ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 25068.3—2022
代替 GB/T 25068.4—2010

信息技术　安全技术　网络安全 第3部分：面向网络接入场景的威胁、设计技术和控制

Information technology—Security techniques—Network security—Part 3: Threats, design techniques and control for network access scenarios

(ISO/IEC 27033-3:2010, Information technology—Security techniques—Network security—Part 3: Reference networking scenarios—Threats, design techniques and control issues, MOD)

2022-10-12 发布　　2023-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　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 GB/T 25068《信息技术 安全技术 网络安全》的第 3 部分。GB/T 25068 已发布了以下部分：

——第 1 部分：综述和概念；

——第 2 部分：网络安全设计和实现指南；

——第 3 部分：面向网络接入场景的威胁、设计技术和控制；

——第 4 部分：使用安全网关的网间通信安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护。

本文件代替 GB/T 25068.4—2010《信息技术　安全技术　IT 网络安全　第 4 部分：远程接入的安全保护》。与 GB/T 25068.4—2010 相比，除结构调整和编辑性改动外，主要技术变化如下：

——本文件主要内容由远程接入的安全保护改为面向网络接入场景的威胁、设计技术和控制；

——本文件对原系列标准中的每个技术应用场景进行了重新归纳和修改；

——删除了“接入点”“高级加密标准”“回叫”等术语和定义，增加了“恶意软件”“不透明性”“外包”等术语和定义（见第 3 章，2010 年版的第 3 章）；

——增加了“员工的互联网访问服务”“企业对企业的服务”“企业对客户的服务”“增强协作服务”“网络分段”“为居家办公和小型商务办公场所提供网络支持”等内容，删除了“远程访问连接类型”“远程访问连接技术”“选择和配置指南”等内容（见第 7 章～第 15 章，2010 年版的第 6 章～第 8 章）；

——增加了“威胁目录”“互联网使用策略示例”，删除了“远程接入安全策略示例”“RADIUS 实施和部署的最佳实践”“FTP 的两种模式”“安全邮件服务核查表”“安全 Web 服务核查表”“无线局域网安全核查表”（见附录 A、附录 B，2010 年版的附录 A～附录 F）。

本文件修改采用 ISO/IEC 27033-3：2010《信息安全　安全技术　网络安全　第 3 部分：参考网络场景—威胁、设计技术和控制》。

本文件与 ISO/IEC 27033-3：2010 相比做了下述结构调整：

——将附录 A 调整为附录 B，附录 B 调整为附录 A。

本文件与 ISO/IEC 27033-3：2010 的技术差异及其原因如下：

——用规范性引用的 GB/T 29246 代替 ISO/IEC 27000（见第 3 章、第 6 章），GB/T 25068.1 代替 ISO/IEC 27033-1（见第 3 章），以适应我国的技术条件；

——将面向联邦国家或欧盟等政府组织的网络分段指导改为适合我国的跨国组织的网络分段指导，并以“注”的形式出现（见 11.1）。

本文件做了下列编辑性改动：

——将一些适用于国际标准的表述改为适用于我国标准的表述；

——增加了表 1 中的脚注；

——将国际标准附录 A 中面向博客的使用要求扩展为面向所有社交平台的使用要求；

——将国际标准附录 A 中 A.4.3 中的悬置段调整为附录 B 中带序号的 B.4.3.1 等内容；

——删除了国际标准附录 A 中的定义 A.6；

——增加了“参考文献”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:黑龙江省网络空间研究中心、中国电子技术标准化研究院、安天科技集团股份有限公司、黑龙江安信与诚科技开发有限公司、上海工业控制安全创新科技有限公司、哈尔滨理工大学、哈尔滨工业大学。

本文件主要起草人:曲家兴、方舟、于海宁、谷俊涛、肖鸿江、李琳琳、宋雪、李锐、杨霄璇、白瑞、马遥、王大萌、呼大永、树彬、吴琼、上官晓丽、蔡一鸣、杜宇芳、赵超、吴佳兴、曹威、鲁子元、马超、孟庆川、单建中、韩建雍、刘明鸽、黄海、方伟、童松华、刘颖、孙腾、倪华。

本文件及其所代替文件的历次版本发布情况为:

——2010 年首次发布为 GB/T 25068.4—2010;

——本次为第一次修订,调整为 GB/T 25068.3—2022。

引　言

GB/T 25068 的目的是为信息系统网络的管理、运行、使用及互联互通提供安全方面的详细指导，方便组织内负责信息安全特别是网络安全的人员采纳本文件以满足其特定需求。拟由六个部分构成。

——第 1 部分：综述和概念。目的是提出网络安全相关的概念并提供管理指导。

——第 2 部分：网络安全设计和实现指南。目的是为组织如何规划、设计、实现高质量的网络安全体系，确保网络安全适合相应的业务环境提供指导。

——第 3 部分：面向网络接入场景的威胁、设计技术和控制。目的是列举与典型的网络接入场景相关的具体风险、设计技术和控制，适用于所有参与网络安全架构方面规划、设计和实施的人员。

——第 4 部分：使用安全网关的网间通信安全保护。目的是确保使用安全网关的网间通信安全。

——第 5 部分：使用虚拟专用网的跨网通信安全保护。目的是定义使用虚拟专用网络建立安全连接的具体风险、设计技术和控制要素。

——第 6 部分：无线网络访问安全。目的是为选择、实施和监测使用无线网络提供安全通信所必需的技术控制提供指南，并用于第 2 部分中涉及使用无线网络的技术安全架构或设计选项的审查与选择。

GB/T 25068 是在 GB/T 22081《信息技术　安全技术　信息安全控制实践指南》的基础上，进一步对网络安全控制提供了详细的实施指导。GB/T 25068 仅强调业务类型等因素影响网络安全的重要性而不做具体说明。

本文件凡涉及采用密码技术解决保密性、完整性、真实性、抗抵赖性需求的，遵循密码相关国家标准和行业标准。

信息技术　安全技术　网络安全 第3部分：面向网络接入场景的威胁、设计技术和控制

1　范围

本文件描述了与网络接入场景相关的威胁、设计技术和控制问题，为每一个网络接入场景提供了能够降低相关风险的安全威胁、安全设计技术以及控制三个要素的详细指南。

本文件适用于按照GB/T 25068.2来评审技术性安全体系的结构和设计，以及选择和记录首选技术安全架构、设计和相关控制的选项。被评审的网络环境的特征决定了特定信息的选择（包括从GB/T 25068.4、GB/T 25068.5及ISO/IEC 27033-6中选择的信息），即特定信息的选择与特定网络接入场景和“技术”主题有关。

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 29246　信息技术　安全技术　信息安全管理体系　概述和词汇（GB/T 29246—2017，ISO/IEC 27000:2016，IDT）

GB/T 25068.1　信息技术　安全技术　网络安全　第1部分：综述和概念（GB/T 25068.1—2020，ISO/IEC 27033-1:2015，IDT）

3　术语和定义

GB/T 29246、GB/T 25068.1界定的以及下列术语和定义适用于本文件。

3.1

恶意软件　malware

带有恶意设计的软件类别，包含可能直接或间接对用户或用户的计算机系统造成潜在伤害的特性或功能。

[来源：ISO/IEC 27032:2012，4.35]

3.2

不透明性　opacity

对可能通过监测网络活动（例如在互联网上的VoIP呼叫中获得端点的地址）获得的信息给予保护。

注：不透明性同时还保护获得信息的相关行为。

3.3

外包　outsourcing

购买方为支持其业务功能需求而进行的外部购买服务。

3.4

社会工程　social engineering

利用某种方式诱使合法用户执行操作或泄露秘密信息的行为。

4　缩略语

下列缩略语适用于本文件。

AAA：鉴别、授权和计费(Authentication，Authorization and Accounting)

DHCP：动态主机分配协议(Dynamic Host Configuration Protocol)

DNS：域名服务(Domain Name Service)

DNSSEC：DNS安全扩展(DNS SECurity Extensions)

DoS：拒绝服务(Denial of Service)

FTP：文件传输协议(File Transfer Protocol)

IDS：入侵检测系统(Intrusion Detection System)

IP：互联网协议(Internet Protocol)

IPsec：IP安全(IP Security Protocol)

OAM&P：操作、管理、维护和保障(Operations，Administration，Maintenance&Provisioning)

OSI：开放系统互联(Open Systems Interconnection)

PDA：个人数据终端(Personal Data Assistant)

PSTN：公共交换电话网络(Public Switched Telephone Network)

QoS：服务质量(Quality of Service)

SIP：会话发起协议(Session Initiation Protocol)

SMTP：简单邮件传输协议(Simple Mail Transfer Protocol)

SNMP：简单网络管理协议(Simple Network Management Protocol)

SSL：安全套接层(加密认证协议)[Secure Socket Layer(Encryption and authentication protocol)]

VoIP：IP电话(Voice over Internet Protocol)

VPN：虚拟专用网(Virtual Private Network)

5　文档结构

本文件的结构包括：

——为每个参考网络接入场景提供了网络安全防护方法的概述(详见第6章)；

——为每个参考场景(详见第7章～第15章)提供了详细描述：

- 描述了存在于参考场景的威胁；
- 描述了在第6章的方法的基础上可能采用的安全控制措施和技术。

本文件中的场景按照表1进行排序，其目的是评估给定场景的功能：

——接入用户的类型，可能包括机构内部的用户、从外部访问机构资源的员工，或外部用户(消

费者、供应商、业务合作伙伴）；

——被访问信息资源的类型，开放、受限、外包的访问资源。

表1呈现一个一致性结构，使得更易于管理增加新的场景，也表明本文件各个场景的必要性。

表1 网络接入场景资源访问框架

可访问的信息资源	接入用户		
	内部用户	外部员工	外部用户
开放	——员工的互联网访问服务； ——企业对企业的服务		——企业对客户的服务
受限	——增强协作服务； ——企业对企业的服务； ——网络分段[a]； ——居家办公和小型商务办公场所的网络支持	——移动通信； ——流动用户的网络支持	——增强协作服务； ——企业对企业的服务； ——企业对客户的服务
外包	——外包服务		——外包服务
[a] 网络分段是指网络的分离或隔离（通常使用一个或多个防火墙），它可能意味着出于安全原因，物理隔离网络。			

本文件中列出的场景顺序如下：

——员工的互联网访问服务（见第7章）；

——企业对企业的服务（见第8章）；

——企业对客户的服务（见第9章）；

——增强协作服务（见第10章）；

——网络分段（见第11章）；

——为居家办公和小型商务办公场所提供网络支持（见第12章）；

——移动通信（见第13章）；

——为流动用户提供网络支持（见第14章）；

——外包服务（见第15章）。

6 概述

本文件基于以下方法对每个已识别的参考网络接入场景提供指导：

——评审网络接入场景的背景信息和范围；

——描述与网络接入场景相关的威胁；

——对已发现的漏洞进行风险分析；

——分析潜在的漏洞对业务的影响；

——确定用以保护网络的实施建议。

为了解决网络安全性问题，需采用一种提供端到端评估的系统化方法。这种方法的复杂性取决于一定范围内网络的性质和规模。然而，随着技术的不断发展，评估方法的一致性对管理安全性非

常重要。

安全评估中需考虑的首要因素是确定拟保护的资产。这些资产大致可以分为基础设施、服务及应用程序。机构可自定义其资产类别，但要注意不同的资产类别所受威胁和攻击具有差异化。例如，如果路由器被归类为基础设施类资产，而 VoIP 被归类为终端用户服务类资产，那么针对 DoS 攻击就需要采取不同的策略。具体来看，路由器需在其物理端口上防御伪数据包泛洪，而 VoIP 服务需保护用户的账户及服务信息不被删除或损坏，以保障合法用户不会被阻止访问服务。

网络安全还需要保护网络上支持的各种活动，如管理活动、控制指令消息、终端用户数据(本地数据和传输数据)。例如，管理员界面可能会由于未经授权的访问而被公开(易被破解的管理员账户和密码)。通信流量易被伪造 IP 地址的操作系统发出的 OA&M 指令破坏，被嗅探泄露，被数据包泛洪中断。

本文件对资产和行为的识别方法，有助于对威胁模块化和系统化的分析。根据已知的威胁集检查每个参考网络接入场景，以确定可适用哪些威胁。附录 A 提供了已知的行业威胁的列表，尽管该列表不能完全覆盖已知的行业威胁，但它提供了一个基点。一旦确定了网络的威胁概况，就可以对漏洞进行分析，以确定在特定资产环境中可能出现的威胁。这样的分析将有助于确定缺少哪些防御措施，以及需要部署哪些策略来实现对目标的保护，采取的策略将降低入侵成功的可能性或降低其影响。风险分析是通过发现漏洞来实现的，业务影响分析是通过应对每个漏洞的业务决策来实现的，业务决策包括补救、承受风险或转移风险。

任何安全评估方法均需包括为保护漏洞不受威胁而设计的策略和实施的控制措施。根据 GB/T 29246，对资产、信息保护来说，相关控制措施的选择和实施是至关重要的。该标准要求保持信息的保密性、完整性和可用性，除此之外，还可能涉及信息的真实性、抗抵赖性和可靠性等其他属性。

以下是本文件中使用的一组安全属性，用于客观的设计策略和实施控制措施以降低风险。下面是对每个安全属性(不限于保密性、完整性和可用性)需求的合理化描述。

——保密性是指保护数据免遭未经授权的泄露。

——完整性是指维护数据的正确性和准确性，防止未经授权的修改、删除、创建和复制。

——可用性是指允许对网元、存储信息、信息流、服务和应用程序的授权访问。

——访问控制是指通过使用鉴别和授权，对网络设备和服务的访问进行控制，并确保只允许经过授权的人员或设备访问网元、存储信息、信息流、服务和应用程序。例如，在 IPTV 部署中，禁用访问用户机顶盒的调试接口就是出于对访问控制属性考虑的安全建议之一。对保密性、完整性或可用性的评审不会产生异议。

——鉴别是指在获得授权的访问控制时确认或证实用户或通信方的身份，并确保实体不会试图伪装或未经授权地重放攻击。例如，个人可获得对网络管理系统的访问权，但是需要通过认证才能更新订阅用户服务记录。因此，不能仅通过采用保密性、完整性、可用性或访问控制来确保网络管理行为具备可执行性。

注：在基于角色的访问控制中(鉴别和授权函数为空值)，授权是通过将用户划分为不同角色来实现的。访问控制是指在授予访问权限之前验证该用户是否为具有访问权限的角色。同样，访问控制列表根据策略授予访问权，如果用户满足策略要求，那么就被授予访问权。

——通信或传输安全是指确保信息只在授权的端点之间流动而不被转移或拦截。

——抗抵赖性是指保留审核记录，以保证数据的来源或事态、操作的起源不可否认。对受保护数据执行未经授权操作的人员进行识别，该识别行为不影响数据的保密性、完整性和可用性。

——不透明性是指保护网络活动不被监视，进而保护网络活动产生的信息。实现不透明性除了保护信息之外还需要保护网络活动。保护信息是通过实施保密性来实现的，保护网络活动是通

过保护甲乙之间的通话来保护他们的机密信息，进而确保了信息的不透明性。

在本文件所描述的所有场景中，都将上述安全属性作为安全设计技术和控制措施阶段的一部分进行评审。表2展示了一些网络安全属性的实现机制的示例，这些安全属性可用于降低潜在风险。

表2 网络安全技术示例

安全事项	安全机制、技术
访问控制	门禁系统，访问控制列表(ACL)，职责分离
鉴别	简单登录、简易密码，数字证书，数字签名，传输层安全协议 v1.2，单点登录，询问握手认证协议
可用性	冗余备份，防火墙，入侵检测、入侵防御(用于阻止 DoS)，业务连续性，使用服务水平协议管理的网络和服务
通信安全	IPsec、第二层隧道协议，私有线路，隔离网络
保密性	加密，访问控制列表，文件许可
完整性	IPsec，哈希消息认证码，循环冗余校验，反病毒软件
抗抵赖性	日志，基于角色的访问控制，数字签名
不透明性	IP 包头加密(如：具有 IPsec 隧道模式的 VPN)，网络地址转换(针对 IPv4)

在本文件中，每个参考网络接入场景的环境中讨论的策略设计和技术实施均需考虑上述安全事项。通常来说，组织将从 GB/T 22081 中选择相关控制要素以达成其业务目标，而本文件旨在提供实施所选控制要素的网络等级的注意事项。

7 员工的互联网访问服务

7.1 背景

当组织需要为员工提供互联网访问服务时，可采用本章所提供的网络接入场景，以确保员工访问互联网的内容是明确的且已被授权的，而不是一般的开放访问。组织需考虑如何管理访问权限，避免因员工不受控制访问互联网而导致网络带宽损失，甚至可能承担连带法律责任。

随着越来越多的互联网违法案例的出现，员工的互联网访问控制日益受到关注。因此，组织有责任通过评估以下场景，来建立、监测和执行一个明确的互联网访问策略：

——出于业务目的访问互联网；

——是否允许出于私人目的以受限形式访问互联网，允许使用哪些服务；

——是否允许增强协作服务；

——是否允许员工使用聊天系统、论坛等。

通常情况下，尽管既定策略可阻止大多数违规使用互联网行为，但组织仍然面临巨大的信息安全风险。下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

7.2 安全威胁

与员工互联网访问服务相关的安全威胁包括以下内容。

——病毒攻击和恶意软件的入侵：

- 使用互联网的员工是恶意软件的主要攻击目标，这些恶意软件可导致信息的丢失或破坏，造成IT基础设施失控，给组织的网络安全带来巨大风险。
- 用户下载的文件或程序可能包含恶意代码。由于即时消息传输、对等文件共享和IP电话等应用程序的普及，员工可能会在不经意间下载并安装恶意应用程序，这些恶意应用程序可能使用灵活的端口配置（在开放端口之间跳跃）和加密等技术来规避网络防御。此外，可以利用对等文件共享应用程序作为僵尸网络的隐通道。
- Web浏览器或其他Web应用程序中的漏洞可被恶意软件利用，并导致感染病毒和木马。一旦感染，病毒传播活动将导致网络过载严重影响可用性，未授权的实体借由木马获得访问权限，破坏了保密性。

——信息泄露：

- 允许将信息上传到Web服务器的应用程序上，可导致组织内部与互联网间不受控的数据传输。如果使用加密会话（例如传输层安全协议），那么甚至无法记录此类行为。当在组织内部的系统上植入未经认证的代码时，也会引入类似的安全风险。

——未经授权的使用和访问：

- 基础设施、系统和应用程序的失控可能导致欺诈、拒绝服务和设施的滥用。

——违法违规责任：

- 因不遵守法律法规或监管义务而产生的法律责任；
- 不符合组织使用的策略可能导致违反法律法规。

——因带宽不足或稳定性问题而降低网络可用性：

- 过度使用高带宽服务，如流媒体或对等文件共享，可导致网络过载。

7.3 安全设计技术和控制措施

表3描述了与员工的互联网访问服务有关的安全设计技术和控制措施。

评审每个安全属性在降低可预测的安全风险方面的适用性，随后在第二列中给出相应的技术实施示例。例如，完整性、访问控制和鉴别可用于防御恶意代码。

表3 员工的互联网访问服务场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
病毒攻击和恶意软件的入侵	
——完整性 ——访问控制 ——鉴别	——只向员工提供与业务相关的互联网服务。利用黑名单管理授权服务，进而拒绝使用聊天系统或Web邮件服务，或对等文件共享网络协议。 ——在连接互联网的网关上使用防病毒软件，以扫描所有出入互联网的流量。扫描宜覆盖所有授权使用的网络协议。确保自动安装防病毒更新，或提醒用户存在可用更新。 ——在所有客户端系统上使用防病毒软件，特别是员工使用的客户端系统。 ——对文件和所有存储的信息进行病毒、木马及其他形式的恶意软件的扫描。 ——使用如杂凑、校验码、证书等算法对数据、文件进行完整性验证。 ——阻止弹出窗口和网络广告。 ——通过使用少量受控的安全网关来控制互联网访问服务的流量。 ——活动内容鉴别

表 3　员工的互联网访问服务场景下的安全控制措施（续）

适用于已识别威胁的安全属性	设计和技术的实施
信息泄露	
——通信安全 ——完整性 ——访问控制	——在互联网网关上为移动代码设置过滤器。 ——只接受来自非关键的、白名单站点的移动代码。 ——只接受由认证机构或认可供应商签名的移动代码，并在客户端启用相应的配置选项，例如主动管理和设置一个允许代码签名认证机构的白名单
未授权的使用和访问	
——访问控制 ——抗抵赖性	——只向员工提供与业务相关的互联网服务。利用黑名单管理未授权服务，例如聊天频道或 Web 邮件服务，为非授权协议（如对等文件共享网络协议）设置过滤器。 ——限制使用极易传输大量数据的服务。 ——确保对所有可能将数据传输到互联网的服务进行适当的日志记录和监控。 ——在专用策略中明确界定授权或未授权互联网访问的情况（见附录 B）。 ——通过适当的教育和培训确保用户的安全意识
违法违规责任	
——抗抵赖性	——用户日志，时间戳。 ——用户的网络安全提示机制和培训制度
降低网络可用性	
——完整性 ——可用性	——根据漏洞的严重程度，在规定的时间内对已知系统漏洞进行适当的管理和修补。 ——漏洞管理宜关注全部接收互联网流量的系统，无论是在传输层还是应用层，包括使用互联网的网关的所有系统，以及用于访问互联网服务的终端用户系统，特别是在使用 Windows 操作系统的情况下。 ——限制流媒体带宽（仅在业务策略允许的情况下）。 ——宜监控网络和系统资源（入侵检测系统、日志、审计等），从而对系统、安全性和操作事态进行检测

8　企业对企业的服务

8.1　背景

组织与其他组织进行交易（如制造商、批发商、零售商）宜考虑本章所提供的网络接入场景。

一般来说，企业对企业的服务通过租用专用线路或网络分段来实现。互联网和相关技术确实提供了更多选择，但实施此类服务的同时也引入了新的安全风险。不断发展的 B2B 电子商务模式允许组织通过互联网开展业务，应用程序则聚焦于通过使用互联网、外联网或两者兼用以达到改善业务伙伴关系（相互已知且经过注册）的目的，这有别于企业对客户的情况。

通常组织基于自己的需求来选择企业对企业的服务。例如，可用性和可靠性就是非常重要的需

求，因为组织开展工作通常直接依赖于企业对企业的服务。

当基于互联网来实现企业对企业的服务时，经过验证的措施，例如租用专线的服务质量预期不再适用，因此就要用与以往不同的方式处理可用性和可靠性等需求。新的安全风险需通过适当的设计技术和控制措施来降低。重点是通过防止访问未经授权的数据和保持业务系统间的隔离，来加强组织之间的信任。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

8.2 安全威胁

与企业对企业的服务有关的安全威胁包括以下内容。

——病毒攻击和恶意软件的入侵：

- 利用恶意软件对系统进行渗透，可导致敏感信息被破坏或被未经授权访问；
- Web 浏览器或其他 Web 应用程序中的漏洞可被恶意软件利用，并导致感染病毒和木马。

——针对企业对企业门户网或外联网的 DoS 攻击和 D-DoS 攻击。

——授权业务伙伴间的内部攻击。

——伪造事务内容(邮件未送达预期收件人或数据在传送过程中被篡改)。

8.3 安全设计技术和控制措施

表 4 描述了与企业对企业的服务相关的信息安全设计技术和控制措施。

表 4 企业对企业的服务场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
病毒攻击和恶意软件的入侵	
——完整性 ——访问控制 ——鉴别	——在连接互联网的网关上使用防病毒软件，以扫描所有出入互联网的流量。扫描宜覆盖所有授权使用的网络协议。确保自动安装防病毒更新，或提醒用户存在可用更新。 ——对文件和所有存储的信息进行病毒、木马及其他形式的恶意软件的扫描。 ——使用如杂凑、校验码、证书等算法对数据、文件进行完整性验证。 ——通过使用少量受控的安全网关来控制互联网访问服务的流量。 ——活动内容鉴别
拒绝服务攻击	
——可用性 ——不透明性	——禁用未使用的端口和服务，以防止它们对未经授权的扫描或嗅探作出响应，这可能会导致泛洪流量 DoS 攻击。 ——从告警提示中排除描述性信息可以防止向攻击者提供目标信息

表 4　企业对企业的服务场景下的安全控制措施（续）

适用于已识别威胁的安全属性	设计和技术的实施
内部攻击	
——访问控制 ——抗抵赖性	——明确定义访问管理安全策略(用于业务关系管理)。 ——明确的角色和职责。 ——定制告警提示。 ——限制特权用户。 ——使用日志记录所有关键、非关键事务
伪造事务内容	
——抗抵赖性	——详细事务日志。 ——使用数字签名

9　企业对客户的服务

9.1　背景

组织与客户进行交易时宜考虑本章所提供的网络接入场景。

企业对客户的服务，也称为电子商务服务，包括电子商务、电子银行和电子政务等服务。在企业对客户的服务中，安全性需要在实施交易与维护品牌和商业价值之间取得平衡。

信息安全要求包括：

——保密性(特别是关于电子银行业务)；

——鉴别；

——完整性；

——数据通信安全性，即终端用户期望业务服务能够提供一条用以保护用户和提供者之间的交易路径，以抵抗复杂攻击(例如“中间人”或“浏览器中间人”攻击)；

——可用性是电子商务提供商的一个重要衡量度。

信息安全特征包括：

——只有在组织控制下的终端平台上才能“保证”安全性，才能为实施控制措施和维护良好的平台级安全提供良好的环境；

——客户端上的安全性一般较差。难以在这样的环境中实施控制措施，因此客户端在这种场景(如约定中没有“安全连接的条件”的要求集合)下会存在重大风险。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

9.2　安全威胁

与企业对客户的服务的相关安全威胁包括以下内容。

——病毒攻击和恶意软件的入侵：

- 利用恶意软件对系统进行渗透，可导致敏感信息被破坏或被未经授权访问；
- Web 浏览器或其他 Web 应用程序中的漏洞可被恶意软件利用，并导致感染病毒和木马。

——未经授权的访问：

- 未经授权访问后台数据库，如结构化查询语言注入攻击、跨站脚本攻击；
- 账户获取，这是一种通过 Web 应用程序响应用户鉴别而获得有效账户信息的方法；自动化脚本通常用于获取有效的用户 ID 和账户名；
- 使用社会工程攻击（通过使用欺骗性技术）窃取线上身份，例如网络钓鱼攻击和基于 DNS 的攻击，这些攻击将用户连接到看似合法但实际不合法且具有欺诈性的 Web 服务器上；
- 未经授权访问系统或网络，恶意复制、修改或破坏数据；
- 非法破解导致侵犯版权和内容盗用。

——DoS 攻击。

——伪造事务内容（邮件未送达预期收件人或数据在传送过程中被篡改）。

9.3 安全设计技术和控制措施

表 5 描述了与企业到客户的服务相关的安全设计技术和控制措施。

表 5 企业对客户的服务场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
病毒攻击和恶意软件的入侵	
——完整性 ——访问控制 ——鉴别	——在连接互联网的网关上使用防病毒软件，以扫描所有出入互联网的流量。扫描宜覆盖所有授权使用的网络协议。 ——对文件和所有存储的信息进行病毒、木马及其他形式的恶意软件的扫描。 ——使用如杂凑、校验码、证书等算法对数据、文件进行完整性验证。 ——通过使用少量受控的安全网关来控制互联网访问服务的流量。 ——活动内容鉴别

表 5　企业对客户的服务场景下的安全控制措施（续）

适用于已识别威胁的安全属性	设计和技术的实施
未经授权的访问	
——访问控制 ——鉴别 ——保密性 ——通信安全 ——完整性 ——不透明性	——限制 Web 应用访问后台数据库的权限。 ——在非军事区内进行网络分段和划分安全层，以防止直接指向公司数据资产的连接路径。 ——用户注册安全，确保访问证书只颁发给可信的用户，例如使用独立的注册机构进行注册的用户。 ——使用数字证书、密码、生物识别或智能卡进行鉴别。 ——建立防火墙和访问控制列表，以防止未经授权的用户访问。 ——基于角色的访问控制，以限制用户可执行的功能。 ——检查 Web 应用程序日志，以识别和遏制攻击。 ——设置适当的存储信息的加密级别。 ——使用 SSLv3、传输层安全协议等技术确保 Web 浏览器和 Web 服务器之间的安全性。 ——使用例如简单对象访问协议消息保护 Web 服务的基本通信。 ——使用如杂凑、校验码、证书等算法对数据、文件进行完整性验证。 ——对于 Web 应用程序中的统一资源定位符、小型文本文件或隐藏的表单元素数据完整性： ● 加密所有数据（即便在使用 SSLv3 的情况下）； ● 使用带变量的时间戳； ● 对敏感数据进行数字签名或使用加密哈希算法。 ——在 Web 服务器和外网之间使用反向代理
拒绝服务攻击	
——可用性 ——不透明性	——禁用未使用的端口和服务，以防止它们对未经授权的扫描或嗅探作出响应，这可能会导致泛洪流量 DoS 攻击。 ——从告警提示中排除描述性信息可以防止向攻击者提供目标信息
伪造事务内容	
——抗抵赖性	——详细的事务日志。 ——使用数字签名

10　增强协作服务

10.1　背景

组织在利用涉及多个员工的服务时宜考虑本章所提供的网络接入场景。示例如下：

——群件；

——文件服务器；

——邮件列表；

——基于 Web 的服务。

增强协作服务让集成各种通信和文档共享这一行为更具可能性，是业务环境的一个重要方面。

这种协作服务通常将视频电话、聊天频道的语音通信、电子邮件系统以及文档共享和在线协作环境集成为一体。

组织使用的此类服务有两种基本方式：

——仅作为内部服务使用，但存在不能与外部合作伙伴一起使用的缺点等；

——作为内部和外部服务使用。这种方式收益更多，但与仅在内部使用相比，也会产生更多的安全风险。

实施方面的服务可包括：

——内部实施；

——来自第三方。

如果服务要在内部和外部使用，那么从第三方购买协作服务可能是更合适的解决方案。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

10.2 安全威胁

与增强协作服务相关的安全威胁包括以下内容。

——未经授权的访问导致敏感信息的泄露：

- 滥用协作工具，非法共享受版权保护的资料、获取保密数据，将用户暴露于不良内容或宣传中；
- 通过监视使用模式、垃圾邮件和身份攻击来破坏不透明性。

——病毒攻击和恶意软件的入侵：

- 利用共享资源传播和执行恶意软件。

——降低网络可用性：

- 利用合法流量造成网络过载；
- 利用协作服务中使用的协议漏洞。

10.3 安全设计技术和控制措施

表 6 描述了与增强协作服务相关的信息安全设计技术和控制措施。

表 6 增强协作服务场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
未经授权的访问导致敏感信息泄露	
——访问控制 ——鉴别 ——保密性 ——通信安全 ——抗抵赖性	——基于角色访问应用程序、网络和存储器； ——将用户赋予不同的角色以适用不同虚拟局域网下的不同通行权； ——基于角色来确定使用权限和资源访问策略，例如用户可以运行哪些应用程序； ——访问控制列表； ——强鉴别和授权； ——用于网络虚拟化的虚拟局域网； ——基于主机的入侵检测系统； ——数据加密

表 6　增强协作服务场景下的安全控制措施（续）

适用于已识别威胁的安全属性	设计和技术的实施
病毒攻击和恶意软件的入侵	
——完整性	——使用屏幕传输软件，如终端服务器，以尽量减少数据和潜在恶意软件进入共同环境的可能性
降低网络可用性	
——可用性	——利用虚拟存储区域网络来提高静态数据的可用性和安全性； ——利用软件工具防止复制、粘贴信息，阻止试图写入可移动介质或打印，防止信息被转移； ——利用监视软件检测违反策略的行为（例如非法访问应用程序和其他网络资源）

11　网络分段

11.1　背景

组织按组织结构将内网划分为多个域时宜考虑本章所提供的网络接入场景。

网络分段是一种可用于增强系统和应用程序访问控制的技术。网络分段可用于对特定类型的行为、应用程序或系统进行分组，以便根据权限进行分组访问。通过这种方式，网络访问控制增强了其他端点访问控制措施，并提供了更深层次的防御。例如，网络分段用于：

——将管理和维护功能与普通用户对业务应用程序的访问隔离；

——将关键应用程序与其他应用程序隔离；

——将数据库与大多数用户隔离。

注：对于跨国组织来说，国家的特定法律法规对信息安全要求有很大的影响。为了满足跨国组织在其开展业务的国家对信息安全的不同要求，按照国家边界对网络进行分段是一种有效的方法。例如，某个国家的立法可要求对客户或客户数据进行特定保护，并且不允许将此类数据传输到另一个国家，这通常需要额外的信息安全控制，以确保遵守此类法规。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

11.2　安全威胁

为满足合规性要求而对网络分段的安全威胁包括以下内容。

——因监管不合规而产生的责任。

——数据泄露：

- 违反保密规定，例如客户或客户资料是从不宜提供该资料的渠道取得的；
- 违反法律法规特定的隐私要求；
- 因未满足客户对保密性或不透明性的期望而导致的信誉风险。

11.3 安全设计技术和控制措施

表7描述了与网络分段有关的信息安全设计技术和控制措施。

表7 网络分段场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
不合规而产生的责任	
——不透明性 ——保密性	——策略和用户认知： ● 隐私相关的法律法规； ● 加密技术； ● 数据存储、传输相关的法律法规； ● 合法监听的法律法规
数据泄露	
——访问控制 ——鉴别 ——完整性	——安全网关； ——应用程序级代理； ——数据加密

12 为居家办公和小型商务办公场所提供网络支持

12.1 背景

组织需要为居家办公或小型办公场所的员工提供内部资源访问权限时宜考虑本章所提供的网络接入场景。

居家办公和小型商务办公场所通常需要将组织的内网扩展到其所在地，这种情况下成本是一个关键问题，通过成本效益分析来看，其实施成本不宜过高。这意味着用于保护此类网络扩展的安全控制措施的成本有限，因此通常不使用已建立的网间安全控制措施来连接更多的内联网段。

在许多居家办公或小型办公场所场景中，除商业用途外，基础设施可能也用于私人用途，这可能会导致额外的信息安全风险。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

12.2 安全威胁

与居家办公和小型商务办公场所网络相关的安全威胁包括以下内容。

——未经授权的访问：

- 网络访问设备配置设置薄弱，如居家办公路由器(小型办公场所、居家办公)；
- 使用隧道分离技术；
- 物理安全控制措施缺失或薄弱；
- 由于网络连接的“始终在线”特性，可能导致机会窗口期更长；

- 使用访客账户和默认设置。

——病毒攻击和恶意软件的入侵：

- 在缺乏安全控制措施的情况下(例如恶意软件保护缺失或薄弱等)操作、使用居家办公或小型办公场所网络中的设备(如 PCs)；
- 私有环境和业务环境混合引入的问题，例如私自使用本身具有高风险的协议(如对等文件共享协议)；
- 修补失败；
- 一旦感染病毒，由于病毒传播导致网络过载会严重影响可用性。

——未经授权泄露敏感信息：

- 在居家办公或小型办公场所网络中存储和传输的数据未加密；
- 在居家办公或小型办公场所网络中可能存在的不当访问，如无线局域网访问；
- 缺乏对终端用户认知和安全最佳实践的培训；
- 由于该网络接入场景不能提供与办公室分支机构互联网关相同的保护级别，导致对内联网保护的预判失效。

12.3 安全设计技术和控制措施

表 8 描述了与居家办公和小型商务办公场所网络支持相关的信息安全设计技术和控制措施。

表 8 用于居家和小型商务办公场所场景的网络安全控制

适用于已识别威胁的安全属性	设计和技术的实施
未经授权的访问	
——访问控制 ——鉴别 ——通信安全	——禁用未使用的网络接口和服务； ——安装主机防火墙，丢弃或拒绝所有来自外部的连接； ——隧道分离的设计与技术保护； ——系统不宜使用空白、空值或默认的密码； ——所有用户都宜使用强密码，不宜允许匿名、访客访问； ——技术符合性检查，以确保所有安全敏感设备(如路由器或无线局域网接入点)的正确配置和设置； ——网络访问组件(如路由器)中的安全 VPN 技术
病毒攻击和恶意软件的入侵	
——完整性 ——可用性	——维护当前的软件版本和补丁； ——确保自动安装防病毒更新，或提醒用户存在可用更新； ——在适用的前提下，至少使用基于主机的入侵检测系统(HIDS)检测软件、数据库完整性； ——对文件和所有存储的信息进行病毒、木马及其他形式的恶意软件的扫描； ——备份配置数据和用于事件响应和恢复的文件

表 8　用于居家和小型商务办公场所场景的网络安全控制（续）

适用于已识别威胁的安全属性	设计和技术的实施
未经授权泄露敏感信息	
——保密性 ——不透明性	——用户认知和安全最佳实践的培训； ——存储和传输数据的加密

13　移动通信

13.1　背景

组织允许员工使用移动设备访问网络时宜考虑本章所提供的网络接入场景。

此场景关注机构使用和部署移动设备和应用程序时的安全问题。虽然消费者市场是推动智能手机或 PDA 等移动设备新功能快速发展的主要动力，但这些功能也同样适用于商务环境。移动设备通常是私有物，但也被用于商务用途。有时机构提供的移动设备，也可用于个人用途。因为设备供应商希望在竞争激烈的市场中获得尽可能多的业务，所以针对商务领域的设备也需要引入消费者市场具备的功能。

移动通信设备允许远程用户同步个人数据库，并提供对无线电子邮件、Web 浏览和互联网等网络服务的访问。当个人将同一个设备用于私人和商务目的时，就会有避开或忽视使用策略的倾向，从而给机构带来重大的信息安全风险。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

13.2　安全威胁

与移动通信设备相关的安全威胁包括以下内容。

——未经授权访问存储在移动设备上的信息：

- 对敏感信息的访问控制或保护不足；
- 缺乏安全认知和弱口令；
- 弱配置；
- 异常设备劫持攻击；
- 终端用户缺少对信息安全保护要求的认知，例如将私人信息和商务信息混合在一起。

——未经授权泄露敏感数据和位置信息：

- 基于位置的服务可以将用户的位置信息泄露给未经授权的第三方，从而导致隐私泄露问题；
- 窃听；
- 通信流中介入了未受充分保护的第三方；
- 使用明文或未受充分保护的传输协议；
- 处置程序不当。

——未经授权修改、删除存储信息(包括软件):

- 安装未授权来源的软件而引入恶意软件;
- 利用底层操作系统中的漏洞。

——垃圾邮件导致:

- 增加服务费用;
- 网络钓鱼攻击;
- DoS 攻击。

——失窃或意外损失,两者都可能导致:

- 当设备上存储的数据没有镜像或异地备份时,会丢失敏感数据;
- 未充分保护设备上存储的敏感数据而产生的保密问题;
- 数据备份的安全问题。

13.3 安全设计技术和控制措施

表 9 描述了与个人移动通信设备相关的数据安全设计技术和控制措施。

表 9 移动通信场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
未经授权访问存储在移动设备上的信息	
——访问控制 ——鉴别 ——抗抵赖性	——用户对物理控制的认知; ——避免默认配置; ——强鉴别; ——启用日志审计选项; ——超时锁; ——防火墙; ——针对密码和商务使用的组织安全策略(限制个人使用机构设备)
未经授权泄露敏感数据和位置信息	
——保密性 ——鉴别 ——安全通信 ——不透明性	——加密存储和传输(无线)数据; ——密码保护; ——拒绝要求明文访问传输数据的第三方服务,在无法拒绝的情况下则宜确保按保密性要求处理数据; ——确保安全的同步过程; ——远程访问连接使用安全的 VPN; ——适当的清除敏感数据的处置过程; ——用户对位置使用的许可

表 9　移动通信场景下的安全控制措施（续）

适用于已识别威胁的安全属性	设计和技术的实施
未经授权的修改、删除存储信息(包括软件)	
——保密性 ——可用性 ——完整性	——禁用未使用的无线接口、服务和应用程序； ——操作系统的最新补丁； ——适当的清除敏感数据的处置过程； ——确保自动安装防病毒更新，或提醒用户存在可用更新； ——软件只能从机构软件分发系统中下载(避免安装未经授权的软件)； ——验证下载源的数字签名
垃圾邮件	
——访问控制	——内容过滤； ——提升用户安全意识
失窃或意外损失	
——保密性 ——可用性	——远程资产管理(禁用、锁定设备)； ——定期安全备份； ——对资产跟踪和策略的一致性实施集中管理

14　为流动用户提供网络支持

14.1　背景

组织在允许流动中的员工访问机构资源时宜考虑本章所提供的网络接入场景。

流动用户网络支持方案和产品通常侧重于功能方面，主要面向消费者市场。从信息安全的角度来看，现行功能级别引入了新的风险，可能影响有关信息安全的预判，或导致预判失效。举例来说，如果内联网的远程访问没有采用适当的控制措施，那么预判其控制良好且受到良好保护的可能性存疑。

下述条款针对内部、内外部、使用行为情况，描述了安全威胁和关于安全设计技术与控制措施的建议，以减轻相关风险。

14.2　安全威胁

与流动用户提供网络支持有关的安全威胁包括以下内容。

——未经授权的访问：

- 滥用流动用户网络支持，未经授权访问组织的内联网；
- 违背在内联网边界使用安全网关的原则；
- 未经授权而直接访问存储在移动用户设备上的数据。

——降低网络可用性：

- 因未满足客户对网络支持的期望而导致的可用性问题。

14.3 安全设计技术和控制措施

表 10 描述了与流动用户联网支持有关的信息安全设计技术和控制措施。

表 10 为流动用户提供网络支持场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施
未经授权的访问	
——访问控制 ——鉴别 ——通信安全 ——保密性	——增强鉴别技术(基于证书的鉴别、双因素鉴别或激励响应鉴别)。 ——为流动用户提供基于传输层安全协议、SSLv3 保护的 Web 接口服务。 ——在客户端系统(如个人防火墙)中,使用安全 VPN 技术连接私有安全网关: ● 在 2、3 层实施,如 IPsec; ● 应用层 VPN,如基于传输层安全协议。 ——加密存储用户数据
降低网络可用性	
——可用性	——选择保障可靠性和性能的服务水平协议的全球服务提供商

15 外包服务

15.1 背景

组织使用外包服务时宜考虑本章所提供的网络接入场景。

组织使用外包服务是因为它被视为一种可行的业务策略,但它也带来了组织和操作的复杂性,特别是在保障质量和安全性的情况下。

机构由于依赖于服务提供商而承担了其带来的附加风险。例如,服务提供商或供应商可能要求直接访问机构内部资产以解决技术支持服务问题或突发事件,从而使关键资产面临安全风险。一些技术支持服务需要永久访问权限,而其他的技术支持服务可能只需临时访问权限。通常技术支持服务需要高访问权限才能完成任务。

无论外包场景的类型如何,均需在约定中体现安全性考量和安全监督。本文件仅给出与外包服务有关的威胁和相关事项的概述。有关外包服务安全的更多深入信息,见 ISO/IEC 27036。

下述条款针对内部、内外部、使用行为情况,描述了安全威胁和关于安全设计技术与控制措施的建议,以减轻相关风险。

15.2 安全威胁

与外包服务有关的安全威胁包括以下内容。

——未经授权访问其他内部系统(当供应商访问内部系统进行远程技术支持服务和维护时):

- 滥用远程维护端口;
- 滥用管理员权限。

——服务提供商未经授权泄露敏感数据:

- 未遵守知识产权相关规定；
- 未区别对待多客户环境；
- 缺乏信息安全最佳实践(如随意的口令共享)；
- 存储介质处置不当；
- 使用非安全通信方法。

——恶意软件(在软件开发环境中)的入侵：

- 软件开发和发布过程中的安全性不足；
- 文件和数据的不安全传输；
- 不安全的在线协同。

——因不遵守规章而产生的责任：

- 跨国服务提供商缺乏对我国法律法规的了解；
- 服务提供商或供应商缺乏对其所在国相关法律法规的了解。

15.3 安全设计技术和控制措施

表 11 描述了与外包服务有关的信息安全设计技术和控制措施。

表 11 外包服务场景下的安全控制措施

适用于已识别威胁的安全属性	设计和技术的实施 (实施可由机构或服务提供商或供应商根据约定的任务分配来承担)
未授权访问内部系统	
——访问控制 ——鉴别 ——抗抵赖性	——严格分配个人用户 ID； ——对根用户、超级管理员登录的强鉴别(例如双因素鉴别)； ——受用户 ID 和密码保护的本地控制端口或带外端口(在服务提供商需要现场物理访问的情况下)； ——全面记录访问行为和日志评审
未经授权的敏感信息泄露	
——保密性	——通过加密保护客户端数据的最佳实践； ——安全意识和安全培训； ——创建监视和评审的设施和程序； ——明文规定的安全策略和程序指令
恶意软件的入侵	
——完整性	——安全编码实践； ——变更管理过程； ——确保自动安装防病毒更新，或提醒用户存在可用更新
因不遵守规章而承担的责任	
——保密性 ——不透明性	——了解法规； ——使用兼容的加密软件； ——不透明机制(IPsec VPNs)

附 录 A
（资料性）
威胁目录

A.1 故意给出错误的权限和授权

包括但不限于下列行为：

a) 虚假授权；
b) 授予其他用户密码、密钥或证书（如系统管理员）；
c) 个人用户未经授权获取和使用用户服务相关的鉴别信息（如用户 ID、用户密码、会话密钥）；
d) 未经授权获取和使用管理员鉴别信息（如用户 ID、密码）；
e) 涉及信号传输的重放攻击。

A.2 窃取服务行为

包括但不限于下列行为：

a) 非法获取服务提供商的利益，以剥夺服务提供商的合法收益；
b) 服务提供商欺诈；
c) 未经授权删除或更改计费信息；
d) 设备克隆；
e) 控制增稳系统；
f) 大量复制、传播服务中信息，导致服务被盗用。

A.3 侵害用户隐私和窃听

包括但不限于下列行为：

a) 呼叫跟踪模式用以发现身份信息、从属关系、存在状态和使用情况。
b) 流量（包括管理流量和信令流量）捕获，未经授权的流量记录，包括数据包记录、数据包日志记录和数据包嗅探。
c) 未经授权访问订阅用户的媒体流。
d) 未经授权访问 OAM&P 流量。
e) 未经授权访问信令流量。
f) 信息收集，蓄意捕获身份信息，为实现后续信息窃取和执行未授权通信做准备。身份信息由 ID 集合组成，ID 可以是数字、字符串、统一资源定位符等。
g) 媒介重构，未经授权对视频通信的某一部分（包括身份、展现形式和状态）进行监视、记录、存储、重建、识别、解释、翻译或特征提取。
h) 未经授权泄露订阅用户服务能力。
i) 未经授权泄露订阅用户曾经或当前使用情况或行为（如订阅用户观看广播或视频点播内容的历史、在线游戏活动等）。
j) 涉及媒体的重放攻击（出于不当获利的目的捕获媒体并重放，或出于侵犯隐私目的重放个人使用的媒体）。

A.4 拦截和修改

包括但不限于下列行为：

a) 会话模拟和劫持，使用信息对通信的任何部分进行注入、删除、添加、移除、取代或部分替换修改其内容，以更改其内容或任何一方的身份、展现形式和状态，包括管理和信令流量；
b) 未经授权访问、修改或删除数字信息；
c) 劫持数据流，以未经授权的方式插入、修改和删除数据流；
d) 任何形式的垃圾邮件；
e) 出于政治或其他原因未经授权传输资料。

A.5 流量、数据包泛洪

包括但不限于下列行为：

a) 用户端的 DoS 攻击是通过发送大量有效数据包致使服务中断，进而导致应用程序因过载而停止，其中一些 DoS 攻击甚至可以影响网元；
b) 端点数据包泛洪场景导致网元或服务器崩溃、重启或耗尽所有资源；
c) DoS 导致的带宽消耗、资源消耗，流量泛洪（例如，到多播组）；
d) 影响海量订阅用户的潜在可能（例如，支持海量订阅用户的服务器）。

A.6 封包攻击和畸形消息

包括但不限于下列行为：

a) 使用无效消息导致端点失效，DoS 攻击端点（如服务器），通过发送大量无效消息，可能导致端点崩溃、重启或耗尽所有资源；
b) 畸形协议消息，向设备发送畸形的协议消息（例如，带有溢出或下溢的消息），导致设备性能下降而无法处理正常消息；
c) 导致缓冲区溢出的畸形消息；
d) 影响海量订阅用户的潜在可能（例如，支持海量订阅用户的服务器）。

A.7 欺骗消息

包括但不限于下列行为：

a) DoS 攻击，通过提前结束会话导致中断服务。
b) 控制消息的欺骗。在通信中注入恶意控制流量，导致应用程序或服务器发生故障，或将流量发送到错误的目的地。伪造控制消息，用于改变组播分布树的结构，影响组播树之间的数据分布。DoS 攻击如伪造信道损失率高或阻塞率高的广播消息，导致信号源将降低传输速率影响其他用户。
c) 伪造端使用消息，和应用程序或服务器响应；
d) 更改 IP 和 MAC 地址以欺骗其他用户的 MAC 和 IP 地址，以捕获数据流。

A.8 底层平台 DoS

包括但不限于下列行为：

a) 应用程序或服务运行的底层操作系统或固件漏洞；
b) 利用互联网上可免费下载的“开箱即用”的资源；
c) DoS 攻击会降低设备性能。这可能会影响到海量设备（例如，客户端）。可能需要重新部署或维护海量设备。

A.9 已安装软件、服务相关数据或系统配置的危害

包括但不限于下列行为：

a) 恶意软件、间谍软件、rootkit 插入；
b) 未经授权复制、安装、修改或删除生产软件和配置文件；
c) 未经授权复制、泄露、创建、修改或删除服务相关数据(如系统日志、账单信息、解密密钥、解密密钥存储容器等)；
d) D-DoS 利用被感染的设备造成服务崩溃；
e) 未经授权创建或修改订阅用户服务相关信息(如鉴别信息、会话密钥)；
f) 未经授权或不必要的激活或停用逻辑(协议)端口。

A.10 资源耗尽

包括但不限于下列行为：
a) 导致系统内存资源(如缓冲区)耗尽的软件或硬件缺陷；
b) 系统中消耗大部分中央处理器资源的软硬件缺陷；
c) 限制通信链路可用带宽的硬件或软件错误；
d) 软件或硬件缺陷，产生不必要的消息，减少带宽资源。如无限的软件循环，路由循环。

A.11 未经授权的网络扫描和探测

包括但不限于下列行为：
a) 执行端口扫描、包互联网查询工具 ping 命令扫描。攻击者可以在连接到网络的主机上运行公开可用的扫描软件。监视端口的设备上的主机服务将作出响应，可能向攻击者提供信息。
b) 执行漏洞扫描(如 nessus 工具)、网络映射(如 NMAP)。攻击者可以在连接到查询设备配置和网络拓扑的网络的主机上运行公开可用软件。
c) 未经授权远程访问设备上的软件或功能(例如，利用 rootkit 提供后门)。

A.12 泄露用户应用数据

包括但不限于下列行为：
a) 未经授权的泄露、创建、修改、复制、删除用户通过可访问应用程序创建或使用的数据；
b) 包括用户存储在服务提供商网络中的信息(如 nDVR 录制的视频内容)。

A.13 窃取内容

包括但不限于下列行为：
a) 捕获数字证书以获取订购内容，进而向其他订阅者重新分发该内容；
b) 捕获家庭网络和 IP 子网上的数据包；
c) 从模拟端口输出到外部记录设备；
d) 从数字端口输出到外部记录设备；
e) 执行超次数播放；
f) 访问非法内容(如盗版内容)；
g) 绕开控制增稳系统；
h) 复制服务器或终端用户设备上的存储内容。

A.14 访问不当内容

包括但不限于下列行为：
a) 意外访问；
b) 蓄意访问。

A.15 泄露用户信息

包括但不限于下列行为：

a) 获取用户信息的社会工程；

b) 未经授权泄露、创建、修改、复制或删除用户信息(如地址、电话号码、账户号码、信用卡信息、DNS信息、ENUM信息等)。

A.16 会话劫持和服务伪装

包括但不限于下列行为：

a) 冒充合法服务提供商，从数字证书拥有者处获取数字证书以修改流或修改任何信息；

b) 模拟合法网络设备、视频服务器、游戏服务器、数字版权管理服务器；

c) 中间人攻击；

d) 将视频流重定向到未授权设备。

A.17 未经授权的管理

包括但不限于下列行为：

a) 未经授权使用板载管理应用程序或执行管理命令。例如，篡改调制解调器配置来阻止特定的服务。

b) 伪造或修改管理协议消息。例如，篡改调制解调器配置来阻止或允许特定的协议(例如SNMP)。

c) 修改远程管理信息(如MITM)。

d) 非法订阅用户的自配置操作。例如，重新配置机顶盒以消除带宽限制，以便为其他订阅用户生成慢速连接或为自己增加带宽。

e) 由授权管理代理程序执行未经授权行为。

f) 未经授权的内容管理。例如，加载、删除内容或修改触发日期(对公众开放内容的日期)。

g) 未经授权订阅用户的管理。例如，未经授权的订阅用户获取服务的行为，包括订阅用户查看权限的升级、降级。

附 录 B
（资料性）
互联网使用策略示例

B.1 综述

可接受的信息安全使用策略不宜与开放、信任和公正的企业文化相违背。信息安全致力于保护企业的员工、合作伙伴和企业免受个人有意或无意的非法或破坏性行为。

包括但不限于计算机设备、软件、操作系统、存储媒体、提供电子邮件的网络账户、WWW 浏览和 FTP 等与互联网、内联网、外联网相关的系统，属于企业。在常规操作下，将系统应用于商务目的，以便于为企业创造利益，同时也要保障其客户的利益。

有效安全需通过团队协作获得 。每个计算机用户都有责任了解这些指导策略，并据此开展活动。

B.2 目的

本策略列举了企业中计算机设备的可接受用途，制定这些规则是为了保护员工和企业。不恰当使用本策略将导致企业暴露于风险（包括病毒攻击、网络系统和服务受损以及法律问题等）中。

B.3 适用范围

本策略适用于企业的员工、承包商、顾问、临时工和其他员工（包括所有与第三方有关联的人员）。本策略适用于企业拥有或租用的所有设备。

B.4 策略

B.4.1 一般用途及所有权

虽然企业旨在提供一个具有合理不透明度的网络管理环境，但用户宜注意，他们在企业系统上创建的数据仍属于企业。出于企业保护网络的需要，管理层无法保证在企业所属网络设备上存储信息的保密性。

员工有责任对个人使用网络的合理性做出判断。各部门负责制定有关个人使用互联网、内联网、外联网系统的指导策略。若企业无既定策略，员工宜以部门的个人使用策略为指导，如有不确定情况，员工宜咨询其主管或经理。

出于信息安全的考虑，企业宜对用户认为敏感或易受攻击的任何信息进行加密。有关信息定密的指导原则，请参见信息安全相关的信息敏感性政策。有关加密电子邮件和文档的指导策略，请参阅相关文件。

出于安全和网络维护的目的，企业内的授权个人可以根据信息安全的审计策略随时监视设备、系统和网络流量。

企业保留定期审核网络和系统的权利，以确保遵守本策略。

B.4.2 安全和专有信息

与互联网、内联网、外联网有关的系统所载资料的用户接口，应按企业保密准则的定义，分为机密或非机密两类，详情可参阅相关文件。机密信息包括但不限于：企业自有信息、企业战略、竞争对手敏感信息、商业机密、规章、客户名单和研究数据。员工需遵守必要流程以防止未经授权访问信息。

确保密码安全，不要共享账户。授权用户对其密码和账户的安全性负责。系统级密码宜每季度更

换一次，用户级密码宜每六个月更换一次。

所有的个人电脑、笔记本电脑和工作站都宜配备有密码保护的屏幕保护程序，保护程序的自动激活功能设置在 10 min 或更短时间内，或者在主机无人值守时通过注销（Windows 用户的 control-alt-delete）进行保护。

按照信息安全加密政策对信息进行加密。

由于便携式计算机上的信息特别容易受到攻击，因此宜特别小心。按照“笔记本电脑安全提示”保护笔记本电脑。

除在企业授权情况下，员工从企业的电子邮件地址向新闻组发布的邮件中，宜包含一份免责声明，声明所表达的观点完全是员工自己的，并不代表企业态度。

员工使用的所有连接到企业互联网、内联网、外联网的主机，无论是属于员工的还是企业名下的，除部门或企业指定的情况下，均宜持续使用当前病毒数据库，执行经批准的病毒扫描软件。

员工在打开来自未知发件人的电子邮件附件时宜特别小心，这些附件可能包含病毒、电子邮件炸弹或木马代码。

B.4.3 不当使用

B.4.3.1 不当使用行为

一般情况下，禁止下列行为，员工在履行其合法的工作职责期间可以免受这些限制（例如，某主机扰乱了生产服务，系统管理人员可禁用该主机的网络访问）。

在任何情况下，企业的员工在使用企业拥有的资源时，均不得从事任何违法违规活动。

B.4.3.2 系统和网络行为

包括但不限于下列行为：

a) 侵犯受知识产权和相关法律法规保护的任何个人或企业的权利，包括但不限于安装或传播“盗版”或其他未授权使用的软件产品；
b) 未经授权复制受版权保护的资料，包括但不限于数字化处理和传播受版权保护的图片（书籍、杂志或其他受版权保护的来源）、音乐，以及企业或终端用户安装任何没有有效许可的受版权保护的软件；
c) 导致恶意程序入侵网络或服务器（如病毒、蠕虫、特洛伊木马、电子邮件炸弹等）；
d) 向他人（包括家庭成员）透露个人账户密码或允许他人使用个人账户；
e) 使用企业计算机，主动发起或传播有违当地公序良俗的行为；
f) 以企业账户对产品、项目或服务进行虚假宣传；
g) 做任何超出正常工作职责外的保证声明；
h) 造成安全漏洞或网络通信中断（包括但不限于网络嗅探、洪泛攻击、包欺骗、DoS 和恶意伪造路由信息），安全漏洞包括但不限于员工访问发给非预期收件人的数据，或员工超出职权范围登录未明确授权访问的服务器或账户；
i) 在未事先通知信息安全部门情况下，进行端口扫描或安全扫描；
j) 越权使用未授权主机进行网络监视；
k) 绕过任何主机、网络或账户的用户鉴别或安全流程；
l) 干扰或拒绝向员工主机以外的任何用户提供服务（例如，DoS 攻击）；
m) 通过任何方式（本地或通过互联网、内联网、外联网），使用任何程序、脚本、命令，或发送任何类型的消息，以干扰或禁用用户的终端会话；
n) 向企业以外的各方提供企业员工的信息或名单。

B.4.3.3 电子邮件和通信活动

包括但不限于下列行为：

a) 发送未经请求的电子邮件信息，包括发送“垃圾邮件”或向没有特殊要求的个人发送其他广告资料；
b) 通过电子邮件、电话等任何形式的骚扰（无论信息的语言、发送频率，或信息量）；
c) 未经授权使用或伪造电子邮件标题信息；
d) 以骚扰或收集回复为目的，索取发件账户以外的任何其他电邮地址；
e) 制造或转发“连锁信件”“庞氏骗局”或其他任何类型的“金字塔”骗局；
f) 使用企业网络（由其他网络服务提供商提供的互联网、内联网、外联网）发送未经请求的电子邮件，或通过由企业网络托管或连接的任何服务来做广告。

B.4.4 社交平台

B.4.4.1 员工使用企业系统或个人电脑系统在社交平台上发布内容时，也受本策略的限制。有限且偶尔使用企业系统在社交品台上发布内容是可以接受的，但需以专业和负责任的方式进行，不违反企业的相关规定，不损害企业的利益，不影响员工的正常工作。在企业系统上向社交平台发布内容也受监管。

B.4.4.2 企业的信息保密方案也适用于社交平台。因此，禁止员工在社交平台上发布内容时泄露企业机密、专有信息、商业机密或企业信息保密方案所包含的其他任何内容。

B.4.4.3 员工不得通过社交平台发布任何可能伤害或损害企业及其员工形象、声誉、商誉的内容。员工也不得在社交平台上发表任何歧视、轻蔑、诽谤或骚扰性评论。

B.4.4.4 员工在使用社交平台时也不可将个人陈述、意见或信仰同企业相关联。员工不得以企业赋予的身份表达其个人信仰或观点。员工承担所有与所发布内容相关的风险。

B.4.4.5 在社交平台相关行为中，不得越权或违法使用企业的商标、徽章及任何其他知识产权标识。

B.5 执行

任何被发现违反本策略的员工可能会受到纪律处分，包括终止雇佣关系。

B.6 修订历史

如有修订历史，请列于此处。

参 考 文 献

[1] GB/T 22081 信息技术 安全技术 信息安全控制实践指南

[2] GB/T 25068.2 信息技术 安全技术 网络安全 第2部分:网络安全设计和实现指南

[3] GB/T 25068.4 信息技术 安全技术 网络安全 第4部分:使用安全网关的网间通信安全保护

[4] GB/T 25068.5 信息技术 安全技术 网络安全 第5部分:使用虚拟专用网的跨网通信安全保护

[5] ISO/IEC 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity

[6] ISO/IEC 27033-6 Information technology—Security techniques—Network security—Part 6: Securingwireless IP network access

[7] ISO/IEC 27036(all parts) Cybersecurity—Supplier relationships