# 国家电子政务外网标准

GW0104—2014

# 国家电子政务外网
# 安全等级保护实施指南

Implementation guide for classified protection of

National E-Government Network

2014-1-28 发布　　2014-1-28 实施

国家电子政务外网管理中心

# 目　　次

# 前　言

为规范国家电子政务外网安全等级保护的工作，落实信息安全等级保护相关技术要求，根据国家标准GB/T22239-2008《信息安全技术 信息系统安全等级保护基本要求》和国家电子政务外网管理中心文件《关于加快推进国家电子政务外网安全等级保护工作的通知》(政务外网[2011]15号)，针对政务外网的具体情况，特制定《国家电子政务外网安全等级保护实施指南》（以下简称本指南）。

本指南由国家电子政务外网管理中心提出。

本指南由国家电子政务外网管理中心归口。

本指南主要起草单位：国家电子政务外网管理中心办公室、公安部信息安全等级保护评估中心

本指南主要起草人：周民、邵国安、任卫红、杨绍亮、张宇翔、罗海宁、吕品、焦迪、冷默

本指南由国家电子政务外网管理中心负责解释。

# 引　言

2003年8月发布的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）文件中明确要求我国的信息安全保障工作实行等级保护制度，提出了“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”的要求，2007年6月公安部等信息安全管理部门联合发布的“关于印发《信息安全等级保护管理办法》的通知”（公通字[2007]43号）进一步强调了开展等级保护工作的重要意义，规定了实施信息安全等级保护制度的原则、内容、职责分工、基本要求和实施计划，具体部署了实施信息安全等级保护工作的操作办法。国家电子政务外网是我国电子政务重要的行政基础设施，开展政务外网的安全等级保护工作是保证政务外网及各级政务部门业务应用安全的基础性工作。

本指南是国家电子政务外网安全等级保护相关系列标准之一。

本指南与国标《计算机信息系统安全等级保护划分准则》（GB17859-1999）、《信息安全技术 信息系统安全等级保护基本要求》（GB/T22239-2008）、《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010）等标准以及《国家电子政务外网网络安全等级保护基本要求》共同构成了国家电子政务外网安全等级保护的相关配套标准。是各级政务外网实施安全等级保护的基本要求。本指南依据国家标准要求和政务外网安全等级保护基本要求，逐条提出了有针对性、可操作的实施意见，供参考使用。

对于承载涉及国家秘密信息系统的网络保护要求，按照国家相关法律法规和信息安全主管部门的相关规定和标准实施。

对于涉及密码的使用和管理，按照国家密码管理主管部门的相关规定和标准实施。

凡涉及政务外网数字证书的相关要求，参照国家电子政务外网管理中心印发的相关管理和技术规定执行。

# 国家电子政务外网安全等级保护实施指南

## 1 范围

本指南规定了国家电子政务外网（以下简称政务外网）安全等级保护在实施过程中，为达到国家标准规定和政务外网的基本要求而提出的安全等级保护的方法和手段，适用于指导各级政务外网的安全等级保护工作在定级、整改、报备、检查、测评和运维等实施过程中参考；各级在新建政务外网时可参照本指南开展安全等级保护工作；也可作为政务外网外包服务时对第三方提出安全保障要求的依据。

## 2 规范性引用文件

下列文件中的条款通过本指南的引用而成为本指南的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本指南。凡是不注明日期的引用文件，其最新版本适用于本指南。

GB/T 5271.8 信息技术 词汇 第8部分：安全

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 25058信息安全技术 信息系统安全等级保护实施指南

YD/T 1729电信网和互联网安全等级保护实施指南

中华人民共和国计算机信息系统安全保护条例(1994年2月18日中华人民共和国国务院令147号发布)

公安部、国家保密局、国家密码管理局和国务院信息化工作办公室关于印发《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）

国务院信息化工作办公室《电子政务信息安全等级保护实施指南（试行）》（国信办[2005]25号）

公安部、国家保密局、国家密码管理局和国务院信息化工作办公室“关于印发《信息安全等级保护管理办法》”（公通字[2007]43号）

国家电子政务外网管理中心《关于加快推进国家电子政务外网安全等级保护工作的通知》（政务外网[2011]15号），其中附件2《国家电子政务外网安全等级保护基本要求（试行）》

## 3 术语和定义

GB/T 5271.8和GB 17859确定的术语和定义适用于本指南。

## 4 实施概述

### 4.1 实施原则

政务外网安全等级保护应首先满足政务外网安全防护工作提出的适度安全原则以及标准化、可控性、完备性和最小影响的原则，为所承载的各级政务部门信息系统提供网络传输通道的安全保障。在此基础上，政务外网安全等级保护工作在实施过程中还应重点遵循以下原则：

a) 自主定级原则

各级政务外网的建设管理单位按照本实施指南的定级方法和国家相关等级保护的标准，自主确定本级政务外网的安全等级，并根据国家相关标准和政务外网相应的安全等级保护基本要求，对所管辖网络实施安全保护。

b) 政务外网与所承载的信息系统分别定级原则

各接入政务外网的政务部门负责各自局域网络及业务应用系统和数据的安全，并按国家信息系统安全等级保护的法规和标准要求实施定级与保护，应与政务外网的管理、安全防护与运维保障系统分别进行定级。

c) 分域保护原则

政务外网等级保护应根据所承载的业务应用系统实际的需要，将政务外网划分为公用网络区、专用网络区、互联网访问区、托管服务区、安全接入区等不同的安全区域，实施不同的安全策略进行边界防护。对不同安全等级网络的互联及各用户局域网的接入，应采取有效的边界访问控制策略，对非授权访问、异常流量、病毒木马、网络攻击等行为进行控制和监测，保证网络和业务的安全。

d) 同步建设原则

政务外网在新建、改建、扩容过程中，应按安全等级保护的基本要求同步规划和建设安全设施。

e) 适时调整原则

根据政务外网网络结构及所承载的电子政务信息系统安全保护等级的变化情况，适时调整政务外网的安全等级，并根据相应的安全等级基本要求及时调整与之相适应的安全保护措施。

## 4.2 角色与职责

政务外网安全等级保护实施过程中涉及的各类角色和职责如下：

a) 国家等级保护主管部门

地（市）级以上公安机关作为国家信息安全等级保护主管部门，负责本地辖区内政务外网安全等级保护工作的监督、检查，负责受理当地政务外网建设管理部门对本地辖区政务外网安全保护等级定级的报备及相关指导工作。

b) 政务外网主管部门

负责本级电子政务外网管理工作，并对政务外网建设管理单位定级的政务外网负责审核并提出批准相应安全保护等级的意见。

c) 政务外网建设管理单位

是具体负责落实管辖内政务外网安全等级保护工作的责任单位。负责政务外网的建设和日常管理工作，负责监督、检查和指导政务外网运营维护工作；负责确定其管辖内政务外网的安全定级，并报其主管部门审核批准；根据已确定的安全保护的等级，到当地公安机关办理备案手续；负责对下级政务外网运维单位的技术指导，制定各项安全管理制度，定期进行检查；负责选择符合国家相关规定的等级测评机构对本辖区政务外网定期进行等级测评等相关工作。

d) 政务外网运行维护单位

各级政务外网运行维护单位由当地政务外网主管部门或建设管理单位指定，按政务外网建设管理部门的要求，具体负责所辖政务外网的运行维护工作，负责依照国家信息安全等级保护的管理规范和技术标准、政务外网相关技术要求，进行政务外网的运行维护和安全保护的技术实施等具体工作。

e) 等级保护测评机构

由公安部公布的全国信息安全等级保护测评机构推荐目录中的第三方测评机构。根据政务外网建设管理部门的委托，依照国家信息安全等级保护的管理规范和技术标准及政务外网相关技术要求，对政务外网进行安全等级保护的测评工作。

### 4.3 政务外网定级对象

政务外网的定级对象为本级政务外网管辖范围内（由边界设备确定）的所有网络、计算、存储和安全防护等各类设备、各种用于网络运维管理、安全保障的应用系统、各种通信线路及支持所有软硬件正常运行的机房等基础环境设施等。

门户网站系统、跨部门的数据共享与交换系统、数据中心内的各业务应用系统以及各级政务部门的各类业务应用系统不包含在政务外网的等级保护范围内，这些信息系统应按国家标准《信息系统安全等级保护基本要求》（GB/T 22239-2008）中的规定由信息系统的责任主体单位自行实施定级和保护。

### 4.4 安全等级保护目标

安全等级保护的目标是通过推进安全等级保护工作，加强政务外网整体的安全防护能力，确保国家政务外网全网的安全性、可靠性和一致性，保证所承载的各级政务部门电子政务业务的畅通和安全。

政务外网安全等级保护首先是网络防护，保证所承载各级政务部门信息系统的网络畅通，抵御病毒和人为的攻击，在所管辖的网络边界范围内，管理好统一的互联网出入口、安全接入平台并做好各单位局域网接入边界的访问控制，及网络管理系统、安全管理系统（SOC）等自身业务信息系统的安全保障。

### 4.5 安全等级保护区域边界

国家电子政务外网可分为中央级政务外网、省级政务外网、地（市）级政务外网和县级政务外网，依据其管辖范围来确定管理边界。通常该边界为广域网络与广域网络之间、广域网络和与城域网络之间，以广域网的接入路由器为边界；城域网络与单位局域网之间，以城域网络放在接入单位内的接入路由器为边界；政务外网与互联网或其他公众通信网络之间，以接入设备或安全网关设备为边界，按边界设备的资产归属为划分原则（含自建或租用的长途电路）确定管理范围。

## 5 网络功能及安全分域

### 5.1 网络功能描述

政务外网建立在基础电信传输网络之上，其传输网可分为MSTP网、SDH网和光纤网络等，在传输网之上的I P承载网按网络结构及所处位置可分为广域网、城域网和局域网。

#### 5.1.1 广域网

a) 各级政务外网广域网内主要传输电子政务的数据、视频、图像等相关业务。跨部门及跨省、跨地区的业务协同及信息共享的系统，可以直接在政务外网的广域网上传输业务信息，政务外网可通过 MPLSVPN 或其他安全技术手段，对不同的业务或信息系统进行隔离。

b) 政务外网中央级和省级广域网内原则上不承载传输直接访问互联网的业务，接入政务外网的政务部门访问互联网时，应由当地城域网负责。省级以下广域网是否承载访问互联网的业务，可根据自身的实际情况来确定，原则上互联网出入口应属地化。如果地（市）级政务外网的互联网出口统一集中，县级政务外网及以下接入单位没有互联网出口时，则地（市）到县的广域网可以传输访问互联网的业务，但必须在广域网中采用 VPN 隔离技术，区分访问互联网的业务与电子政务业务（数据、视频、图像等），并应采用 QoS 保障机制，优先保证各级电子政务业务的传输带宽和质量。

#### 5.1.2 城域网

a) 政务外网的城域网通过专线连接到本地各政务部门的局域网络，城域网内应采用 VPN 技术来保证不同业务之间的有效隔离，并在汇聚层设备上增加相应的边界访问控制策略。

b) 政务外网城域网为各政务部门提供统一的互联网接入服务时，应通过 MPLS VPN 或其他网络隔离技术，区分访问互联网业务和电子政务业务并做好相应的安全防护工作，，统一接入到当地的互联网服务提供商（ISP）同时应采用有效的 QoS 保障机制，优先保证电子政务业务传输带宽和质量。

### 5.1.3 局域网

局域网通常是由各政务部门自行管理的网络，用以连接终端、服务器、存储设备及业务信息系统等。局域网是政务部门连接政务外网的主要载体。其所有网络设备、终端、服务器、各类应用软件及系统安全保障均由局域网的责任单位负责，应按国家信息系统安全等级保护基本要求相关标准及主管部门的要求进行定级、报备、测评、整改并接受主管部门的检查。

同一单位分几个办公区域办公，建议采用当地电信运营商提供的专线或自建光纤，组建一个完整的局域网络，再统一接入到政务外网。

各省的政务外网建设情况不同，对政务外网功能区的划分可以有所不同，其功能区域划分示意如图1所示。

## 5.2 安全区域划分

按照国家电子政务外网统一技术路线的要求，在广域网、城域网内可通过MPLS VPN或其他VPN隔离技术、路由控制、防火墙、认证网关、边界访问控制设备等技术手段，划分不同的区域来保证政务外网和业务信息系统的安全。根据所承载电子政务业务的需要，政务外网按其功能和作用可划分为如下安全域：

a) 公用网络区：是各部门、各地区互联互通的网络区域，为政务部门公共服务及开展跨部门、跨地区的业务应用、协同和数据共享提供支撑平台。此外该区域还提供政务外网的公共网络服务，如政务外网门户网站、DNS 服务等。要求互联网用户不能直接访问这个区域的数据和信息系统。

b) 专用网络区：是为有特定安全需求的部门或业务设置的网络区域，实现本部门内的全国性业务在政务外网上开展，保证与不同部门业务应用系统的相互隔离，非本部门用户和互联网用户不能直接访问这个区域的数据和信息系统。

c) 互联网区：是政务部门通过逻辑隔离安全接入互联网的网络区域，满足政务部门利用互联网开展公共服务、社会管理、经济调节和市场监管的电子政务业务需要。

## 5.3 功能区域划分

a) 互联网出入口安全防护区：为各政务部门提供互联网访问业务，互联网出口应部署防火墙、IPS、防 DDOS 攻击设备及流量控制设备等，或具有上述功能的综合网关类设备，保证自身业务和全网的安全。各地政务外网可统一建设互联网门户网站群、电子邮件系统、政府公众服务等面向社会公共服务的信息系统等。将政务部门用户主动访问互联网的流量与互联网公众用户访问政府门户网站的流量在城域网分开，通过各种 VPN 技术等安全手段进行隔离，进一步保证政务外网城域网的安全。

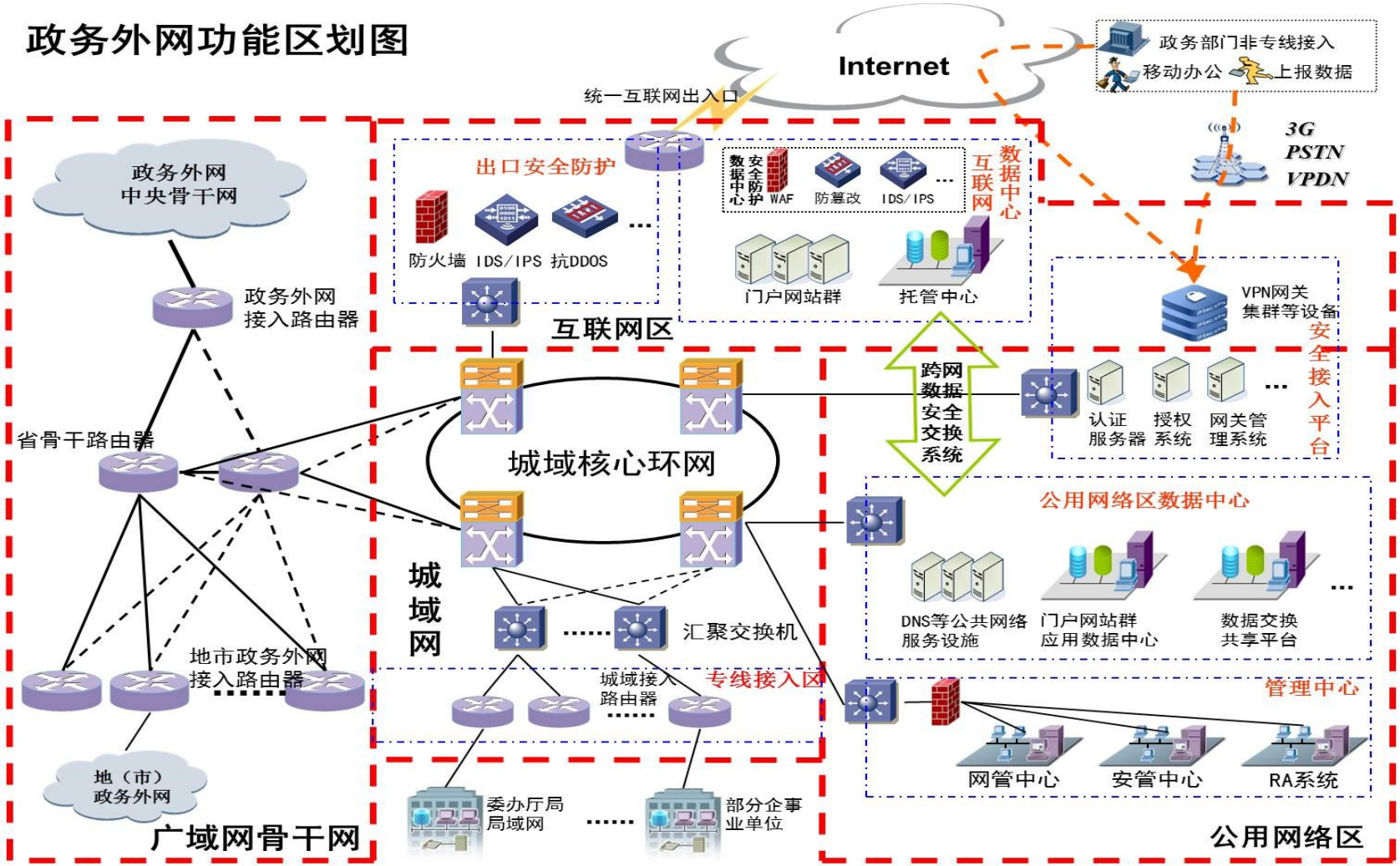



图1　政务外网功能区划图

b) 安全接入平台区：通过 IPSec VPN、3A 认证、数字证书、VPDN 等技术手段，将移动 PC 终端或各类智能移动终端通过 3G 网络或互联网等公众网络安全接入政务外网公用网络区或政务部门的专用网络区，实现移动办公、现场执法等各类移动政务业务安全接入到政务外网内。平台应具有对各类移动智能终端的实时管理等安全保障功能，通过终端身份认证、加密传输等安全手段将移动终端接入到相应的业务应用系统，保证数据和应用系统的使用安全。

c) 网络管理区：根据网络业务及安全自身的需要，将网络管理系统、安全管理系统、电子认证服务等信息系统部署在管理区，并设置与之相适应的访问控制策略。安全等级保护确定为第三级的政务外网，应建立安全管理系统（SOC），对安全防护设备的日志进行采集和综合关联分析，提出安全整改建议。对于安全事件和网络攻击等应能实时告警，有条件的相关设备应能联动，防止网络攻击等事件的进一步扩大，积极有效地保护政务外网的安全。

d) 数据中心区：可分为互联网区和公用网络区，实现相关政务部门各类业务的分业务分区域集中部署或托管等。放置在数据中心互联网区或公用网络区机房托管的各相关信息系统由责任主体单位与托管中心的责任单位签订合同、明确责任和边界，并按国家信息系统安全等级保护的要求进行定级和采取相应的安全防护措施。

## 6 网络域间互联要求

### 6.1 广域网与广域网的互联要求

中央和省级广域网互联或省级和地（市）级广域网互联时，应加强对边界接入设备的监控和管理，采取有效的边界访问控制策略，并保证所承载各类业务的畅通和连续性。

### 6.2 广域网与城域网的互联要求

a) 安全保护等级定级均为第三级的广域网与城域网互联时，应有主电路和备用电路，按主备电路互为备份或负载分担的方式提供网络承载服务。其核心路由设备应放置在不同的机房，保证其可靠性。广域网应与城域网的两个不同的汇聚设备或具有 PE 功能的核心设备互联，之间可不串接防火墙等边界访问控制设备。

b) 安全保护等级定级为第三级的广域网与安全保护等级定级为第二级的城域网互联时，广域网应在边界接入设备上采取有效的边界访问控制策略，对非授权访问、异常流量、病毒木马、网络攻击等行为进行控制，如串接防火墙作为边界访问控制设备时，应保证所承载各类业务的畅通和连续性。

### 6.3 城域网与接入局域网的互联要求

a) 各级政务部门的局域网络及其信息系统的安全及等级保护工作由各单位自行负责。其信息系统需要利用政务外网城域网和广域网时，应将政务外网的安全保护等级定级情况与需要定级的信息系统一起作为定级对象进行安全等级保护和报备，但安全等级保护的测评工作可分开实施。

b) 政务部门的局域网接入政务外网，应符合一定的安全要求，如边界访问控制、IP 地址转换等，对于访问政务外网的系统和终端应具有病毒防范、审计等功能，终端安全应根据各单位的安全要求增加终端安全管理系统和选择不同网络区域的安全措施等。如局域网有互联网出口，应采取有效的安全保护措施，保证自身和全网安全的一致性。

c) 在 IP 地址转换、VPN 对接等方面，由政务外网建设管理单位与业务发起部门一起协商，提出可实施的技术方案，保证业务的接入。

d) 在城域网的汇聚层设备上，应做好局域网接入的边界访问控制，如异常流量的监测、非授权访问、病毒攻击等安全策略及防护措施，如串接防火墙作为边界访问控制设备时，应保证所承载各类业务的畅通和连续性。

### 6.4 城域网与互联网的互联要求

当城域网与互联网服务提供商（ISP）互联时，在互联网出入口应部署防火墙、入侵防御、防DDOS攻击、防病毒等安全防护设备，应对互联网的出入口实施流量控制、行为审计、入侵检测，有条件的地方应与当地信息安全管理部门联合做好统一互联网出入口的监测与管理工作。

### 6.5 城域网与3G等公众网络互联要求

当各地政务外网提供各类移动终端通过LTE（4G）、3G VPDN、PSTN或互联网接入时，应在省级或地（市）级的城域网统一建设安全接入平台，应对各类接入终端进行身份认证、权限控制、传输加密、行为审计等各类安全措施。

## 7 定级方法

政务外网安全等级的确定，首先应针对服务地域、责任主体、管理范围等因素，确定本级政务外网的管辖范围和边界。其次是对政务外网合理划分不同安全域，并确定其边界。三是依据所承载的各级政务部门业务信息系统，明确每个安全域的业务内容和安全要求，科学合理的划分安全等级。

### 7.1 定级要素

确定政务外网的安全等级应根据社会影响、规模和服务范围及服务对象重要性这3个相互独立的定级要素来确定，并以这3个定级要素的最高赋值来确定政务外网的安全等级。

a) 社会影响

政务外网的社会影响表示其受到破坏后对国家安全、社会秩序、经济运行和公共利益的损害程度，其社会影响赋值原则见表1所示。

**表1 社会影响的赋值原则**

| 社会影响 | 赋值 |
|---|---|
| 政务外网受到破坏后，所承载的政务部门业务应用系统无法正常运行，造成的社会影响较小，不损害国家安全、社会秩序、经济运行和公共利益 | 1 |
| 政务外网受到破坏后，所承载的政务部门业务应用系统无法正常运行，造成的社会影响较高，不损害国家安全，但对社会秩序、经济运行和公共利益造成损害 | 2 |
| 政务外网受到破坏后，所承载的政务部门业务应用系统无法正常运行，造成的社会影响大，对国家安全造成损害，或对社会秩序、经济运行和公共利益造成严重损害 | 3 |

损害国家安全的事项包括（但不限于）以下几个方面：

- 影响国家政权稳固和国防实力；
- 影响国家统一、民族团结和社会安定；
- 影响国家对外活动中的政治、经济利益；
- 影响国家重要的安全保卫工作；
- 影响国家经济竞争力和科技实力等。
- 使保护国家秘密的措施可靠性降低或者失效；
- 使国家机关依法行使职权失去保障。

损害社会秩序的事项包括（但不限于）以下几个方面：

- 影响政务部门社会管理和公共服务的工作秩序；

- 影响各种类型的经济活动秩序；
- 影响各级政务部门的正常工作秩序；
- 影响公众有法律约束和道德规范下的正常生活秩序等。

损害经济运行的事项包括（但不限于）以下几个方面：

- 直接或间接导致国家经济活动主体的经济损失；
- 影响各级政务部门对经济调节等相关数据的收集、分析和公告等。
- 损害公共利益事项包括（但不限于）以下几个方面：
- 影响各级政务部门通过政务外网提供的公众服务；
- 影响企事业单位和公众等通过政务外网获取公开信息资源。

对此项定级要素进行赋值时，应先确定对国家安全的损害程度，再确定对社会秩序、经济运行和公共利益的损害程度。定级对象的社会影响赋值应是对国家安全和社会秩序、经济运行、公共利益的损害程度最严重者。

b) 规模和服务范围

定级对象的规模表示其政务外网的接入单位数量多少，服务范围表示其服务的区域范围大小，定级对象的规模和服务范围赋值如表2所示。

**表2 规模和服务范围的赋值原则**

| 规模和服务范围 | 赋值 |
|---|---|
| 政务外网被破坏后对较少政务部门的业务应用系统造成影响，或者对较小的地区造成影响（如乡镇或部分县级单位） | 1 |
| 政务外网被破坏后对较多的政务部门业务应用系统造成影响，或者对较大的地区造成影响（如县级和多个乡镇、社区） | 2 |
| 政务外网被破坏后对很多的政务部门业务应用系统造成影响，或者对多个省或很大的地区造成影响（如部分中央部门，省级单位、地市级和多个县级及以下） | 3 |

c) 服务对象重要性

政务外网所提供服务的对象是各级政务部门的各类电子政务应用，承载其应用的政务外网被破坏后，将直接影响到各级政务部门的各类电子政务的应用。因此，承载其业务应用的政务外网网络部分的重要性与电子政务的信息系统的重要性应该是一致的，例如所承载的电子政务信息系统最高定级为安全等级保护第三级的，其政务外网的服务对象及重要性赋值就应该是3，各级政务部门信息系统安全等级保护的定级结论应作为各级政务外网的安全等级保护定级的重要依据。

## 7.2 定级要求

a) 政务外网开展安全等级保护工作的重点是广域网和各级城域网。政务外网中央至省、省至地（市）广域网和中央、省级、地（市）级城域网应达到安全等级保护第三级要求，地（市）级至区县广域网和地（市）以下城域网应至少达到安全等级保护第二级的要求。

b) 政务外网在确定管理边界和责任主体的前提下，依据政务外网的社会影响、规模和服务范围及服务对象重要性三个定级要素来确定相应的赋值，最高赋值在 2 及以下的，其安全等级可定级为第二级及以下，最高赋值为 3 的，其安全等级可定级为第三级。

c) 政务外网作为承载网，可以承载不同安全等级保护的政务信息系统，各级政务外网的安全保护等级最高可定为第三级。如果所承载的政务信息系统安全等级高于第三级时，其信息系统按国家标准的规定对数据和信息系统进行保护，使其达到信息系统相应安全等级保护的要求。

# 8 网络等级保护实施过程

实施政务外网安全等级保护工作的基本过程见政务外网安全等级保护定级工作流程图（图2），政务外网的建设管理单位作为定级工作的主体，组织并确定所管辖政务外网的安全等级，其主要工作有以下几个阶段：

### 8.1 定级

遵循“自主定级、专家评审、主管部门审批、公安机关审核”的原则进行定级，由政务外网建设管理单位根据政务外网的情况及所承载的电子政务业务应用，自主确定政务外网的安全等级。

安全等级确定为第三级的政务外网要明确网络的管理边界、安全等级保护的对象、规模及服务范围，绘制网络拓扑图，确定等级保护范围内的关键设备，制定相应规章制定和管理办法，按附录C：《政务外网安全等级保护定级报告》模板起草定级报告，组织相关专家对定级情况进行评审并出具专家评审意见，报上级主管部门审批同意，（具体实施可参考附录A：《安全等级保护第三级政务外网定级案例》）。

安全等级确定为第二级的政务外网，由责任单位绘制网络拓扑图，确定网络管理边界，制定相应规章制定和管理办法，按附录C：《政务外网安全等级保护定级报告》模板起草定级报告，报上级主管部门审批同意，（具体实施可参考附录B：《安全等级保护第二级政务外网定级案例》）。

### 8.2 安全整改

根据上级主管部门审批同意的政务外网安全等级，依据国家标准《信息安全技术信息系统安全等级保护基本要求》及《国家电子政务外网安全等级保护基本要求》，逐项对照，针对拟定级报备的政务外网存在的安全问题进行分析归类，对不符合要求的项目按其轻重缓急，制定整改计划，并予以实施。因经费等原因暂时无法解决的，应向政务外网主管部门说明理由和解决的办法与时间，逐步分阶段实施解决，保证基本要求的有效实施。

### 8.3 测评

政务外网建设管理单位应选择由公安部公布的全国信息安全等级保护测评机构推荐目录中的第三方测评机构对已定级的政务外网进行测评，测评的依据是国家标准《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）及《国家电子政务外网安全等级保护基本要求》（政务外网[2011]15号）。测评方法按公安部的相关要求进行，测评发现不符合要求的项目，政务外网建设管理单位应进行必要的整改，直至第三方测评机构提交出合格的测评报告。

### 8.4 报备

已投入运行的政务外网，其安全等级保护定级在第二级或第三级的，应当在安全等级保护确定后30日内（新建政务外网应在投入运行后的30日内），由建设管理单位到所在地（市）级以上的公安机关办理备案手续，取得公安机关颁发的备案证明。

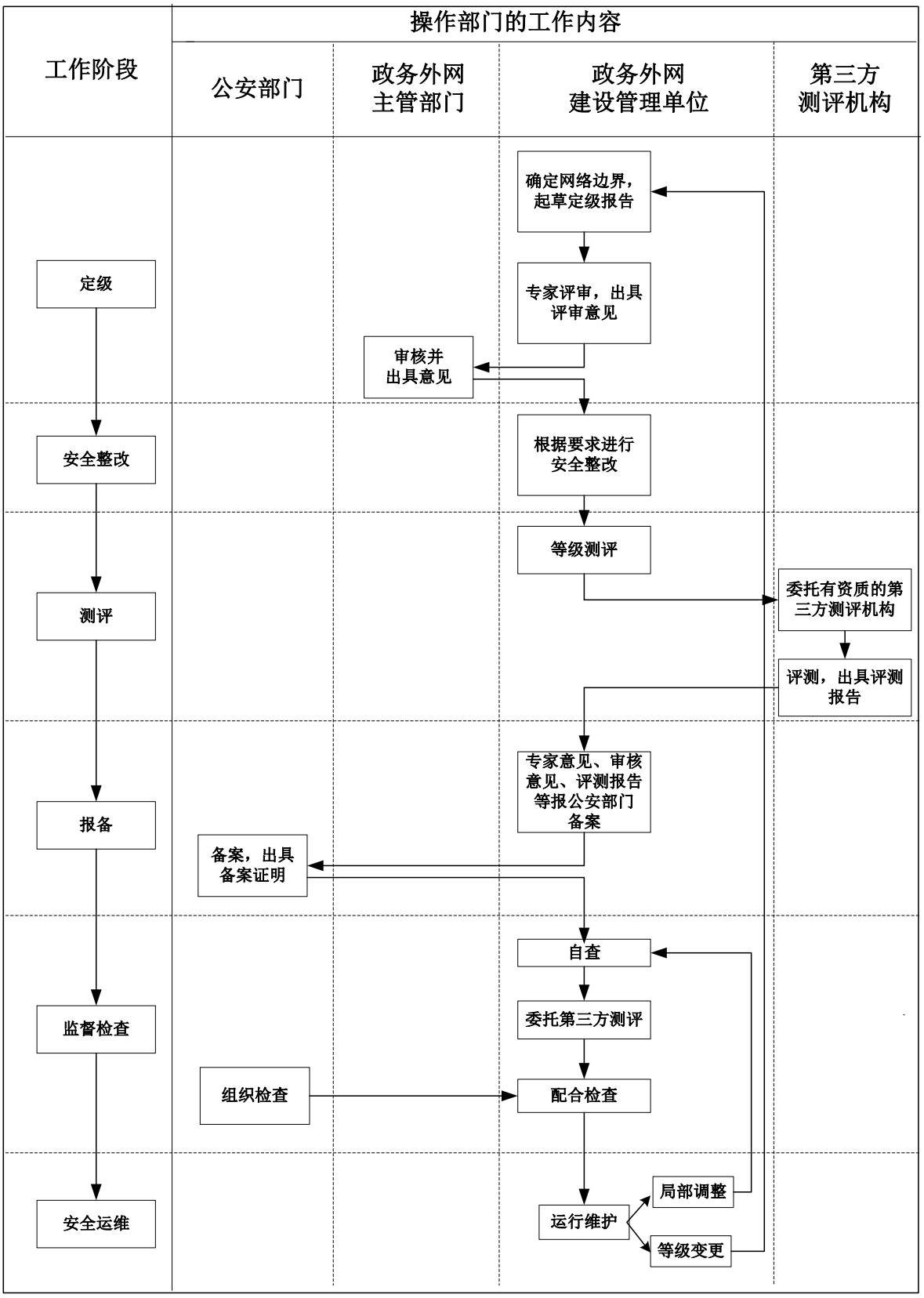



图2　政务外网安全等级保护定级工作流程图（以安全等级保护第三级的定级为例）

办理政务外网安全等级保护备案手续时，应当填写公安机关的关于《信息系统安全等级保护备案表》，安全等级保护定级为第三级的政务外网系统备案时，应同时提供以下材料：

- 政务外网拓扑结构及说明；
- 单位的安全组织机构和管理制度；
- 政务外网安全保护设施设计实施方案或改建实施方案；
- 政务外网定级范围内使用的信息安全防护设备清单及其认证、销售许可证明；
- 安全保护等级定级专家评审意见；
- 测评后符合系统安全等级保护的技术检测评估报告；
- 主管部门审核批准政务外网安全保护等级定级的意见。

各级政务外网建设管理单位在取得备案证明后应将定级报告、备案表及相关材料和备案证明复印件应在10个工作日报上一级政务外网管理单位备案。

### 8.5 监督检查

确定安全保护等级为第三级的政务外网，应每年进行一次自查，发现问题及时整改。应每年选择在公安部备案的第三方测评机构进行一次安全保护等级的测评，测评报告应报上一级政务外网管理部门备案。应接受当地公安机关和上级政务外网管理部门的检查。公安机关按《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736号）的要求进行检查并出具检查反馈意见单，政务外网建设管理单位应按反馈意见单的要求及时整改。

国家外网管理中心每年会同当地公安机关或组织相关人员和专家对省级政务外网安全等级保护工作进行检查或抽查，省级以下政务外网由省政务外网主管部门组织进行检查或抽查，保证政务外网的全网安全。

确定安全保护等级为第二级的政务外网，应至少每年进行一次安全自查，发现问题应及时整改。每三年应选择在公安部全国等级保护测评机构推荐目录中的第三方测评机构进行全面的安全保护等级测评工作。

### 8.6 安全运维

政务外网建设管理单位应通过对网络的运行状况、安全状态监控及对网络发生安全事件的及时响应，确保管辖的政务外网及相关系统的正常运行，并根据安全检查情况和业务需要的变化及时调整政务外网的安全措施和安全等级。通过定期的安全等级保护的测评，确保政务外网及相关系统满足相应安全等级的要求。

当政务外网接入单位及相关信息系统增加、网络拓扑变更、安全要求发生局部调整等情况时，如果不影响其安全等级，应从安全运维阶段开始，重新调整和实施安全措施，保证政务外网满足安全等级保护的要求。

当政务外网及相关系统发生重大变更影响其安全等级时（如行政区划的改变，网络拓扑及管理边界的较大变化等），应对管辖内的政务外网进行重新定级，重新开始一次安全保护等级的定级实施过程。

## 9 具体实施要求

政务外网安全等级保护基本要求包括两部分，一是国家标准GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》，二是国家电子政务外网管理中心针对政务外网的特点并作为国家标准的补充印发的《国家电子政务外网安全等级保护基本要求（试行）》，各级政务外网在实施安全等级保护时应同时满足国家标准要求和政务外网的要求，下列表格针对基本要求逐条提出实施建议，供各地方执行时参考。

表3　国家标准安全等级保护基本要求实施建议表

| | 基本要求指标项 | 实施建议 |
|---|---|---|
| 序号 | GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》以安全等级保护第三级为例，其中不加黑为第二级要求，**加黑为第三级应达到的要求。** | **以下提出的实施建议仅供参考，如有其他方法能达到基本要求，也认可达到相关安全等级的要求。** |
| 1 | 7 第三级基本要求 | |
| 2 | 7.1　技术要求 | |
| 3 | 7.1.1　物理安全 | |
| 4 | 7.1.1.1　物理位置的选择（G3） | |
| 5 | 本项要求包括： | |
| 6 | 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； | 在机房选择时应符合要求 |
| 7 | 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。** | 在机房选择时应符合要求，根据设备情况主要考虑机房承重等因素。 |
| 8 | 7.1.1.2　物理访问控制（G3） | |
| 9 | 本项要求包括： | |
| 10 | 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； | 应符合要求 |
| 11 | 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； | 应符合要求，制定机房人员出入的规章制度。 |
| 12 | 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；** | 应符合要求，如根据政务外网的特点，划分公共区、互联网区和托管区等，并按要求设置物理隔离装置。 |
| 13 | 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。** | 应符合要求，对安装网络与重要服务器等核心设备的机房或区域应配置门禁系统，并采用密码或指纹识别技术。 |
| 14 | 7.1.1.3　防盗窃和防破坏（G3） | |
| 15 | 本项要求包括： | |
| 16 | a)应将主要设备放置在机房内； | 应符合要求 |
| 17 | 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； | 标记应明确服务对象、IP 地址、固定资产编号、物理位置、设备维护责任人等信息，并粘贴在明显的位置。 |
| 18 | c)应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； | 应符合要求，并在线缆的两端做好标记。 |
| 19 | d)应对介质分类标识，存储在介质库或档案室中； | 对存储介质应进行分类，做好标识，并符合要求。 |
| 20 | e)**应利用光、电等技术设置机房防盗报警系统；** | 在监控室和值班室应安装具有声、光、电提醒的防盗报警系统。 |
| 21 | f)**应对机房设置监控报警系统。** | 应在机房入口、机柜走道、重要服务器等位置安装摄像头和图像存储、监控系统。 |
| 22 | 7.1.1.4　防雷击（G3） | |
| 23 | 本项要求包括： | |

| | | |
|---|---|---|
| 24 | a)机房建筑应设置避雷装置； | 应符合要求。 |
| 25 | b)**应设置防雷保安器，防止感应雷；** | 应符合要求。 |
| 26 | c)机房应设置交流电源地线。 | 交流电地线与保护地线应分开设置，地线电阻值应满足要求。 |
| 27 | 7.1.1.5　防火（G3） | |
| 28 | 本项要求包括： | |
| 29 | 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；** | 根据机房面积的实际情况，可选用有管网或无管网等消防设施，应采用机房专用的消防设施并满足消防安全要求， |
| 30 | 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；** | 应符合要求 |
| 31 | 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。** | 政务外网的重要设备如广域网核心路由器、城域网核心交换机等，应与其他网络和应用设备隔离放置，并按消防要求采取相应的防火措施。 |
| 32 | 7.1.1.6　防水和防潮（G3） | |
| 33 | 本项要求包括： | |
| 34 | a)水管安装，不得穿过机房屋顶和活动地板下； | 在选择机房及设计时应符合要求。 |
| 35 | b)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 应符合要求 |
| 36 | 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； | 应符合要求，并在机房内做好隔热层，并注意楼层之间的温差不要太大。 |
| 37 | 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。** | 可在机房的适当位置安装传感器及检测系统，做到对机房实时防水检测和告警。 |
| 38 | 7.1.1.7 防静电（G3） | |
| 39 | 本项要求包括： | |
| 40 | a)**主要设备**应采用必要的接地防静电措施； | 应符合要求 |
| 41 | b)**机房应采用防静电地板。** | 应符合要求，防静电地板应与保护地线连接并接触良好。 |
| 42 | 7.1.1.8　温湿度控制（G3） | |
| 43 | 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。 | 应符合要求，一般机房日常温度应控制在 10～28℃，湿度 30～70%。定为三级的政务外网机房应具有联网监控和自动报警、并及时通知相关运维人员等功能。 |
| 44 | 7.1.1.9　电力供应（A3） | |
| 45 | 本项要求包括： | |
| 46 | a)应在机房供电线路上配置稳压器和过电压防护设备； | 应符合要求 |
| 47 | 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； | 应设置 UPS 电池供电，并至少保证断电时主要设备在满负荷情况下 2 小时的正常运行。 |
| 48 | c)**应设置冗余或并行的电力电缆线路为计算机系统供电；** | 应符合要求。 |

| | | |
|---|---|---|
| 49 | d)**应建立备用供电系统。** | 政务外网的备用供电系统，如果是采用 UPS 电池供电，应至少保证主要设备满负荷情况下 2 小时的供电容量。其关键设备机房的供电，如每年停电在 10 小时以上的，应考虑采用备用发电机供电，或与当地电力部门签订备用机供电协议，保证政务外网关键设备的供电。 |
| 50 | 7.1.1.10　电磁防护（S3） | |
| 51 | 本项要求包括： | |
| 52 | 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；** | 所有设备应良好接地 |
| 53 | b)电源线和通信线缆应隔离铺设，避免互相干扰； | 电源线和通信线应隔离铺设，平行超过 30 米时，其铺设间隔应大于 200 毫米。 |
| 54 | c)**应对关键设备和磁介质实施电磁屏蔽。** | 应符合要求 |
| 55 | 7.1.2　网络安全 | |
| 56 | 7.1.2.1　结构安全（G3） | |
| 57 | 本项要求包括： | |
| 58 | 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； | 广域网和城域网的核心设备均是政务外网的关键设备，应具有冗余能力，其核心设备间链路的带宽应满足接入单位政务业务和访问互联网业务高峰带宽的需要，并留有适当的余量。 |
| 59 | b)应保证**网络各个部分的带宽**满足业务高峰期需要**；** | 在政务外网中，广域网、城域网线路带宽应满足业务高峰期的需要。应保证互联网出入口、单位局域网接入及安全接入平台等网络带宽满足业务高峰期的需要。 |
| 60 | 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；** | 可在业务终端与服务器之间的路由器、交换机上建立 ACL（访问控制列表）。 |
| 61 | d)应绘制与当前运行情况相符的网络拓扑结构图； | 拓扑图应与实际部署一致，其各类安全设备也应标注在图上，建议拓扑图挂在机房内，以便故障处置，有利于运维人员直观、便捷的查看 |
| 62 | 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； | 在政务外网中，应根据需要，为各部门建立 VPN 及根据功能划分不同的安全域，采用相应的安全策略。 |
| 63 | 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；** | 应划分不同的安全域，分配不同的 VLAN，重要网段禁止部署在网络边界处，并采用相应的访问控制策略。 |
| 64 | 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。** | 在政务外网中，应对重要信息系统的带宽分配优先级，并保证其在使用过程中优先占用网络带宽，并具有 QoS 功能。 |
| 65 | 7.1.2.2　访问控制（G3） | |
| 66 | 本项要求包括： | |

| | | |
|---|---|---|
| 67 | a)应在网络边界部署访问控制设备，启用访问控制功能； | 在政务外网中，在广域网与城域网之间、城域网与局域网之间的边界，可部署访问控制设备或模块，启用访问控制功能，主要防范异常流量、病毒、短包攻击及非授权访问等。 |
| 68 | 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**； | 可采用基于 802.1X 协议、网络端口和 MAC 地址的访问控制和认证策略。 |
| 69 | 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；** | 在网络管理边界做好访问控制，并对相关内容进行过滤和审计，保证应用层相关协议命令级的控制。 |
| 70 | 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；** | 网络应有实时监控功能，对会话处于非活跃 30 分钟以上或会话结束后及时终止网络连接。 |
| 71 | e)**应限制网络最大流量数及网络连接数；** | 应根据所承载的业务和带宽的实际情况确定网络最大流量数和网络连接数。 |
| 72 | f)**重要网段应采取技术手段防止地址欺骗；** | 可采用防火墙的包过滤或传输控制协议，做好边界访问控制，防止地址欺骗。 |
| 73 | 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进行资源访问，控制粒度为单个用户； | 可在应用服务器前设置防火墙、认证网关或授权管理系统，对单个用户的访问进行策略控制。 |
| 74 | h)应限制具有拨号访问权限的用户数量。 | 如采用 ISDN 或通过电话交换机拨号访问应用系统时，应限制拨号用户的访问权限及有效控制并发的用户数量。 |
| 75 | 7.1.2.3　安全审计（G3） | |
| 76 | 本项要求包括： | |
| 77 | 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； | 应符合要求 |
| 78 | 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； | 应符合要求 |
| 79 | c)**应能够根据记录数据进行分析，并生成审计报表；** | 对数据进行分析时，应能发现异常并主动告警，审计报表应能根据用户需要修改，相关信息应能上报到安全管理系统。 |
| 80 | 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。** | 审计记录应保存至少半年以上。 |
| 81 | 7.1.2.4　边界完整性检查（S3） | |
| 82 | 本项要求包括： | |
| 83 | 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，准确定出位置，并对其进行有效阻断；** | 在局域网可采用 MAC、IP 地址、交换机端口绑定等技术，或采用终端管理系统等技术手段，对接入局域网的终端进行有效管理。 |
| 84 | 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，**准确定出位置，并对其进行有效阻断。** | 可采用终端管理系统等手段进行管理控制 |
| 85 | 7.1.2.5　入侵防范（G3） | |
| 86 | 本项要求包括： | |

| | | |
|---|---|---|
| 87 | 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； | 在网络边界处可部署防火墙、入侵防御、防 DDOS 攻击等设备或具有左边各项功能的综合网关类设备。 |
| 88 | 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** | 应部署安全管理系统(SOC),对网络攻击行为进行综合分析,对发现有严重入侵事件时应实时告警。 |
| 89 | 7.1.2.6　恶意代码防范（G3） | |
| 90 | 本项要求包括： | |
| 91 | a)**应在网络边界处对恶意代码进行检测和清除；** | 可在网络边界处部署防火墙、入侵防御及专用检测设备。 |
| 92 | b)**应维护恶意代码库的升级和检测系统的更新。** | 应符合要求 |
| 93 | 7.1.2.7　网络设备防护（G3） | |
| 94 | 本项要求包括： | |
| 95 | a)应对登录网络设备的用户进行身份鉴别； | 应指定专人维护网络设备，并通过用户名和密码进行身份鉴别。 |
| 96 | b)应对网络设备的管理员登录地址进行限制； | 应对登录网络设备的维护终端地址进行限制，禁止其他无关终端登录网络设备。 |
| 97 | c)网络设备用户的标识应唯一； | 应符合要求 |
| 98 | 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；** | 应采用用户名密码和数字证书或生物特征等两种或两种以上鉴别技术对管理员进行身份鉴别。 |
| 99 | 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； | 用户口令应不少于 12 位，数字和字母组成，至少 3 个月更换一次。 |
| 100 | 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； | 应符合要求,当一次登录密码错误次数超过 6 次，应能自动关闭并告警。 |
| 101 | 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； | 远程管理时，应通过终端地址绑定、ACL 列表、用户名密码等手段和措施限制远程用户数量及权限。 |
| 102 | h)**应实现设备特权用户的权限分离。** | 网络管理员、系统管理员和安全审计员应分开，并按职责分工限制各自权限。 |
| 103 | 7.1.3　主机安全 | 本指南的主机主要是针对 DNS、网络管理、安全管理等系统服务器设备。 |
| 104 | 7.1.3.1　身份鉴别（S3） | |
| 105 | 本项要求包括： | |
| 106 | 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； | 对网络管理系统和安全管理系统的管理员登陆地址应进行限制，禁止在内部网络中的任何终端均可登陆到管理系统，应在管理系统前的防火墙上做好访问控制。 |
| 107 | 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； | 系统管理员的登录身份标识应唯一，口令应至少 12 位以上，且数字和字母大小写组合，每半年应更改一次。 |
| 108 | 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； | 当登录次数错误超过 6 次，应自动退出并告警 |

| | | |
|---|---|---|
| 109 | 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； | 当需要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，如在防火墙上限制远程管理终端的数量并绑定 IP 地址，关闭其他无关的服务器端口，规范开放管理端口的流程和访问控制策略等，也可采用 IPSec VPN 对传输加密的方法来保证远程管理安全可靠。 |
| 110 | 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。 | 应符合要求 |
| 111 | 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。** | 应采用用户名密码和数字证书或生物特征等两种鉴别技术对管理员进行身份鉴别。 |
| 112 | 7.1.3.2　访问控制（S3） | |
| 113 | 本项要求包括： | |
| 114 | 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； | 应符合要求 |
| 115 | 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；** | 应将网络管理员、系统管理员和安全审计员分离，并授予所需要的最小权限。 |
| 116 | c)应实现操作系统和数据库系统特权用户的权限分离； | 应符合要求 |
| 117 | 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； | 应符合要求。在使用中应减少或不用默认账户名和口令，对于简单的口令应按要求及时修改。 |
| 118 | e)应及时删除多余的、过期的帐户，避免共享帐户的存在。 | 应定期（每半年）清理服务器中多余、过期的账户。 |
| 119 | f)**应对重要信息资源设置敏感标记；** | 可对重要服务器采取安全加固措施，并设置敏感标记。 |
| 120 | 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；** | 应符合要求 |
| 121 | 7.1.3.3　安全审计（G3） | |
| 122 | 本项要求包括： | |
| 123 | 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； | 应符合要求 |
| 124 | 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； | 应符合要求 |
| 125 | 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； | 应符合要求 |
| 126 | d)**应能够根据记录数据进行分析，并生成审计报表；** | 审计分析系统应具有这些功能，并对异常行为实时告警。 |
| 127 | e)**应保护审计进程，避免受到未预期的中断；** | 应符合要求 |
| 128 | f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 审计记录至少应保存半年。 |
| 129 | 7.1.3.4　剩余信息保护（S3） | |
| 130 | 本项要求包括： | |

| | | |
|---|---|---|
| 131 | 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；** | 应符合要求 |
| 132 | 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。** | 应符合要求 |
| 133 | 7.1.3.5　入侵防范（G3） | |
| 134 | 本项要求包括： | |
| 135 | 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；** | 通过重要服务器加固，及授权管理、网关等边界访问控制设备对入侵行为提供实时告警 |
| 136 | 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；** | 应符合要求 |
| 137 | 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。 | 应符合要求 |
| 138 | 7.1.3.6　恶意代码防范（G3） | |
| 139 | 本项要求包括： | |
| 140 | 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； | 应符合要求 |
| 141 | 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；** | 防恶意代码的产品应选用不同厂商的产品，此类产品有防恶意代码软件或防病毒软件。 |
| 142 | c)应支持防恶意代码的统一管理。 | 应符合要求 |
| 143 | 7.1.3.7　资源控制（A3） | |
| 144 | 本项要求包括： | |
| 145 | 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； | 可通过网络端口、IP 地址、终端 MAC 地址绑定等限制终端登录。 |
| 146 | b)应根据安全策略设置登录终端的操作超时锁定； | 通过终端管理系统对登录终端进行管理。 |
| 147 | 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；** | 可通过网络管理系统或安全管理系统对重要服务器进行监视并对服务器的运行状况异常实时告警。 |
| 148 | d)应限制单个用户对系统资源的最大或最小使用限度； | 应符合要求 |
| 149 | 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。** | 通过监测系统设定报警门限值。 |
| 150 | 7.1.4　应用安全 | |
| 151 | 7.1.4.1　身份鉴别（S3） | |
| 152 | 本项要求包括： | |
| 153 | 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； | 可采用堡垒机等方式，对登录用户的身份进行标识和鉴别。 |
| 154 | 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；** | 应采用用户名密码和数字证书或生物特征等两种或两种以上鉴别技术对管理员进行身份鉴别。 |
| 155 | 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； | 应符合要求 |

| | | |
|---|---|---|
| 156 | 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； | 当登录次数错误超过 6 次，应自动退出并告警 |
| 157 | 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。 | 应符合要求 |
| 158 | 7.1.4.2　访问控制（S3） | |
| 159 | 本项要求包括： | |
| 160 | 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； | 可在应用服务器和数据库服务器前部署防火墙、授权管理、网关类设备对用户进行控制 |
| 161 | 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； | 应符合要求 |
| 162 | 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； | 在应用服务器和数据库服务器前部署网关或授权管理系统，对主体配置访问控制策略。 |
| 163 | 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。 | 对每个系统管理员根据其所承担的任务，设置其工作权限，网络、系统和安全管理员应分别设置，不能由一个人同时兼任。 |
| 164 | e)**应具有对重要信息资源设置敏感标记的功能；** | 可对重要服务器采取安全加固措施，并对重要信息资源设置敏感标记。 |
| 165 | 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；** | 服务器加固系统应有此功能。 |
| 166 | 7.1.4.3　安全审计（G3） | |
| 167 | 本项要求包括： | |
| 168 | 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； | 应符合要求 |
| 169 | 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； | 应符合要求 |
| 170 | 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； | 应符合要求 |
| 171 | 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。** | 审计系统应有此功能 |
| 172 | 7.1.4.4　剩余信息保护（S3） | |
| 173 | 本项要求包括： | |
| 174 | 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；** | 应符合要求 |
| 175 | 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。** | 应符合要求 |
| 176 | 7.1.4.5　通信完整性（S3） | |
| 177 | 应采用**密码技术**保证通信过程中数据的完整性。 | 应符合要求 |
| 178 | 7.1.4.6　通信保密性（S3） | |
| 179 | 本项要求包括： | |

| | | |
|---|---|---|
| 180 | 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； | 在应用软件编程中，应对通信的保密性提出要求。 |
| 181 | b)应对通信过程中的**整个报文或会话过程**进行加密。 | 在应用软件编程中，应对通信的保密性提出要求。 |
| 182 | 7.1.4.7　抗抵赖（G3） | |
| 183 | 本项要求包括： | |
| 184 | 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；** | 应用软件中应有此项功能 |
| 185 | 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。** | 应用软件中应有此项功能 |
| 186 | 7.1.4.8　软件容错（A3） | |
| 187 | 本项要求包括： | |
| 188 | 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； | 应用软件应有此项功能。 |
| 189 | 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。** | 应用软件应提供断点保护和恢复功能。 |
| 190 | 7.1.4.9　资源控制（A3） | |
| 191 | 本项要求包括： | |
| 192 | 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； | 如果通信双方中有一方在 10 分钟内未作任何响应，则应自动结束会话，释放网络连接。 |
| 193 | b)应能够对系统的最大并发会话连接数进行限制； | 应提供系统的实际要求，设定最大并发会话连接数。 |
| 194 | c)应能够对单个帐户的多重并发会话进行限制； | 应符合要求 |
| 195 | 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；** | 由业务应用系统和实际需要设定。 |
| 196 | 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；** | 应符合要求 |
| 197 | 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；** | 在网络管理系统或安全管理系统中，对重要服务器运行状况设定门限值，实时监测，低于门限值时，应及时告警。 |
| 198 | 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。** | 在系统中应可根据用户的权限设定服务等级及优先级，并保证优先级用户首先使用系统资源的权力。 |
| 199 | 7.1.5　数据安全及备份恢复 | |
| 200 | 7.1.5.1　数据完整性（S3） | |
| 201 | 本项要求包括： | |
| 202 | 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**； | 在应用系统编程时，提出此项要求。 |
| 203 | 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。** | 在应用系统编程时，提出此项要求。 |
| 204 | 7.1.5.2　数据保密性（S3） | |
| 205 | 本项要求包括： | |

| | | |
|---|---|---|
| 206 | 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；** | 可采用 SSL 或 IPSec VPN 等密码技术数据实现在传输过程中的保密性。 |
| 207 | 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。 | 在数据存储前，增设安全加密网关设备，通过密码技术对重要数据实现加密存储。 |
| 208 | 7.1.5.3　备份和恢复（A3） | |
| 209 | 本项要求包括： | |
| 210 | 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；** | 对网络管理和安全管理系统等重要信息系统应提供本地的数据备份和恢复功能，并按要求备份。 |
| 211 | 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；** | 对重要信息系统的数据，应提供异地数据备份的功能，定时批量或增量备份，数据异地备份至少每月一次。 |
| 212 | 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；** | 在政务外网的广域网和城域网络拓扑结构中，其关键设备应采用冗余设计，与主备链路一起，构成主备互用，避免关键节点的单点故障，提高可靠性。 |
| 213 | 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。** | 广域网和城域网的关键设备应采用双电源、双引擎，通信线路应采用环型或双链路等手段，保证网络的高可用性。 |
| 214 | 7.2　管理要求 | |
| 215 | 7.2.1　安全管理制度 | |
| 216 | 7.2.1.1　管理制度（G3） | |
| 217 | 本项要求包括： | |
| 218 | 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； | 对管辖内的政务外网安全应有统一的安全策略，针对安全防护设备的位置，确定相应的安全策略并逐步落实，定期检查。 |
| 219 | 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； | 应符合要求 |
| 220 | 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； | 应符合要求 |
| 221 | 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**。 | 应符合要求 |
| 222 | 7.2.1.2　制定和发布（G3） | |
| 223 | 本项要求包括： | |
| 224 | 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； | 应符合要求 |
| 22 | b)**安全管理制度应具有统一的格式，并进行版本控制；** | 应符合要求 |
| 226 | 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； | 应符合要求 |
| 227 | d)**安全管理制度应通过正式、有效的方式发布；** | 应符合要求 |
| 228 | e)**安全管理制度应注明发布范围，并对收发文进行登记** | 应符合要求 |
| 229 | 7.2.1.3　评审和修订（G3） | |
| 230 | 本项要求包括： | |

| | | |
|---|---|---|
| 231 | 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；** | 应符合要求 |
| 232 | 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。 | 安全管理制度应具有可操作性，对出现的新情况及新要求，要及时修订需要改进的管理制度。 |
| 233 | 7.2.2　安全管理机构 | |
| 234 | 7.2.2.1　岗位设置（G3） | |
| 235 | 本项要求包括： | |
| 236 | 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； | 政务外网安全等级确定为三级的，应设立职能部门，并明确安全管理责任人的岗位和职责。 |
| 237 | 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； | 应符合要求 |
| 238 | 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；** | 应符合要求 |
| 239 | 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。** | 应符合要求 |
| 240 | 7.2.2.2　人员配备（G3） | |
| 241 | 本项要求包括： | |
| 242 | 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； | 应符合要求 |
| 243 | b)**应配备专职安全管理员，不可兼任；** | 应符合要求 |
| 244 | c)**关键事务岗位应配备多人共同管理。** | 应符合要求 |
| 245 | 7.2.2.3　授权和审批（G3） | |
| 246 | 本项要求包括： | |
| 247 | 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； | 应符合要求 |
| 248 | 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；** | 应符合要求 |
| 249 | 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；** | 应符合要求 |
| 250 | d)**应记录审批过程并保存审批文档。** | 审批文档保存应符合单位相关文档保存的要求。 |
| 251 | 7.2.2.4　沟通和合作（G3） | |
| 252 | 本项要求包括： | |
| 253 | 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**； | 应符合要求 |
| 254 | b)应加强与兄弟单位、公安机关、电信公司的合作与沟通； | 应符合要求 |
| 255 | 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；** | 应符合要求 |
| 256 | 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；** | 应符合要求 |

| | | |
|---|---|---|
| 257 | 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。** | 应符合要求 |
| 258 | 7.2.2.5　审核和检查（G3） | |
| 259 | 本项要求包括： | |
| 260 | 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； | 安全管理员应至少每月对管辖的系统和设备日志、系统漏洞、数据备份情况检查一次。 |
| 261 | 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；** | 每年应自查一次，并积极配合上级单位和公安部门的检查。 |
| 262 | 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；** | 应符合要求 |
| 263 | 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。** | 应符合要求 |
| 264 | 7.2.3　人员安全管理 | |
| 265 | 7.2.3.1　人员录用（G3） | |
| 266 | 本项要求包括： | |
| 267 | a)应指定或授权专门的部门或人员负责人员录用； | 应符合要求，并按单位人员录用的规定执行 |
| 268 | 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； | 应符合要求 |
| 269 | c)**应签署保密协议**； | 对关键岗位的人员，应签署保密协议。 |
| 270 | 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**。 | 应符合要求 |
| 271 | 7.2.3.2　人员离岗（G3） | |
| 272 | 本项要求包括： | |
| 273 | 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； | 应符合要求 |
| 274 | 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； | 应符合要求 |
| 275 | 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**。 | 应符合要求 |
| 276 | 7.2.3.3　人员考核（G3） | |
| 277 | 本项要求包括： | |
| 278 | 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； | 应符合要求 |
| 279 | 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；** | 考察内容主要应包括技能、工作责任心、保密意识和工作态度、再学习能力等各方面。 |
| 280 | c)**应对考核结果进行记录并保存**。 | 应符合要求 |
| 281 | 7.2.3.4　安全意识教育和培训（G3） | |
| 282 | 本项要求包括： | |
| 283 | 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； | 应符合要求 |

| | | |
|---|---|---|
| 284 | 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； | 应符合要求 |
| 285 | 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； | 应明确关键岗位的技术要求，并制定有针对性的培训计划，定期进行培训，接受再教育。 |
| 286 | 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。 | 应符合要求 |
| 287 | 7.2.3.5　外部人员访问管理（G3） | |
| 288 | 本项要求包括： | |
| 289 | 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； | 应在出入机房管理办法中明确，并严格执行 |
| 290 | 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**。 | 应符合要求 |
| 291 | 7.2.4　系统建设管理 | |
| 292 | 7.2.4.1　系统定级（G3） | |
| 293 | 本项要求包括： | |
| 294 | a)应明确信息系统的边界和安全等级保护； | 应符合要求 |
| 295 | b)应以书面的形式说明确定信息系统为某个安全等级保护的方法和理由； | 可在定级报告中明确 |
| 296 | 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；** | 按公通字[2007]43 号文件要求执行 |
| 297 | d)应确保信息系统的定级结果经过相关部门的批准。 | 按公通字[2007]43 号文件要求执行 |
| 298 | 7.2.4.2　安全方案设计（G3） | |
| 299 | 本项要求包括： | |
| 300 | a)应根据系统的安全等级保护选择基本安全措施，并依据风险分析的结果补充和调整安全措施； | 应符合要求 |
| 301 | 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；** | 可委托信息化工程建设咨询单位对管辖内的政务外网安全建设进行总体规划。 |
| 302 | 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；** | 应符合要求 |
| 303 | 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； | 应符合要求 |
| 304 | 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。** | 应符合要求 |
| 305 | 7.2.4.3　产品采购和使用（G3） | |
| 306 | 本项要求包括： | |
| 307 | a)应确保安全产品采购和使用符合国家的有关规定； | 按公通字[2007]43 号文件要求执行 |
| 308 | 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； | 应符合要求 |
| 309 | c)应指定或授权专门的部门负责产品的采购； | 应符合要求 |

| | | |
|---|---|---|
| 310 | 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。** | 应符合要求 |
| 311 | 7.2.4.4　自行软件开发（G3） | |
| 312 | 本项要求包括： | |
| 313 | 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；** | 应符合要求 |
| 314 | 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； | 应符合要求 |
| 315 | 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；** | 应符合要求 |
| 316 | 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； | 应符合要求 |
| 317 | e)**应确保对程序资源库的修改、更新、发布进行授权和批准。** | 应符合要求 |
| 318 | 7.2.4.5　外包软件开发（G3） | |
| 319 | 本项要求包括： | |
| 320 | a)应根据开发需求检测软件质量； | 应符合要求。 |
| 321 | b)应在软件安装之前检测软件包中可能存在的恶意代码； | 应用软件上线前，应委托第三方对软件中可能存在的恶意代码专门进行检测，并提交检测报告。 |
| 322 | c)应要求开发单位提供软件设计的相关文档和使用指南； | 应符合要求 |
| 323 | 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。 | 应符合要求 |
| 324 | 7.2.4.6　工程实施（G3） | |
| 325 | 本项要求包括： | |
| 326 | 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； | 应采用监理制，加强工程实施过程中的管理 |
| 327 | 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**； | 应符合要求 |
| 328 | 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。** | 应符合要求 |
| 329 | 7.2.4.7　测试验收（G3） | |
| 330 | 本项要求包括： | |
| 331 | 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**； | 应符合要求 |
| 332 | 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； | 应符合要求 |
| 333 | 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；** | 应符合要求 |
| 334 | 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；** | 应符合要求 |

| | | |
|---|---|---|
| 335 | 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。 | 应符合要求 |
| 336 | 7.2.4.8　系统交付（G3） | |
| 337 | 本项要求包括： | |
| 338 | 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； | 系统交付清单应符合建立固定资产的要求。 |
| 339 | 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； | 应符合要求 |
| 340 | 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； | 应符合要求 |
| 341 | 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；** | 应符合要求 |
| 342 | 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。** | 应符合要求 |
| 343 | 7.2.4.9　系统备案（G3） | |
| 344 | 本项要求包括： | |
| 345 | 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；** | 按公通字[2007]43 号文件要求执行 |
| 346 | b)**应将系统等级及相关材料报系统主管部门备案；** | 按公通字[2007]43 号文件要求执行 |
| 347 | 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。** | 按公通字[2007]43 号文件要求执行 |
| 348 | 7.2.4.10　等级测评（G3） | |
| 349 | 本项要求包括： | |
| 350 | 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；** | 按公通字[2007]43 号文件要求执行 |
| 351 | 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；** | 应符合要求 |
| 352 | 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；** | 经公安部认可的第三方安全等级保护测评机构对管辖范围内的政务外网进行测评。 |
| 353 | d)**应指定或授权专门的部门或人员负责等级测评的管理。** | 应符合要求 |
| 354 | 7.2.4.11　安全服务商选择（G3） | |
| 355 | 本项要求包括： | |
| 356 | a)应确保安全服务商的选择符合国家的有关规定； | 应符合要求 |
| 357 | 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； | 应符合要求 |
| 358 | c)应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。 | 应符合要求 |
| 359 | 7.2.5　系统运维管理 | |
| 360 | 7.2.5.1　环境管理（G3） | |
| 361 | 本项要求包括： | |
| 362 | a)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； | 应符合要求 |

| | | |
|---|---|---|
| 363 | 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； | 应符合要求 |
| 364 | 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； | 应符合要求 |
| 365 | 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。 | 应符合要求 |
| 366 | 7.2.5.2　资产管理（G3） | |
| 367 | 本项要求包括： | |
| 368 | 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； | 应符合要求 |
| 369 | 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； | 应符合要求 |
| 370 | 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；** | 应符合要求 |
| 371 | 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。** | 应符合要求 |
| 372 | 7.2.5.3　介质管理（G3） | |
| 373 | 本项要求包括： | |
| 374 | 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；** | 应符合要求 |
| 375 | 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； | 应符合要求 |
| 376 | 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； | 应符合要求 |
| 377 | 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；** | 应符合要求 |
| 378 | 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；** | 如果有备份数据需要异地存储，应符合要求 |
| 379 | 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 | 应符合要求 |
| 380 | 7.2.5.4　设备管理（G3） | |
| 381 | 本项要求包括： | |
| 382 | 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； | 应符合要求 |
| 383 | 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； | 应符合要求 |

| | | |
|---|---|---|
| 384 | 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；** | 应符合要求 |
| 385 | 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； | 应符合要求 |
| 386 | 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。 | 制定相应的管理办法，并严格执行。 |
| 387 | 7.2.5.5　监控管理和安全管理中心（G3） | |
| 388 | 本项要求包括： | |
| 389 | a)**应对通信线路、主机、网络设备和应用软件的运行状况、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；** | 应定期分析政务外网广域网、城域网的运行状况（如可用率），及网络利用率（如流量），应定期对监测和报警记录进行分析形成分析报告，发现可疑行为时，应采取必要的应对措施，其设备记录的保存时间应与设备使用生命周期相同。 |
| 390 | 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；** | 应能按周、月、季和年度形成分析报告，并指导采取相应的解决措施。 |
| 391 | 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。** | 安全管理系统主要对防护设备的状态、日志、恶意代码、补丁升级等进行集中管理及分析，并针对问题提出整改建议。 |
| 392 | 7.2.5.6　网络安全管理（G3） | |
| 393 | 本项要求包括： | |
| 394 | 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； | 应符合要求 |
| 395 | 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； | 应符合要求 |
| 396 | 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； | 应符合要求 |
| 397 | 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； | 应符合要求 |
| 398 | 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； | 应符合要求 |
| 399 | f)应保证所有与外部系统的连接均得到授权和批准； | 应符合要求 |
| 400 | 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；** | 应符合要求 |
| 401 | 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。** | 应符合要求 |
| 402 | 7.2.5.7　系统安全管理（G3） | |
| 403 | 本项要求包括： | |
| 404 | 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； | 应符合要求 |
| 405 | 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； | 至少每半年对系统服务器等进行漏洞扫描，对高危漏洞应及时修补。 |

| | | |
|---|---|---|
| 406 | 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； | 为防止系统因补丁程序导致瘫痪，影响工作，测试和备份是必须要做的，并应做好记录。 |
| 407 | 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； | 应针对各个不同的系统，制定与之相对应的安全策略和操作流程等规定，并严格执行。 |
| 408 | 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；** | 对系统管理员应制定岗位责任和操作规程，规范其在系统管理过程中的行为。 |
| 409 | 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； | 应符合要求 |
| 410 | 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。 | 应每月对系统运行日志和审计数据进行分析，并提交分析报告。 |
| 411 | 7.2.5.8　恶意代码防范管理（G3） | |
| 412 | 本项要求包括： | |
| 413 | 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； | 应符合要求 |
| 414 | 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； | 应符合要求 |
| 415 | 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； | 应符合要求 |
| 416 | 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。** | 每个月应检查一次信息系统内各类恶意代码库的升级情况。 |
| 417 | 7.2.5.9　密码管理（G3） | |
| 418 | **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。 | 应符合要求 |
| 419 | 7.2.5.10　变更管理（G3） | |
| 420 | 本项要求包括： | |
| 421 | a)应确认系统中要发生的变更，并制定变更方案； | 因网络、需求、功能、性能等改变而引起系统的变更时，应制定相关的实施方案，保证系统稳定可靠运行。 |
| 422 | 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； | 应制定系统变更的管理制度和流程，明确软件开发商、集成商、管理、运维等各方的职责和工作内容，并根据系统的影响范围通告相关人员和领导。 |
| 423 | 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；** | 应符合要求 |

| | | |
|---|---|---|
| 424 | 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。** | 应符合要求 |
| 425 | 7.2.5.11　备份与恢复管理（G3） | |
| 426 | 本项要求包括： | |
| 427 | 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； | 针对已接入使用的信息系统，应列出哪些属于重要信息、系统数据和软件系统，并建立档案。 |
| 428 | 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； | 应根据所负责的信息系统安全等级，制定相关管理制度。 |
| 429 | 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； | 制定系统和数据的备份及恢复策略，并按要求实施。 |
| 430 | 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；** | 应符合要求 |
| 431 | 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。** | 每年应至少执行恢复程序一次，可与应急演练相结合，并保证其有效性和可靠性。 |
| 432 | 7.2.5.12　安全事件处置（G3） | |
| 433 | 本项要求包括： | |
| 434 | 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； | 对于所发现的问题，应及时报告，禁止在生产网络环境中尝试验证，而应在模拟环境中验证或通知相关厂商处置。 |
| 435 | 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； | 应符合要求 |
| 436 | 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； | 应符合要求 |
| 437 | 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；** | 应符合要求 |
| 438 | 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；** | 在各类事件处置过程中，应做好记录，形成的文档应妥善保存，如具有典型案例时，可进入案例库，实现全网共享。 |
| 439 | 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。** | 政务外网应建立网络、系统中断和信息安全事件的处理及报告流程。 |
| 440 | 7.2.5.13　应急预案管理（G3） | |
| 441 | 本项要求包括： | |
| 442 | 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； | 应制定各类不同事件的应急预案。 |
| 443 | 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；** | 在运维费用中，应充分保证应急处置时有足够的资源。 |
| 444 | 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 | 应符合要求 |

| | | |
|---|---|---|
| | 至少每年举办一次； | |
| 445 | 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；** | 对各类的应急预案，根据不同的情况，每年至少进行一次应急演练，检验预案的可操作性及应急处置能力。 |
| 446 | 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。** | 每年应审查应急预案并及时更新相关内容。 |

表4　国家电子政务外网安全等级保护基本要求实施建议表

| | **基本要求指标项** | **实施建议** |
|---|---|---|
| **序号** | **政务外网标准《国家电子政务外网安全等级保护基本要求》中第三级基本要求的全部内容** | **以下提出的实施建议仅供参考，如有其他方法能达到基本要求，也认可达到相关安全等级要求。** |
| 1 | **7.1.1.　广域网** | |
| 2 | **7.1.1.1.　结构安全（G3）** | |
| 3 | a)关键设备的业务处理能力应具有一定的设备和链路冗余等保护措施，网络的组织和分布应满足各类业务稳定性、可靠性和安全性的要求； | 广域网的核心设备属于关键设备，其业务处理能力应满足所有经过核心设备的各类业务流量和管理开销的要求。 |
| 4 | b)广域网的链路带宽应满足承载业务和数据传输的需要，**其带宽至少为历史峰值的 1.5 倍；** | 应符合要求 |
| 5 | c)IP 层的网络设备时钟应与上级设备时钟同步； | 应符合要求 |
| 6 | **d)主用与备用的核心网络设备应放置在不同物理位置的机房；** | 为保证网络的可靠性和系统的可用性，备用的核心设备可以考虑放在提供网络服务的运营商的机房内。 |
| 7 | **e)应采用物理路由分离的两条骨干链路来提供“1+1”的网络保护方式，两条链路在技术和性能等方面应保持一致；** | 省级以上广域网应满足要求。地（市）到县的广域网，可根据实际情况，随着承载业务的扩大，在保证业务不中断的情况下，完善备用链路的性能。 |
| 8 | **f)地（市）级及以上网络设备应支持 MPLS　VPN 的业务，并保证国家相关业务部门到省、地（市）、县业务的连通；** | 地（市）级城域网应支持 MPLS VPN 功能，保证所承载的政务部门各业务之间的有效隔离及与国家、省相关部门业务的互通。 |
| 9 | **g)应根据需要采用有效的 QoS 和流量管理策略，保证管理和控制信息具有较高的优先级；** | 政务外网应能区分不同的业务类型，对重要信息系统和重点保证单位的业务划分优先级 |
| 10 | **h)应保证国家、省、地（市）广域网的高速畅通，不允许串接相关安全防护设备。** | 应符合要求 |

| | | |
|---|---|---|
| 11 | **7.1.1.2. 网络保护与恢复（A3）** | |
| 12 | **a)国家、省、地（市）的广域网主要设备、模块及链路应采用主备方式；** | 为保证网络的可靠性和系统的可用性，其备用链路可考虑由不同运营商提供，但性能、带宽等技术要求应保持一致。 |
| 13 | b)应能根据各级政务部门业务应用的需要采用链路倒换、聚合等安全保护措施，相关技术指标应达到网络和业务的需要； | 应符合要求 |
| 14 | c)链路的倒换、聚合应不影响各级政务部门重要信息系统和业务的正常使用； | 应符合要求 |
| 15 | d)广域网络设备原则上应与城域网的核心节点互联。 | 应符合要求 |
| 16 | **7.1.1.3. 访问控制（A3）** | |
| 17 | a)应在广域网与城域网或用户局域网之间的网络边界部署相关访问控制设备，启用访问控制功能； | 不同责任单位的广域网与城域网、城域网与局域网之间应具有边界访问控制的功能，可通过在边界路由器加安全模块等手段，防止异常流量、非授权访问、病毒等危害业务及网络的安全。 |
| 18 | b)根据政务外网的网络承载力，应对网络中的广播、组播进行必要的控制； | 应符合要求 |
| 19 | c)在广域网内，专用网络区与公用网络区应采用 MPLS VPN 技术隔离，专用网络区及公共网络区域之间路由不可达，数据不能直接访问； | 在政务外网广域网内，应保证各 VPN 之间隔离的有效性，每年至少应检查一次。 |
| 20 | **d)应具备限制网络最大流量数及网络连接数的能力；** | 根据网络带宽和实际业务应用的流量情况，进行限制。 |
| 21 | **e)根据国家有关互联网出口属地化原则，政务外网中央和省级广域网不得承载互联网的流量。** | 为保证国家、省、地（市）电子政务业务的畅通和安全，其省级广域网内不得承载地（市）的访问互联网业务，地（市）访问互联网业务可通过本地的 ISP 出口。 |
| 22 | **7.1.1.4. 安全审计（S3）** | |
| 23 | a)安全审计日志记录要求保存至少半年以上； | 应符合要求 |
| 24 | b)应能够根据记录数据进行分析，并生成审计报表，相关信息应报送安全管理系统。 | 应符合要求 |
| 25 | **7.1.2. 城域网** | |
| 26 | **7.1.2.1. 结构安全（G3）** | |
| 27 | a)城域网的核心设备应具有一定的设备冗余，核心设备之间的骨干应至少保证不同路由主备链路或环进行保护，其链路带宽应满足业务的需要； | 核心设备至少有二台以上，部署在不同的物理位置，采用双链路或环型保护。 |
| 28 | b)城域网的骨干路由带宽应满足业务的需要； | 骨干路由带宽应考虑所有接入单位的各类政务和互联网业务的流量，并应预留至少 50%的带宽容量。 |
| 29 | c)应根据实际需要及接入单位的分布情况，合理设置汇聚节点的数量和位置； | 当接入单位较集中时，可设置汇聚层路由设备，专线接入相关政务部门。 |
| 30 | d)城域网络设备的时钟应能与广域网络设备的时钟同步； | 应符合要求 |
| 31 | **e)国家、省级城域网的核心原则上应采用网状或环状网络结构；** | 应符合要求 |

| | | |
|---|---|---|
| 32 | **f)汇聚节点与核心节点原则上应至少有两条不同物理路径的连接，防止设备或链路故障影响业务系统的正常使用；** | 应符合要求 |
| 33 | **g)应根据需要采用有效的 QoS 和流量管理策略，保证重要信息系统和数据具有较高的优先级；** | 要求给业务系统分类、分级，以及有效的质量保证和流量管理策略。 |
| 34 | **h)自建用于政务外网的传输系统（含管理软件、SDH 设备、MSTP 多业务传输平台等），可与 IP 承载网同步定级，其安全等级应与城域网安全等级一致。** | 底层的通信传输平台（包括光纤、传输设备、管理系统等），如果只为政务外网服务，可作为政务外网的组成部分与政务外网一起定级，反之，则应分开分别确定安全等级并按要求实施保护。 |
| 35 | **7.1.2.2. 访问控制（A3）** | |
| 36 | a)应在城域网与用户局域网连接边界及安全等级不同的网络边界配置相应的访问控制功能； | 为保证城域网的安全，可在汇聚层设备做边界访问控制的保护，采用安全模块或串接防火墙设备等措施，做好边界访问控制。 |
| 37 | **b)城域网内根据接入业务的需要划分其他区域（或服务层）时，应按业务和安全的要求，制定相应访问控制策略，保证数据和信息系统的安全；** | 城域网可按接入单位的业务纵向划分 VPN，或按接入业务的类型横向划分 VPN，目标是保证政务业务系统和数据的安全。 |
| 38 | **c)应在广域网与城域网或用户接入网之间的网络边界部署相关访问控制设备，启用访问控制功能，对接入用户的边界访问控制，根据条件其访问控制设备也可放在汇聚层；** | 广域网与城域网之间，主要应保证业务和 VPN 的连通，依据责任分工，在边界可串接防火墙或安全模块，主要监测异常流量、病毒等网络攻击行为。 |
| 39 | **d)城域网应支持 MPLS VPN 技术，按接入业务的需要和数据交换与共享的要求区分不同的网络区域；** | 各省根据自身网络和业务的情况，可纵向按单位性质划分，也可横向按业务划分不同的网络区域，并保证不同 VPN 之间的隔离。 |
| 40 | **e) 城域网中的专用网络区、公用网络区和互联网接入区等其他网络区域应采用 VPN 隔离措施，不同区域的系统和数据不能直接访问；** | 应符合要求 |
| 41 | f)公用网络区与互联网接入区等区域之间需要进行数据交换时，应采用防火墙、路由控制、**网闸、数字证书**等相关安全措施，并对交换数据进行病毒扫描和审计。 | 具体措施可参考《国家电子政务外网跨网数据安全交换技术要求与实施指南》 |
| 42 | **7.1.3. 用户局域网** | |
| 43 | a)用户局域网内的安全防护和安全责任由用户单位自行负责； | 管理和责任边界以接入路由器为边界，按资产归属为原则来确定。 |
| 44 | b)用户单位的信息系统已按国家要求进行了安全等级保护二级或三级备案时，在接入政务外网时需提供信息系统安全等级保护备案证明； | 政务部门的接入线路应根据其信息系统的重要性决定是否采用双线路上联到汇聚层交换设备，如果政务外网承载的政务部门信息系统定级为第三级重要信息系统，则政务外网应提供双路由上联，保证其信息系统的可靠性。一般情况下，则专线单路由接入政务外网即可。 |

| | | |
|---|---|---|
| 45 | c)局域网内的终端如既能访问政务外网的业务、又能访问互联网，各政务部门可根据自身业务的重要性，采取技术措施，逐步达到控制该终端访问互联网，其现有的技术手段如下，但不仅限于此：<br>i.通过接入互联网侧的防火墙的访问控制策略对该终端访问互联网加以必要的限制；<br>ii.通过对终端硬盘分区，加密保存业务数据或相关工作文档，通过安全软件，当进行工作文档编写、数据处理时，自动断开该终端的互联网连接；<br>iii.通过插入 USBKey 时自动断开该终端的互联网连接，只能访问指定的政务外网服务器和应用系统；<br>iv.可采用虚拟终端等的技术，保证同一台终端不能同时访问政务外网业务和互联网业务。 | 由接入单位自行负责并决定采用何种方式。 |
| 46 | **7.2. 业务区域网络** | |
| 47 | **7.2.1. 公用网络区** | |
| 48 | **7.2.1.1. 结构安全（G3）** | |
| 49 | a)公用业务服务器应采用统一规划的 IP 地址，保证跨部门、跨地区业务的交换与共享； | 外网管理中心分配给各省 59 段地址是公网地址，不存在地址冲突，主要分配给网络设备、共享服务器使用。 |
| 50 | b)应根据所部署系统的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； | 为保证业务的安全，根据不同业务划分安全域是必须的，如公共网络区应划分管理区（如部署网管、安管系统等），与共享区（如部署网站、共享系统等），并配备防火墙，设置不同的边界访问控制策略。 |
| 51 | c)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时候优先保护重要业务的畅通； | 应符合要求 |
| 52 | **d)公用网络区的主要网络设备应具备设备冗余、链路冗余等保护措施，应满足各类业务带宽、稳定性、可靠性和安全性的要求。** | 应符合要求 |
| 53 | **7.2.1.2. 访问控制（A3）** | |
| 54 | a)通过互联网或其他公众通信网络对公用网络区的信息系统进行远程访问时，须采用 VPN 网关、信道加密，以及数字证书、IP 地址绑定、审计等安全措施； | 具体措施参见《国家电子政务外网安全接入平台技术规范》，实现通过互联网、3G 等移动通信网安全接入政务外网的要求。 |
| 55 | b)应通过身份认证、授权管理系统等对公用网络区的信息系统进行保护； | 如公用网络区内的网管、安管及跨部门的数据共享等信息系统。 |
| 56 | **c)公用网络区与互联网接入区采用 MPLS VPN 进行逻辑隔离，二个区域的数据和系统不能直接访问；** | 应符合要求 |
| 57 | **d)当公用网络区的主机/服务器需要从互联网接入区获取数据时，应采用安全隔离设备、防火墙、路由策略、身份认证、设备认证、审计等安全措施。** | 具体措施参见《国家电子政务外网跨网数据安全交换技术要求与实施指南》 |
| 58 | **7.2.2. 互联网接入区** | |
| 59 | **7.2.2.1. 结构安全（G3）** | |

| | | |
|---|---|---|
| 60 | **a)应选用二个及以上电信运营商或互联网业务提供商（ISP）作为访问互联网的出口；** | 应符合要求 |
| 61 | b)在采用主备方式或负载均衡等方式时，不同链路的安全策略应该保持一致； | 应符合要求 |
| 62 | **7.2.2.2. 访问控制（A3）** | |
| 63 | a)如需对互联网接入区的信息系统或服务器进行远程维护和管理，应采用身份认证、信道加密、指定终端等安全措施； | 应指定需要开放的服务器、防火墙等控制端口。 |
| 64 | b)应能有效防止以下攻击行为：病毒攻击、端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、SOQ 注入、跨站攻击和网络蠕虫攻击等； | 在互联网的出入口应安装防火墙、入侵防御、防 DDOS 攻击等防护设备或综合网关类设备，在门户网站前应安装网页防篡改、WEB 防火墙等设备。 |
| 65 | c)应具备流量分析控制、异常告警等功能，能区分各类 HTTP、FTP、TELNET、SMTP、POP3、P2P 等网络协议并进行过滤； | 在集中的互联网出入口，应安装流量控制设备和行为审计类设备。 |
| 66 | **d)应具备监测检测恶意代码并实时告警的功能，在有条件的情况下，应能与防火墙、入侵检测等安全防护设备联动，有效阻止敏感信息的泄漏；** | 安全管理系统应对管辖内的安全防护设备进行管理、日志分析、实时告警及关联分析等功能，如有条件，各相关防护设备应能联动 |
| 67 | **e)通过互联网等公众通信网接入政务外网的各类移动业务，应尽量与政务部门访问互联网的出口业务分开，做好相应的访问控制。** | 通过互联网接入政务外网应由统一安全接入平台来实现，并尽量采用独立的互联网入口，将出入的流量分开，有利于管理和实施有效地访问控制策略。 |
| 68 | **7.2.3. 专用网络区** | |
| 69 | **7.2.3.1. 结构安全（G3）** | |
| 70 | **a)各级政务部门根据业务需求在政务外网上构建专用网络承载其业务时，应采用 MPLS VPN 或其他 VPN 技术，实现与其他政务部门的业务逻辑隔离；** | 在政务外网上建立 VPN 通道，实现端到端业务的连接，应保证 VPN 之间逻辑隔离的有效性 |
| 71 | **b)为保证 VPN 的服务质量，应具备对 VPN 的网络性能等相关数据进行分析的能力，对重点接入单位和重要信息系统应采用双链路上联政务外网，保证其可靠性；** | 应具有对 VPN 内业务进行分类及分析的能力，对确定为重要信息系统的接入单位除采用双链路方式外，也可考虑采用 3G 网络、IPSec VPN 等技术手段作为备用链路接入，通过安全接入平台联接到政务外网。 |
| 72 | **c)专用网络区内业务数据流向及安全措施等要求由相应部门自行确定；** | 应符合要求 |
| 73 | **d)应保证广域网络技术的一致性，保证端到端业务的畅通、安全、可靠。** | 应符合要求 |
| 74 | **7.2.3.2. 访问控制（A3）** | |
| 75 | **a)在接入边界处设置网关或防火墙等边界访问控制设备，防止非法用户业务流的进入；** | 在城域网与用户接入局域网之间，其边界应有访问控制措施，可在 PE 设备上串接防火墙或安全防护模块。 |
| 76 | **b)应具有网络流量控制能力，防止由于资源挤占而影响其他重要信息系统和网管信息的正常传送；** | 应符合要求 |

| | | |
|---|---|---|
| 77 | **c)通过互联网或其他公众通信网络接入 VPN 时，应采用政务外网数字证书、加密传输、安全网关等安全技术措施，保证数据和信息系统的安全；** | 实施措施参照《国家电子政务外网安全接入平台技术规范》，解决通过互联网、3G 等手段实现各类智能终端安全接入政务外网的问题。 |
| 78 | **d)专用网络区内的信息系统的安全等级，相关的访问控制、入侵防护、数据安全等由相应部门自行确定。** | 各政务外网接入单位应按国家信息系统安全等级保护相关标准组织实施。 |
| 79 | **7.3. 管理区域网络** | |
| 80 | **7.3.1. 网络管理区（S3）** | |
| 81 | a)政务外网 IP 承载网的相关网络设备与网管系统应作为一个整体按信息系统安全等级保护的要求实施保护； | 应符合要求 |
| 82 | b)**根据网络结构、管理分界，原则上采用国家、省二级或国家、省、地（市）三级分级的管理方式，根据实际需要设置分级权限，实现对网络的灵活管理；** | 应符合要求 |
| 83 | c)应绘制与当前运行情况相符的网络拓扑结构图、有相应的网络配置表，包含设备 IP 地址等主要信息，并及时更新、妥善保管并做好备份，且不得对外公开； | 应符合要求 |
| 84 | d)应保证网管系统数据安全、可靠； | 应符合要求 |
| 85 | e)网络管理系统应具有资产管理、图形展现、实时告警并具有声、光、电等功能，告警信息能通过各种技术手段及时通知相关人员； | 应符合要求 |
| 86 | f)网络管理用的终端应专用，有专人负责，并不得访问互联网； | 网管终端应专用，专人负责，通过技术手段禁止该终端访问互联网。 |
| 87 | h)应确保网管系统与设备间、网管系统之间的管理信息通信通畅； | 应符合要求 |
| 88 | i)**网管网络应与电子政务业务网络逻辑隔离，确保网管数据的安全；** | 在局域网内，网管系统和数据应单独划分 VLAN。 |
| 89 | j)**应具备异构网络管理系统的互联功能，实现相关管理数据的共享；** | 应符合要求 |
| 90 | k)**对重要主机/服务器的运行状况（如 CPU 利用率、内存使用情况等）进行监测；** | 网管系统应对所管辖的重要服务器的运行状况实时进行监测，发现异常应及时告警，保证应用的正常使用。 |
| 91 | l)**网络管理系统应对同一管理员采用两种或两种以上组合的鉴别技术进行身份鉴别。** | 对网络管理员登录系统时，应采用数字证书和密码等两种方式进行身份鉴别。 |
| 92 | **7.3.2. 安全管理区（S3）** | |
| 93 | a)安全管理系统（或平台）可与安全防护设备、网关、审计系统等，作为一个信息系统的整体，按信息系统安全等级保护的要求实施保护； | 安全管理系统是政务外网安全保障的重要组成部分，根据实际情况，可以与 IP 网络、网管系统一起作为一个整体来定级，也可单独作为信息系统来定级并进行安全保护。 |
| 94 | b)安全管理系统应能对管辖内的安全防护设备的日志、故障、病毒攻击、安全运行状态进行监测； | 应符合要求 |
| 95 | c)安全管理用的终端应专用，有专人负责，并不得访问互联网； | 应符合要求 |

| | | |
|---|---|---|
| 96 | d)应按日、周、月、季、年或按管理部门的要求出具安全运行报告，**并对相关病毒攻击、信息安全事件提出建议；** | 系统应具有对安全事件的关联分析功能，结合相关知识库、案例库等，提出有针对性的处置建议。 |
| 97 | **e)对网络及管辖区域内安全风险提出预警、对安全运行情况及态势进行分析等；** | 对网络的安全状况进行实时的监测，应具有对网络攻击定位、预警等功能。 |
| 98 | **f)应具备异构安全管理系统的互联功能，实现相关管理数据的共享、分析，为全网的安全事件应急响应、安全事件预警提供技术支撑。** | 全网的安全监测，依托于安全管理系统的互联，其互联技术要求参照《国家电子政务外网安全管理平台（SOC）技术要求和接口规范》。 |
| 99 | **7.3.3. 电子认证区** | |
| 100 | 对于此区域的安全防护和要求，请参考国家法律法规和密码管理主管部门关于密码管理的相关规定及国家对信息系统的安全等级保护相关标准进行保护。 | 有关电子认证、密码使用等，国家有相关标准和规范，请按要求执行。 |

# 附　录　A
（资料性附录）
## 安全等级保护第三级政务外网定级案例（以省级为例）

1、首先应确定省级政务外网的主管单位、建设管理单位和运行维护单位，明确省级政务外网责任主体单位。

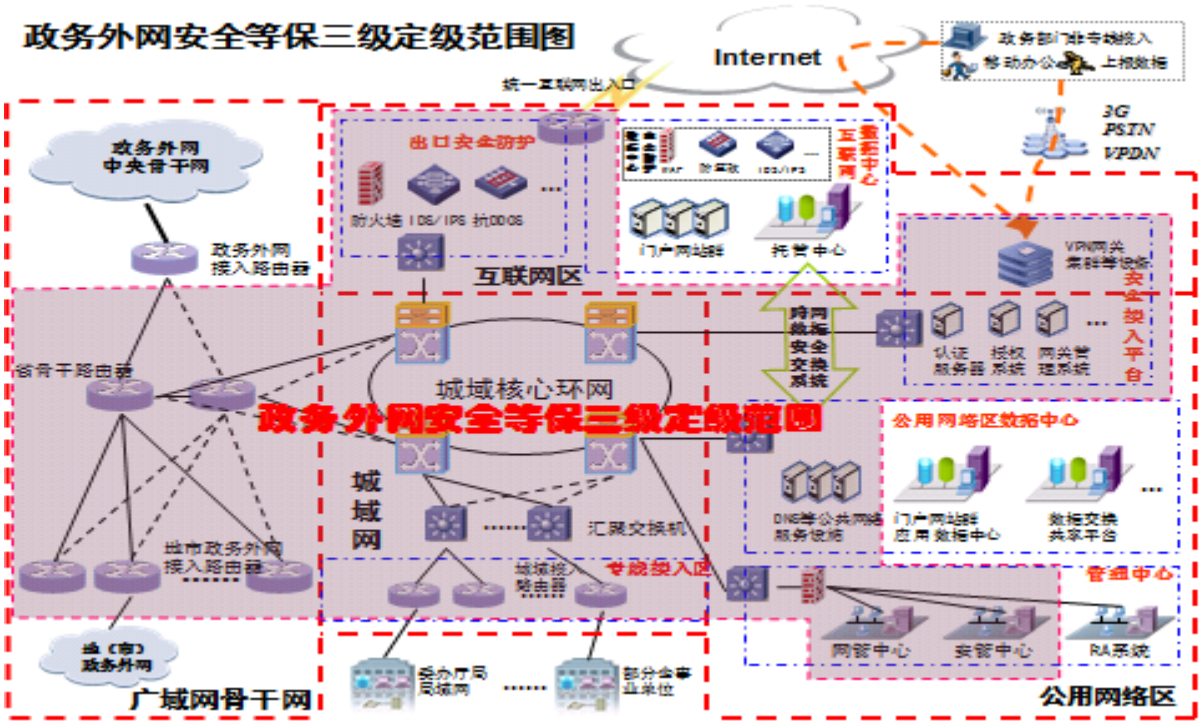
2、确定省级政务外网的管理边界，原则是网络的运行维护单位负责到哪里，边界就划到哪里。如广域网的边界：中央政务外网接入路由设备的下联端口、从省到各地（市）的接入路由设备（含长途电路）；城域网的边界：到省级委办厅局和其他政务部门的接入路由设备，该设备将其局域网络和信息系统接入到政务外网上；以及统一的互联网出口路由设备等。

3、将管内政务外网划分不同的安全域，如广域网域、城域网域、数据共享与交换域、网络与安全管理域、统一接入平台管理域、互联网接入域、统一互联网政府门户区域等，并明确每个安全域的边界，根据业务需要和安全要求对相应的区域采取不同的访问控制策略。安全区域的划分以保证安全、方便业务开展和管理为原则，可以按单位纵向划分，也可以按业务类别横向划分。

4、可以将与政务外网相关的管理系统（如网络管理系统、安全管理系统、统一安全接入平台管理系统等）及公共服务设施或系统纳入到政务外网的定级范围内，如域名解析（DNS）服务等。

5、可以将CA、RA系统及门户网站、跨部门的数据共享与交换系统等作为独立的信息系统，按国家信息系统安全等级保护的基本要求分别进行定级。

政务外网安全等保三级定级范围示意图如下：




图A.1　政务外网安全等保三级定级范围示意图

# 附　录　B
（资料性附录）
## 安全等级保护第二级政务外网定级案例（以区、县为例）

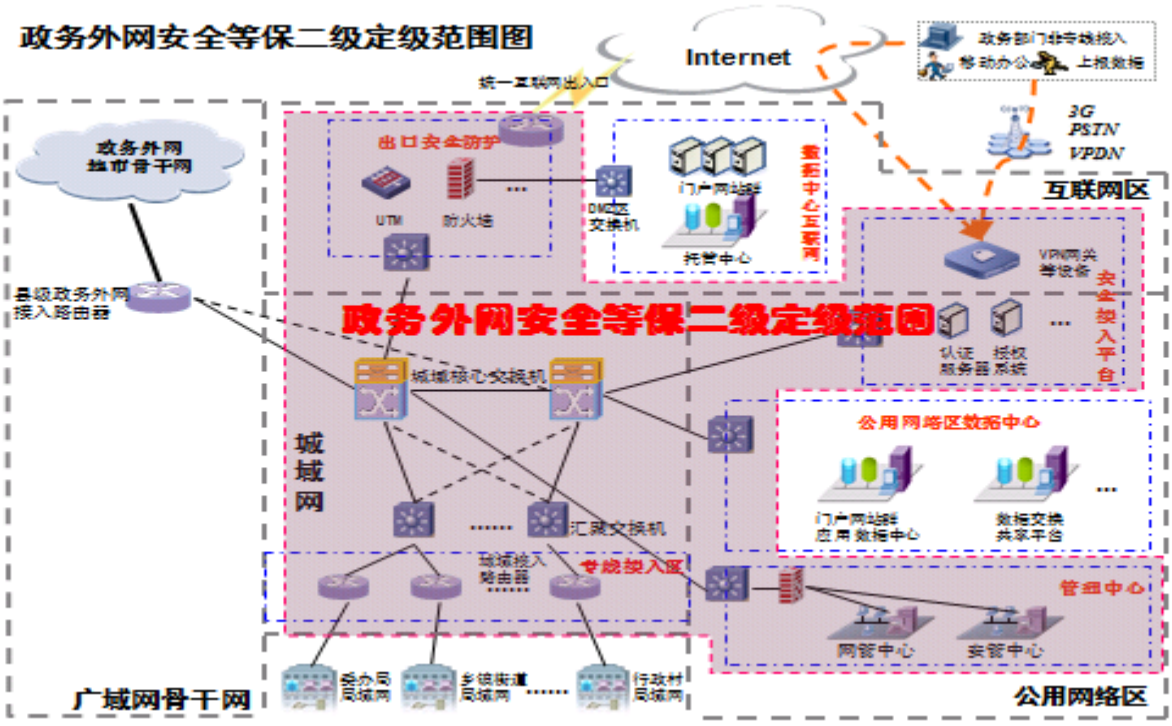
1、首先应确定区县级政务外网的主管单位、建设管理单位和运行维护单位，明确区县级政务外网责任主体单位。

2、确定区县级政务外网的管理边界，原则是网络的运行维护单位负责到哪里，边界就划到哪里。如地（市）级广域网下联端口的边界，城域网与各接入单位局域网的边界，区县政务外网专线到街道、乡镇、社区及行政村的接入设备边界，互联网出入口的边界等。

3、按承载业务的不同和需要划分不同的安全域，如数据共享与交换域、网络与安全管理域、统一安全接入平台管理域、互联网接入域、统一互联网政府门户区域等，对相应的区域采取不同的边界安全访问控制策略，安全区域的划分以保证安全、方便业务开展和管理为原则，可以按单位纵向划分，也可以按业务类别横向划分。

4、政务外网安全等级保护确定为第二级的，可以将网络管理系统、安全管理系统纳入到政务外网的安全等级保护范围内，一并定级，并在定级报告中描述清楚。

政务外网安全等级保护第二级定级范围示意图如下：




图B.1　政务外网安全等保二级定级范围示意图

附 录 C

（资料性附录）

《政务外网安全等级保护定级报告》模板

# XX省省级政务外网安全等级保护定级报告

## 一、 省级政务外网描述

XX省政务外网是全省电子政务重要的行政基础设施，是国家政务外网的重要组成部分。XX省政务外网主要由省级政务外网、地（市）和县级政务外网组成，XX省省级政务外网由XX单位负责管理，其主管部门是XXXX，XX省的省级政务外网主要由以下部分组成：**省级广域网**：纵向连接XX个地(市)，实现省与地（市）级政务外网的互联互通；**省级城域网：**横向连接省级党委、人大、政府、政协、法院和检察院等部门，支持相关政务部门局域网络的接入，提供统一的互联网出口及安全防护设备，提供统一的安全接入平台，满足政务部门移动办公、现场执法等远程接入政务外网的需要。具体的网络拓扑图和定级范围图如下：（可参照附录A的图为例，将本省省级政务外网功能区划和定级范围图附上）

## 二、 省级政务外网安全保护定级的确定

### （一） 政务外网业务信息安全保护等级的确定

1、 业务信息描述

XX省的省级政务外网的网络、域名解析等为国家相关部门到省的电子政务业务和全省各级政务部门的非涉密信息系统提供网络承载及跨部门数据共享与交换服务，其省级各部门的信息系统安全等级均在第三级，如XX部门的

XX 信息系统。

2、 业务信息受到破坏时所侵害客体的确定

如果省级政务外网的网络、域名解析服务器受到破坏，将影响到省级政务部门的电子政务信息系统的正常运行，对政府的社会管理、公众服务、经济调节、市场监管等产生间接影响，即对社会秩序和公众利益造成损害。

3、 业务信息受到破坏后对侵害客体的侵害程度的确定

政务外网业务信息系统受到破坏后，将对社会秩序和公众利益造成损害。

4、 业务信息安全保护等级的确定

依据政务外网业务信息系统受到破坏后，对侵害客体的侵害程度，其省级政务外网业务信息安全保护等级确定为第二级。

（二） 政务外网服务安全保护等级的确定

1、 政务外网服务描述

XX 省省级政务外网的服务对象是省级党委、人大、政府、政协、法院和检察院等部门的电子政务信息系统，以及有相关政务业务接入需要的企事业单位。XX 省省级政务外网提供政务部门电子政务业务的网络承载和域名解析服务，服务范围是全省相关政务部门的社会管理、公众服务、经济调节、市场监管等电子政务业务。

2、 政务外网服务受到破坏时所侵害客体的确定

政务外网服务受到破坏时所侵害的客体是社会秩序和公众利益。

3、 政务外网服务受到破坏时所侵害客体的侵害程度的确定

政务外网服务受到破坏时将对社会秩序和公众利益造成严重损害。

4、 政务外网服务安全保护等级的确定

依据政务外网服务受到破坏后，对侵害客体的侵害程度，其省级政务外网的服务安全保护等级确定为第三级。

## （三） 政务外网安全保护等级的确定

XX 省省级政务外网的安全保护等级由业务信息安全保护等级和服务安全保护等级较高者决定，最终确定 XX 省省级政务外网安全保护等级为第三级。

| 信息系统名称 | 安全保护等级 | 业务信息安全等级 | 服务安全等级 |
| --- | --- | --- | --- |
| XX 省省级政务外网 | 3 | 2 | 3 |