网络空间安全管理体系技术规范

文件编号：DNI-GZ-JS-69

技术规范编号：CTS DNI-CS-2026

文档版本：A/0

编制：技术部　　日期：2026.04.20

审核：杨舒　　日期：2026.04.20

批准：杨舒　　日期：2026.04.20

受控状态：受控文件

发布日期：2026年4月20日　　实施日期：2026年4月20日

发布单位：数网信认证服务（北京）有限公同

变更履历

日期	变更描述	版本/版次	审核	批准
2026.04.20	初始发布	A/0	杨舒	杨舒

网络空间安全管理体系技术规范

1 范围

本技术规范提供：

—阐释了互联网安全、网络安全、网络安全与网络安全之间的关系；

—互联网安全的概述；

—识别相关方及其在互联网安全中的角色描述；

—处理常见互联网安全问题的高级指导。

本规范适用于使用互联网的组织。其基于ISO/IEC 27032:2023转换为对网络空间安全提出了信息安全控制要求，是我机构开展网络空间安全管理体系认证的认证依据。

本技术规范特别要求组织已依据GB/T 22080-2025/ISO/IEC27001:2022建立信息安全管理体系并运行，以使达到管理体系的基本特性。

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规范必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本规范；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本规范。

ISO/IEC 27000 信息技术——安全技术——信息安全管理体系——概述和词汇

GB/T 22080-2025/ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 信息安全管理体系要求

ISO/IEC 27002:2022 信息安全 网络安全和隐私保护—信息安全控制

ISO/IEC 27032:2023 网络安全——互联网安全指南

3 术语和定义

为本规范之目的，适用ISO/IEC 27000所载术语及定义，并包含ISO与IEC维护用于标准化工作的术语数据库。

3.1攻击载体

攻击者为实施恶意行为而入侵计算机或网络服务器的途径或手段

3.2攻击者

指蓄意利用技术性与非技术性安全控制措施中的漏洞，以窃取或破坏信息系统及网络，或损害合法用户获取信息系统与网络资源可用性的个人

3.3混合攻击

通过结合多种攻击载体（3.1）以最大化损害严重性及传播速度的攻击

3.4机器人

用于执行特定任务的自动化软件程序

注释1：该词常用于描述通常在服务器上运行的程序，这类程序能自动执行转发或分类电子邮件等任务。

条目注释2：机器人亦指代作为用户或程序代理运行、或模拟人类活动的程序。在互联网领域 ，最常见的机器人是访问网站并收集 内容用于搜索引擎索引的程序，这类程序亦称作蜘蛛或爬虫。

3.5僵尸网络

由远程控制的恶意机器人组成的集合体，这些机器人在受感染计算机上自主或自动运行

示例：分布式拒绝服务（DDoS）节点，其中僵尸网络控制器可指挥用户计算机向第三方网站发送流量，作为协同DDoS攻击的一部分。

3.6网络安全

保护个人、社会、组织和国家免受网络风险的侵害。注1：保护意味着将网络风险控制在可承受范围内。

3.7暗网

互联网中仅能通过特定软件访问的秘密网站网络

3.8欺骗性软件

在未事先告知用户该软件将在计算机上执行何种操作，或未征得用户同意的情况下，擅自对用户计算机执行操作的软件

3.9黑客攻击

未经用户或所有者授权而故意访问计算机系统

3.10黑客行动主义

出于政治或社会动机的黑客行为（3.9）

3.11互联网

全球公共领域互联网络系统

3.12互联网安全

保障互联网信息（3. 11）的保密性、完整性和可用性

注1：此外，还可能涉及真实性、可追溯性、不可否认性和可靠性等其他属性。

注2：请参阅ISO/IEC 27000:2018第3章中对保密性、完整性、可用性、真实性、可追溯性、不可否认性和可靠性的定义。

3.13互联网服务提供商 ISP

向用户提供互联网服务并使其客户能够访问互联网的组织

3.14恶意内容

应用程序、文档、文件、数据或其他资源中嵌入、伪装或隐藏的恶意功能或能力

3.15恶意软件

具有恶意意图设计的软件，包含可能直接或间接对用户和/或用户计算机系统造成损害的功能或

3.16组织

具有自身职能、职责、权限及关系以实现其目标的个人或群体

3.17网络钓鱼

欺诈性过程：通过在电子通信中伪装成可信实体，企图获取私人或机密信息

注1：网络钓鱼可通过社会工程学或技术欺骗手段实施。

3.18潜在不需要的软件

具有欺骗性软件特征的欺骗性软件

3.19垃圾邮件

未经请求的电子邮件，可能携带恶意内容和/或诈骗信息

3.20间谍软件

欺骗性软件（3.8），用于从计算机用户处收集私人或机密信息

注1：信息可包括最常访问的网站等内容，或密码等更敏感的信息。

3.21威胁

潜在的意外事件诱因，可能导致系统、个人或组织遭受损害 (3.16)

3.22特洛伊木马

表面上为用户执行有益功能，但误导用户其真实意图的恶意软件（3.15）

3.23vishing

通过伪装成可信实体实施的语音钓鱼 ，旨在获取私人或机密信息

注1：语音诈骗可通过语音邮件、VoIP（网络电话）、固定电话或手机实施。

3.24水坑攻击

诱导人们访问特定网站的技术，该网站含有（大量）恶意软件。注1：水坑攻击亦称水坑攻击。

3.25万维网 Web

可通过网络访问的信息与服务集合体

4 缩略语

AI 人工智慧

API 应用程序编程接口APT

计算机应急响应小组 计算机应急响应小组分布式

拒绝服务 分布式拒绝服务

DLP 数据防泄漏

DMZ 非军事区

DNS 域名系统

DoSE 拒绝服务

DRE’T 终端检测与响应 文件传输协议

HTTP 超文本传输协议

HTTPS 超文本传输协议安全套接层互联网名称与数字地址分配机构

5 互联网安全、网络安全、网络安全与 网络安全之间的关系

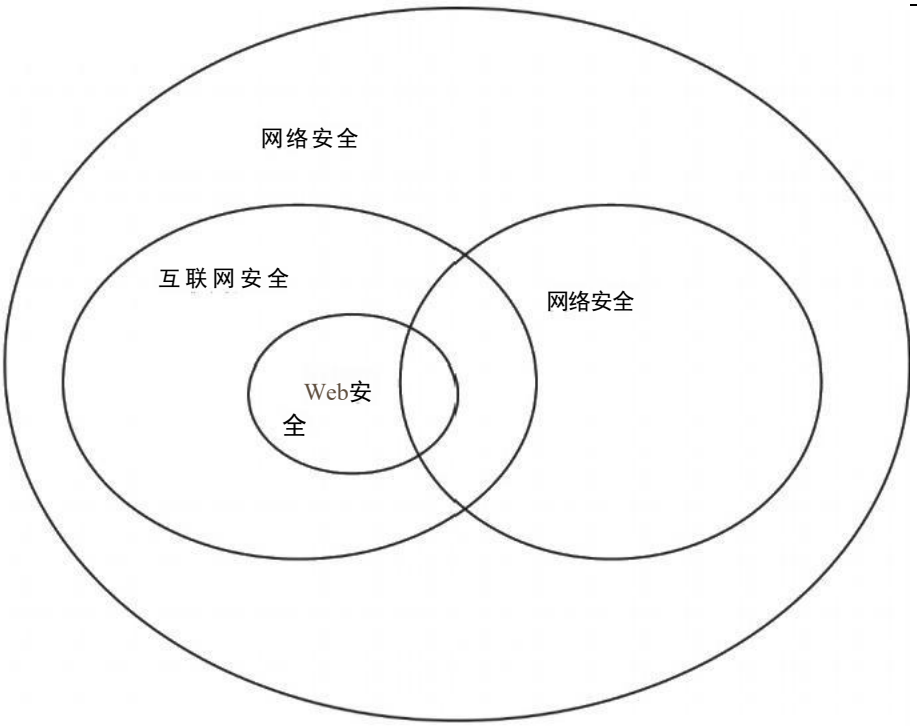

图1—互联网安全、网络安全、网络安全与网络安全之间的关系

互联网是公共领域中相互连接的全球性数字网络系统。互联网上的信息交换也利用移动电话网络，因此该网络是互联网的组成部分。这个全球网络连接了数十亿台服务器、计算机及其他硬件设备。每台设备均可通过互联网连接与其他设备互通。互联网营造了有利于信息共享的环境。

互联网安全作为网络安全的延伸，致力于保护互联网相关服务及关联的ICT系统与网络。这些努力旨在降低组织、客户及其他相关利益相关方面临的互联网安全风险。

互联网安全还确保了互联网服务的可用性和可靠性。通过互联网，各种服务得以提供，例如文件传输服务、邮件服务或任何可与终端用户公开共享的服务。在此背景下，互联网安全涉及通过公共网络安全地交付这些服务。

万维网是互联网信息共享的途径之一(其他途径包括电子邮件、文件传输协议 (FTP)和即时通讯服务)。万维网由数十亿个相互关联的数字文档构成，可通过网页浏览器进行访问。网站是由一组相关网页组成的集合，这些网页经过精心设计和维护，旨在支持单一目标。

网络安全涉及万维网 (www) 环境下的信息安全，以及通过公共网络访问的网络服务安全。网络服务依托HTTP协议实现，该协议允许访问任何已注册的公开URL。 网络安全同样涵盖用于信息交换的HTTP连接安全性。

网络可包含路由器、集线器、布线系统、电信控制器、密钥分发中心及技术控制设备等组件。网络安全广泛涵盖组织内部各类网络，包括局域网、广域网、个人区域网及无线网络。

网络安全涉及网络的设计、实施、运行与优化，以及在组织内部、组织之间以及组织与用户之间识别和处理与网络相关的安全风险。

网络安全则关注信息以数字形式存在于计算机、存储设备及网络中的信息安全风险管理。诸多信息安全控制措施、方法与技术均可应用于网络风险管理。

网络安全还涉及保护联网系统（包括硬件、软件、程序及数据）免受潜在攻击。此类攻击多表现为高度复杂且具有持续性的定向混合攻击。威胁可能源于互联网 ，也可能源于组织在正常业务往来中连接的其他网络系统——包括客户网络、服务提供商网络等内部关联系统。

6 互联网安全概述

互联网用户可识别个人身份的信息（PII）被众多网站及网络服务所采集。其中包括应用服务提供商——这些机构密切追踪用户活动，运用人工智能（AI）技术提供购物、医疗保健、时间管理等领域的推荐服务，并通过大量反馈机制试图让用户的生活与任务管理更为便捷。其中多数网站未经用户许可便收集数据，并将其提供给第三方牟利，用户对此同样毫不知情。相关方正通过网站建立网络存在，开展全球电子商务，提供互联网数字服务，利用公共云服务交付解决方案，并运用基于网络的商业应用与服务。

互联网的许多应用涉及信息交换与服务提供，这些活动并不涉及个人及个人身份信息（PII）。个人身份信息的定义因司法管辖区而异。此类信息与服务的安全性对相关方至关重要。此外，在所谓的物联网中，无论是作为独立设备还是私有网络连接至互联网的硬件设备正迅速增加。物联网中人工智能的自主性与应用，为互联网安全带来了严峻挑战。

尽管互联网能推动重大商业成果，但始终存在诸多需管控的安全风险。必须谨记：互联网最初设计时并未考虑安全特性。企业高度依赖互联网开展业务。由于互联网信任度较低，若缺乏有效管控 ，信息与服务的保密性、完整性及可用性一旦丧失，将对商业运营造成严重不利影响。

虽然有些人谨慎管理自己的网络身份，但大多数人仍会上传个人资料详情与他人分享。许多网站（尤其是社交网络和聊天室）上的个人资料可被第三方下载并存储。这可能导致个人数据被整合成数字档案，面临被滥用、泄露或用于二次数据收集的风险。尽管这些数据的准确性与完整性存疑 ，却形成了难以彻底清除的个人与组织关联链。通信、娱乐、交通、购物、金融、保险及医疗领域的技术发展，正为互联网相关方制造新型风险。由此可见，网络隐私泄露可能引发多重风险。

信息与通信技术的融合、从台式机、笔记本电脑到移动设备及物联网设备的便捷联网方式，以及个人空间的不断压缩，正日益引起恶意行为者和犯罪组织的关注。

这些实体正利用网络钓鱼、垃圾邮件和间谍软件等手段，并开发零日攻击、语音钓鱼、恶意网站及其他欺骗技术，竭力利用网络中发现的任何漏洞。

近年来，互联网安全攻击已从个人为名利而实施的黑客行为，演变为有组织的犯罪或网络犯罪。此前在孤立网络安全事件中观察到的众多工具和流程，如今正被整合用于多层混合攻击，且往往伴随着影响深远的恶意目的。

许多此类工具也可在公共软件库及其他公开资源中获取。攻击目的涵盖人身攻击、身份盗窃、金融诈骗或盗窃，乃至网络黑客行动及互联网信息操纵。大量被盗的个人数据和客户数据同样出现在暗网中，这些数据可能被公开获取。各类组织（尤其是中小企业）应充分认识到在互联网上"操纵"信息所带来的实际后果。这些安全风险正是用户使用互联网时面临的网络风险。

由于互联网是全球公共网络，交易可能源自世界任何角落，攻击亦然。在互联网上开展的多种商业交易模式正成为网络犯罪集团的目标。从企业对企业、企业对消费者到消费者对消费者的服务，所面临的风险本质上是复杂的。

另一重复杂性源于这样一个事实：所有相关方—即使他们并非怀有恶意—对其需求、要求和威胁

的认知各不相同，因此他们列出的风险清单及应对措施也各异。这意味着不存在"万能"的解决方案。

构成交易或协议的标准取决于不同司法管辖区的具体法律和监管环境。这些标准还取决于法律的解释以及关系中各方如何管理其责任。通常，在交易或关系过程中收集的数据使用问题往往未得到充分解决。这最终可能导致信息泄露等安全隐患。

这些互联网问题带来的法律和技术挑战具有深远影响且具有全球性特征。唯有通过信息安全技术界、法律界以及不同地区之间的协作，制定协调一致的战略，方能应对这些挑战。该战略应在国际合作框架内，充分考虑各利益相关方的角色定位及现有举措。

信息在互联网中瞬时传播，这意味着攻击同样可能瞬间发生。由于人类思维难以捕捉这种速度 ，攻击往往在发生很久之后才被发现，而此时损害可能已相当巨大。在多数情况下，攻击者的身份处于隐蔽状态。因此，人们常提议运用人工智能（AI）来抵御此类攻击。

7 相关利益方

7.1 概述

互联网安全相关方包括：

—通过互联网使用服务者；

—通过互联网提供服务者；

—提供互联网基础设施及通信能力者；

—在全球范围内协调互联网的运行；

—制定并执行法律法规。

互联网安全的利益相关方可分为用户（2）、协调机构与标准化组织（7 3）、政府机构（4）、执法机构（7 5）以及互联网服务提供商（6）。

7.2 用户

用户是指使用互联网的个人、最终用户以及私营和公共组织。私营组织包括中小企业（SMEs）和大型企业。 政府及其他公共机构统称为公共组织。当个人或组织接入互联网或使用任何互联网服务时，即成为用户。用户可利用互联网服务、浏览或收集信息，亦可提供特定信息——这些信息可能存在于应用程序空间内，或仅限于该应用程序空间内的特定成员/群体访问，或向公众开放。

用户角色包括但不限于以下类型：

—普通互联网应用用户（或称普通用户），如在线游戏玩家、即时通讯用户或网页浏览者；

—买卖双方：在拍卖及交易平台发布商品服务供买家选购，或反向获取所需商品服务；

—博主及其他内容贡献者（例如维基百科文章作者），其发布的文本及多媒体信息（如视频片段）面向公众或特定受众；

—组织成员（如公司雇员或其他形式的公司关联人员）；

—其他角色，即用户可能在非自愿或未经同意的情况下被分配角色。

示例1:当用户访问需要授权的网站时，无论有意或无意获得访问权限，该用户都可能被标记为入侵者。

示例2：个人作为买卖方参与交易时，可能在不知情的情况下卷入赃物销售或洗钱等犯罪活动。

组织常利用互联网发布公司及相关信息，推广产品与服务。同时将互联网作为网络组成部分，用于收发电子邮件等信息及传输文件等文档。

秉承作为优秀企业公民的相同原则，这些组织应将企业责任延伸至互联网领域，主动确保其在互联网使用中的实践与行为不会给互联网用户群体引入更多安全风险。

主动措施包括：

—通过实施并运行有效信息安全管理体系（ISMS）实现信息安全管理（参见ISO/IEC 27001中对信息安全管理体系的要求 ） ；

—依据ISO/IEC 27002及其他相关标准实施控制措施（无需运行ISMS）；

—安全监控与事件响应机制。

—将安全性纳入软件开发生命周期（SDLC），其中系统内置的安全级别应根据组织数据的关键性确定；

—通过持续的技术和流程更新，定期对组织内用户进行安全教育，并追踪最新技术发展动态；

—在使用过程中发现安全问题时，理解并通过适当渠道与供应商和服务提供商进行沟通。

7.3 协调机构与标准化组织

协调与标准化组织（如ICANN、IETF、W3C等）制定互联网使用及服务提供商技术标准，并指导各组织明确其在互联网中的角色与责任。

7.4 政府机构

政府掌握着国家安全、战略、军事、情报等诸多涉及政府与国家层面的信息，同时还拥有海量涉及个人、组织及整个社会的信息资源。

各国政府应保护本国基础设施和信息免遭未经授权的访问与利用。利用互联网提供电子政务服务的趋势日益增长且不断扩展。这为发起攻击并获取上述信息开辟了新的渠道，若攻击得逞，可能对地区、政府及社会造成严重影响。

政府机构在执法部门间发挥协调作用，是危机爆发时信息传播与资源调配的核心枢纽——无论是国家级还是企业级层面，尤其当遭遇大规模网络攻击时。这亦涵盖计算机应急响应小组（CERT）等机构，具体职责分配需依据不同区域的实际情况而定。

各国政府要求大学和高中实施网络安全教育计划，并确保建立适当的公私合作伙伴关系，配备必要的法律框架，协调执法机构并明确其职责。

7.5 执法机构

执法机构负责执行法规，并要求所有相关方在其国家管辖范围内遵守相关法规。

7.6 互联网服务提供商

服务提供组织可分为两类：

— 为员工及合作伙伴提供互联网接入服务的机构；

— 面向互联网消费者的服务提供商。

此类服务可面向封闭社区（例如注册用户）或公众提供，通过互联网交付应用程序（包括云服务提供商）。消费者亦可成为服务提供商，若其通过互联网提供服务或使其他消费者能够接入互联网。

服务提供商也可理解为运营商或批发商，与接入服务的分销商和零售商相对。这种区分在安全领域 ，尤其是执法层面具有重要意义。当分销商或零售商无法提供充分的安全保障或合法接入时，支持服务往往会回溯至运营商或批发商。互联网服务提 供商（ISP）可通过监控"流量"并提供替代路由或主机来控制流量，从而提供支持。他们还能侦测互联网上的"危险"传输行为。在获得必要法律授权及

用户许可后，他们可过滤危险内容——例如通过"沙盒"解决方案对传输文件进行恶意软件检测。当发现威胁模式时，ISP可向客户发出预警。

8 互联网安全风险评估与 处理

8.1 概述

ISO 31000提供了风险管理的原则和通用指南，而ISO/IEC 27005则为组织的信息安全风险管理提供了指南和流程，支持根据ISO/IEC 27001 建立信息安全管理体系（ISMS）的要求。这些文件提供的指南和流程被推荐用于处理互联网环境中的风险管理。相关方有责任定义其风险管理方法。 在ISO/IEC 27005框架下，可采用多种现有方法论开展风险评估，并管理组织使用互联网过程中涉及的相关威胁、漏洞及网络安全问题所衍生的风险。

在资源有限的组织中，控制措施必须兼顾组织对安全性的需求与资源投入的合理性，以避免控制选择失误。不当的控制选择可能导致额外风险或控制失效。

8.2 威胁

威胁主体是指在攻击执行或支持过程中扮演任何角色的个人或团体。对其动机（宗教、政治、经济等）、能力（知识、资金、规模等）及意图（娱乐、犯罪、间谍活动等）的全面理解，对于评估漏洞与风险、制定并部署控制措施至关重要。

恶意软件可能导致安全控制措施失效（如密码截取与泄露）、信息意外泄露、信息意外篡改、信息破坏及/或系统资源被非法使用。此类软件通常通过病毒、蠕虫和木马程序传播，其危害影响深远。

病毒是一种可执行且可复制的程序，它将自身代码植入合法程序中，旨在破坏宿主计算机（例如删除文件和程序、破坏存储设备及操作系统）。蠕虫在最基础形态下是一种计算机程序，通过向用户通讯录中所有地址发送外发消息实现自我复制并传播至其他计算机，从而耗尽系统资源。此外，蠕虫与病毒类似，可传播破坏宿主的代码。此类代码称为有效载荷（例如勒索软件的文件加密功能，以及安装允许远程访问的系统后门）。特洛伊木马则是伪装或嵌入在合法软件中的恶意程序，其目标与病毒和蠕虫相似，但不同于二者的是，它不会自行复制或传播。

互联网安全对用户个人身份信息（PII）的威胁主要围绕身份问题展开，其根源在于个人信息的泄露或盗取。若个人网络身份遭窃取或冒用，当事人可能被剥夺关键服务与应用程序的访问权限。在更严重的场景中，后果可能从财务损失升级至国家层面的事件。未经授权访问个人财务信息还可能导致资金盗窃和欺诈行为。

示例1:信用信息可在黑市或暗网交易，从而助长网络身份盗窃行为。

示例2:其他威胁生命安全的网络威胁还包括网络欺凌、在线跟踪以及包括儿童剥削和人口贩卖在内的剥削犯罪。

另一种威胁是终端设备（包括个人设备和自带设备BYOD）可能沦为僵尸网络或僵尸程序。计算设备一旦被入侵，便可能成为大型僵尸网络的一部分。组织机构的在线存在及网络业务常遭不法分子蓄意攻击，其意图远不止于恶作剧。

更大范围而言，支撑互联网的基础设施同样可能遭受攻击。虽然这不会永久性破坏互联网功能，但会影响基础设施的可靠性和可用性，进而危及互联网安全。

在国家或国际层面，互联网已成为特定司法管辖区内非法行为滋生的温床。由于互联网的本质特征——尤其是界定边界与疆域的挑战——对其使用方式的监管与控制变得异常困难。

犯罪分子既可合法购买助长其犯罪活动的应用程序、服务和资源，也可通过非法手段获取这些资源以规避侦查追踪。这包括借助僵尸网络获取海量计算资源。

另一类威胁涉及蓄意篡改公开信息或专有数据，或制造虚假信息与骗局——若被误信，将造成严重损害。

8.3 漏洞

漏洞是指资产或控制措施中可被威胁利用的弱点。制造商、软件开发商及其他技术开发者在发现并解决这些弱点后，会发布安全更新和补丁进行修复。随着系统接收补丁，更新或新增元素将被添加。当系统过时、不再获得供应商支持或未更 新至最新版本时，可能引入新的漏洞。相关方应全面了解待评估资产或控制措施，并掌握相关威胁、威胁载体及风险,方能开展综合评估。需特别注意那些尚未发布补丁的零日漏洞。

通过互联网访问的Web应用程序容易受到多种漏洞的威胁，这些漏洞源于设计缺陷、代码编写不当以及生产环境库和可执行文件构建质量低下。此类漏洞的典型例子包括身份验证绕过、数据库注入攻击和跨站脚本攻击。在这些攻击中，攻击者可通过操纵请求来滥用Web服务器的功能。

8.4 攻击载体

攻击载体是指攻击者为实施恶意行为而入侵计算机或网络服务器的路径或手段。

端口扫描器是攻击者使用最久且至今仍非常有效的工具之一。它们扫描面向互联网系统的所有可用端口，以确认哪些端口处于开放状态。这通常是潜在攻击者针对目标互联网系统执行的首要步骤之一。虽然初始攻击总是瞄准面向公众的系统（如路 由器、服务器、防火墙、网站等），攻击者也可能试图利用连接至这些公共系统的私有网络内部资产。

监听通信渠道是一种简单易行的攻击手段，也是最古老的攻击方式之一。复制并分析流量数据对于发现入侵入口点和启动其他威胁载体具有极高价值。攻击者还可通过通信劫持（尾随或搭便车）伪装成合法用户身份或凭证，在用户毫不知情的情况下窃取其资源。

许多网络攻击都是通过恶意软件实施的，例如间谍软件、蠕虫和病毒。信息通常通过网络钓鱼技术收集。攻击可能以单一攻击载体形式发生，也可能作为混合攻击或定向攻击实施。这些攻击可通过多种途径传播，例如可疑网站、未经验证的下载、垃圾邮件、远程利用、零日漏洞利用以及受感染的可移动存储介质。

其他日益普及且日益复杂的攻击机制，是基于社交网站和利用合法网站上的受损文件。合法网站同样可能遭到入侵，其部分文件被篡改后成为实施攻击的媒介。用户往往对常访问的网站抱有隐性信任。 攻击者可采用水坑攻击技术，通过感染高频访问的网站，针对特定终端用户群体实施攻击。除人为攻击者发起的攻击外，受恶意软件感染的计算机还会向周边联网设备发起各类攻击。

技术，通过感染高频访问网站来破坏特定终端用户群体。除人为攻击外，受恶意软件感染的计算机还会向周边联网设备发起各类攻击。

随着点对点应用的普及（常用于共享数字音乐、视频、照片等文件），攻击者正日益精进地利用交换文件作为木马载体，掩饰自身及恶意代码的攻击行为。一旦攻击者通过身份盗用伪装成合法联系人 ，便能诱使他人参与其中，从而为各类攻击开辟新的途径。

另一种技术是IP欺骗 ，攻击者通过篡改消息关联的IP地址，试图伪装成已知可信来源，从而获得对系统的未经授权访问权限。

攻击者不会始终使用相同的攻击途径，而是频繁切换多种攻击方式。某些攻击手段隐蔽性极强，往往在用户察觉时为时已晚。防御者应对此保持警惕，构建针对多重攻击途径的防御体系，而非仅针对已知攻击手段。

物联网设备、智能手机等均可联网。若这些设备在接入组织网络时缺乏有效管控，便可能如同其他联网设备般成为额外 的攻击载体。

高级持续性威胁（APT）是一种旨在长期窃取信息的攻击手段，攻击者通过持续访问组织网络、隐蔽潜伏、横向移动、侦察学习等方式，在网络中长期驻留。

另一种传统攻击手段是暴力破解。该方法通过反复尝试猜测登录凭证、加密密钥或寻找隐藏网页 ，攻击者穷尽所有可能组合 进行尝试，企图破解正确组合以侵入组织网络获取信息。

9 互联网安全指南

9.1 通用原则

相关方可通过评估资产所面临的威胁来识别风险。此类分析有助于选择控制措施以应对风险 ，并将风险降至可接受水平。实施控制措施旨在降低风险发生概率或减轻其后果 ，同时满足相关方的安全要求（无论是直接满足，还是通过指导其他方间接 实现）。

在实施控制措施后，系统仍可能存在漏洞。此类漏洞可能被威胁主体利用。相关方在其他约束条件下，应努力将风险降至最低。相关方在允许资产暴露于特定威胁之前，应确信控制措施足以应对资产所面临的威胁。若相关方不具备评估控制措施所有方面的能力，可寻求外部组织进行评估。

应对互联网安全风险的有效途径需综合运用多种策略，并兼顾各方利益相关者的诉求。

这些策略包括：

—行业特定方法，通过所有相关方的协作来识别和应对互联网问题与风险；

—开展广泛的消费者和员工教育，提供可信赖的资源，指导如何识别并应对组织内部及互联网用户群体中的具体风险；

—创新技术解决方案，帮助消费者抵御已知网络攻击，保持技术更新并防范新型漏洞利用；

—更新立法法规体系，确保跨司法管辖区的司法公正得以实现。

9.2 互联网安全管控措施

9.2.1 通用

大多数组织利用互联网开展多种活动，包括网页浏览、博客撰写、社交网络互动、公共云服务访问，以及信息共享和电子商务业务。这些活动涉及在线交易过程中机密商业信息的共享，其中包含个人隐私数据。作为公共网络，互联网存在特定的独特威胁。若不加以防范，这些威胁将演变为难以应对的攻击事件。

组织应制定政策、流程及响应机制以：

a)制定员工互联网使用准则；

b)界定可通过互联网公开的服务范围；

c)识别威胁、漏洞、攻击途径及其相关风险；

d)界定互联网各类使用者的角色与责任；

e)开展用户安全上网意识教育；

f)明确处理网络安全问题的责任部门；

g)建立网络安全事件响应机制；

h)开展安全演练以检验应对互联网攻击的响应机制。

基于风险评估，可发现各类相关互联网安全风险，并通过下述各项控制措施加以应对。

9.2.2 互联网安全策略

组织应制定并发布关于人员及其他相关方使用互联网的政策，该政策需与安全目标保持一致。此政策将确定可使用的互联网服务类型、授权使用人员范围以及具体安全目标。该政策将指导所有其他关于安全连接及使用互联网的准则。

互联网安全政策应经管理层批准后发布，并传达给相关人员、承包商及外部方，且须获得其确认。该政策应明确授权访问互联网的人员范围、可浏览内容、禁止的网络行为等事项。所有涉及互联网的活动，以及所有适用于互联网安全的具体控制措施的设计、审批、实施、运行和监控工作，均应明确责任归属。

ISO/IEC 27002标准为互联网安全政策提供了进一步指导。

9.2.3 访问控制

访问控制不仅涵盖用户权限，还包括设备、应用程序或自动化流程等其他实体的访问权限。因此 ，所有连接均需经过身份验证，所有操作都应依据业务规则和安全规则所设定的角色与权限获得正式授权，且每个实体都应被赋予最低特权权限。此举可增强对信息和资产访问的可追溯性，同时降低匿名性以提升安全性。

应根据业务和信息价值制定并实施规则，以控制对信息、资产、其他与互联网相关的资产以及信息处理设施的物理和逻辑访问。涉及关键信息、资产、其他与信息相关的资产以及信息处理设施的访问规则，应符合既定的访问控制政策和信息分类政策。

账户应仅限于因工作职责或职能获得授权的用户使用。每位用户应拥有独立账户，不得共享账户，且同一密码不得用于多个账户。

信息、系统、应用程序及服务的访问权限应依据组织访问控制政策与流程进行配置、审查、调整、修改及撤销。特权 访问权限的分配与使用应受到限制和管控。应基于信息访问限制及相关访问控制规则实施安全认证技术与流程。需建立密码管理系统以管理和支持密码创建过程及其质量保障。

直接连接互联网的信息系统（如防火墙基础设施、网络边界设备等）可能存在一个或多个特权实用程序，这些程序具备覆盖系统及应用程序控制的能力。若攻击者入侵任何系统，且这些特权实用程序未受妥善管控 ，则可能导致攻击者获得特权访问权限。

这些程序应由组织充分管控，以防止入侵者获取此类特权实用程序的访问权限并绕过系统及应用程序控制。有效的访问管理应包括：

—定期审查所有访问权限；

—定期审查管理日志。

ISO/IEC 27002与ISO/IEC 29146标准对访问管理提供了进一步指导。

9.2.4 教育、意识培养与培训

组织人员（包括高层管理人员、系统管理员、IT人员及特权用户等）应定期接受主要威胁（如网络钓鱼和语音钓鱼）的更新培训，并掌握预防措施及不当操作时的应对方案。

互联网上每天都有大量新型威胁涌现，这些威胁持续演变，变得越来越隐蔽和复杂。当实施控制

措施来应对攻击时，用户可能并未意识到自己正遭受新型或更复杂攻击的侵害。

组织应通过多种形式（如电子邮件通讯、在线培训及内联网信息推送）定期向员工提供安全意识培训材料，使其了解网络威胁、合规使用义务及事件上报要求。此举既能提升员工认知水平，又能唤起其保护自身与组织的责任意识。

ISO/IEC 27002标准对教育、意识培养及培训提供了进一步指导。

9.2.5 安全事件管理

互联网安全事件涵盖范围广泛，既包括针对组织面向互联网资源的各类网络攻击，也涉及位于这些资源后端的服务器、数据库及应用程序。安全事件可能由互联网任意节点触发，有时发起攻击的主机本身就是遭入侵的主机。某些事件具有高度复杂性，需要特殊技能才能有效应对。安全事件常跨越国界、地域及组织边界，事件发展过程中信息传播与态势变化的速度，往往使响应人员和组织面临时间紧迫的困境。

应建立由事件响应团队（IRT）提供支持的事件管理团队（IMT）， 以赋予组织评估、应对并从事件中汲取经验的能力。事件响应流程应涵盖通过人工或自动手段检测并上报安全事件（包括潜在及实际事件）的机制。组织部署的监控工具可识别安全事件并触发响应流程。威胁情报是关于威胁及威胁行为者的信息，有助于缓解网络空间中的危害事件。信息安全人员应持续扫描社交媒体情报、人力情报、技术情报及深网/暗网情报等威胁情报来源，收集信息并进行分析。

应建立支持信息共享与协调的技术解决方案，以协助准备和应对安全事件及网络安全事件。这是组织机构在实施安全控制措施时应采取的重要步骤。该解决方案应涵盖安全、有效、可靠且高效的信息共享与协调机制。

涉及互联网安全的事件应由组织内指定联系人及其他相关人员或利益相关方予以响应。 实施事件管理程序时，应考虑任何要求在规定时限内向相关利益方报告事件的外部要求（例如向监管机构在规定时限内提交事件通知的要求）。组织应建立并保 持与相关法律、监管及监督机构的联络渠道，同时应与特殊利益团体、专业安全论坛及行业协会保持沟通。

互联网安全领域的相关方亟需建立高效的信息共享、协调机制及事件处理流程。此类协作应以安全可靠的方式开展，同时保 障相关个人的隐私权。众多相关方可能分布于不同地理区域和时区，且可能受制于不同的监管要求。

信息共享与协作涵盖：

—建立信任的关键要素考量；

—协作及信息交换共享的必要流程；

—不同相关方之间系统集成与互操作性的技术要求。

使用互联网的组织应制定并实施信息识别、收集、获取和保存程序，这些信息可在发生安全事件时作为证据使用。若监控日志及其他数字证据证实事件源自他国，则应以符合相关国家法院或国际机构法律认可标准的方式收集证据。

在发生安全事件时，数字证据可跨越组织或管辖边界。此类情况下，应确保组织有权收集所需信息作为数字证据，以供后续 行动使用。正确设置计算机时钟对确保审计日志的准确性至关重要——这些日志既可用于调查互联网攻击事件，也可作为潜在法律行动的证据依据。

通过评估面向互联网系统的安全事件所获得的信息，应用于识别重复或相关事件，从而规划并实

施变更措施以降低未来类似事件发生的概率或影响。可基于安全事件评估结果重新配置入侵防御系统（IPS）和安全信息与事件管理（SIEM）等工具，并启动相关政策修订以预防未来事件。

ISO/IEC 27002及ISO/IEC 27035系列标准为事件管理提供了进一步指导。

9.2.6 资产管理

应识别包含关键信息和应用程序的ICT组件。传统上，组织被要求了解其资产的物理位置，以便充分保护这些资产。组织不仅应建立受控范围内最新ICT资产的清单，还需维护信息资产登记册，记录信息处理、存储、传输的具体位置——无论是在内部网络中，还是使用云/互联网托管解决方案。通过这种方式，组织能够管理信息在任何位置存在的风险，并基于风险评估决定是否允许信息存储在组织控制环境之外。同样地，针对网络组件，组织需明确敏感资产相对于潜在攻击者入口点的具体位置。这可能包括通过防火墙的官方互联网接入点，以及所有其他设备连接（如智能手机、物联网设备）。组织还应识别用于访问敏感ICT资产或在内部网络传输敏感信息的关键路径。这些路径不应被入侵者察觉、访问或监控。缺乏此类认知将导致网络隔离措施失效。该清单应包含网络架构（功能模块位置）与基础设施图，清晰标注所有互联网络的互联网接入/连接点。

应明确、记录并实施资产、其他与互联网相关的资产及相关处理设施的可接受使用规则和处理程序。组织应建立并运用评估程序，以确定信息及其存储和传输所依赖的ICT资产的关键性。这将使组织能够在通用政策和网络安全层面明确界定保护对象及其保护等级。

ISO/IEC 27002标准对资产管理提供了进一步指导。

9.2.7 供应商管理

应制定并实施相关流程与程序，以管理使用供应商所涉及的互联网安全风险。需根据供应商类型及相关风险，与每位供应商共同确立并达成所有相关信息安全要求。针对ICT供应商及其存储、利用或可访问的信息实施风险管理，是制定合同的关键环节，旨在确保组织的信息安全目标得以持续实现。

应与互联网相关供应商（如互联网服务提供商和云服务提供商）建立并记录协议，确保组织与供应商双方就履行相关信息安全要求的义务达成明确共识。组织应与ISP、电信服务商、云服务商及合作伙伴建立开放协作机制，及时通报/预警检测到的入站威胁。需评估并定期监控互联网服务商以安全方式管理约定服务的能力。组织与服务商应就审计权限达成共识。

对于通过互联网访问且由组织订阅的云服务，组织应审查并与云服务提供商协商云服务协议。组织应开展相关风险评估，识别使用云服务相关的风险，并在协议有效期内管理这些风险。云服务协议应涵盖组织的保密性、完整性、可用性及个人身份信息处理要求。对于无法协商协议条款的云服务，组织应保持清醒认知，充分理解使用该服务的风险，并明确在协议有效期内如何管理这些风险。

基于云的工具（如网络会议工具、网络聊天工具和云存储工具）若存在可被恶意行为者利用的固有安全漏洞 ，将对组织构成风险。因此，组织必须建立针对这些云工具使用的安全管控措施。

为满足已识别的互联网安全要求，可在协议中纳入以下条款：

a)法律法规要求，包括互联网服务提供商端的信息保护要求，如防范DDoS攻击及其他攻击手段；

b)各签约方实施约定控制措施的义务，包括访问控制、网络与系统监控、报告及审计；同时明确供应商遵守组织安全要求的责任；

c)事件管理要求与流程（尤其侧重事件修复期间的通知与协作机制）；

d)供应商服务的监控、审查和变更管理，以确保遵守协议中的信息安全条款和条件，并允许监控

服务绩效水平以验证协议遵守情况，监控供应商所做的变更以及供应商服务的变更。

ISO/IEC 27002、ISO/IEC 27036系列、ISO/IEC TR 23187及ISO/IEC 27017提供与供应商相关的进一步指导。

9.2.8 基于互联网的业务连续性

某些业务活动（如基于互联网的交易及其他电子商务活动）依赖于组织内部的互联网基础设施。互联网服务中断可能由恶意行为者的DoS/DDoS攻击、边界设备故障或ISP端中断引发。恶意行为者亦可能对ISP端发起DoS/DDoS攻击，导致互联网骨干网完全瘫痪。信息处理设施应具备满足可用性要求的冗余设计。

任何互联网基础设施中断均构成组织业务连续性风险，需由组织主动应对。作为基础连续性措施，组织应规划从不同ISP采购互联网服务。组织应部署安全措施避免中断，例如为保障网络设备持续性而实施抗DDoS措施。组织亦可要求相关ISP在其网络内部署抗DDoS措施。无论采用何种持续性服务，组织在任何解决方案中都应持续考虑信息安全问题 ，即使处于业务持续性模式时亦不例外。

ISO/IEC 27002、ISO 22301和ISO/IEC 27031提供了与信息通信技术（ICT）连续性相关的进一步指导。

9.2.9 互联网上的隐私保护

多数服务提供商控制或处理个人身份信息（PII）。 当此类信息被用于与数据主体利益相悖的目的时，将引发隐私问题。托管 服务提供商在其网络和数据中心处理PII作为商业服务的一部分。这些服务（包括网站及其他在线应用程序）常被托管订阅者 重新包装并转售给其他消费者（如小型企业及终端用户），并通过互联网提供访问。

若托管用户设置不安全的服务器，或在其网站或应用程序中托管恶意内容，将对消费者安全造成不利影响，包括此类在线应用程序存储的个人身份信息（PII）。因此，服务提供商至少应遵守涵盖用户隐私要求的最低协议条款，以符合最佳实践标准。除面向互联网的网站或应用程序需具备数据保护及个人隐私条款外，服务提供商还应要求在其网络托管的此类网站或应用程序上线前，在应用层实施一套最佳实践安全控制措施。在签约互联网服务前，组织应开展隐私影响评估（PIA），识别可能被使用、收集、处理、存储或传输的个人信息及其相关隐私风险，据此判断风险是否可接受并实施相应管控。此类评估不仅涵盖为提供服务而收集的客户数据，还应包括收集浏览者IP地址或地理位置等元数据网站。组织应在其网站上发布隐私声明，明确告知所有用户使用其在线服务时的相关要求。数据屏蔽应依据组织的访问控制政策和业务需求实施，同时需考虑法律要求。对处理、存储或传输敏感信息的系统和网络应采取数据防泄漏措施。部分互联网浏览器具备技术特性，允许用户自行调整隐私设置。

ISO/IEC 27002、ISO/IEC 27701、ISO/IEC 29100及ISO/IEC 27018标准提供了与隐私相关的进一步指导。

9.2.10 漏洞管理

应及时获取所用信息通信技术系统的漏洞信息。需评估组织面临的漏洞风险，并采取适当措施应对相关风险。应建立、记录、实施、监控和审查硬件、软件、服务及网络的安全配置等各项配置。

提供技术产品（防火墙、入侵检测系统、入侵防御系统等）及服务（网络服务、VoIP服务、托管安全服务等）的组织，应持续有效地实施措施以识别、处理并披露其所供产品与服务的漏洞。基于产品及服务供应商披露的漏洞信息，应实施适当防护 措施以应对相关漏洞。

随着互联网恶意软件的日益泛滥，服务提供商可能收到涉及恶意软件和间谍软件感染及其他安全问题的报告。此类信息对相关厂商评估恶意软件感染风险至关重要，有助于其及时更新必要工具，确保能有效清除或禁用任何新发现的恶意软件或间谍软件。为此，组织应主动联系安全供应商，向其提交相关报告及恶意软件样本以供后续处理，尤其当感染率出现激增迹象时。多数供应商设有专用邮箱接收此类报告或样本，以便进行分析与后续处置。

在计算设备上未经控制地安装软件可能引入安全漏洞。组织应制定并严格执行用户可安装软件类型的政策。当软件补丁有助于消除或降低安全漏洞时，应及时应用这些补丁。

用于互联网运营系统的供应商软件应保持在供应商支持的版本级别。随着时间推移，软件供应商将停止支持旧版本软件。组织应评估在运营系统中使用无支持软件（包括开源软件）的风险。用于运营系统的开源软件应保持在最新适用的版本。

其他漏洞缓解措施包括：

a)变更操作实践；

b)重新配置技术系统；

c)通过管理互联网访问来规避风险；

d)培训员工和用户；

e)实施深度防御措施，即当某项控制措施失效时，另有独立方法持续提供防护；

f)系统安全测试、安全软件开发生命周期（SDLC）以及部署前对补丁和更新的测试。

ISO/IEC 27002、ISO/IEC 30111及ISO/IEC 29147标准为漏洞管理提供进一步指导。

9.2.11 网络管理

减少联网资产的暴露程度可降低与未经授权访问、篡改或损坏相关的风险。应实施控制措施以确保联网信息的安全性，并保护联网服务免受未经授权的访问。需建立控制机制以保障通过互联网传输数据的机密性和完整性，同时保护联网系统与应用程序。可联网系统应受限制管控，允许访问时须实施身份验证。应针对组织互联网基础设施相关的网络设备及系统实施日志记录与监控，以记录并检测可能影响或涉及互联网安全的操作行为。组织应考虑通过将联网系统与私 有网络、DMZ等其他组织网络隔离来管理其安全性。该隔离网络的边界需明确定义，并通过网关（如防火墙、过滤路由器）进行管控。

实施网络安全时应考虑以下事项：

—确保组织内部网络与互联网之间存在受监控且可靠的接口，该接口需对所有实体实施访问控制 ，而不仅限于授权人员。

在授予内部基础设施的访问权限时，还应同时对信息和应用程序进行管控。

—通过建立具备充分访问控制的隔离区或集群，将内部网络划分为关键资产区与通用资产区。采用过滤路由器构建子网并嵌套子网结构 ，避免关键资产存在直达路径。

—监控并分析内部流量，以检测和阻止非法活动。

—确保互联网及其服务（包括与物理设施外人员通信）的访问和使用不受影响。

—确保内部网络通过内部边界防护实现充分隔离 ，将关键组件与入口点及易于访问的内部传输通道隔离。

应制定互联网及网络服务使用规则，至少涵盖以下方面：

a)用户可访问的互联网网络服务及其授权程序；

b)用于保护互联网连接及网络服务访问权限的网络管理措施、技术控制手段及操作规程；

c)访问互联网及互联网服务的手段（例如HTTPS、VPN）；

d)对通过互联网访问的服务进行监控（例如带宽监控、安全信息与事件管理）。

防火墙是关键的网络边界设备，组织应考虑采用能更有效应对互联网攻击的防火墙技术。该设备旨在抵御来自互联网的威胁，防止专有信息向互联网的无控传输。路由器技术可通过内置功能或附加模块增强网络安全性，并能应对拒绝服务（DoS）和分布式拒绝服务（DDoS）攻击等网络风险。

基于网络的入侵检测系统（IDS）和入侵防御系统（IPS）可结合人工智能与机器学习技术，应对包含已知特征模式及行为模式在内的复杂网络攻击。企业可根据自身网络架构，选用集成多种安全模块的网络设备，例如内置防火墙、IPS 、数据防泄漏（DLP）及DNS攻击防护功能的解决方案。

ISO/IEC 27002 及ISO/IEC 27033系列标准为网络安全提供了进一步的指导。

9.2.12 防范恶意软件

反恶意软件通过扫描数据和程序来识别与恶意软件相关的可疑模式。为确保能检测到新型恶意代码 ，必须保证扫描软件始终保持最新状态，理想情况下应实现每日更新。

鉴于新型恶意软件可能利用零日漏洞发起攻击，现有软件可识别已知变种。这包括能识别潜在攻击模式的技术。虽然并非万无一失，但这类软件仍能提供比不使用更高的防护水平。多个主流操作系统虽内置了防御常见恶意软件的功能，但在高风险环境中仍需辅以反恶意软件技术。

反恶意软件措施应扩展至保护不受欢迎的互联网流量及双向数据交换，因用户通常在不知情的情况下接收和发送恶意软件。应实施预防、检测、纠正和恢复措施以抵御恶意软件，同时配合适当的用户意识培养。

组织应考虑以下指导原则：

a)在互联网网关部署反恶意软件，对所有进出互联网的流量进行扫描，涵盖所有授权使用的网络协议；

b)在所有客户端系统（特别是员工用于互联网访问的设备）部署反恶意软件；

c)扫描文件、电子邮件、即时通讯附件、网页及外部链接中的病毒、勒索软件、木马及其他形式的恶意软件；

d)拦截可疑弹窗、网页广告、已知或疑似恶意网站，并通过屏蔽列表阻止未经授权的服务（如聊天频道或网页邮件服务）；

e)提醒用户通过外部链接与外部方交互时存在更高的恶意软件风险；

f)验证恶意软件相关信息的准确性，确保其来源于合格且信誉良好的渠道（如可靠的互联网站点或反恶意软件供应商）；

g)对所有可能向互联网传输数据的服务实施日志记录与监控机制；

h)限制使用未经授权的服务，这些服务能够传输大量数据；

i)实施非授权协议过滤器，例如点对点网络协议；

j)根据漏洞严重程度在规定时限内修复已知系统漏洞，重点关注所有接收互联网流量的系统；

k)配置互联网访问的系统和应用程序，禁用非必要功能（如宏）；

l)制定应对恶意软件攻击的恢复方案，包括所有必要的数据和软件备份（涵盖在线与离线备份）

及恢复措施。ISO/IEC 27002提供了关于防范恶意软件的进一步指导。

9.2.13 变更管理政策

应建立变更管理政策和流程，确保组织能够更便捷地实施IT基础设施变更、管理IT系统与应用程序变更，从而防止意外中断、数据损坏或丢失。组织应将互联网安全相关的变更纳入其变更管理流程，涵盖托管于互联网的系统。这些流程有助于组织对变更进行申请、优先级排序、授权、审批、排期实施变更。变更管理政策需明确系统管理员职责、软件文件导入规范、访问控制等条款。所有网络组件或结构变更（含修改、迁移、移除及新增）均需纳入管理，确保架构与基础设施图纸实时更新。

ISO/IEC 27002标准对变更管理提供了进一步指导。

9.2.14 适用法律法规的识别与合规性要求

互联网正日益成为部署各类在线交易服务的平台。涉及交易细节的保密性、完整性及可用性保护，可能存在数据安全、网络安全及隐私相关的法律法规。

由于涉及数字形式的资金流动，银行交易、支付渠道、基于移动应用的交易及其他电子商务活动通常受到监管。所有与信息安全及网络安全相关的法律、法规、监管要求及合同条款，以及组织为满足这些要求所采取的措施，均应予以识别、记录并保持最新状态。

通过互联网访问的在线系统所维护的记录，应依据法律、法规、监管要求、合同及业务需求，受到保护以防止丢失、毁损、篡改、未经授权的访问及未经授权的披露。这些记录可作为组织依法合规运营的证据，用于防范潜在的民事或刑事诉讼，或向相关方证实组织的财务状况。

ISO/IEC 27002标准就法律法规与合规要求提供了进一步指引。

9.2.15 加密技术应用

密码技术是保障传输信息安全、防止流量分析手段之一。虚拟专用网络（VPN）即为简易解决方案。密码技术在密钥管理及加密设备管理方面存在特定约束，相关设备应视为机密且关键资产予以管控。

应采用密码技术保护通过互联网传输信息的机密性、真实性及/或完整性。虚拟专用网络（VPN）和安全超文本传输协议（HTTPS）的实施均运用密码技术建立安全连接。密码算法、密钥长度及使用规范应遵循最佳实践原则。完善的密钥管理需建立安全流程，涵盖密码密钥的生成、存储、归档、检索、分发、退役及销毁全过程。

所有加密密钥均需防范篡改与遗失风险。此外，公钥与私钥需同时防范未经授权的使用及泄露。用于生成、存储和归档密钥的设备应在必要时实施物理防护。使用加密技术时需注意：不同法规与国家限制可能适用于加密技术的使用及跨境加密信息流动问题。

ISO/IEC 27002标准对密码技术应用提供了进一步指导。

9.2.16 面向互联网的应用程序的安全性

可为互联网基础设施中的系统采用新技术。应分析新技术的安全风险，并根据已知的攻击模式审查设计方案。系统设计阶段应将安全性嵌入其中。还应定期审查系统，确保其在应对新潜在威胁方面保持最新状态，并适应所应用技术和解决方案的发 展。

组织应遵循安全工程原则，包括实施安全开发生命周期 ，以识别并缓解开发中产品与解决方案的风险。此过程需涵盖威胁建模、用户认证技术、供应链组件、安全会话控制、数据验证与净化，并通过安全导向的设计审查来识别潜在风险。

面向互联网系统的安全漏洞。面向互联网的应用程序代码应从安全角度进行设计，其设计前提是

该代码始终可能遭受攻击，无论是因错误还是恶意事件所致。

组织应制定安全合理使用互联网资源的规则，包括限制访问不良或不当网站及网络应用程序，并向员工传达相关规定。此举可有效阻止员工尝试访问此类网站。相关规则应保持及时更新，因这类网站可能包含非法信息、病毒及网络钓鱼材料。限制不良或不当网站的一种技术手段是屏蔽相关网站的IP地址或域名。部分浏览器及反恶意软件技术可自动实现此功能，或可通过配置实现屏蔽。

应用程序的设计与开发应遵循安全编码标准。若应用程序所有者可通过直接远程访问服务器获取脚本，攻击者原则上同样具备此能力。此类情况下，应配置Web服务器以阻止目录浏览行为。组织应记录代码行为，并评估该行为是否可能涉及间谍软件或欺骗性软件的潜在范畴。若涉及后者，组织应聘请具备相应资质的评估人员，依据遵循最佳实践的反间谍软件供应商客观标准，评估代码是否符合其判定标准。此举可确保组织为终端用户提供的软件工具不会被反间谍软件供应商标记为间谍软件。众多反间谍软件供应商均公开其软件评级标准。

组织应为其二进制文件实施数字代码签名，以便反恶意软件和反间谍软件供应商能轻松确定文件所有者。独立软件供应商（ISV）采用包括数字代码签名在内的最佳实践持续开发的软件，可归类为可能安全的软件。若组织发现有助于减少间谍软件或恶意软件问题的有效软件技术，应考虑与供应商合作推广这些技术。

对于通过互联网处理交易的应用程序，应考虑以下事项：

— 为维护交易细节的保密性和完整性所需的保护级别要求；

— 通过互联网传输交易细节时需采用充分的安全控制措施（例如加密传输路径、数字认证）；

— 将交易细节存储于任何公开可访问环境之外，并确保存储介质无法直接通过互联网访问；

— 抵御攻击的弹性要求，包括保护相关应用服务器或确保服务交付所需网络互联可用性的要求；

— 在需要高度依赖软件产品安全性的情况下，应按照ISO/IEC 15408系列标准所述，在通用标准框架下对产品进行独立验证。

安全测试应作为系统或组件接入互联网前的测试环节不可或缺的部分。组织可运用自动化工具（如代码分析工具和漏洞扫描器），并在系统上线前验证安全缺陷的修复情况。

安全测试应涵盖以下内容：

a)安全功能，例如用户身份验证、访问限制、API的安全使用以及密码学应用；

b)安全配置，包括操作系统、防火墙及其他安全组件的配置。

ISO/IEC 15408系列提供应用程序保障的指导。ISO/IEC 27002及ISO/IEC 27034系列提供应用程序安全相关的指导。

9.2.17 终端设备管理

存储于经由或可通过终端设备（如物联网设备、USB设备、自带设备）访问的信息应受到保护。在安全区域携带及使用终端设备应实施适当管控。需制定并实施终端设备安全策略，该策略应涵盖设备防火墙管理、邮件专用过滤工具、互联网安全与过滤、移动设备管理及安全工具、加密技术与入侵检测工具等内容。

随着终端设备逐渐突破组织边界，用户可能通过互联网访问云端及组织内部网络资源，终端安全的重要性愈发凸显。当终端遭受入侵时，必须立即采取行动阻断攻击者并限制进一步损害。企业应在终端部署技术能力，以检测来自未知来源和恶意行为者的异常流量并作出响应。此类技术亦称为终端

检测与响应（EDR）技术。企业需建立机制确保所有适用于终端用户系统及设备的组织安全策略始终处于启用状态。相关技术应确保终端用户无法禁用或绕过其设备上安装的安全功能。

终端设备（包括移动设备）的丢失或遭入侵可能对其中存储的数据构成重大风险。组织应部署技术手段确保能追踪这些设备，并在设备丢失或遭入侵时，即使在恶意行为者窃取数据前 ，也能远程清除设备内容。

ISO/IEC 27002标准对终端设备管理提供了进一步指导。

9.2.18 监控

应生成、保护、保存并分析记录活动、异常、故障及其他相关事件的日志。日志应存放于安全位置以供日志分析和审计。某些法规要求将日志存储特定时长。需对面向互联网的网络、系统和应用程序进行异常行为监控，并采取适当措施评估潜在信息安全事件。

ISO/IEC 27002标准对监控活动提供了进一步指导。