28项网络信息安全规范和标准今日起正式实施

刚经过了四年一遇的日子，正式进入2020年3月份，而今天将有28项重要的项网络与信息安全规范和标准正式实施。

**1、《网络信息内容生态治理规定》最严网络信息审核规定2020年3月1日正式实施，不得散布暴力、恐怖淫秽、禁止网络暴力、人肉搜索等 。**

网络信息内容生产者不得制作、复制、发布含有“危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一”和“损害国家荣誉和利益”等内容的违法信息，应当采取措施，防范和抵制制作、复制、发布含有“使用夸张标题，内容与标题严重不符”和“炒作绯闻、丑闻、劣迹”等内容的不良信息。

网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。

网络信息内容服务使用者和生产者、平台不得开展网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等违法活动。

**2、《GB/T 25058-2019  网络安全等级保护实施指南》**
关注公众号，回复：等保2.0 即可获取[等保2.0系列标准](http://mp.weixin.qq.com/s?__biz=MzUyNjk2MDU4MQ==&mid=2247483873&idx=1&sn=0e858a3665f0f661f2b4686ea0f6e916&chksm=fa07934bcd701a5d819ae95e7141f11d719f4bbc981bf968cb559bd8aa05d5b2675db678ffee&scene=21#wechat_redirect)。

该标准是等级保护2.0系列标准中的重要标准之一，代替十年前发布的GB/T25058-2010，规定了等级保护对象实施网络安全等级保护工作的过程，适用于知道网络安全等级保护工作的实施。

**3、《GB/T 20272-2019 操作系统安全技术要求》**
该标准规定了五个安全等级操作系统的安全技术要求，适用于操作系统安全性的研究、测试、维护和评价。

**4、《GB/T 37962-2019 工业控制系统产品信息安全通用评估准则》**

该标准定义了工业控制系统产品信息安全评估的通用安全功能组件和安全保障组件集合，规定了工业控制系统产品的安全要求和评估准则，适用于工业控制系统产品安全保障能力的评估，产品安全功能的设计、开发和测试也可参照使用。

**5、《GB/T 21050-2019 网络交换机安全技术要求》**
该标准规定了网络交换机达到EAL2和EAL3的安全功能要求及安全保障要求，涵盖了安全问题定义、安全目的、安全要求等内容，适用于网络交换机的测试、评估和釆购，也可用于指导该类产品的研制和开发。

**6、《GB/T 20009-2019 数据库管理系统安全评估准则》**
该标准依据GB/T 20273-2019规定了数据库管理系统安全评估总则、评估内容和评估方法，适用于数据库管理系统的测试和评估，也可用于指导数据库管理系统的研发。

**7、《GB/T 18018-2019 路由器安全技术要求》**
该标准分等级规定了路由器的安全功能要求和安全保障要求，适用于路由器产品安全性设计和实现，对路由器产品进行的测试、评估和管理也可参照使用。

**8、《GB/T 20979-2019 虹膜识别系统技术要求》**
该标准规定了采用虹膜识别技术进行身份识别的虹膜识别系统的结构、功能、性能、安全要求及等级划分，适用于虹膜识别系统的设计与实现，对虹膜识别系统的测试、管理也可参照使用。

**9、《GB/T 37971-2019 智慧城市安全体系框架》**
[关注公众号，回复：37971 即可获取该标准。见：此处下载|安全标准|GBT 37971-2019 智慧城市安全体系框架](http://mp.weixin.qq.com/s?__biz=MzUyNjk2MDU4MQ==&mid=2247483858&idx=1&sn=82d685a10fe0398021ec450cdbcbfeb1&chksm=fa079378cd701a6ef1610f05dc82a8ab4c5223b36a93d0c3048cb431a23b0e8a8deb7978ea48&scene=21#wechat_redirect)

智慧城市是运用物联网、云计算、大数据、空间地理信息集成等新一代信息技术，促进城市规划、建设、管理和服务智慧化的新理念和新模式，是新一代信息技术创新应用与城市转型发展深度融合的产物，是推动政府职能转变、推进社会管理创新的新手段和新方法，是城市走向绿色、低碳、可持续发展的本质需求。本标准以信息通信技术（ICT）为视角，在参考信息保障技术框架（IATF）、信息安全管理体系（ISMS）、防护/检测/响应/恢复（PDRR）和预警/保护/检测/响应/恢复/反击（WPDRRC）的安全模型、网际空间安全指南、关键基础设施网络安全框架、新型智慧城市评价指标体系、智慧城市技术参考框架以及我国信息安全领域标准的基础上，针对智慧城市保护对象和安全目标,从安全角色和安全要素的视角提出了体现智慧城市特点、具有可操作性的安全体系框架。

**10、《GB/T 37973-2019 大数据安全管理指南》**

关注公众号，回复：37973 即可获取该标准。
大数据技术的发展和应用影响着国家的治理模式、企业的决策架构、商业的业务模式以及个人的生活方式。我国大数据仍处于起步发展阶段，各地发展大数据积极性高，行业应用得到快速推广,市场规模迅速扩大。在面向大量用户的应用和服务中，数据采集者希望能获得更多的信息，以提供更加丰富、高效的个性化服务。随着数据的聚集和应用,数据价值不断提升。而伴随大量数据集中，新技术不断涌现和应用，使数据面临新的安全风险，大数据安全受到高度重视。
目前拥有大量数据的组织的管理和技术水平参差不齐，有不少组织缺乏技术、运维等方面的专业安全人员，容易因数据平台和计算平台的脆弱性遭受网络攻击，导致数据泄露。在大数据的生命周期中,将有不同的组织对数据做出不同的操作,关键是要加强掌握数据的组织的技术和管理能力的建设，加强数据采集、存储、处理、分发等环节的技术和管理措施，使组织从管理和技术上有效保护数据，使数据的安全风险可控。本标准指导拥有、处理大数据的企业、事业单位、政府部门等组织做好大数据的安全管理、风险评估等工作，有效、安全地应用大数据，釆用有效技术和管理措施保障数据安全。

**11、《GB/T 20273-2019 数据库管理系统安全技术要求》**
该标准规定了数据库管理系统评估对象描述,不同评估保障级的数据库管理系统安全问题定义、安全目的和安全要求,安全问题定义与安全目的、安全目的与安全要求之间的基本原理，适用于数据库管理系统的测试、评估和采购，也可用于指导数据库管理系统的研发。

**12、《GB/T 37980-2019 工业控制系统安全检查指南》**

**关注公众号，回复：37980 即可获取该标准。**[**见：此处下载|安全标准|GB∕T 37980-2019 工业控制系统安全检查指南**](http://mp.weixin.qq.com/s?__biz=MzUyNjk2MDU4MQ==&mid=2247483882&idx=1&sn=14eb70399914c32257bd69a6317c3925&chksm=fa079340cd701a56061d96d78831f42acebc7d31d943a0dcc6fc266fe01314ae92d8bfa63e3d&scene=21#wechat_redirect)

随着工业化和信息化的深度融合，工业控制系统广泛应用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供、供热以及其他与国计民生紧密相关的領域。工业控制系统指应用于工业領域的数据釆集、监视与控制系统，是由计算机设备、工业过程控制组件和网络组成的控制系统，是工业領域的神经中枢。工业領域使用的控制系統包括监控与数据采集系统(SCADA),分布式控制系统(DCS)、可编程逻辑控制器(PLC)系统等。近年来针对工业控制系统的攻击事件层出不穷，工业控制系统的安全性将直接关系到国家重要基础工业设施生产的正常运行和广大公众的利益。

该标准制定的目的是为了指导我国国家关健基础设施中相关工业控制系统行业用户开展工业控制系統信息安全自评工作,掌握工业控制系統信息安全总体状况，及时有效发现工业控制系統存在的问题和薄弱环节环节，进一步健全工业控制系统信息安全管理制度，完善工业控制系统信息安全技术措施，提高工业控制系统信息安全防护能力，为国家对重点行业工业控制系統信息安全检査等工作提供支撑，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。

该标准輸出了工业控制系统信息安全检査的范围、方式、流程、方法和内容，适用于开展工业控制系統的信息安全监督检査、委托检査工作，同时也适用于各企业在本集团（系统）范围内开展相关系统的信息安全自检査。

**13、《GB/T 37931-2019  Web应用安全检测系统安全技术要求和测试评价方法》**

该标准规定了 Web应用安全检测系统的安全技术要求、测评方法及等级划分，适用于Web应用安全检测系统的设计、开发与测评。

**14、《GB/T 37934-2019 工业控制网络安全隔离与信息交换系统安全技术要求》**

该标准规定了工业控制网络安全隔离与信息交换系统的安全功能要求、自身安全要求和安全保障要求，适用于工业控制网络安全隔离与信息交换系统的设计、开发及测试。

**15、《GB/T 37932-2019  数据交易服务安全要求》**

数据正日益对全球生产、流通、分配、消费活动以及经济运行机制、社会生活方式和国家治理能力产生重要影响。数据交易可以促进数据资源流通,破除数据孤岛，有效支撑数据应用的快速发展，发挥数据资源的经济价值。然而,数据交易面临诸多安全问题和挑战，影响了数据应用的进一步健康发展。为规范数据资源交易行为，建立良好的数据交易秩序，促进数据交易服务参与者安全保障能力提升，本标准将对数据交易服务进行安全规范，增强对数据交易服务的安全管控能力，在确保数据安全的前提下，促进数据资源自由流通，从而带动整个数据产业的安全、健康、快速发展。

该标准规定了通过数据交易服务机构进行数据交易服务的安全要求，包括数据交易参与方、交易对象和交易过程的安全要求，适用于数据交易服务机构进行安全自评估，也可供第三方测评机构对数据交易服务机构进行安全评估时参考。

**16、《GB/T 37933-2019信息安全技术 工业控制系统专用防火墙技术要求》**

该标准规定了工业控制系统专用防火墙（以下简称工控防火墙）的安全功能要求、自身安全要求、性能要求和安全保障要求，适用于工控防火墙的设计、开发和测试。

随着工业化与信息化的深度融合,来自信息网络的安全威胁正逐步对工业控制系统造成极大的安全威胁，通用防火墙在面对工业控制系统的安全防护时显得力不从心，因此急需要一种能应用于工业控制环境的防火墙对工业控制系统进行安全防护。

应用于工业控制环境的防火墙与通用防火墙的主要差异体现在：

——通用防火墙除了需具备基本的五元组过滤外,还需要具备一定的应用层过滤防护能力。

用于工业控制环境的防火墙除了具有通用防火墙的部分通用协议应用层过滤能力外，还具有对工业控制协议应用层的过滤能力。

——用于工业控制环境的防火墙比通用防火墙具有更高的环境适应能力。

——工业控制环境中，通常流量相对较小，但对控制命令的执行要求具有实时性。

因此，工业控制防火墙的吞吐量性能要求可相对低一些,而对实时性要求较高。

——工业控制环境下的防火墙比通用防火墙具有更高的可靠性、稳定性等要求。

**17、《GB/T 37988-2019信息安全技术 数据安全能力成熟度模型》**

关注公众号，回复：37988 即可获取该标准。见：[此处下载|安全标准|GB∕T 37988-2019信息安全技术 数据安全能力成熟度模型](http://mp.weixin.qq.com/s?__biz=MzUyNjk2MDU4MQ==&mid=2247483904&idx=1&sn=cccaedaa42468353cbc75744a5449491&chksm=fa0790aacd7019bca606cab69d4b60c6d416e51a2bb1fe4d58668bd193850e188243d9d13f0d&scene=21#wechat_redirect)

该标准给出了组织数据安全能力的成熟度模型架构,规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全的成熟度等级要求，适用于对组织数据安全能力进行评估,也可作为组织开展数据安全能力建设时的依据。

**18、《GB/T 37972-2019 云计算服务运行监管框架》**

**关注公众号，回复：37972 即可获取该标准。**见：[此处下载|安全标准|GB/T 35279-2017信息安全技术 云计算安全参考架构](http://mp.weixin.qq.com/s?__biz=MzUyNjk2MDU4MQ==&mid=2247483907&idx=1&sn=9e8e34ff3af0bc2978ea2efe63ed8f43&chksm=fa0790a9cd7019bf9acb05c2a55b9d6d7e2dab92df36756add861653064586a2295a55223b12&scene=21#wechat_redirect)

该标准确定了云计算服务运行监管框架，规定了安全控制措施监管、变更管理监管和应急响应监管 的内容及监管活动，给出运行监管实现方式的建议，适用于对政府部门使用的云计算服务进行运行监管，也可供重点行业和其他企事业单位使 用云计算服务时参考。

**19、《GB/T 37935-2019 可信计算规范 可信软件基》**

该标准规定了可信软件基的功能结构、工作流程、保障要求和交互接口规范，适用于可信软件基的设计、生产和测评。

**20、《GB/T 37941-2019 工业控制系统网络审计产品安全技术要求》**

该标准规定了工业控制系统网络审计产品的安全技术要求，包括安全功能要求、自身安全要求和安全保障要求，适用于工业控制系统网络审计产品的设计、生产和测试。

**21、《GB/T 37939-2019 网络存储安全技术要求》**

该标准规定了网络存储的安全技术要求，包括安全功能要求、安全保障要求，适用于网络存储的设计和实现,网络存储的安全测试和管理可参照使用。

**22、《GB/T 37964-2019 个人信息去标识化指南》**

该标准描述了个人信息去标识化的目标和原则,提出了去标识化过程和管理措施。针对微数据提供具体的个人信息去标识化指导，适用于组织开展个人信息去标识化工作，也适用于网络安全相关主管部门、第三方评估机构等组织开展个人信息安全监督管理、评估等工作。

**23、《GB/T 37950-2019 桌面云安全技术要求》**

该标准规定了基于虚拟化技术的桌面云在应用过程中的安全技术要求，适用于桌面云的安全设计、开发，可用于指导桌面云安全测试。

**24、《GB/T 37954-2019 工业控制系统漏洞检测产品技术要求及测试评价方法》**

该标准规定了针对工业控制系统的漏洞检测产品的技术要求，包括安全功能要求、自身安全要求和安全保障要求，以及相应的测试评价方法，适用于工业控制系统漏洞检测产品的设计、开发和测评。

**25、《GB/T 37952-2019 移动终端安全管理平台技术要求》**

该标准规定了移动终端安全管理平台的技术要求，包括安全功能要求和安全保障要求，适用于移动终端安全管理平台产品的设计、开发与检测，为组织或机构实施移动互联应用的安全防护提供参考。

**26、《GB/T 37953-2019 工业控制网络监测安全技术要求及测试评价方法》**

该标准规定了工业控制网络监测产品的安全技术要求和测试评价方法，适用于工业控制网络监测产品的设计生产方对其设计、开发及测评等提供指导，同时也可为工业控制系统设计、建设和运维方开展工业控制系统安全防护工作提供指导。

**27、《GB/T 37955-2019 数控网络安全技术要求》**

该标准提出了数字化工厂或数字化车间的数控网络安全防护原则，规定了数控网络的安全技术要求，包括设备安全技术要求、网络安全技术要求、应用安全技术要求和数据安全技术要求，适用于数控网络安全防护的规划、设计和检查评估。

**28、《GB/T 37956-2019 网站安全云防护平台技术要求》**

该标准规定了网站安全云防护平台的技术要求，包括平台功能要求和平台安全要求，适用于网站安全云防护平台的开发、运营及使用，为政府部门、企事业单位、社会团体等组织或个人选购网站安全云防护平台提供参考。