ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31506—2015

信息安全技术
政府门户网站系统安全技术指南

Information security technology—
Security technology guidelines for web portal system of government

2015-05-15 发布　　2016-01-01 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 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/TC 260)提出并归口。

本标准起草单位:北京信息安全测评中心、中国信息安全研究院有限公司、首都之窗运营管理中心。

本标准主要起草人:刘海峰、钱秀槟、左晓栋、张晓梅、闵京华、赵章界、李晨旸、李媛、梁博、王春佳、胡冰、李垚、陈萍、王喆。

引　言

由于网站具有面向互联网提供信息服务的特点，带有多种动机的攻击者可能会利用互联网网站的开放性和交互性进行漏洞探测，进而实施非授权访问、页面篡改、信息窃取或拒绝服务攻击。政府门户网站系统由于其代表政府的特殊属性，与普通网站相比更容易遭到来自互联网的攻击。

为了提高政府网站包括防篡改、防泄露、防中断、防恶意控制在内的综合安全防范能力，为各类政府机构保障网站安全提供技术指导，特制定本标准。

信息安全技术
政府门户网站系统安全技术指南

1 范围

本标准给出了政府门户网站系统安全技术控制措施。

本标准适用于指导政府部门开展门户网站系统安全技术防范工作，也可作为对政府门户网站系统实施安全检查的依据。

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/T 2887—2011 计算机场地通用规范

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

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 50174—2008 电子信息系统机房设计规范

3 术语和定义

GB/T 25069—2010 界定的以及下列的术语和定义适用于本文件。

3.1

政府门户网站 web portal of government

政府机构利用互联网发布政务信息、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。

3.2

政府门户网站系统 web portal system of government

政府门户网站及支撑其运行的物理环境、网络环境、服务器操作系统和数据库系统等。

3.3

网站用户 users of website

网站的访问者，既包括来自外部、访问获取网站资源的前台用户，也包括负责网站系统管理、内容管理的后台用户。

4 缩略语

下列缩略语适用于本文件。

ARP：地址接卸协议(Address Resolution Protocol)

CPU：中央处理器(Central Processing Unit)

DNS：域名系统(Domain Name System)

FTP:文件传输协议(File Transfer Protocol)
HTTP:超文本传输协议(Hypertext Transfer Protocol)
IDC:互联网数据中心(Internet Data Center)
IP:互联网协议(Internet Protocol)
IIS:互联网信息服务(Internet Information Services)
MAC:介质访问控制层(Media Access Control)
OA:办公自动化(Office Automation)
PV:页面浏览量(Page View)
SQL:结构化查询语言(Structured Query Language)
SSH:安全外壳协议(Secure Shell)
UPS:不间断电源(Uninterruptible Power System)
VLAN:虚拟局域网(Virtual Local Area Network)
VPN:虚拟专用网(Virtual Private Network)
WWW:万维网(World Wide Web)

5 概述

5.1 逻辑结构及运行模式

5.1.1 政府门户网站系统逻辑结构

政府门户网站系统主要面向互联网履行社会管理、公共服务职能,提供信息发布、在线服务、互动交流等服务,可根据功能需要通过指定的方式与 OA 系统、审批系统等政府部门其他业务系统交换数据。政府门户网站系统逻辑结构如图 1 所示。系统中,公众、企业、团体等用户通过互联网访问页面展示子系统的信息发布、在线服务、互动交流等服务,管理用户使用专用的管理终端从本地网络或通过在互联网上建立可信的 VPN 安全通道等方式访问内容管理及系统管理子系统,并对相关设备进行维护。网站数据处理子系统用于实现网站系统相关数据的存储及管理。

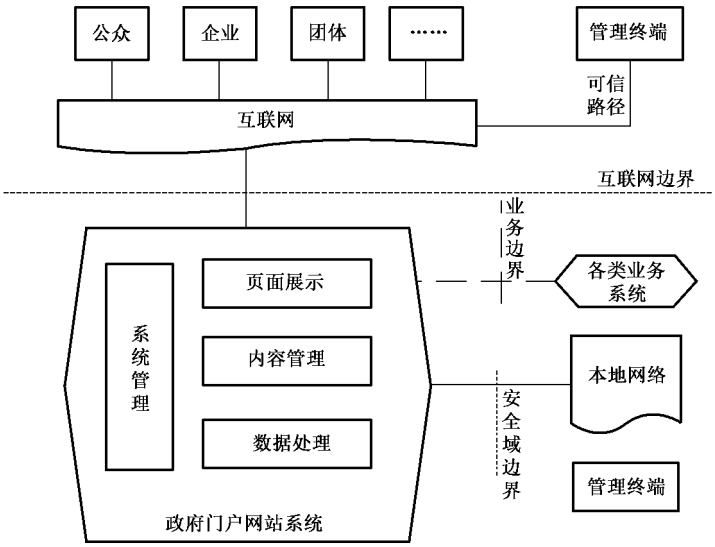

图 1 政府门户网站系统逻辑结构示意图

政府门户网站系统为互联网用户提供交互服务,系统与互联网之间存在互联网边界;与部署在本地网络不同安全域中的其他业务系统及终端进行交互,系统与本地网络之间存在安全域边界;与本地网络

中的其他业务系统交互特定数据，系统与本地其他业务系统之间存在业务边界。

5.1.2 政府门户网站系统组成结构

政府门户网站系统由门户网站及支撑其运行的物理环境、网络环境、服务器操作系统和数据库系统等构成，并与 OA 等其他业务系统之间存在数据交互的接口。系统组成结构可分为物理层、网络层、主机层、数据层和网站层五个层面，如图 2 所示。

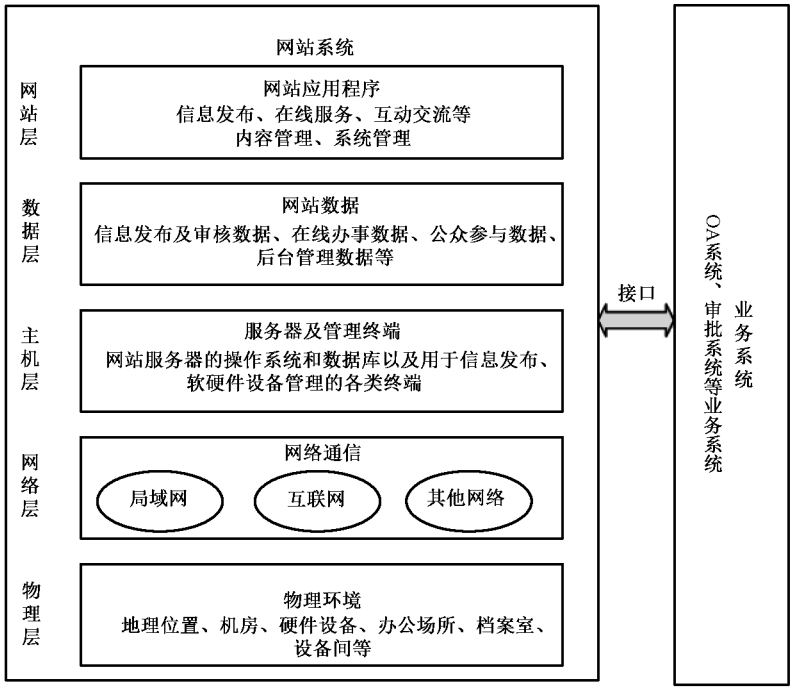

图 2 政府门户网站系统组成结构图

5.1.3 政府门户网站系统的常见运行模式

根据政府门户网站系统的实际运行情况，可分为以下三种主要运行模式：

a) 自建自管模式：单位自行设立网站服务器并组织管理。

b) 主机托管模式：单位将网站服务器委托专业的运营机构或互联网数据中心(IDC)来管理。

c) 主机租用模式：单位未设立网站服务器，租用运营商的服务器或虚拟服务器。

5.2 安全目标及防护措施

5.2.1 安全目标

政府门户网站系统由于其代表政府的特殊属性，与普通网站相比更容易遭到来自互联网的攻击。攻击者为了破坏政府形象、干扰政府工作秩序或窃取政府门户网站的敏感信息，采用 Web 应用攻击、拒绝服务攻击、暴力破解攻击、上传恶意木马等方式，实现篡改网页、中断服务、窃取信息、控制网站等攻击目标。因此，政府门户网站系统的安全防护工作应重点实现以下目标：

a) 提升网页防篡改及监测、恢复能力，降低网页被篡改的安全风险；

b) 提高入侵防范能力及系统可用性，降低网站服务中断的安全风险；

c) 强化数据安全管控措施，降低网站敏感信息泄露的安全风险；

d) 构建纵深防御体系，降低网站被恶意控制的安全风险。

5.2.2 安全技术措施概述

由于构成政府门户网站系统的物理层、网络层、主机层、数据层、网站层中的任何一层存在脆弱性，都可能导致政府门户网站出现内容篡改、服务中断、信息泄露及恶意控制等安全风险。为了实现上述安全目标，既需要针对构成网站系统的各层面存在的脆弱性提出安全控制措施，也需要针对政府门户网站系统提出综合性的安全控制措施。表 1 给出了政府门户网站系统的主要安全技术措施类别，具体安全技术措施详见第 6 章和第 7 章。

表 1 政府门户网站系统安全技术措施

网站系统安全技术措施					
层面防护		整体防护			
网站层	Web 应用安全 域名安全	运行支撑	攻击防范	安全监控	应急响应
数据层	内容发布及数据安全				
主机层	服务器安全 管理终端安全				
网络层	边界安全				
物理层	物理安全				

5.2.3 安全技术措施级别选择

本标准中的政府门户网站系统安全技术措施按其保障强度可划分为基本级安全技术措施、增强级安全技术措施两个等级。各单位可依据政府门户网站系统的行政级别、访问量、注册用户数和业务重要度选择相应强度级别的安全技术措施，见表 2。其中，**满足任意一条级别选择指标要求**的政府门户网站系统均宜选择增强级安全技术措施集。对于安全需求更高的政府门户网站系统，在实施增强措施的基础上，应按附录 A 中的高级安全技术措施进一步加强防护。

在本标准的安全技术措施描述中的粗体字表示较低等级安全技术措施中未出现或较高等级安全技术措施中加强的内容。

表 2 政府门户网站系统安全技术措施级别选择方法

级别选择因素	级别选择指标		适用的安全技术措施级别
行政级别	部委网站或省级网站	是	增强级安全技术措施集
		否	基本级安全技术措施集
访问量	有效日均访问次数≥20 万 PV	是	增强级安全技术措施集
		否	基本级安全技术措施集
注册用户数	累计注册用户总数≥50 万	是	增强级安全技术措施集
		否	基本级安全技术措施集
业务重要度	在线办事程度较高且网站受到破坏后，会对社会秩序和公共利益造成严重损害或者对国家安全造成损害； 或按照 GB/T 22240 要求安全保护等级级别定为三级以上(含三级)的网站	是	增强级安全技术措施集
		否	基本级安全技术措施集
注：有效日均访问次数应避免重复统计同一访问源在短时间内进行的多次访问。			

6 基本级安全技术措施

6.1 运行支撑

6.1.1 运行模式

本项措施包括：

a) 政府门户网站系统可选用自建自管、主机托管或虚拟主机等各种模式建设运行；

b) 政府门户网站系统如采用主机托管或虚拟主机方式建设运行，应优先选择由当地政府集中建设的数据中心。如采用主机托管或主机租用模式，应选择在物理安全、网络安全、主机安全等方面符合本标准基本级要求或 GB/T 22239 中第二级基本要求的数据中心；

c) 政府门户网站系统采用主机托管或虚拟主机方式运行时，网站系统的主管单位应明确本单位和数据中心双方的安全责任边界，建立对网站系统运行环境、安全技术措施运行情况的监督机制。

6.1.2 网站部署

本项措施包括：

a) 政府门户网站系统的 Web 应用程序应部署在独立的物理服务器或虚拟服务器上；

b) 同一政府门户网站系统的 Web 应用程序与数据库系统应部署在不同的物理服务器或虚拟服务器上；

c) 政府门户网站系统采用虚拟主机方式运行时，不应与非政务信息系统共用物理服务器。

6.1.3 边界确定

本项措施包括：

a) 明确政府门户网站系统与互联网之间的访问需求，以确定网络边界；

b) 明确政府门户网站系统与其他业务系统之间的访问需求，以确定安全域边界；

c) 如政府门户网站系统与其他业务系统存在数据交互，明确数据交互发生的业务边界（如发生交互的功能模块），并明确交互数据的性质和类型。

6.1.4 资源保障

6.1.4.1 性能保障

本项措施包括：

a) 应分析政府门户网站系统的性能需求，从网络带宽、服务器的处理能力、应用程序的并发处理能力等方面对网站性能予以保障；

b) 政府门户网站系统对外提供服务的互联网独享带宽不宜低于 2 Mbit/s。共享带宽条件下，网站互联网出口 HTTP 协议带宽不宜低于 2 Mbit/s；

c) 如政府门户网站系统访问量较大或提供在线视频等服务，可以依据网站的日均页面访问量（次）及业务高峰期（包括日高峰及高峰日）访问量酌情调整出口带宽。

6.1.4.2 设备冗余部署

应为支撑政府门户网站系统运转的关键设备提供硬件冗余措施，关键设备包括但不限于出口路由器、核心交换机、应用及数据库服务器等。

6.1.4.3 电力保障

可采用配备 UPS 等供电措施为政府门户网站系统提供短期备用电力。

6.2 物理安全

6.2.1 物理位置选择

不应使用境外机构提供或位于境外的物理服务器或虚拟主机。

6.2.2 物理环境控制

本项措施包括：

a) 政府门户网站系统关键设备所在机柜柜门应上锁；
b) 机房等重要区域应配置电子门禁系统，以便控制、鉴别和记录人员出入；
c) 需要进入机房对政府门户网站系统进行操作时，应由网站安全责任人或其指定的专人陪同；
d) 机房场地在防火、防水、防震、防盗、防尘、防静电、防雷、防电磁、监控、温湿度控制等方面应符合 GB/T 22239—2008 中第二级基本要求的物理安全要求。机房场地安全要求可参考 GB/T 50174—2008、GB/T 2887—2011 等国家标准中的相应要求。

6.2.3 传输线路保护

本项措施包括：

a) 应采用有效方法防范对信息传输线路的物理接触，如：将通信线缆铺设在地下或管道内等隐蔽处，以防止传输过程中的数据篡改、干扰以及对线缆的物理破坏；
b) 电源线和通信线缆宜隔离铺设，避免互相干扰。

6.3 边界安全

6.3.1 互联网边界安全

6.3.1.1 边界隔离方式

应在政府门户网站系统与互联网之间的网络边界处部署防火墙等边界隔离设备，并配置合理的边界访问控制策略，实现网站系统与互联网之间的逻辑隔离。

6.3.1.2 边界防护策略

本项措施包括：

a) 互联网边界隔离设备的默认过滤策略应设置为禁止任意访问；
b) 应仅允许互联网用户及单位内部普通用户终端访问网站服务器提供的 HTTP 服务等指定的服务和端口；
c) 应限制网站系统中的服务器主动访问互联网；
d) 应仅允许指定的 IP 地址访问网站服务器提供的内容管理、系统管理等服务和端口；
e) 应限制网站系统中的服务器主动访问单位内部网络，仅允许访问单位内部网络提供的指定交互业务、补丁更新、病毒库升级等服务。

6.3.1.3 地址转换

网站相关服务器应使用私有 IP 地址，通过边界防火墙或路由器实现私有 IP 地址与互联网 IP 地址

之间的地址转换。

6.3.2 安全域边界安全

6.3.2.1 边界隔离方式

应采用在交换设备上划分 VLAN 或部署安全域边界防火墙等方式实现政府门户网站系统所在安全域与其他业务系统所在安全域之间的逻辑隔离。

6.3.2.2 边界防护策略

本项措施包括：

a) 安全域逻辑隔离设备的默认过滤策略应设置为禁止任意访问；

b) 明确各安全域之间的实际访问需求，合理配置相应的安全域边界过滤策略。

6.3.3 业务边界安全

本项措施包括：

a) 宜建立网站应用程序与其他业务系统交互的数据列表，规范交互数据的内容及格式；

b) 宜采用身份鉴别、访问控制、加密传输和加密存储等安全措施确保业务数据交互过程的安全性。

6.4 服务器安全

6.4.1 系统设置

6.4.1.1 最小化安装

操作系统和数据库系统宜遵循最小安装原则，仅安装业务必需的服务、组件和软件等。

6.4.1.2 身份鉴别

本项措施包括：

a) 可采用用户名/口令等鉴别机制实现服务器操作系统及数据库系统的身份鉴别；

b) 口令应由大小写字母、数字及特殊字符组成，普通用户的口令长度不宜短于 8 个字符，系统管理员用户的口令长度不宜短于 10 个字符，且每半年至少修改一次；

c) 应采取措施防范口令暴力破解攻击，可采用设置登录延时、限制最大失败登录次数、锁定账号等措施。

6.4.1.3 访问控制

本项措施包括：

a) 针对服务器操作系统及数据库系统应设置必要的用户访问控制策略，为不同用户授予其完成各自承担任务所需的最小权限，限制超级管理员等默认角色或用户的访问权限；

b) 应及时清除服务器操作系统及数据库系统中的无用账号、默认账号，不应出现多人共用同一个系统账号的情况；

c) 应限制网站 Web 服务器、数据库服务器等重要服务器的远程管理；

d) 服务器操作系统及数据库系统需要远程进行管理时，宜采用 SSH 等安全方式实现；

e) 应仅开启业务所需的最少服务及端口。

6.4.1.4 安全审计

本项措施包括：

a) 应实现服务器操作系统及数据库系统的安全审计，对系统远程管理、账号登录、策略更改、对象访问、服务访问、系统事件、账户管理等行为及 WWW、FTP 等重要服务访问进行审计，并设置审计日志文件大小的阈值以及达到阈值的处理方式(覆写、自动转存等)；

b) 针对安全审计记录及审计策略设置必要的访问控制以避免未授权的删除、修改或覆盖等；

c) 审计记录应独立保存，保存时间不少于 90 d。

6.4.2 系统更新

本项措施包括：

a) 应统一采购、部署正版软件以及相关服务，并定期开展系统漏洞扫描工作；

b) 应通过操作系统软件、数据库系统软件官方网站或其他合法渠道获得补丁程序，并在补丁程序通过安全测试后及时更新。

6.5 管理终端安全

6.5.1 连接控制

6.5.1.1 外联控制配置

本项措施包括：

a) 应对管理终端的远程登录 IP 地址及 MAC 地址进行限制；

b) 可设置并启用管理终端的外联控制策略，对管理终端未经授权的外联行为进行监测和处置。

6.5.1.2 移动存储介质接入安全配置

设置并启用管理终端的移动存储介质接入安全策略，检验移动存储介质的合法性，并对接入的移动存储介质进行恶意代码扫描。

6.5.2 系统配置

6.5.2.1 操作系统配置

本项措施包括：

a) 操作系统各类账号的口令应由大小写字母、数字及特殊字符组成，普通账号的口令长度不宜短于 6 个字符，系统管理员账号的口令长度不宜短于 8 个字符；

b) 口令生存周期宜设置为不长于 180 d，限制口令修改频度和使用周期；

c) 关闭操作系统默认共享，对于必须开启的共享文件夹应明确文件夹的共享权限，并在不再使用时及时关闭；

d) 关闭操作系统的自动播放功能；

e) 设置并启用系统有口令保护的屏幕保护程序，屏幕保护的等待时间不宜长于 5 min；

f) 设置并启用主机防火墙，根据网站管理需求，设置端口、协议等访问控制策略，非授权用户不应远程访问管理终端。

6.5.2.2 软件安装配置

本项措施包括：

a) 统一采购正版或合法软件以及相关服务，建立软件资产清单，安装和配置前宜进行安全审核；
b) 设置并启用软件进程监测策略，对违反策略的行为进行处置；
c) 可对软件的增加、修改、删除等软件变更情况进行审计，审计信息应包括日期、时间、来源、用户、操作及结果等要素，审计数据至少保存 90d，并确保数据的保存独立于管理终端。

6.5.3 系统更新

本项措施包括：
a) 可定期进行管理终端软件安全漏洞扫描，及时评估和修补已经发布的软件安全漏洞；
b) 在实施关键漏洞的修补前，应从操作系统软件官方网站或其他合法渠道获得补丁程序，并在补丁程序通过安全测试后及时更新。

6.6 Web 应用安全

6.6.1 安全功能设计

6.6.1.1 身份鉴别

本项措施包括：
a) 网站对浏览用户可不进行鉴别，对前台注册用户、后台内容管理用户及系统管理用户应采用用户名/口令等身份鉴别机制实现用户身份鉴别，并启用验证码机制；
b) 各用户口令应由大小写字母、数字及特殊字符组成，前台注册用户的口令长度不宜少于 8 个字符，后台内容管理用户及系统管理用户的口令长度不宜短于 10 个字符，且每半年至少修改一次；
c) 应设置网站用户登录超时重鉴别、连续登录失败尝试次数阈值等措施。

6.6.1.2 访问控制

本项措施包括：
a) 应提供访问控制功能，授予网站用户为完成各自承担任务所需的最小权限，限制默认角色或用户的访问权限；
b) 应实现系统管理用户、内容编辑用户及内容审核用户等特权用户的权限分离。

6.6.1.3 安全审计

本项措施包括：
a) 应提供安全审计功能，包括：
- 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，内容包括但不限于用户姓名、手机号码、注册时间、注册地址、登录时间、登录地址、操作用户信息、操作时间、操作内容及操作结果等；
- 针对后台内容管理用户的登录、网站内容编辑、审核及发布等行为进行日志记录，内容包括但不限于用户登录时间、登录地址以及编辑、审核及发布等行为发生时的用户信息、时间、地址、内容和结果等；
- 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，内容包括但不限于网站用户登录时间、登录地址以及管理操作对象、操作内容、操作结果等。

b) 宜设置日志文件的大小及达到阈值的操作方式；
c) 应对安全审计记录及审计策略设置必要的访问控制以避免未授权的删除、修改或覆盖等；
d) 审计记录应独立保存，保存时间不少于 90 d。

6.6.1.4 资源管控

本项措施包括：

a) 应根据网站访问需求限制最大并发会话连接数；

b) 如用户在一段时间内未作任何操作，网站应自动结束当前会话。

6.6.2 源代码安全

本项措施包括：

a) 在网站需求设计阶段，应制定源代码安全编写规范，约束特定语言相关的编程规则，并对应用程序代码存在的常见安全缺陷提出规范要求，包括但不限于表3所示编码安全要求。

b) 在网站开发阶段，应遵循制定的源代码安全编写规范，并在网站投入使用前委托第三方专业机构对网站应用程序源代码进行全面的安全审查。

表3 政府门户网站编码安全要求示例（基本级）

类别	具体措施
输入输出处理规范	集中验证所有的输入信息，用户输入的数据不应被直接用到程序的逻辑中；在程序中清晰界定可信和不可信数据的边界，当数据要从不可信的区域进入可信区域时需使用验证逻辑进行判断
Web技术规范	校验来自客户端的任何数据，并在服务器端进行安全验证；传输敏感信息时，采用加密措施；构造通用的错误提示信息，限制用户短时间内重复访问的次数
文件系统规范	限制应用程序文件及临时文件的访问权限；对来自文件系统的所有值进行合适的输入验证
网络系统规范	对来自网络的任何数据进行校验，确保数据包的大小和内容与预期要求相符
数据库规范	正确的使用参数化的结构化查询语句，数据不应指向改变的方法；对来自数据库的数据进行验证，确保其格式正确且能够安全的使用
日志处理规范	根据操作的重要程度划分日志等级，保证日志记录的一致性；日志文件应独立保存于应用程序目录外，使用严格的访问权限控制日志文件
密码技术规范	使用经过国家有关部门批准的、符合相关国家政策与标准的密码算法；无用私密信息的存活时间宜尽量缩短；尽量少的共享私密信息，不应在客户端长期保存秘密信息
认证技术规范	鉴别信息在网络中加密传输，不应在源代码中明文存储和显示；谨慎给出认证反馈信息，限制一个账号连续失败登录的次数并有相应的处理措施等
口令管理规范	使用统一的口令策略，使用安全的方法存储和传输口令；不应在源代码中存储口令；在注册登录时启用验证码机制
随机数规范	使用一种生成代价小并满足安全需求的随机数生成方法来生成应用程序需要的随机数

6.6.3 系统更新

本项措施包括：

a) 应定期针对应用程序或代码、Web应用服务器（如IIS、Apache等）、FTP等网络应用程序进行漏洞扫描，及时修补存在的安全漏洞；

b) 当应用程序的版本需要变更时，应经过验证、审核及批准，并保存相应记录。

6.7 域名安全

6.7.1 域名注册管理

本项措施包括：

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。

6.7.2 域名信息管理

本项措施包括：

a) 应指定专人对域名信息进行管理，妥善保存域名系统或第三方域名托管平台的用户名及口令信息，口令应由大小写字母、数字及特殊字符组成，长度不宜短于 8 个字符，且每半年至少修改一次；

b) 应规范域名信息的变更管理，当域名信息需要变化时，应经审核批准后，由指定专人负责实施并及时记录。

6.7.3 域名系统安全

本项措施包括：

a) 采用安全的操作系统平台和域名解析软件，并关注软件商发布的最新安全漏洞，定期升级软件系统；

b) 不应以超级管理员身份运行域名解析服务；

c) 应确保域名解析服务的独立性，运行域名解析服务的服务器上不应同时开启其他端口的服务；

d) 修改域名服务器的相关配置文件，隐藏域名解析服务软件的版本信息和服务器信息；

e) 限制区域传输，依据安全策略限制在不同域名解析服务器之间的数据同步；

f) 应关闭递归查询功能，避免因向外部的域名服务器发送查询请求而遭受地址欺骗攻击；

g) 应关闭线索查找功能，避免因此引发的欺骗攻击；

h) 提供域名服务的安全审计功能，并定期分析和备份 DNS 服务日志。

6.8 内容发布及数据安全

6.8.1 内容发布安全

本项措施包括：

a) 政务门户网站内容管理模块应提供内容审核功能，并提供网站内容编辑与审核发布权限分离的功能；

b) 政务门户网站应仅面向经身份验证的注册用户提供信息发布功能，且提供信息经审核人员审核后才能发布的功能选项。

6.8.2 数据安全

6.8.2.1 网页防篡改

根据网站规模和信息发布方式选择相应的网页防篡改产品，至少对网站关键的静态页面（首页）和动态页面进行监控和保护。

6.8.2.2 数据加密

本项措施包括：

a) 针对掌握公民、法人及其他组织的个人信息及隐私的政府门户网站系统，个人信息及隐私信息在远程传输过程中宜采用加密措施进行保护；
b) 政府门户网站系统的各类用户鉴别信息、关键配置参数、重要业务数据等敏感信息（文件），在远程传输及本地存储过程中宜采用加密措施进行保护；
c) 政府门户网站系统与其他业务系统进行数据交互时，宜限定数据交互的格式，并采用密码技术保证传输数据的机密性和完整性。

6.8.2.3 备份恢复

针对政府门户网站系统的应用程序、系统数据（用户信息、发布信息等）、配置数据（网站应用、操作系统、数据库及网络、安全设备的配置信息等）及审计日志等宜定期进行备份，至少每周进行一次完全备份，并至少 6 个月实施一次备份恢复演练。

6.9 攻击防范

6.9.1 恶意代码防范

本项措施包括：

a) 在网络边界、服务器、管理终端等处应采取恶意代码防范措施，实行统一有效的恶意代码防范软件机制，并及时更新恶意代码防范软件版本和恶意代码特征库，对恶意代码进行实时检测和清除；
b) 将安装于服务器及管理终端的恶意代码防范软件设置为开机自动启动，定期对所有本地存储介质进行安全扫描，及时对接入介质及其文件进行安全扫描；
c) 宜对恶意代码防范软件的运行状态进行监测，并对关闭进程或修改配置的行为进行监测。

6.9.2 入侵防范

本项措施包括：

a) 可针对信息系统中的安全事件进行实时监控，监测和阻断端口扫描、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常见网络攻击行为，并监测和阻断目录遍历攻击等 Web 服务器漏洞攻击行为以及 SQL 注入、跨站脚本攻击等网站自身漏洞攻击行为；
b) 在特定的时间、地点、事件环境条件下，可通过加强物理安全、人员意识教育和培训、完善安全策略、事件响应计划等措施防御社会工程类攻击行为。

6.10 安全监控与应急响应

6.10.1 网站状态监控

本项措施包括：

a) 应利用网站状态监控系统或人工监控的方式，实时监测政府门户网站的运行状态，对网站异常状况进行实时报警和处置。网站页面监测深度宜不少于主页访问路径下的第 2 层；
b) 应利用网络管理系统或人工监控的方式，实时监测重要服务器和数据库系统的运行状态及 CPU、内存、硬盘等资源的使用情况，并对异常情况进行报警和处置；
c) 应定期对网站应用程序、操作系统及数据库、管理终端进行全面扫描，根据扫描结果判断网站存在的安全风险，及时调整监测策略。

6.10.2 网站挂马监控

应利用木马监控系统或第三方安全服务等方式及时发现并处置网站挂马事件。

6.10.3 网站内容篡改监控

应利用网页防篡改系统、人工自检或第三方安全服务等方式及时发现网站篡改事件并迅速处理。

6.10.4 应急响应

本项措施包括：

a) 政府单位可根据其门户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、处置流程及保障措施等内容；

b) 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，每两年至少开展各类典型安全事件的应急演练一次；

c) 可建立应急值班制度，工作时间内安排专人 8 h 值班。8 h 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 24 h 值班，并定期进行信息报送；

d) 信息安全事件发生时，应按照应急预案的要求及时组织应急处置并记录。

7 增强级安全技术措施

7.1 运行支撑

7.1.1 运行模式

本项措施包括：

a) 政府门户网站系统**宜采用自建自管模式建设运行，也可选择由政府集中建设的数据中心以主机托管或虚拟主机的方式建设运行**；

b) 政府门户网站系统如采用主机托管或虚拟主机方式建设运行，应优先选择由当地政府集中建设的数据中心。如采用主机托管或主机租用模式，应选择在物理安全、网络安全、主机安全等方面符合本标准基本级要求或 GB/T 22239 中**第三级**基本要求的数据中心；

c) 政府门户网站系统采用主机托管或虚拟主机方式运行时，网站系统的主管单位应明确本单位和数据中心双方的安全责任边界，建立对网站系统运行环境、安全技术措施运行情况的监督机制。

7.1.2 网站部署

本项措施包括：

a) 政府门户网站的 Web 应用程序应部署在独立的物理服务器或虚拟服务器上；

b) 同一政府门户网站系统的 Web 应用程序与数据库系统应部署在不同的物理服务器或虚拟服务器上；

c) 政府门户网站系统采用虚拟主机方式运行时，不应与非政务信息系统共用物理服务器；

d) **政府门户网站系统的数据库应与其他数据库分开部署，对于共用数据库管理系统的，应通过设置数据库管理系统的身份鉴别、权限控制功能等方式，实现网站系统的数据库与其他应用的数据库系统之间的安全隔离**。

7.1.3 边界确定

本项措施包括：

a) 明确政府门户网站系统与互联网等网络之间的访问需求，以确定网络边界；

b) 明确政府门户网站系统与其他业务系统之间的访问需求，以确定安全域边界；
c) 若政府门户网站系统与其他业务系统存在数据交互，明确数据交互发生的业务边界（如发生交互的功能模块），并明确交互数据的性质和类型。

7.1.4 资源保障

7.1.4.1 性能保障

本项措施包括：
a) 应分析政府门户网站系统的性能需求，从网络带宽、**负载均衡**、服务器的处理能力、应用程序的并发处理能力等方面对网站性能予以保障；
b) 政府门户网站系统对外提供服务的互联网独享带宽不宜低于 5 **Mbit/s**；共享带宽条件下，网站互联网出口 HTTP 协议带宽不宜低于 5 **Mbit/s**；
c) 若政府门户网站系统访问量较大或提供在线视频等服务，可以依据网站的日均页面访问量（次）及业务高峰期（包括日高峰及高峰日）访问量酌情调整出口带宽；
d) **对于业务量较大，单台服务器难以支撑的政府门户网站系统，可采用部署负载均衡设备、分布式部署等方式实现链路和主机层面的负载均衡，链路层面至少应实现多条互联网接入链路之间的负载均衡，主机层面至少应实现多应用服务器之间、多数据库服务器之间的负载均衡。**

7.1.4.2 链路和设备冗余部署

本项措施包括：
a) **应至少部署 2 条由不同互联网接入服务商提供的互联网接入链路；**
b) 应为支撑政府门户网站系统运转的关键设备提供硬件冗余措施，关键设备包括但不限于出口路由器、核心交换机、应用及数据库服务器等。

7.1.4.3 电力保障

应采取**双路市电供电**，并采用配备 UPS 等措施为系统提供短期备用电力，**对于业务连续性要求更高的政府门户网站系统，可采用备用发电机等供电措施。**

7.2 物理安全

7.2.1 物理位置选择

不应使用境外机构提供的或位于境外的物理服务器或虚拟主机。

7.2.2 物理环境控制

本项措施包括：
a) 政府门户网站系统关键设备所在机柜柜门应上锁；
b) 机房等重要区域应配置电子门禁系统，以便控制、鉴别和记录人员出入；
c) 需要进入机房对政府门户网站系统进行操作时，应由网站安全责任人或其指定的专人陪同；
d) 机房场地在防火、防水、防震、防盗、防尘、防静电、防雷、防电磁、监控、温湿度控制、**电磁屏蔽**等方面应符合 GB/T 22239—2008 中**第三级**基本要求的物理安全要求。机房场地安全要求可参考 GB/T 50174—2008、GB/T 2887—2011 等国家标准中的相应要求。

7.2.3 传输线路保护

本项措施包括：

a) 应采用有效方法防范对信息传输线路的物理接触，如：将通信线缆铺设在地下或管道内等隐蔽处，以防止传输过程中的数据篡改、干扰以及对线缆的物理破坏；
b) 电源线和通信线缆宜隔离铺设，避免互相干扰。

7.3 边界安全

7.3.1 互联网边界安全

7.3.1.1 边界隔离方式

应在政府门户网站系统与互联网的网络边界处部署防火墙等边界隔离设备，并配置合理的边界访问控制策略，实现网站系统与互联网之间的逻辑隔离。

7.3.1.2 边界防护策略

本项措施包括：
a) 互联网边界隔离设备的默认过滤策略应设置为禁止任意访问；
b) 应仅允许互联网用户及单位内部普通用户终端访问网站服务器提供的 HTTP 服务等指定的服务和端口；
c) 应限制政府门户网站系统中的服务器主动访问互联网；
d) 应仅允许指定的 IP 地址访问网站服务器提供的内容管理、系统管理等指定的服务和端口；
e) 应限制政府门户网站系统中的服务器主动访问单位内部网络，仅允许访问单位内部网络提供的指定交互业务、补丁更新、病毒库升级等服务；
f) **在会话处于非活跃状态 5 min 后或会话结束后宜终止网络连接；**
g) **应限制边界隔离设备的远程管理方式。若需要采用远程管理方式时，宜采用 SSH 等加密方式进行设备的远程管理，并适当增加边界隔离设备系统管理员账号鉴别口令的强度和更新频率，或采用数字证书等高强度鉴别方式。**

7.3.1.3 地址绑定及转换

本项措施包括：
a) **应对重要服务器采取 IP 地址/MAC 地址绑定措施，以防范地址欺骗；**
b) 网站相关服务器应使用私有 IP 地址，通过边界防火墙或路由器实现私有 IP 地址与互联网 IP 地址之间的地址转换。

7.3.2 安全域边界安全

7.3.2.1 边界隔离方式

应采用在交换设备上划分 VLAN 或部署安全域边界防火墙等方式实现政府门户网站系统所在安全域与其他业务系统所在安全域之间的逻辑隔离。

7.3.2.2 边界防护策略

本项措施包括：
a) 安全域逻辑隔离设备的默认过滤策略应设置为禁止任意访问；
b) 明确各安全域之间的实际访问需求，合理配置相应的安全域边界过滤策略。

7.3.3 业务边界安全

a) 应建立网站应用程序与其他业务系统交互的数据列表，规范交互数据的内容及格式；

b) 宜采用身份鉴别、访问控制、加密传输及加密存储等安全措施确保业务数据交互过程的安全性。

7.4 服务器安全

7.4.1 系统选用

可选择安全操作系统或根据网站系统性能、可用性、安全要求等需求对操作系统进行定制(包括:内核、服务、应用、端口等),或借助第三方机构对操作系统和数据库系统进行安全加固。

7.4.2 系统设置

7.4.2.1 最小化安装

操作系统和数据库系统宜遵循最小安装原则,仅安装应用必需的服务、组件、软件等。

7.4.2.2 身份鉴别

本项措施包括:

a) 可采用用户名/口令等鉴别机制实现服务器操作系统及数据库系统的身份鉴别;

b) 口令应由大小写字母、数字及特殊字符组成。普通用户的口令长度不宜短于 10 **个字符**,系统管理员用户的口令长度不宜短于 12 **个字符**,且每**三个月**至少修改一次;

c) 应采取措施防范口令暴力破解攻击,宜设置登录延时、限制最大失败登录次数、锁定账号等措施。

7.4.2.3 访问控制

本项措施包括:

a) 针对服务器操作系统及数据库系统宜设置必要的访问控制,为不同用户授予其完成各自承担任务所需的最小权限,**并在不同用户之间形成权限相互制约关系**,限制超级管理员等默认角色或用户的访问权限;

b) 及时清除操作系统及数据库系统的无用账号、默认账号,不应出现多人共用同一个系统账号的情况;

c) 应限制 Web 服务器、数据库服务器等重要服务器的远程管理;

d) 服务器操作系统及数据库系统需要远程进行管理时,宜采用 SSH 等安全方式进行,**并对远程管理的系统管理员采用数字证书等高强度鉴别方式**;

e) 宜开启业务所需的最少服务及端口。

7.4.2.4 安全审计

本项措施包括:

a) 应实现服务器操作系统及数据库系统的安全审计,对系统远程管理、账号登录、策略更改、对象访问、服务访问、系统事件、账户管理等行为及 WWW、FTP 等重要服务访问进行审计,并设置审计日志文件大小的阈值以及达到阈值的处理方式(覆写、自动转存等);

b) **指定独立的安全审计员负责管理审计日志**,针对安全审计记录及审计策略设置必要的访问控制以避免未授权的删除、修改或覆盖等;

c) 审计记录应保存于专用的日志服务器上,保存时间不宜少于 180 **d**。

7.4.3 系统更新

本项措施包括:

a) 应统一采购、部署正版软件以及相关服务，并定期开展系统漏洞扫描工作；
b) 应通过操作系统软件、数据系统软件官方网站或其他合法渠道获得补丁程序，并在补丁程序通过安全测试后，利用升级服务器统一、及时实行系统补丁更新和版本升级。

7.5 管理终端安全

7.5.1 连接控制

7.5.1.1 连接控制策略

本项措施包括：

a) 应采取技术措施对接入的内容管理终端及网站、主机和网络管理终端应进行身份认证，身份认证通过后方可接入和使用网络资源；
b) 应采取技术措施自动对接入的管理终端实行安全状态检查，对未通过安全状态检查的管理终端需经修复后方可接入；
c) 在关键网络设备上绑定接入管理终端的 MAC 地址，提高针对 ARP 欺骗类网络攻击的防范能力；
d) 管理终端不应以无线方式接入办公网及网站系统所在安全域。

7.5.1.2 外联控制配置

本项措施包括：

a) 应对管理终端的远程登录 IP 地址及 MAC 地址进行限制；
b) 设置并启用管理终端的外联控制策略，对管理终端未经授权的外联行为进行监测和处置；
c) 设置并启用管理终端外联控制策略，未经授权不应通过任何形式连接外部网络，不应使用 USB 接口为手机等外部设备充电，并对管理终端未经授权的外联行为进行监测和处置。

7.5.1.3 移动存储介质接入安全配置

设置并启用管理终端的移动存储介质接入安全策略，检验移动存储介质的合法性，并对接入的移动存储介质进行恶意代码扫描。

7.5.2 系统配置

7.5.2.1 操作系统配置

本项措施包括：

a) 操作系统各类账号的口令宜由大小写字母、数字及特殊字符组成，普通账号的口令长度不宜短于 8 个字符，系统管理员账号的口令长度不宜短于 10 个字符；
b) 口令生存周期策略宜设置为不长于 90 d，限制口令修改频度和使用周期；
c) 应关闭操作系统默认共享，对于必须开启的共享文件夹应明确文件夹的共享权限，并在不再使用时及时关闭；
d) 应关闭系统的自动播放功能；
e) 应设置并启用系统有口令保护的屏幕保护程序，屏幕保护的等待时间不长于 5 min；
f) 可设置并启用主机防火墙，根据网站管理需求，设置端口、协议等访问控制策略，非授权用户不应远程访问管理终端。

7.5.2.2 软件安装配置

本项措施包括：

a) 统一采购正版或合法软件以及相关服务，建立软件资产清单，安装和配置前宜进行安全审核；
b) 设置并启用软件进程监测策略，对违反策略的行为进行处置；
c) 可对软件的增加、修改、删除等软件变更情况进行审计，审计信息应包括日期、时间、来源、用户、操作及结果等要素，审计数据至少保存 60 d，并确保数据的保存独立于管理终端。

7.5.3 系统更新

本项措施包括：

a) 应定期对管理终端软件进行安全漏洞扫描，及时评估和修补已经发布的软件安全漏洞；
b) **应设置升级服务器对软件安全漏洞进行集中管理**，在实施关键漏洞的修补前，宜通过升级服务器从操作系统软件官方网站或其他合法渠道获得补丁程序，在通过安全测试后集中修补。

7.6 Web 应用安全

7.6.1 安全功能设计

7.6.1.1 身份鉴别

本项措施包括：

a) 网站对浏览用户可不进行鉴别，对前台注册用户、后台内容管理用户及系统管理用户等不同类型的用户**宜设置不同强度的鉴别机制**；
b) 前台注册用户应至少采用用户名/口令机制进行身份鉴别并启用验证码机制，口令应由大小写字母、数字及特殊字符组成，口令长度不宜少于 **10 个字符**，且每**三个月**至少更新一次；
c) 选择高强度认证方式的前台注册用户、后台内容管理用户及系统管理用户**宜采用两种或两种以上组合的鉴别技术实现用户身份鉴别（动态口令、生物认证、数字证书等）**，口令长度不宜少于 **12 个字符**，且每**三个月**至少修改一次；
d) 应针对各类网站用户启用登录超时重鉴别、连续登录失败尝试次数阈值等措施。

7.6.1.2 访问控制

本项措施包括：

a) 应提供访问控制功能，授予网站用户为完成各自承担任务所需的最小权限，限制默认角色或用户的访问权限；
b) 应实现系统管理用户、内容编辑用户、内容审核用户等特权用户的权限分离。

7.6.1.3 安全审计

本项措施包括：

a) 应提供安全审计功能，包括：
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，内容包括但不限于用户姓名、手机号码、注册时间、注册地址、登录时间、登录地址、操作用户信息、操作时间、操作内容及操作结果等；
针对后台内容管理用户的登录、网站内容编辑、审核及发布等行为进行日志记录，内容包括但不限于用户登录时间、登录地址以及编辑、审核及发布等行为发生时的用户信息、时间、地址、内容和结果等；
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，内容包括但不限于网站用户登录时间、登录地址以及管理操作对象、操作内容、操作结果等。
b) **宜定期监测安全审计日志记录，针对关键业务操作应进行实时监测和处置**；

c) **应指定独立的安全审计员负责管理审计日志**，并设置日志文件的大小以及达到阈值的操作方式；

d) 针对安全审计记录及审计策略宜设置必要的访问控制，避免未授权的删除、修改或覆盖等；

e) 审计记录应保存于专用的日志服务器上，保存时间不少于 180 d。

7.6.1.4 资源管控

本项措施包括：

a) 应根据网站访问需求限制最大并发会话连接数；

b) 如用户在一段时间内未作任何操作，网站应自动结束当前会话。

7.6.2 源代码安全

本项措施包括：

a) **源代码安全应贯穿网站系统的整个生命周期**；

b) 在网站需求设计阶段，可制定源代码安全编写规范，约束特定语言相关的编程规则，并对应用程序代码存在的常见安全缺陷提出规范要求，包括但不限于表 4 所述编码安全要求。

c) 在网站开发阶段应遵循制定的源代码安全编写规范，**在单元测试期间和开发完成后可实施代码安全性测试**，并在网站投入使用前委托第三方专业机构对网站应用程序源代码进行全面的安全审查。

d) **在网站运行阶段，定期对网站进行渗透性测试，并在网站程序更新后及时进行源代码安全检查**。

e) **在网站废弃阶段，应彻底删除程序源代码，避免代码遭到非授权访问**。

表 4 政府门户网站编码要求示例（增强级）

类别	具体措施
输入输出处理规范	集中验证所有的输入信息，用户输入的数据不应被直接用到程序的逻辑中；在程序中清晰界定可信和不可信数据的边界，当数据要从不可信的区域进入可信区域时需使用验证逻辑进行判断
Web 技术规范	校验来自客户端的任何数据，并在服务器端进行安全验证；传输敏感信息时，采用加密措施；构造通用的错误提示信息，限制用户短时间内重复访问的次数
文件系统规范	限制应用程序文件及临时文件的访问权限；对来自文件系统的所有值进行合适的输入验证
网络系统规范	对来自网络的任何数据进行校验，确保数据包的大小和内容与预期要求相符
数据库规范	正确的使用参数化的结构化查询语句，数据不应指向改变的方法；对来自数据库的数据进行验证，确保其格式正确且能够安全的使用
日志处理规范	根据操作的重要程度划分日志等级，保证日志记录的一致性；日志文件应独立保存，使用严格的访问权限控制日志文件
密码技术规范	使用经过国家有关部门批准的、符合相关国家政策与标准的密码算法；无用私密信息的存活时间宜尽量缩短；尽量少的共享私密信息，不应在客户端长期保存秘密信息
认证技术规范	使用动态口令、生物认证及数字证书等较强的强身份鉴别方式；鉴别信息在网络中加密传输，不应在源代码中明文存储和显示；谨慎给出认证反馈信息，限制一个账号连续失败登录的次数并有相应的处理措施等
口令管理规范	使用统一的口令策略，使用安全的方法存储和传输口令；不应在源代码中存储口令；在注册登录时使用验证码机制
随机数规范	使用一种生成代价小并满足安全需求的随机数生成方法来生成应用程序需要的随机数

7.6.3 系统更新

本项措施包括：

a) 应定期针对应用程序或代码、Web 应用服务器(如 IIS、Apache 等)、FTP 等网络应用程序进行漏洞扫描，及时修补存在的安全漏洞；

b) 当应用程序的版本需要变更时宜经过审核批准，并保存相应记录。

7.7 域名安全

7.7.1 域名注册管理

本项措施包括：

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。

7.7.2 域名信息管理

本项措施包括：

a) 宜指定专人对域名信息进行管理，妥善保存域名系统或第三方域名托管平台的用户名及口令信息，口令应由大小写字母、数字及特殊字符组成，长度不宜短于 10 个字符，且每三个月至少修改一次；

b) 应规范域名信息的变更管理，当域名信息需要变化时，经审核批准后，由指定专人负责实施并及时记录。

7.7.3 域名系统安全

7.7.3.1 域名系统安全配置

本项措施包括：

a) **应至少启用一台辅助域名服务器实现域名服务的冗余备份；**

b) 不应以超级管理员身份运行域名解析服务；

c) 应关闭递归查询功能，避免因向外部的 DNS 发送查询请求遭受地址欺骗攻击；关闭线索查找功能，避免因此引发的欺骗攻击；

d) 应确保域名解析服务的独立性，运行域名解析服务的服务器上不应同时开启其他端口的服务；

e) 采用安全的操作系统平台和域名解析软件，并关注软件商发布的最新安全漏洞，定期升级软件系统；

f) 修改域名服务器的相关配置文件，隐藏域名解析服务软件的版本信息和服务器信息；

g) 限制区域传输，根据安全策略限制在不同域名解析服务器之间的数据同步，**针对域名解析服务器之间必要的数据同步应采用加密通道的方式实现；**

h) 提供域名服务的安全审计功能，定期分析和备份 DNS 服务日志。

7.7.3.2 域名系统安全监控

可对域名解析的正确性、域名服务器边界网络设备的流量及数据包进行监控，以发现可能的恶意攻击。

7.8 内容发布及数据安全

7.8.1 内容发布安全

本项措施包括：

a) 政府门户网站内容管理模块应提供内容审核功能，并提供网站内容编辑与审核发布权限分离的功能；

b) 政府门户网站应仅面向经身份验证的注册用户提供信息发布功能，且提供信息经审核人员审核后才能发布的功能选项；

c) **可提供技术手段辅助进行网站发布内容的过滤**。

7.8.2 数据安全

7.8.2.1 网页防篡改

可根据网站规模和信息发布方式选择相应的网页防篡改产品，对网站**所有静态页面和动态页面**进行监控和保护。

7.8.2.2 数据传输加密

本项措施包括：

a) 针对掌握公民、法人及其他组织的个人信息及隐私的政府门户网站系统，个人信息及隐私信息在远程传输过程中应采用加密措施进行保护；

b) 网站的各类用户鉴别信息、关键配置参数、重要业务数据等敏感信息(文件)，在远程传输过程中应采用加密措施进行保护；

c) 政府门户网站系统与其他业务系统进行数据交互时，宜限定数据交互的格式，并采用密码技术保证传输数据的保密性和完整性。

7.8.2.3 数据存储加密

本项措施包括：

a) **针对掌握公民、法人及其他组织的个人信息及隐私的政府门户网站系统，个人信息及隐私在本地存储介质和数据库中应加密存储；**

b) **政府门户网站系统的各类用户鉴别信息在本地存储介质和数据库中应加密存储。**

7.8.2.4 抗抵赖

系统可提供基于审计日志、电子签章等技术的抗抵赖功能，产生和储存对发送信息和接收到信息的相关证据。

7.8.2.5 备份恢复

本项措施包括：

a) 针对政府门户网站系统的应用程序、系统数据(用户信息、发布信息等)、配置数据(网站应用、操作系统、数据库及网络、安全设备的配置信息等)及审计日志等宜定期进行备份，至少每周进行一次完全备份，并至少 3 个月实施一次备份恢复演练；

b) **针对内容发布、在线办事等网站关键业务的重要数据、个人信息及隐私信息，可采取异地数据备份措施，将关键数据定时批量传送至备用场地。**

7.9 攻击防范

7.9.1 恶意代码防范

本项措施包括：

a) 应在网络边界、服务器、管理终端等处采取恶意代码防范措施，实行统一有效的恶意代码防范软件机制，并及时更新恶意代码防范软件版本和恶意代码特征库，对恶意代码进行实时检测和清除；

b) 将安装于服务器及管理终端的恶意代码防范软件设置为开机自动启动，定期对所有本地存储介质进行安全扫描，及时对接入介质及其文件进行安全扫描；

c) 应对恶意代码防范软件的运行状态进行监测，并对关闭进程或修改配置的行为进行监测。

7.9.2 入侵防范

本项措施包括：

a) 应针对信息系统中的安全事件进行实时监控，监测和阻断端口扫描、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常见网络攻击行为，并监测和阻断目录遍历攻击等 Web 服务器漏洞攻击行为以及 SQL 注入、跨站脚本攻击等网站自身漏洞攻击行为；

b) 在特定的时间、地点、事件环境条件下，可加强物理安全、人员意识教育和培训以及制定安全策略、事件响应计划等控制措施防御社会工程攻击行为。

7.10 安全监控与应急响应

7.10.1 网站状态监控

本项措施包括：

a) 可利用网站状态监控系统或人工方式，实时监测政府门户网站的运行状态，对网站异常状况进行实时报警和处置。网站页面监测深度不宜少于主页访问路径下的第 2 层；

b) 应利用网络管理系统或人工监控的方式，实时监测重要服务器和数据库系统的运行状态及 CPU、内存、硬盘等资源的使用情况，并对异常情况进行报警和处置；

c) 应定期对网站应用程序、操作系统及数据库、管理终端进行全面扫描，根据扫描结果判断网站存在的安全风险，及时调整监测策略。

7.10.2 网站挂马监控

应利用木马监控系统或第三方安全服务等方式对网站挂马情况进行**实时监测和处置**。

7.10.3 网站内容篡改监控

应利用网页防篡改系统并综合采用人工自检方式或第三方安全服务等方式，对网站内容篡改情况进行**实时监测和处置**。

7.10.4 应急响应

本项措施包括：

a) 政府单位可根据其门户网站系统具体特点，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、处置流程及保障措施等内容；

b) 可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、维护不同事件应急预案，每年至少开展各类典型安全事件的应急演练一次；

c) 可建立应急值班制度，工作时间内安排专人 8 h 值班；8 h 工作时间外，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 24 h 值班，并定期进行信息报送；

d) 信息安全事件发生时，应按照应急预案的要求及时组织应急处置并记录。

附 录 A
（规范性附录）
高级安全技术措施

A.1 物理安全

本项措施包括：

a） 机房出入口及重要区域宜配置电子门禁系统，以便控制、鉴别和记录人员出入；

b） 重要区域的活动行为宜进行实时监视和记录；

c） 关键区域应避免外部人员访问。

A.2 服务器安全

本项措施包括：

a） 针对服务器操作系统及数据库系统宜采用两种或两种以上组合的鉴别技术实现用户身份鉴别（动态口令、数字证书等）；

b） 针对服务器操作系统及数据库系统宜进行集中审计，确保系统时钟与时钟服务器保持同步。

A.3 接入控制

不应使用便携式或移动式设备作为政府门户网站系统的内容管理终端。

A.4 Web 应用安全

本项措施包括：

a） 应用系统宜避免默认角色或用户的访问权限；

b） 应用系统应提供集中安全审计功能，确保系统时钟与时钟服务器保持同步。

A.5 数据安全

本项措施包括：

a） 针对重要通信过程应采用基于硬件化的设备实现加解密运算和密钥管理；

b） 针对网站的应用程序、系统数据（用户信息、发布信息等）及配置数据（网站应、操作系统、数据库及网络、安全设备的配置信息等）等应进行定期备份及恢复，至少每周进行一次完全备份，并至少 3 个月实施一次备份恢复演练；

c） 针对内容发布、在线办事等网站业务关键数据、个人信息及隐私信息，可提供异地实时数据备份功能，将关键数据实时传送至备用场地；

d） 根据网站的备份技术要求，制定相应的灾难恢复计划，并对计划进行测试，测试内容包括运行系统恢复、人员协调、通信连接等；并根据测试结果，对不适用的规定进行修改或更新。

A.6 攻击防范

应对信息系统中的安全事件进行实时监控，监测和**自动阻断**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常见的网络攻击行为，并监测和**自动阻断**目录遍历攻击等 Web 服务器漏洞攻击行为以及 SQL 注入、跨站脚本攻击等网站自身漏洞攻击行为。

A.7 应急响应

应急预案应随着网站的变更进行重新评估、修订和完善。