ICS 35.240
L 60

# 团　　体　　标　　准

T/ISC XXXX—XXXX

# 在线协作文档 第 2 部分：安全技术要求和测试方法

Technical specification and test method for online-collaboration-document: Part 2 Security capacity

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中　国　互　联　网　协　会　　发 布

# 目　　次

# 前　　言

本标准按照GB/T 1.1-2020给出的规则起草。

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。

本标准由中国互联网协会归口。

本标准主要起草单位：……

本标准主要起草人：……

删除[作者]: 2020

# 引　言

在线协作文档作为办公软件的新生事物，近年来得到了快速的演进和发展，不仅实现了将传统离线文档的简单在线化，其更强大、更丰富的功能、可依据需求提供的信息串联、多形态结构化内容呈现等优势，突破了传统文档以图文编辑、排版为核心的能力边界，可为企业和个人用户提供更定制化的服务，提升用户体验。

当前阶段，在线协作文档产品尚未制定统一的标准要求，多为各家的私有解决方案，不同产品所能提供的能力和体验存在很大差异，相互之间还存在排他性，同时产品的隐私保护和内容合规性等方面未设定统一要求。从产业的长远发展来看，此状态不利于在线协作文档的产品普及推广、以及行业的快速成长。因此，有必要尽快制定行业统一的在线协作文档的规范，协调产业共识，本着促进行业健康发展的原则，形成产品统一要求和考量，从而为该类产品的未来能力发展和普及奠定技术保障。

# 在线协作文档 第 2 部分：安全技术要求和测试方法

## 1 范围

本文件规定了在线协作文档的安全技术要求和测试方法。

本文件适用于在线协作文档的开发者、提供商及专业测评机构开展通用能力测试工作，为提升在线协作文档能力水平、强化测试能力、健全技术手段提供指引和依据。

## 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/T25069—2010信息安全技术术语

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

**在线协作文档 online collaborative documents**

在线协作文档需包含以下三个要素：

文档：作为主要载体（即可供人阅读的信息载体），具备可阅读的信息，并具有永久属性。

在线：在线编辑能力，整体信息存储采用云存储形式，可以做到多设备均可编辑，各设备内文档信息应保证一致性。

协作：协作能力，支持多名用户同时对文档内容进行编辑且文档信息在各用户（包含仅阅览用户）处保持一致的能力。

## 4 安全技术要求

### 4.1 功能安全

#### 4.1.1 备份能力

1、 历史记录查阅要求，历史记录查看/恢复/备份；

2、 如对于历史文档数据，应确保用户需要取回时，可在合理时间内取回所有原始文档数据；（可选）

3、文档副本能力，自动备份能力；

4、非正常关闭的自动恢复能力；（可选）

5、对错误/无效输入具有容错性；（可选）

删除[作者]: 容灾

删除[作者]: 功能

设置格式[作者]: 缩进: 悬挂缩进: 5.6 毫米, 编号 + 级别: 1 + 编号样式: 1, 2, 3, ... + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 7.4 毫米 + 缩进位置: 13 毫米

删除[作者]: 回

删除[作者]: 。

#### 4.1.2 身份认证功能

支持登录功能，不同用户仅可通过自身用户角色参与在线协作文档。

## 4.2 应用安全

### 4.2.1 系统安全

1、禁止存在破坏操作系统原有安全框架，严重违反原有系统安全设计原则，

2、所有能对系统进行管理的人机接口以及跨信任网络的机机接口必须有接入认证机制，标准协议没有认证机制的除外。（可选）

3、服务端数据运维操作，应具备完整详细的审计日志。（可选）

### 4.2.2 存储安全

1、文档加密存储，加密方案，加密算法；

2、不能出现内容丢失、被篡改等问题、需要保留全部历史版本；（可选）

3、存储的数据应具备加密能力，应用开发及运维人员也无法查看源数据；（可选）

### 4.2.3 传输安全

传输加密要求，算法。包含传输的链路安全和被传输数据自身的加密要求，不得明文传输用户数据。

### 4.2.4 安全管理

应具备日志管理、三权分立角色的划分。

## 4.3 数据安全

1、用户数据（包括文档内容）的读取需经用户确认

2、不应存在未明示用户且未经用户同意收集使用用户数据（含文档内容），主要涉及增删改操作（可选）

3、不应在日志中记录用户文档内容相关信息（可选）

## 4.4 权限设置

账号登录；

个人权限：创作者、管理员、协作者

企业权限（可选）：平台方不得非法查看、保存、删除用户隐私内容；
文档传阅，文档上传方不得利用在线文档进行违反法律规定的行为；

高级权限（可选）：细粒度权限管控，可设置复制、水印、访问期限，同时提供用户安全水印、数字签名、加密等方式，避免文档内容外泄。

# 5 安全测试方法

## 5.1 功能安全

| | |
|---|---|
| 编号 | 4.1.1 备份能力 |
| 预置条件 | 用户登录系统 |
| 测试方法 | 1. 检查在线协作系统同一用户在不同时间编辑同一个文档，是否保存为不同的历史文档版本；<br>2. 检查在线协作系统不同用户在系统中编辑同一个文档，是否保存为不同的 |

设置格式[作者]: 缩进: 首行缩进: 0 字符

删除[作者]: 1、

删除[作者]: 可能被外界质疑为后门的行为，

删除[作者]: 2

删除[作者]: 一定期限内的

设置格式[作者]: 非突出显示

删除[作者]: 内容安全

应支持本地化和云端数据的内容安全检测。

设置格式[作者]: 突出显示

删除[作者]: 针对用户数据的需满足国家相应法律法规。

删除[作者]: 非法

删除[作者]: （可选）

设置格式[作者]: 突出显示

删除[作者]: 容灾备份功能

设置格式[作者]: 突出显示

| | |
|---|---|
| | 历史文档版本；<br>3.检查在线协作系统有权限的用户是否可以访问文档历史版本；<br>4.检查在线协作系统有权限的用户是否可以将历史版本恢复为当前版本；<br>5.检查在线协作系统用户在文档编辑界面下，编辑文档内容，关闭网页或软件，重新打开刚才编辑的文档，是否能恢复关闭之前的文档内容；<br>6. 检查在线协作系统用户在文档编辑界面下，编辑文档内容，断掉网络，继续编辑文档，重新联网后是否能将断网后编辑的文档内容同步到云端； |
| 预期结果 | 1.在线协作系统同一用户在不同时间编辑的文档自动保存为不同版本的文档；<br>2.检查在线协作系统不同用户在系统中编辑的文档自动保存为不同版本的文档；<br>3.在线协作系统有权限的用户可以访问文档历史版本，可以打开不同版本的历史文档；<br>4.在线协作系统有权限的用户在查看历史版本文档是，可以操作将历史文档恢复为当前版本，且能正常恢复；<br>5.在线协作系统有权限的用户在文档编辑界面下，编辑文档内容，关闭网页或软件，重新打开刚才编辑的文档.可以正常查看、编辑关闭网页和软件关闭之前的内容；<br>6.在线协作系统重新联网后，编辑的内容可以自动同步到云端； |

| | |
|---|---|
| 编号 | 4.1.2 身份认证功能 |
| 预置条件 | 系统管理员登录系统 |
| 测试方法 | 1.系统管理员创建用户账号<br>2.用户输入正确的帐号和密码进行登录；<br>3.用户输入错误的帐号或密码进行登录； |
| 预期结果 | 1.用户账号可以正常创建；<br>2.用户可以正常登录；<br>3.用户不能登陆，且能弹出错误提示； |

## 5.2 应用安全

| | |
|---|---|
| 编号 | 4.2.1 系统安全 |
| 预置条件 | 无 |
| 测试方法 | 1.检查在线协作系统是否具有口令安全性验证功能；<br>2.检查在线协作系统是否具有身份验证功能；<br>3.检查在线协作系统是否具有用户权限验证功能；<br>4.检查在线协作系统是否具有非授权攻击验证功能；<br>5.检查在线协作系统是否具有访问控制策略验证功能；<br>6.检查在线协作系统是否具有用户行为日志，文档操作日志记录功能； |
| 预期结果 | 1.在线协作系统可以接受有效的密码<br>2.在线协作系统可以拒绝无效的密码；<br>3.在线协作系统对于无效的用户或密码登陆有提示； |

删除[作者]: 7.检查在线协作系统是否具有配置管理验证功能；
8.检查在线协作系统是否具有功能失效、异常带来的安全风险验证功能；

| | |
|---|---|
| | 4.在线协作系统支持将超时不操作用户强制退出系统；<br>5.在线协作系统对于弱口令进行信息提示强制修改；<br>6. 在线协作系统对于非授权攻击验证，是否采取应对措施，如：用户冻结、IP 速率限制、延时操作等；<br>7.在线协作系统可以接受有权限的用户访问文档；<br>8.在线协作系统可以拒绝没有权限的用户访问文档；<br>9.在线协作系统具有操作日查看功能，具有操作日志查询功能； |

| 编号 | 4.2.2 存储安全 |
|---|---|
| 预置条件 | 无 |
| 测试方法 | 1.检查文档在云端采用加密存储功能；<br>2.检查文档在云端采用碎片化存储功能； |
| 预期结果 | 1. 存储文档可在服务器端均进行数据完整性验证，确保文件独一无二防止篡改；<br>2.同一份文档分布式存储于多个节点，确保硬盘 copy 的方式无法获得完整的文档； |

| 编号 | 4.2.3 传输安全 |
|---|---|
| 预置条件 | 无 |
| 测试方法 | 1.检查系统网络连接是否使用了加密协议，传输的数据本身是否被加密；<br>2.检查用户端和服务端是否进行了证书校验；<br>4.检查传输的数据是否采用碎片化传输； |
| 预期结果 | 1.在线协作系统网络连接使用了加密协议或在线协作系统产生的数据在传输过程中通过密文形式传输；<br>2.在线协作系统用户端和服务端进行了证书校验；<br>3 在线协作系统产生的数据在传输过程中均是经过加密和模糊的数据碎片，任何第三方通过窃听、嗅探、拦截等非法手段获取的数据都是不可读的无效数据 |

| | |
|---|---|
| | |
| | |
| | |
| | |

| 编号 | 4.2.4 安全管理 |
|---|---|
| 预置条件 | |
| 测试方法 | 1.检查在线协作系统是否具有日志审计功能；<br>2.检查在线协作系统审计记录是否包含用户、时间、内容等完整信息； |

删除[作者]: MD5 哈希校验或其它手段验证

删除[作者]: HTPPS

删除[作者]: 3.

删除[作者]: 检查传输的数据本身是否被加密；

删除[作者]: HTPPS

删除[作者]: 3.在线协作系统产生的数据在传输过程中通过密文形式传输；

删除[作者]: 4.

删除[作者]: 编号

删除[作者]: 4.2.4 内容安全（可选）

删除[作者]: 预置条件

删除[作者]: 测试方法

删除[作者]: 1.检查系统是否具有敏感词库功能；
2.检查系统是否可以根据敏感词库检测本地文档、在线文档；

删除[作者]: 预期结果

删除[作者]: 1.在线协作系统具有敏感词库功能，可以添加、修改、删除敏感词；
2. 在线协作系统可以根据敏感词库对本地文档、在线文档内容进行检测，包含敏感词的文档会进行提示；
3.带有敏感词的文件在文件上传和下载都收到严格管控；

删除[作者]: 5

| | |
|---|---|
| 预期结果 | 1.在线协作系统具有日志系统模块，文件编辑、删除、分享等操作后会记录在日志系统；<br>2.在线协作系统具有详细的记录了文档创建、编辑、删除、分享等动作的时间、操作人、文档类型等信息； |

5.3 数据安全

| | |
|---|---|
| 编号 | 4.3 数据安全 |
| 预置条件 | |
| 测试方法 | 1、 文档开发者应提供用户数据隐私协议全文内容并提供选项让用户自行勾选；<br>2、 提供日志脱敏证明截图 |
| 预期结果 | 1、用户数据（包括文档内容）的读取需经用户确认<br>2、不应存在未明示用户且未经用户同意收集使用用户数据（含文档内容），主要涉及增删改操作<br>3、不应在日志中记录用户文档内容相关信息（可选） |

5.4 权限设置

| | |
|---|---|
| 编号 | 4.4 权限设置 |
| 预置条件 | |
| 测试方法 | 1.检查在线协作系统是否提供多种数据安全权限控制的标准接口，支持精确到每一个按钮的用户权限；<br>2.检查在线协作系统权限设置设置是否支持水印功能； |
| 预期结果 | 1. 在线协作系统具有多种数据安全权限控制的标准接口，支持精确到每一个按钮的用户权限；<br>2.在线协作系统数据安全权限设置具有水印 |

设置格式[作者]: 编号 + 级别: 1 + 编号样式: 1, 2, 3, ... + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 毫米 + 缩进位置: 6.4 毫米

删除[作者]: 编号

4.3 数据安全

预置条件

测试方法

1. 检查当用户在系统首次注册的时候启用多重认证机制，例如特定问题验证、企业邮箱随机码、预留手机验证码等方式；

2.检查在线协作系统是否将用户的敏感个人信息，比如姓名、手机、身份证号和邮箱等，采用可逆加密之后存储；

预期结果

1. 在线协作系统注册功能具有多重认证机制，例如特定问题验证、企业邮箱随机码、预留手机验证码等方式；

2.在线协作系统存储用户信息至少采用 SHA（安全散列算法，Secure Hash Algorithm）-2256 和较新的国密等的算法进行加密；

删除[作者]: 文字

删除[作者]: 、查看者用户 ID 水印、图片水印、水印的适用范围、使用方式、显示方式及透明度等细粒度设置

删除[作者]: 文字

删除[作者]: 、查看者用户 ID 水印、图片水印功能，能管理水印的适用范围、使用方式、显示方式及透明度等信息；

# 附 录 A
（规范性附录/资料性附录）
XXX