.6 受控维护

本项目包括但不限于:

- a) 根据供应商的规格说明以及自身的业务要求, 对云计算平台组件的维护和修理进行规划、实施、记录, 并对维护和修理记录进行审查。
- b) 审批和监视所有维护行为, 现场维护、远程维护, 以及对设备的异地维护。
- c) 在将云计算平台组件转移到云服务商外部进行非现场的维护或维修前, 对设备进行净化, 清除介质中的信息。
- d) 在对云计算平台或组件进行维护或维修后, 检查所有可能受影响的安全措施, 以确认其仍正常发挥功能。
- e) 在维护记录中, 至少应包括: 维护日期和时间、维护人员姓名、陪同人员姓名、对维护活动的描述、被转移或替换的设备列表 (包括设备标识号) 等信息。
- f) 确保在将云计算平台的组件转移到云服务商外部进行非现场维护或维修前, 获得批准。

#### 6.5.7 维护工具

本项目包括但不限于:

- a) 云服务商应审批、控制并监视维护工具的使用。
- b) 检查由维护人员带入设施内部的维护工具, 以确保维护工具未被不当修改。
- c) 在使用诊断或测试程序前, 对其进行恶意代码检测。
- d) 为防止具有信息存储功能的维护设备在非授权情况下被转移出云服务商的控制范围, 采取以下一种或多种措施, 并获得本组织安全责任部门的批准:
  - 1) 确认待转移设备中没有云服务商和用户的信息。
  - 2) 净化或破坏设备。
  - 3) 将设备留在场所内部, 规定不得移出。

#### 6.5.8 维护人员

本项目包括但不限于:

- a) 建立对维护人员的授权流程, 对已获授权的人员建立列表。
- b) 确保只有列表中的维护人员, 才可在没有人员陪同时进行系统维护; 不在列表中的人员, 必须在授权且技术可胜任的人员陪同与监管下, 才可开展维护活动。

#### 6.5.9 监控管理和安全管理中心

本项目包括但不限于:

- a) 应对通信线路、主机、网络设备和应用程序的运行状况、网络流量、用户行为等进行监测和报警, 形成记录并妥善保存;
- b) 应组织相关人员定期对监测和报警记录进行分析、评审, 发现可疑行为, 形成分析报告, 并采取必要的应对措施;
- c) 应建立安全管理中心, 对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

#### 6.5.10 网络安全管理

本项目包括但不限于：

- a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
- c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
- d) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
- e) 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
- f) 应保证所有与外部系统的连接均得到授权和批准；
- g) 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；
- h) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

#### 6.5.11 外部信息系统的使用

本项目包括但不限于：

- a) 确保只在以下情况下允许授权人员通过外部信息系统进行访问，或利用这些信息系统处理、存储、传输云计算平台上的信息：
  - 1) 外部信息系统正确实现了云服务商的信息安全策略和安全计划所要求的安全措施，并通过了独立第三方机构的测试。
  - 2) 与外部系统所在实体签订了系统连接或处理协议，该协议应经过独立第三方机构的评价。
- b) 授权人员在外部信息系统上使用由云服务商控制的移动存储介质。

#### 6.5.12 系统安全管理

本项目包括但不限于：

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
- b) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- c) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
- d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
- e) 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
- f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

#### 6.5.13 恶意代码防范管理

本项目包括但不限于：

- a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
- d) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

#### 6.5.14 密码管理

本项目包括但不限于：

- 应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

#### 6.5.15 变更管理

本项目包括但不限于：

- a) 应确认系统中要发生的变更，并制定变更方案；
- b) 应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；

c) 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

d) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

#### 6.5.16 变更控制

本项目包括但不限于：

a) 明确云计算平台中有哪些变更需要包含在系统受控配置列表中，如主机配置项、网络配置项等。

b) 明确需定期变更的受控配置列表，并按照[赋值：云服务商定义的频率]对病毒库、入侵检测规则库、防火墙规则库、漏洞库等与信息安全相关的重要配置项进行更新。

c) 审查所提交的信息系统受控配置的变更事项，根据安全影响分析结果决定批准或否决，并进行记录。

d) 保留信息系统中受控配置的变更记录。

e) 定期对涉及系统受控配置变更的有关活动进行审查。

f) 明确受控配置变更的管理部门，负责协调和监管涉及受控配置变更的有关活动。

g) 根据客户要求，确定应报告的配置变更事项。在实施变更之前，向客户提供下列变更信息：

1) 变更计划发生的日期和时间。

2) 系统变更的详细信息。

3) 变更的安全影响分析结论。

h) 在云计算平台上实施变更之前，对受控配置变更项进行测试、验证和记录。

#### 6.5.17 备份与恢复管理

本项目包括但不限于：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d) 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；

e) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

#### 6.5.18 安全事件处置

本项目包括但不限于：

a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；

d) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

e) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

#### 6.5.19 应急预案管理

本项目包括但不限于：

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c) 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；

d) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；

e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。



#### 6.5.20 支撑客户的业务连续性计划

本项目包括但不限于：

a) 对云计算服务为客户业务连续性带来的风险进行评估，包括云计算服务失败、云服务商和客户之间网络连接中断、云计算服务终止等，并将相关的风险信息告知客户。

b) 将应急响应计划、灾难恢复计划及支撑客户实施业务连续性计划的有关措施告知客户，并根据客户的业务连续性计划的需要，对应急响应计划、灾难恢复计划进行调整。

### 参考文献

- (1) GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求
  - (2) GB/T31167-2014 信息安全技术 云计算服务安全指南
  - (3) GB/T31168-2014 信息安全技术 云计算服务安全能力要求
  - (4) 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〔2014〕14号)
  - (5) 国务院管理促进云计算创新发展培育信息产业新业态的意见(国发〔2015〕5号)
-