ICS 35.240

L 60

团　　体　　标　　准

T/ISC 0070-2024

企业级协同设计安全能力要求

Enterprise-level collaborative design security capability requirements

（发布稿）

2024 - 11 - 26 发布　　2024 -12 - 25 实施

中 国 互 联 网 协 会　　发布

目录

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。

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这些专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、北京尽微致广信息技术有限公司、北京创作美好科技有限公司、北京高德云图科技有限公司、阿里巴巴控股集团、招商银行股份有限公司 中国银行股份有限公司、中国第一汽车集团有限公司 合众新能源汽车股份有限公司、中央美术学院、中国计量大学、北京飞书科技有限公司、东海证券股份有限公司、科大讯飞股份有限公司、浙江零跑科技股份有限公司、北京三快在线科技有限公司、平安银行股份有限公司、天津大学、天津美术学院、中国邮政储蓄银行、北京师范大学、广州小鹏汽车科技有限公司、北京集度科技有限公司、泰康保险集团股份有限公司、中国电信股份有限公司研究院、福建省农村信用社联合社、宁波银行股份有限公司、北京邮电大学、北京汽车研究总院有限公司、江苏常熟农村商业银行股份有限公司、交通银行股份有限公司、京东科技控股股份有限公司、奇瑞汽车股份有限公司、麒麟软件有限公司、华夏银行股份有限公司、龙盈智达（北京）科技有限公司、清华大学国家服务外包人力资源研究院、北京科技大学、国能数智科技开发（北京）有限公司。

本文件主要起草人：王景尧，吴荻，冯艺卓，曾晨曦，马霁阳，罗琨，黄梦楠，孙继成，张信峰，孙峰，曹海啸，何梦醒，张家珲，常天恩，张然，王人杰，陈明，张乐，王妍，刘佳，钟伟，程峰，王帅，赵默涵，李昭璐，吕贵林，刘杰，高杰，王芊，俞书伟，秦笃印，朱斌，朱一冰，王昊，张卓超，马冬冬，沈越然，张立，赵倩，王兆龙，胡君，赵天娇，朱鹏飞，蒋旎，张欣，郭利菊，张健，周雯，蒋希娜，马丁，明芳文，范召国，董智明，刘馨，郝小超，李铁萌，马洋，胡丁丁，李莎莎，潘琳，吴佳虎，陆文杰，黄河东，盖胜平，王双，忻运跃，杨明星，陈芳，杨迎，邓焕玉，何雄，窦金花，李夏光，刘斐。

企业级协同设计安全能力要求

1 范围

本文件规定了企业级协同设计安全能力要求。本标准所涉及的企业级协同办公面向民用类产品设计，可包括但不限于工业产品设计、建筑工程、软件开发、机械制造、医疗设备开发、电影和游戏制作、城市规划等。

本文件适用于企业级协同设计安全能力的评价、测试和指导，也可作为第三方权威评估机构衡量企业级协同设计安全能力的标准依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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/T28452—2012信息安全技术软件系统通用安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 企业级协同设计 Collaborative design

在数字化环境下，企业内部或企业与外部合作伙伴之间，利用信息技术工具和平台，进行跨部门、跨地域、跨时间甚至跨公司的设计类任务协作，以完成共同的任务或实现共同的目标。在协同设计中，团队成员共同参与设计过程，共享知识、技能和观点，以实现更全面和创新的解决方案。

3.2 协同设计安全能力 Collaborative design security capability

协同设计安全能力指的是在协同设计过程中，确保设计数据和信息的安全性和保密性的能力。它涵盖了对设计数据的保护、权限管理、数据传输加密、身份验证、访问控制等方面的措施，以防止未经授权的访问、篡改或泄露设计相关的敏感信息。协同设计安全能力的提升可以增强设计团队之间的信任，保护知识产权，防止数据泄露和不良竞争行为，确保设计过程的机密性和可靠性。

4 概述

4.1 使用场景

企业级协同设计是指在数字化环境下，企业内部或企业与外部合作伙伴之间，利用信息技术工具和平台，进行跨部门、跨地域、跨时间甚至跨公司的设计类任务协作，以完成共同的任务或实现共同的目标。这种协同涵盖了各种规模和形式的合作，如云协作、远程协作、虚拟团队等，旨在通过共享信息、资源和知识，提高工作效率，优化业务流程，降低成本，并促进企业内部的创新和发展。本标准所涉及的企业级协同办公面向民用类产品设计，可包括但不限于以下使用场景：

a) 工业产品设计： 在工业产品的设计过程中，不同专业的设计师和工程师需要协同工作，共同开发新产品。例如，汽车设计团队可能包括外观设计师、内饰设计师、系统工程师、安全专家等，他们需要共同合作，确保设计满足功能性、美观性、安全性以及生产成本的要求。

b) 建筑工程： 建筑工程项目中，建筑师、结构工程师、机电工程师、施工团队等多方需要协同设计，以确保建筑物既美观又实用，同时符合安全标准和预算限制。通过协同设计，各方可以共享信息、讨论方案，并及时解决设计和施工过程中的问题。

c) 软件开发： 软件开发项目中，产品经理、UI/UX 设计师、前端开发者、后端开发者、测试工程师等需要紧密合作，共同开发出满足用户需求的软件产品。团队成员需要通过敏捷开发方法和工具进行沟通和协作，确保软件的设计和开发符合预期目标。
d) 机械制造：机械制造领域的协同设计包括但不限于汽车、民用飞机或航天器的系统设计、结构设计、动力系统设计等多个方面。工程师们需要使用先进的仿真和建模工具来协同工作，确保设计的可行性和性能。
e) 医疗设备开发： 医疗设备的开发需要医生、生物医学工程师、产品设计师、法规专家等多方的协同设计。团队成员能够通过协同设计系统，共同考虑设备的功能性、安全性、用户界面设计以及法规要求，以开发出既有效又安全的医疗产品。
f) 城市规划： 城市规划项目中，城市规划师、交通规划师、环境专家、建筑师、工程师等需要协同设计城市空间，以满足居民的生活、工作和娱乐需求。团队成员需要通过协同设计系统，综合考虑城市的可持续发展、交通流、公共空间设计等多方面因素。

4.2 安全风险

数字化转型驱动了系统集成的需求激增，数据流动性需求变大，传统的安全解决方案越来越不能满足业务需要。跨网络域、跨系统，乃至打通客户和关联企业的特性对“分区分域”的传统安全理念产生了挑战。由于企业级协同设计强调跨部门、跨领域的整合与协作，以打破传统的信息孤岛和部门壁垒，能够实现企业内部资源的最大化利用，但也更容易面临着各类安全风险。

a) 数据泄露风险：在数字化协同系统中，大量的敏感数据（如客户信息、业务数据、知识产权等）在各部门和人员之间共享和传输。如果系统的安全防护措施不到位，数据可能会被未经授权的第三方访问、窃取或篡改，导致数据泄露风险。这种泄露可能源自网络攻击、内部人员操作失误或第三方服务供应商的问题。
b) 网络安全风险：随着企业级协同设计场景意味着数据必须在多样化的业务、平台、设备、用户之间流动，导致网络安全边界变得模糊，难以通过边界防护实现灵活、动态的访问控制需求。同时，数字化协同系统依赖于网络进行数据传输和通信，因此面临着各种网络安全威胁。恶意软件、僵尸网络、钓鱼攻击等可能导致系统被攻击或感染病毒，进而影响系统的正常运行和数据安全。
c) 身份认证和授权风险：企业级协同设计场景下，随时随地接入网络的人员、设备多样性导致安全可控性降低，大量业务数据存放在终端上，一旦发生敏感数据泄露将会给金融机构带来巨大影响。如果数字化协同系统的身份认证和授权机制不完善，可能存在非法用户冒用合法用户身份的风险，或者用户获得超出其权限范围的访问权限。这将威胁到系统的数据完整性和机密性。

4.3 安全体系

为了降低以上安全风险，本文件从数据安全、网络与边界安全、账号体系安全、系统安全和安全管理维度出发，对企业级协同设计的安全能力提出了安全防控要求，旨在确保设计团队在协同工作中能够保护敏感信息和设计数据的安全性。

5 通用数据安全

5.1 数据加密

协同设计过程中，数据的流通与共享相较于传统场景都更为普遍，更容易出现敏感信息泄露的数据安全风险。因此，在协同设计场景中，所有敏感数据在存储和传输过程中，应使用加密算法进行加密，确保数据安全。

5.2 用户隐私保护

用户隐私保护指保护用户的隐私信息，不收集不必要的个人信息，对收集的信息进行合理的使用和存储。

5.3 链接安全

分享的链接可由分享者设置为单次失效、在某一时间段内有效或长期有效，根据数据的安全级别进行发放。

5.4 导入导出

如需导入外部数据、或导出数据，需要经过管理员确认，且有数据传输日志可供追踪。（可选）

5.5 水印能力

提供通过水印展示使用者信息的能力，降低由截图、拍照等行为带来的信息泄露风险。（可选）

6 多模态数据安全

6.1 图像数据

a) 图像加密：应使用加密算法对敏感图像进行加密，确保图像数据的安全性。加密过程不应影响图像的质量或分辨率。

b) 元数据保护：除了图像内容本身，还应保护图像的元数据，防止泄露敏感信息。（可选）

c) 访问控制：确保只有授权用户才能解密和访问图像数据。

d) 加密后验证：加密后应进行验证，确保图像数据的完整性和安全性。（可选）

6.2 语音数据

a) 实时加密：对于实时通信，如VoIP，加密应能够实时处理，不影响通信质量。

b) 压缩数据加密：语音数据通常经过压缩，加密算法应能够处理压缩数据。

c) 格式兼容性：加密后的语音文件应保持与常用音频格式的兼容性，以便在标准播放器中播放。（可选）

d) 端到端加密：在通信过程中，语音数据应实现端到端加密，确保传输过程中的安全。（可选）

6.3 视频数据

a) 高效加密算法：视频数据量大，需要使用高效的加密算法，以减少对播放性能的影响。

b) 多级加密：对于视频内容，可以实现多级加密，以提供不同级别的安全保护。

c) 流媒体支持：对于流媒体视频，加密应支持动态加密，确保实时流的安全。（可选）

d) 播放器集成：加密解决方案应与主流视频播放器集成，以便无缝播放加密视频。（可选）

e) 版权保护：除了保护隐私，视频加密还应支持版权保护，防止未授权的复制和分发。（可选）

f) DRM集成：数字版权管理（DRM）解决方案可以集成到视频加密中，提供额外的版权保护。（可选）

7 网络安全

7.1 零信任

a) 互联网隔离区和内网办公区部署零信任可信应用网关，分别处理来自互联网或内网的访问请求。

b) 内网部署TAC（零信任可信访问控制台），统一控制部署在隔离区、内网办公区的可信应用网关。

c) 内网部署安全工作空间策略服务器，用于安全工作空间策略的管理。（可选）

d) 支持利用零信任技术建立的网络通道实现内网的可信连接，提高了内网数据传输的安全性。（可选）

e) 支持利用内网DNS和内外网TAP配合，实现用户无需根据互联网或内网环境切换接入点，给予用户内外网一致的用户体验。（可选）

f) 支持采用访问控制策略，基于地址、端口、协议、会话、内容的访问控制，支持精细化策略管控。（可选）

7.2 入侵防范

a) 在关键网络节点处检测，防止或限制从外部发起的网络攻击行为。

b) 支持采取技术措施对网络行为进行分析，实现对网络攻击行为的分析。（可选）

c) 应支持集成防病毒引擎、对业务数据整体进行病毒过滤。能够查杀目前已公开的病毒。（可选）

d) 当检测到攻击行为时，能够记录关键攻击信息，并支持报警措施。（可选）

7.3 传输安全

a) 传输层协议应采用TCP或UDP协议。

b) 数据传输过程中应支持TLS 1.2（RFC 5246, 2008）及以上安全协议。

c) 密钥应具备更新机制且支持多版本管理，确保不影响业务持续性。（可选）

d) 账号体系安全（可选）

7.4 账号安全

企业账号能够限制注册方式，使用企业认可的账号注册，且显示公司内的真实姓名、职位，姓名和职位不可由用户随意编辑。

对安全等级较高的场景，宜增加对登录后未产生交互行为的时长限制。（可选）

7.5 关联能力

账号能够与企业认可的账号绑定，离职员工可以同步状态，关闭该账号的全部权限。

7.6 权限管理

由于企业级协同设计涉及不同渠道、不同角色的多用户对数据进行操作，因此需具备细致的管理权限。并支持多团队、多用户批量管理。

例如，企业能够根据员工角色和职责设定不同的访问权限，为每一个设计文件定义不同的权限规则，即哪些用户可以编辑、哪些用户可以查看、哪些用户可以新建或删除文件。

7.7 终端安全

a) 宜在需接入系统的终端中部署包含零信任和安全工作空间功能的统一客户端。（可选）

b) 零信任和安全工作空间权限及策略按照用户及其所使用的终端类型的不同，分配对应的权限和策略。（可选）

8 系统安全

8.1 活动日志

需要记录每个文件的活动日志，记录所有用户的活动及活动时间，包括编辑、数据访问、修改和删除等，以便追踪。

8.2 数据备份

企业能够选择多个历史版本进行备份和恢复数据，防止意外数据损失。

8.3 安全更新

定期发布安全更新，及时修复已知的安全漏洞和问题。（可选）

8.4 本地化部署

设计产生的数字资产需要能够部署在企业内部服务器，外部 IP 访问时应加强安全防控，如外部电脑需报备 mac 地址以申请内网访问权限。（可选）

9 管理能力

9.1 组织架构及人员保障

协同设计安全第一责任人应确保组织与协同设计安全管理相关的职责、权限得到分配、沟通和理解；协同设计安全第一责任人应分配职责和权限，以落实安全管理工作。

9.2 分级管控

a) 组织应在协同设计相关数据资产分类分级的基础上制定不同级别数据的通用管控原则，包括但不限使用审批、权限管理、脱敏、加密等。

b) 组织应识别并确定内部所有数据资产使用场景，并针对不同场景制定明确的审批流程，形成对应审批流程图。（可选）

9.3 持续改进

最高管理层应按计划的时间间隔评审协同设计安全工作开展情况的自评估，并对评估出的问题进行改进和持续跟踪，以确保其持续的适宜性、充分性和有效性。（可选）