ICS 35.240
CCS L 60

DB23

黑 龙 江 省 地 方 标 准

DB 23/T XXXX.3—XXXX

政府网站建设管理规范 第3部分：集约化平台安全防护

征求意见稿

联系人：黑龙江省数字经济研究会 李健航
联系电话：15124541881
邮箱：hljsszjjyjh@people-ai.cn

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

黑龙江省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是《政府网站建设管理规范》的第3部分。《政府网站建设管理规范》已经发布了以下部分：

请注意本文件的某些部分可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

政府网站建设管理规范 第3部分：集约化平台安全防护

1 范围

本文件规定了省、地市两级政府网站集约化管理平台的物理安全、网络安全、边界安全、服务器安全、管理终端安全、Web应用安全、信息发布及数据安全、攻击防范、安全管理措施要求、安全定级与测评。

本文件适用于省、地市两级政府网站集约化平台安全防护体系建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术网络安全等级保护定级指南

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

网站用户

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。

3.2

网络安全

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.3

安全防护能力

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

4 安全防护总体框架

4.1 安全防护目标

政府网站集约化平台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，降低网页防篡改的安全风险；

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。

注：政府网站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，采集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。

4.2 安全防护架构

集约化管理平台安全防护体系应符合GB／T 25070-2019、GB／T 22239-2019等信息安全规范性文件要求，落实等级保护制度。应基于政务云建设统一安全防护体系，与集约化管理平台建设同步规划、同步建设、同步实施。按照等保三级标准设计建设安全防护体系，并综合考虑本文件给出的安全措施。

安全整体架构如图1所示。

图 1 平台安全防护架构示意图

5 安全技术措施要求

5.1 物理安全

集约化管理平台宜统一部署在政务云上，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。集约化管理平台部署环境应与其他业务系统进行隔离，若部署在政务云平台时须采用独立虚拟资源池，或者通过技术措施实现和统一资源池内的其他业务系统逻辑隔离，平台物理部署环境应满足GB／T 22239-2019中第三级关于物理环境的要求。

5.2 网络安全

5.2.1 网络链路安全

集约化管理平台部署的网络架构及通信链路安全应满足以下要求：

a） 应为支撑集约化管理平台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；

b) 政府网站、集约化管理平台、统一信息资源库等应部署在不同区域中，防止后台系统暴露在互联网区；
c) 应采用负载均衡、分布式部署等方式实现链路和主机层的负载均衡，链路层面至少应实现多条互联网联络之间的负载均衡，主机层面应实现多应用服务器之间的应用负载均衡；
d) 应部署由不同互联网接入服务商提供的冗余互联网接入链路；
e) 平台对外提供服务应设置符合实际需求的互联网独享带宽，并支持根据网站的日均网页访问量（次）及业务高峰期（包括日高峰及高峰日）访问量调整出口带宽。

5.2.2 上网行为管理

集约化平台应建设上网行为管理系统，在各个安全自治域及其中的主机均上网行为管理系统。具体应符合下列要求：

a) 应提供上网行为审计功能，对集约化平台中的业务模块及其所依托的网络设备、安全设备、主机操作系统、数据库系统、集约化平台等进行安全审计。
b) 应提供上网行为管控功能，对前台用户的注册、登录、关键业务操作等行为进行记录，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。对后台管理用户的登录、操作行为等行为进行记录，内容包括但不限于用户登录时间、登录地址以及编辑、操作等行为发生时的用户信息、时间、地址、内容和结果等。
c) 应提供访问控制功能，授予集约化平台各类用户为完成各自承担任务所需的最小权限，对集约化平台上不同网站运营者之间的后台内容管理用户进行严格的网络权限划分。

5.3 边界安全

5.3.1 互联网边界安全

集约化管理平台安全部署应划分网络安全区域，严格设置访问策略，建立安全访问路径。应在集约化管理平台与互联网的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，实现集约化管理平台与互联网之间的逻辑隔离。边界防护策略包括但不限于以下内容：

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访问应用服务器提供的 HTTP（HTTPS）服务等指定的服务和端口；
c) 应限制集约化管理平台中服务器主动访问互联网；
d) 应仅允许认证用户访问平台服务器提供的管理平台、内容管理、统一信息资源库等指定的服务和端口；
e) 应限制集约化管理平台中的服务器主动访问内部网络，仅允许访问内部网络提供的指定交互业务、补丁更新、病毒库更新等服务；
f) 应限制边界隔离设备的远程管理方式。如需要采用远程管理方式时，应采用 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；
g) 集约化管理平台应具备互联网全流量的安全审计能力。

5.3.2 安全域边界安全

集约化管理平台应部署跨网数据安全交换系统，实现互联网区和内部其他区域的安全隔离及信息双向交换，系统应具有内容过滤、格式检查及病毒查杀等功能。应采用在交换设备上换份VLAN或部署安全

域边界防火墙等方式实现集约化管理平台所在安全域与其他业务系统所在安全域之间的逻辑隔离。具体包括但不限于下列措施：

a) 政府网站、后台管理系统应单独划分安全域，应在安全域边界部署防火墙或者虚拟防火墙实现基于五元组的访问控制；
b) 安全域访问控制设备的默认过滤策略应设置为禁止任意访问，设置最小化控制规则，细粒度应达到端口级；
c) 使用云计算环境时，集约化管理平台应具备独立的安全策略配置能力，包括定义访问路径、选择安全组件、设置安全策略；
d) 应具有防止、清除和告警云主机传播有害信息的能力。

5.3.3 业务边界安全

集约化管理平台与应用之间、应用与应用之间，应建立数据列表，并规范交互数据的内容及格式。应提供管理用户权限分离机制，为系统管理员、应用管理员等建立不同账户并分配相应的权限。应采用身份鉴别、访问控制、加密传输及加密存储等多种安全措施，确保业务数据交换过程的安全性。加密机制应满足国家商用密码使用相关要求，并满足符合安全可靠要求的主机接入管理。

5.4 服务器安全

5.4.1 系统配置选型

应选择安全操作系统或根据集约化管理平台性能、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。操作系统和数据库系统宜遵循最小安全原则，仅安装应用必须的服务、组件、软件等。

5.4.2 身份鉴别

应根据用户类别设置不同安全强度的鉴别机制，严格设定访问和操作权限，具体措施包括但不限于下列内容：

a) 应采用两种或两种以上组合的鉴别技术，对系统账户和管理员账户进行身份验证，包括对网络设备、安全设备、主机操作系统、数据库基础运行环境中的系统用户账户，确定管理用户身份；
b) 禁止使用系统默认或匿名账户，根据实际需要创建必须的管理用户，及时清除操作系统及数据库系统的无用账号、默认账号，不允许多人共用同一个系统账号，并定期检查；
c) 应采用密码技术确保身份鉴别数据在传输和存储过程中的保密性，应防范口令暴力破解攻击；
d) 应针对各类用户启用登录超时重鉴别、设置登录延时、限制最大失败登录次数、锁定账号、连续登录失败尝试次数阈值等措施，如用户在一段时间内未作任何操作，应自动结束当前会话。

5.4.3 访问控制

服务器管理应具备多种访问控制措施，包括但不限于：

a) 应提供访问控制功能，授予各类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，实现系统管理用户、系统运维用户等的权限分离；
b) 应对登录系统的 IP 和终端环境进行限制，仅允许授权范围内的 IP 地址和通过安全检查的管理终端接入后台管理系统；

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，开启业务所需的最少服务及端口。服务器操作系统及数据库系统需要远程进行管理时，应采用 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。

5.4.4 安全审计

服务器管理应进行安全审计，配置审计功能，对集约化管理平台中的业务模块及其所依托的网络设备、安全设备、主机操作系统、数据库系统等基础设施进行安全审计，包括但不限于下列措施：

a） 对服务器操作系统及数据库系统进行安全审计，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 等的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） 审计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；

c） 审计日志应包括每个用户及应用系统重要安全事件，如用户登录/退出、改变访问控制策略、增加/删除用户、改版用户权限和增加/删除/修改业务数据等；

d） 审计记录应保存于专用的日志服务器上，保存时间应不少于 6 个月。

5.4.5 镜像和快照保护

部署在云计算环境的服务器，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，针对重要业务系统提供加固的操作系统镜像，采取密码技术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。

5.4.6 数据备份恢复

应提供重要数据的本地数据备份与恢复功能、异地备份功能，应提供重要系统的热冗余能力。提供多个可用副本，各个可用的副本数据内容应保持一致。

5.5 管理终端安全

5.5.1 连接控制

应加强后台管理终端的安全管理，定期开展安全检查，防止管理终端成为后台管理系统的风险入口。具体包括但不限于下列措施：

a） 应采取技术措施对管理终端进行身份认证，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集约化管理平台所在安全域；

e） 应对管理终端的远程登录 IP 地址及 MAC 地址进行限制；

f） 管理终端未经授权不应通过任何形式连接外部网络，应具备相关技术手段对管理终端未经授权的外联行为进行监测和处置；

g） 管理终端不得随意接入外部移动存储设备，应对管理终端连接外部移动存储设备的行为进行检测和处置，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。

5.5.2 系统配置

管理终端系统配置包括操作系统配置和软件安装配置两方面，应分别采取安全防护措施。系统应通过启用防火墙和授权访问策略、强化各类账号的口令安全设置、明确操作系统共享设置内容等措施，确保系统配置行为符合安全要求。应采购正版合法软件及相关服务，通过建立软件清单，进行安全审核、启用进程监测、漏洞扫描、强化审计等手段，确保应用软件安装、使用、更新等过程处于安全可控状态。

5.6 Web 应用安全

5.6.1 身份鉴别

网站对浏览用户可不进行鉴别，对前台注册用户、后台系统用户等不同类型的用户应设置不同强度的鉴别机制；

a) 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，应每三个月提醒用户修改口令；
b) 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；
c) 应针对各类集约化管理平台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；
d) 应强制用户首次登录时修改初始口令，当用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；
e) 应定期清理应用系统的账户，及时调整访问控制策略，至少每三个月更换一次口令。

5.6.2 访问控制

应提供访问控制功能，授予集约化管理平台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；

a) 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；
b) 应提供后台管理页面访问控制功能，限制特定用户或地址进行访问；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

5.6.3 安全审计

应提供安全审计功能，包括但不限于以下内容：

a) 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；
b) 应针对后台管理用户的登录、操作行为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、操作等行为发生时的用户信息、时间、地址、内容和结果等；
c) 应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，内容包括但不限于集约化管理平台用户登录时间、登录地址以及管理操作对象、操作内容、操作结果等；
d) 应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；
e) 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；
f) 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；
g) 审计记录应保存于专用的日志服务器上，保存时间不少于 6 个月；

h） 应对审计进程进行保护，防止未经授权的中断。

5.6.4 资源管控

集约化管理平台部署的设备和软件应具备与访问需求相匹配的性能。具体包括但不限于下列措施：

a） 应根据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，系统应自动结束当前会话；
c） 应能够对单个账户的多重并发会话进行限制。

5.6.5 源代码安全

应对应用软件的代码进行安全分析和测试，识别并及时处理可能存在的恶意代码。源代码安全应贯穿平台系统的整个生命周期，具体包括但不限于下列措施：

a） 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；
b） 应在单元测试期间和开发完成后可实施代码安全性测试，并在应用投入使用前委托第三方专业机构对应用程序源代码进行全面的安全审查；
c） 在应用系统部署前应对其进行安全风险评估，在使用过程中定期进行安全检测，及时修补发现的问题；
d） 应定期对集约化管理平台及其应用进行渗透性测试，并在程序更新后及时进行源代码安全检查。

5.6.6 系统更新

应定期针对应用系统、Web应用服务器（如Nginx、Apache等）、Tomcat等应用程序进行漏洞扫描，及时修补存在的安全漏洞；当应用程序的版本需要变更时宜经过审核批准，并保存响应记录。

5.6.7 移动互联安全

应采取有效的移动互联安全措施来保障移动网络、设备、应用等在集约化管理平台建设中的应用，包括但不限于以下措施：

a） 应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰；
b） 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；
c） 无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；
d） 应保证移动终端安装、运行的应用软件由指定的开发者开发；
e） 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；
f） 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
g） 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；
h） 应禁止多个 AP 使用同一个认证密钥；
i） 应能够阻断非授权无线接入设备或非授权移动终端。

5.6.8 域名安全

5.6.8.1 域名解析安全防护

应采取域名系统（DNS）安全协议技术、抗攻击技术等措施，防止域名被劫持、被冒用，确保域名解析安全，并委托具备有应急灾备、抗攻击等能力的域名继续服务提供商对政府网站域名进行集中解析。自行建设运维的政府网站服务器不得放在境外；租用网络虚拟空间的，所租用的空间应当位于服务商的境内节点。使用内容分发网络（CDN）服务的，应当要求服务商将境内用户的域名解析地址指向其境内节点，不得指向境外节点。应支持IPv4和IPv6双栈的域名解析。

5.6.8.2 域名监测处置

政府网站应开展域名安全的日常监测和定期检查评估，及时发现域名被劫持、被冒用等安全问题。清理注销不合格的域名、网站已关停但仍未注销的域名，以及被用于非政府网站的域名。

5.7 信息发布及数据安全

5.7.1 信息发布

集约化管理平台应对信息发布过程安全提供保障，具体包括但不限于以下措施：

a) 平台内容管理系统应具备提供内容编辑与审核发布权限分离的功能，实现内容采编和审核发布权限分离；
b) 统一信息资源库对外提供信息资源，应对资源服务接口采取服务授权认证机制。

5.7.2 内容监测预警

集约化管理平台应对平台信息内容进行监测预警，至少满足以下条件：

a) 应提供错别字、敏感词的事前检查和提醒功能，在内容编辑维护过程中自动提醒错别字、敏感词等信息，并应支持限制性条件，当内容存在不适宜信息时不得提交发布；
b) 应具备对已发布信息进行内容安全监测的能力，对已经发布在政府网站中的不适宜内容进行内容安全提醒。

5.7.3 链接地址

集约化管理平台应建设统一的链接地址监测机制，对内部链接、外部链接、链接状态等进行监测，具体包括但不限于以下措施：

a) 政府网站应建立链接地址的监测巡检机制，确保所有链接有效可用，及时清除不可访问的链接地址，避免产生“错链”、“断链”；
b) 政府网站使用外部链接应经本网站主办单位或承办单位负责人审核，不得链接商业网站、商业广告等；
c) 应对非政府网站链接的加强管理，确需引用非政府网站资源链接的，要加强对相关页面内容的实时监测和管理，杜绝因其内容不合法、不权威、不真实客观、不准确实用等造成不良影响；
d) 打开非政府网站链接时，应有提示信息；
e) 网站所有的外部链接需在页面上显示，避免出现“暗链”，造成安全隐患。

5.7.4 数据安全

5.7.4.1 数据加密要求

应对重要数据、敏感数据进行分类管理，做好加密存储和传输。具体包括但不限于以下措施：

a） 应对存储的信息数据严格管理，通过磁盘阵列等方式定期、全面备份数据，提升容灾备份能力；
b） 应设置专用加密通道，严格控制数据访问权限，确保安全，防止数据泄露、毁损、丢失；
c） 集约化管理平台与其他业务系统进行数据交互时，应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；
d） 集约化管理平台的个人信息及隐私信息等关键信息应在本地存储介质和数据库中应加密存储。

5.7.4.2 数据脱敏与防泄漏

集约化管理平台数据脱敏与防泄漏应满足以下要求：
a） 应对集约化管理平台的各类用户鉴别信息、重要业务数据进行脱敏处理，防止数据泄露；
b） 应通过技术手段防止重要数据被恶意爬取；
c） 应保证存有鉴别信息及敏感数据的存储空间在被释放或重新分配前得到完全清除；
d） 应仅采集和保存业务所必需的用户个人信息，禁止未授权访问和非法使用用户个人信息。

5.7.4.3 数据备份恢复

应针对集约化管理平台的系统数据、配置数据、业务数据及审计日志等定期进行备份，至少每月进行一次完全备份，每天进行一次增量备份。其中关键业务的重要数据、个人信息及隐私信息，应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。应制定合理的备份策略和恢复策略，规定备份信息的备份方式、备份频度、存储介质、保存及存放地点，并至少每6个月实施一次备份恢复演练。

5.8 攻击防范

5.8.1 攻击防范措施

应部署必要的安全防护设备，采取防火墙、恶意代码防范、入侵防范、网页防篡改等措施，保障平台及政府网站安全运行。

5.8.2 防火墙

在集约化管理平台与其他外部网络的接入入口，应配置防火墙系统，实现网络访问控制，防止外部对集约化管理平台网络系统的入侵和破坏。具体包括但不限于下列措施：
a） 防止非法对信息系统组网设备、系统进行攻击；
b） 防止对信息系统组网的入侵、破坏；
c） 对入侵、攻击信息系统的网络行为进行告警和审计。

5.8.3 恶意代码防范

恶意代码防范应包括但不限于以下类别：
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，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） 集约化管理平台中实际使用的操作系统，都应具备病毒防范机制；
c） 应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；
d） 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；

e） 应在服务器、运维终端等处采取恶意代码防范措施，实行统一有效的病毒、木马等恶意代码防范机制，并及时更新恶意代码系统特征库，对恶意代码进行实时检测和清除；
f） 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，进行系统补丁更新和版本升级；
g） 使用云计算服务或虚拟机部署时，应具备虚拟机与宿主机、虚拟机与虚拟机之间的异常行为检测和告警能力。

5.8.4 入侵防范

应建立平台安全监控预警体系，对服务器等基础设施、集约化管理平台、统一信息资源库、政府网站等的运行状态进行有效监控和预警，减少外部攻击发生频率，降低或杜绝外部攻击可能带来的损失，具体包括但不限于下列措施：

a） 应利用系统监控和人工方式结合的方式开展监测预警工作；
b） 应采取实时监控措施，包括但不限于端口扫描、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、网络蠕虫攻击、目录遍历攻击、SQL 注入、跨站脚本攻击等攻击行为，并及时进行阻断；
c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
d） 应加强物理安全、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；
e） 应对集约化管理平台的应用程序、操作系统及数据库、管理终端定期进行全面扫描，根据扫描结果判断平台存在的安全风险，及时调整监测策略；
f） 应提供网络入侵检测功能，对网络入侵行为的检测、告警、取证等。

5.8.5 病毒防御

集约化平台宜建设单机防病毒到网络防病毒的立体防病毒体系,在各个安全自治域及其中的主机均配置防病毒系统。具体应符合下列要求：

a） 支持对网络、服务器和工作站的实时病毒监控。反病毒模块从底层内核与各种操作系统、网络、硬件、应用环境密切协调，确保主动内核在病毒入侵反应时，反病毒操作不会伤及操作系统内核。
b） 能够在中心控制台上对多个目标系统监视病毒防治情况。具有实时治愈、统一管理、分域管理、病毒防火墙、病毒检查，能够在中心控制台上对多个目标系统进行监视，进行自动更新、增强的报警选择等特征。
c） 能够识别广泛的已知和未知病毒，包括宏病毒，具有实时病毒墙、文件动态解压缩、病毒陷阱、宏病毒分析器等功能。
d） 支持对 INTERNET/INTRANET 服务器的病毒防治，能够对恶意的 JAVA 或 Aactive X 小程序的破坏进行报警、阻止。
e） 支持对电子邮件附件的病毒防治，包括 WORD、EXCEL 中的宏病毒。
f） 支持对压缩文件的病毒检测。
g） 支持广泛的病毒处理选项，如对染毒文件进行实时杀毒、移出、删除、重命名等。
h） 支持病毒隔离，当客户机试图上载一个染毒文件时，服务器可自动关闭对该工作站的连接。
i） 提供对病毒特征信息和检测引擎的定期在线更新服务。

5.8.6 网页防篡改

应在前台网站服务器上部署网页防篡改功能，防止政府网站页面被恶意篡改。并利用网页防篡改系统并结合人工自检方式或第三方安全服务等方式，对政府网站篡改情况进行实时监测和处置，采取网页篡改恢复技术，确保网站篡改后能够及时恢复。

6 安全管理措施要求

6.1 安全管理制度

应按照网络安全法等法律法规和政策标准要求，制定完善的安全管理制度和操作规程，包括但不限于《变更管理制度》、《安全管理制度》、《值班管理制度》、《监控管理制度》、《检查审计制度》、《漏洞和风险管理制度》、《恶意代码防范管理制度》、《密码管理制度》、《备份与恢复管理制度》、《安全事件处置制度》、《应急预案管理制度》等，做好集约化管理平台的安全定级、备案、检测评估、整改和检查工作，提高集约化管理平台防篡改、防病毒、防攻击、防瘫痪、防劫持、防泄密能力。具体包括但不限于下列措施：

a) 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等；
b) 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，通过正式、有效的方式发布安全管理制度，并进行版本控制；
c) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；
d) 应对安全管理活动中的各类管理内容建立安全管理制度，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；
e) 应建立政府网站信息数据安全保护制度，收集、使用用户信息数据应当遵循合法、正当、必要的原则。

6.2 安全管理机构

在组织机构中应建立安全管理机构，管理层中应有一人分管安全运维工作，配备相应安全运维技术人员，安全管理机构应满足岗位设置、人员配备、授权和审批、沟通与合作、审核和检查等多方面要求，具体包括但不限于下列措施：

a) 应成立指导和管理网络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担任或授权；
b) 应设立网络安全管理工作的职能部门，设置全面负责安全管理工作的负责人岗位，配备专职的安全管理人员及一定数量的系统管理员、审计管理员和安全管理员；
c) 应明确系统变更、重要操作、物理访问和系统接入等的审批程序，明确审批部门、审批人等信息；
d) 应加强内部安全管理部门和人员之间以及和外部安全组织、专家、厂商等的合作和沟通，定期召开沟通会议，共同协作处理网络安全问题；
e) 应制定安全检查计划，定期进行全面检查和常规安全检查，确保系统正常稳定运行，安全风险可控，安全管理制度体系能被有效验证。

6.3 安全管理人员

安全管理人员应符合人员录用、人员离岗、安全教育和培训、外部人员管理等多方面的管理要求，具体包括但不限于下列措施：

f） 应指定或授权专门的部门或人员负责人员录用工作，对被录用人员的身份、安全背景、专业资格或资质等进行审查，并对其所具有的技术技能进行考核；
g） 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
h） 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章以及机构提供的软硬件设备；
i） 应办理严格的调离手续，在人员承诺调离后的保密义务后，方可离开；
j） 应根据不同的岗位制定不同的培训计划，定期对各类人员进行安全意识、岗位技能、安全基础知识、岗位操作规程等培训，并告知相关的安全责任和惩戒措施，定期进行技能考核；
k） 应对外部人员入场进行严格的管理，明确入场专人负责、申请和备案、权限分配和清除、签署保密协议等多种管理措施。

6.4 安全运维管理

集约化管理平台的安全运维应符合网络安全法等法律法规和政策标准要求，包括但不限于以下内容：

a） 应设置专门机构或人员负责平台及相关应用的安全技术运维保障，做好软硬件系统维护、功能升级、应用开发等工作；
b） 应按照相关法律法规和规范性文件要求，开展监测评估和安全建设；
c） 应定期对政府网站进行安全检查，及时发现消除存在隐患；
d） 应不断完善防攻击、防篡改、防病毒等安全防护措施，加强日常巡检和监测，发现问题或出现突发情况要及时妥善处理，确保集约化平台安全、稳定、高效运行；
e） 建立应急响应机制，制定应急预案并向本地区、本部门政府网主管单位和网络安全应急主管部门备案，明确应急处置流程，开展应急演练，提高对网络攻击、病毒入侵、系统故障等风险的应急处置能力；
f） 应建设平台安全运行监测预警机制，实施监测集约化的硬件环境、软件环境、应用系统、网站数据等运行状态以及网站挂马、内容篡改等攻击情况，并对异常情况进行报警和处置；
g） 定期对网站应用程序、操作系统及数据库、管理终端进行全媒扫描，发现潜在安全风险及时处置；
h） 密切关注网信、电信主管等部门发布的系统漏洞、计算机病毒、网络攻击、网络入侵等预警和通报信息，并及时响应。

7 安全定级与测评

7.1 安全定级

按照GB/T 22239-2019、GB/T 22240的要求对政府网站集约化管理平台进行定级，衡量政府网站集约化平台是否符合信息系统等级保护基本要求，是否具备等级保护三级的安全防护能力，包括但不限于下列要求：

a） 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由，提供《信息系统安全等级保护定级报告》；
b） 应组织相关安全技术专家对定级结果的合理性和正确性进行论证和审定；
c） 应保证定级结果经过相关部门的批准；

d) 应将《信息系统安全等级保护备案表》备案材料报主管部门和属地公安机关备案。

7.2 安全测评

应根据安全运行需求，定期开展安全测评工作。安全技术测评应包括物理安全、网络安全、主机安全、应用安全、数据安全五个方面的内容。安全管理测评应包括安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面的内容。

在信息系统测评过程中，根据第三方信息系统测评公司出具问题整改清单，针对政府网站集约化平台出现中存在的安全问题或安全隐患，评估安全问题或安全隐患将导致的安全威胁，形成差距分析报告，制定安全整改方案和计划，按照整改计划，修复集约化平台出现漏洞等安全问题，完成政府网站集约化平台等保测评工作，确保政府网站集约化平台安全、稳定、高质量运行。