ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 32920—2023/ISO/IEC 27010:2015
代替 GB/T 32920—2016

信息安全技术
行业间和组织间通信的信息安全管理

Information security technology—Information security management for inter-sector and inter-organizational communications

（ISO/IEC 27010:2015，Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications，IDT）

2023-05-23 发布　　2023-12-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　概念和释义 …… 1
4.1　概述 …… 1
4.2　信息共享团体 …… 1
4.3　团体管理 …… 2
4.4　支持性机构 …… 2
4.5　行业间通信 …… 2
4.6　符合性 …… 2
4.7　通信模型 …… 3
5　信息安全策略 …… 3
5.1　信息安全管理指导 …… 3
6　信息安全组织 …… 4
7　人力资源安全 …… 4
7.1　任用前 …… 4
7.2　任用中 …… 4
7.3　任用的终止和变更 …… 4
8　资产管理 …… 4
8.1　有关资产的责任 …… 4
8.2　信息分级 …… 5
8.3　介质处理 …… 5
8.4　信息交换保护 …… 5
9　访问控制 …… 7
10　密码 …… 7
10.1　密码控制 …… 7
11　物理和环境安全 …… 7
12　运行安全 …… 7
12.1　运行规程和责任 …… 7
12.2　恶意软件防范 …… 7
12.3　备份 …… 8

12.4 日志和监视 …… 8
12.5 运行软件控制 …… 8
12.6 技术方面的脆弱性管理 …… 8
12.7 信息系统审计的考虑 …… 8
13 通信安全 …… 8
13.1 网络安全管理 …… 8
13.2 信息传输 …… 9
14 系统获取、开发和维护 …… 9
15 供应商关系 …… 9
15.1 供应商关系中的信息安全 …… 9
15.2 供应商服务交付管理 …… 9
16 信息安全事件管理 …… 10
16.1 信息安全事件的管理和改进 …… 10
17 业务连续性管理的信息安全方面 …… 11
17.1 信息安全的连续性 …… 11
17.2 冗余 …… 11
18 符合性 …… 11
18.1 符合法律和合同要求 …… 11
18.2 信息安全评审 …… 12
附录 A（资料性） 共享敏感信息 …… 13
附录 B（资料性） 信息交换中建立信任 …… 16
附录 C（资料性） 交通灯协议 …… 19
附录 D（资料性） 组织信息共享团体的模型 …… 20
参考文献 …… 24

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。

本文件代替GB/T 32920—2016《信息技术　安全技术　行业间和组织间通信的信息安全管理》,与GB/T 32920—2016相比,主要技术变化如下:

a) 删除了业务连续性和风险管理中信息共享团体成员实施业务连续性风险评估的实现指南(见2016年版的4.1);

b) 增加了信息共享团体信任的说明(见4.2);

c) 信息共享团体管理中,考虑成员组织间差异时,增加了不同的法律或法规环境(见4.3);

d) 删除了符合性评估的说明(见2016年版的4.6);

e) 增加了按优先级分级说明(见8.2.1);

f) “信息分类”更改为“信息的分级”(见8.2.1,2016年版的7.2)。

本文件等同采用ISO/IEC 27010:2015《信息技术　安全技术　行业间和组织间通信的信息安全管理》。

本文件做了下列最小限度的编辑性改动:

——为与我国技术标准体系一致,将标准名称改为《信息安全技术　行业间和组织间通信的信息安全管理》。

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:山东省标准化研究院、中国网络安全审查技术与认证中心、重庆数字城市科技有限公司、山东曙光照信息技术有限公司、中国电子技术标准化研究院、西安邮电大学、陕西省网络与信息安全测评中心、山东正中信息技术股份有限公司、国家计算机网络应急技术处理协调中心、华为技术有限公司、杭州安恒信息技术股份有限公司、长扬科技(北京)有限公司、阿里云计算有限公司、山东省市场监管监测中心、青岛中盛信息技术有限公司、西安电子科技大学青岛计算技术研究院、济宁市标准信息技术中心、莒县政务服务中心、众安信息技术服务有限公司、济南时代确信信息安全测评有限公司、同智伟业软件股份有限公司、万链指数(青岛)信息科技有限公司、浙江河马管家网络科技有限公司、北京辰光融信技术有限公司、山东鲁软数字科技有限公司、山东和同信息科技股份有限公司、方圆标志认证集团山东有限公司、山东腾翔产品质量检测有限公司、深圳大学、OPPO广东移动通信有限公司。

本文件主要起草人:王曙光、公伟、朱丰雪、范博、魏军、张勇、李丹、尤莉莉、赵延军、周伟光、顾丽旺、王文磊、宋丽华、邵萌、梁伟、赵华、袁一鹏、许立前、万谊平、张建成、许志国、秦扬、胡鑫磊、杨向东、杨锐、邓祥武、刘志强、王栋、王建东、张志为、郑伟、张洪艳、李永发、徐彦霞、程燕、戴洪刚、秦峰、孟繁刚、王永起、贾庆佳、何广丰、张志龙、薛念明、李勋、耿哲、张淑贞、崔浩、刘伟丽、李腾。

本文件及其所代替文件的历次版本发布情况为:

——2016年首次发布为GB/T 32920—2016;

——本次为第一次修订。

引　言

本文件是对 GB/T 22080—2016 和 GB/T 22081—2016 在信息共享团体中使用的补充。本文件中的指南是对信息安全管理体系(ISMS,Information Security Management System)标准族其他标准中通用指南的补充。

GB/T 22080—2016 和 GB/T 22081—2016 采用一种通用的方式处理组织间的信息交换。当组织间交换敏感信息[1)]时,可通过建立信息共享团体(尽管团体成员间存在竞争,但在信息交换过程中他们相互信任即相信对方会对已共享敏感信息采取安全控制)信任接收方。

信息共享团体成员间相互信任是团体有效运行的前提。一方面信息发起方需要信任接收方不会泄露或不当地使用数据;另一方面信息接收方基于发起方的资质,信任发起方提供信息的准确性。以上两方面需要信息共享团体明确有效的安全策略和实践的支持。为达到上述目标,信息共享团体成员需要建立一个涵盖共享信息的通用安全管理体系即信息共享团体的信息安全管理体系(ISMS)。

针对行业间不同团体间敏感信息的共享,由于信息发起方无法了解所有接收方,此时可通过在团体及其信息共享协议之间建立信任来进行信息共享。

1)　行业或组织认为可能造成利益损失但又不能成为国家秘密的信息为敏感信息。

信息安全技术
行业间和组织间通信的信息安全管理

1 范围

本文件提供了信息安全管理体系(ISMS)标准族的补充指南,用于在信息共享团体中实现信息安全管理。

本文件为行业间和组织间通信提供了有关发起、实现、维护与改进信息安全的控制和指南。它为如何使用已建立的消息传递和其他技术方法满足规定要求提供了指南和通用原则。

本文件适用于公共的和私有的、国内的和国际的、同一部门或部门之间等各种形式的敏感信息交换与共享。特别的,本文件可适用于与组织或国家关键基础设施的供给、维护和保护相关的信息交换与共享。本文件旨在支持在敏感信息交换与共享时建立信任,从而促进信息共享团体的国际化发展。

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 22080—2016 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2013,IDT)

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南(ISO/IEC 27002:2013,IDT)

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

注:GB/T 29246—2017 被引用的内容与 ISO/IEC 27000:2014 被引用的内容没有技术上的差异。

3 术语和定义

GB/T 29246—2017 界定的术语和定义适用于本文件。

4 概念和释义

4.1 概述

本文件第 5 章～第 18 章给出了针对行业间和组织间通信的信息安全管理体系(ISMS)指南。

GB/T 22081—2016 定义的控制包含了组织间信息交换的控制,以及公开可用信息的通用分发控制。然而当在组织的团体内共享敏感的且仅限于团体成员公开可用的信息时,通常要求这些信息仅对团体内特定个人可用或者有诸如信息匿名化等安全要求。为满足上述要求,本文件在 GB/T 22080—2016 和 GB/T 22081—2016 基础上定义了附加的控制,提供了附加的指南和解读。

本文件包含 4 个附录:附录 A 给出了组织之间共享敏感信息的潜在好处;附录 B 给出了信息共享团体成员评估信息可信度的指南;附录 C 给出了交通灯协议(一种在信息共享团体中广泛使用的机制,用于表示允许的信息分发);附录 D 给出了一些用于组织信息共享团体的模型示例。

4.2 信息共享团体

具有共同利益或特定关系(诸如团体的成员都属于特定行业,或者团体成员具有相同的地理位置或