TC260-PG-20201A

网络安全标准实践指南

—远程办公安全防护

（v1.0-202003）

全国信息安全标准化技术委员会秘书处

2020 年 03 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称“实践指南”）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准化技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

声　明

本实践指南版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译实践指南的任何部分。凡转载或引用本实践指南的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本实践指南得到中国电子技术标准化研究院、华为云计算技术有限公司、阿里云计算有限公司、三六零科技集团有限公司、深圳市腾讯计算机系统有限公司、奇安信科技集团股份有限公司、珠海金山办公软件有限公司、北京飞书科技有限公司等单位的技术支持。

摘　要

本实践指南分析了在线会议、即时通信、文档协作等典型远程办公应用场景中存在的主要安全风险，从安全管理、安全运维等方面，给出了具体的安全控制措施建议，为远程办公安全防护提供参考。

关键词：远程办公；风险；安全控制措施

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

目 录

全国信息安全标准化技术委员会 NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

一、适用范围

本实践指南分析了远程办公面临的主要安全风险，针对远程办公系统使用方和用户分别提出了安全控制措施建议。

本实践指南可为使用方和用户开展安全远程办公提供指导。

二、术语和定义

1. 远程办公

利用远程办公系统，在办公场所以外地点开展的工作相关活动。

2. 远程办公系统

支撑远程办公活动的信息系统。

3. 远程办公系统使用方

使用远程办公系统的组织，简称使用方。

注：使用方包括政府部门、科研机构、企事业单位等。

4. 用户

使用远程办公系统的使用方工作人员，或与使用方存在工作关系的人员。

5. 远程办公系统供应方

提供远程办公系统的组织，简称供应方。

注：供应方和使用方可以为同一组织，也可为不同组织。

6. 设备

用于远程办公的信息技术产品。

注：设备通常包括个人计算机、移动终端等。

7. 用户自有设备

用户用于远程办公的，未按照使用方安全要求进行管理的个人设备。

8. 功能扩展模块

基于远程办公系统编程接口开发的，用于扩展远程办公系统功能的模块。

三、远程办公典型场景

使用方通过部署远程办公系统，为用户提供远程办公服务。本实践指南分析的安全风险和提出的安全控制措施**适用于通过云计算平台部署的远程办公系统**。该部署方式下典型的远程办公场景包括：**在线会议、即时通信、文档协作，以及基于功能扩展模块实现的协同办公，**例如，在线签到、健康情况汇总、活动轨迹填报等。

注：其他远程办公系统部署方式，例如，通过虚拟专用网（VPN）技术或自建应用服务器实现的远程办公访问等，不属于本实践指南讨论范围。

四、安全风险分析

远程办公的主要安全风险包括：

供应方安全风险。目前，提供远程办公系统的供应方安全能力参差不齐，部分供应方在安全开发运维、数据保护、个人信息保护等方面能力较弱，难以满足使用方开展安全远程办公的要求。

远程办公系统自身安全风险。在线会议、即时通信、文档协作等办公场景下系统安全功能不完备，系统自身的安全漏洞，不合适的安全配置等问题，将直接影响使用方和用户的远程办公安全。

数据安全风险。远程办公场景中，通过远程办公系统可访问使用方的数据，由于数据访问权限的不合理设置、远程办公系统自身的安全漏洞、用户不当操作等，可能导致使用方数据泄漏。此外，由于远程办公系统基于云计算平台部署，使用方可能失去对数据的直接管理和控制能力，存在数据被非授权访问和使用的风险。

设备风险。用于远程办公的设备，特别是用户自有设备，在接入远程办公系统时，由于未安装或及时更新安全防护软件，未启用适当的安全策略，被植入恶意软件等原因，可能将权限滥用、数据泄露等风险引入使用方内部网络。

个人信息保护风险。远程办公系统的部分功能（例如，企业通信录、健康情况汇总、活动轨迹填报等），可能收集、存储用户的个人信息（例如，姓名、电话、位置信息、身份证件号码、生物特征识别数据等），存在被滥采、滥用和泄露的风险。

网络通信风险。用户和远程办公系统通常利用公用网络进行通信，存在通信中断，通信数据被篡改、被窃听的风险。同时，远程办公系统可能遭受恶意攻击(例如，分布式拒绝服务攻击等)，导致办公活动难以进行。

环境风险。远程办公通常在居家环境或公共场所进行。居家环境

中，由于家用网络设备安全防护能力和网络通信保障能力较弱，存在网络入侵和通信中断风险。公共场所中，由于网络环境和人员组成复杂，存在设备接入不安全网络、数据被窃取、设备丢失或被盗等风险。

业务连续性风险。远程办公增加了使用方关键业务、高风险业务的安全风险，远程办公系统可能由于负载能力、访问控制措施、容灾备份、应急能力等方面的不足导致业务连续性风险。

人员风险。用户可能由于安全意识缺失或未严格遵守使用方的管理要求，引入安全风险，例如，将设备、账号与他人共享导致对使用方业务系统的恶意攻击；采用弱口令造成身份仿冒等。

五、安全控制措施

（一）使用方安全

1 概述

使用方在开展远程办公前，应充分理解本实践指南第四章中的安全风险。使用方应认识到并非所有业务都适合通过远程办公开展，应综合分析远程办公可能带来的收益，面临的安全风险，以及可采用的安全措施后做出决策。为有效防范远程办公安全风险，使用方应从管理和技术两方面采取安全控制措施。

2 管理要求

2.1 远程办公需求分析

使用方应对业务、数据、业务系统进行安全风险分析，明确可用于远程办公的业务、数据和业务系统，以及相关安全需求。

2.2 供应方和远程办公系统选择

使用方:

a) 应重点考虑供应方的安全能力，包括但不限于安全开发运维、数据保护、个人信息保护等方面;

b) 应充分评估远程办公系统的安全性，按照 3.1 的安全要求选用远程办公系统，重点考虑远程办公系统与网络安全相关标准的符合性、数据存储位置、弹性扩容能力等;

c) 宜选取通过云计算服务安全评估的云计算平台，用于部署远程办公系统。

2.3 运维管理

使用方:

a) 应指定专门人员或团队负责远程办公安全;

b) 应开展远程办公系统配置管理，对安全策略、数据存储方法、身份鉴别和访问控制措施的变更等进行管理;

c) 应制定远程办公安全事件应急响应流程以及应急预案，定期开展应急预案演练;

d) 应根据业务和数据的重要性，制定备份与恢复策略;

e) 应要求供应方提供运维服务，例如，在线技术支撑、应急响应等，保障远程办公系统稳定运行。

2.4 管理制度

使用方:

a) 应制定远程办公安全管理制度，内容包括但不限于办公环境安全、数据安全、设备安全、个人信息保护、安全配置、通信安全、备份与恢复安全等;

b) 应制定远程办公安全操作细则，定期开展远程办公安全教育和培训，提升用户安全意识。

3 技术要求

3.1 远程办公系统安全

3.1.1 服务端安全

3.1.1.1 系统安全要求

使用方采用的远程办公系统应满足 GB/T 22239 《信息安全技术 网络安全等级保护基本要求》、GB/T 31168 《信息安全技术 云计算

服务安全能力要求》、GB/T 35273《信息安全技术 个人信息安全规范》的相关要求。

3.1.1.2 在线会议安全

远程办公系统具备在线会议功能的:

a) 应具备身份鉴别功能，仅授权人员可以参加在线会议;

b) 会议管理员应能够设置参会用户权限;

c) 应支持加密方式存储、传输会议材料;

d) 在会议期间，宜提供参会人员关闭音频、视频设备的功能。

3.1.1.3 即时通信安全

远程办公系统具备即时通信功能的:

a) 应加密存储即时通信消息;

b) 应提供账号管理、即时通信消息群成员的安全设置等功能;

c) 宜提供用户撤回即时通信消息的功能。

3.1.1.4 文档协作安全

远程办公系统具备文档协作功能的:

a) 应支持加密方式对在线协作文档进行传输、存储;

b) 应提供操作审计功能，对重要操作（例如，文档的删除、复制等）进行记录;

c) 应在审计记录中包含账号、操作等信息;

d) 应具备文档内容防泄漏功能，例如，文档加密等;

e) 文档分享链接应仅对授权用户可用;

f) 文档分享链接宜根据分享范围进行控制，例如，限制访问人员等;

g) 宜提供文档数据恢复功能;

h) 宜对文档操作进行权限控制。

3.1.1.5 接入安全

远程办公系统具备功能扩展模块的:

a) 应在接入远程办公系统前进行安全审核，例如，漏洞修复情况审核、内容安全审核;

b) 应具备身份验证、权限管理、输入检验、文件操作管理、数据加密等安全措施;

c) 在访问使用方的敏感数据前，应获得授权。

3.1.2 客户端安全

3.1.2.1 应用程序安全

远程办公系统的应用程序:

a) 应具备运行环境安全和程序完整性检测功能，例如，防篡改检测、模拟器检测等;

b) 应使用安全加固措施，例如，防止反编译、重打包等;

c) 应对使用过程中产生的数据（包括但不限于数据文件、日志文件、数据库文件、配置文件、密钥文件等）进行保护，例如，使用加密存储、安全沙箱等技术;

d) 应保护身份鉴别信息，例如，使用设备登陆检测等技术;

e) 应使用安全协议，例如，传输层安全协议（TLS）、因特网安全协议（IPSec）等，保护传输的保密性和完整性;

f) 应具备权限管理功能，允许使用方和用户根据远程办公需求调整权限;

g) 宜使用多因素鉴别方法对用户身份进行鉴别;

h) 宜具备信息防窃取和数据溯源措施;

i)宜使用安全组件，例如，安全键盘等。

3.1.2.2 浏览器应用安全

远程办公系统的浏览器:

a) 应使用安全的浏览器内核，避免已知漏洞被利用;

b) 应具备恶意网址的识别和拦截能力;

c) 宜具备用户名、Cookie、缓存的加密功能;

d) 宜具备浏览器插件、扩展的黑名单和白名单机制，防止恶意插件、扩展的安装、加载和运行。

3.2 访问控制

使用方:

a) 应建立适用于远程办公的访问控制机制，包括审核用户权限申请、定期审核用户权限、及时清除过期权限等;

b) 应对用户开放远程办公所需的最小权限，禁止用户账号共享。

3.3 业务系统安全

使用方:

a) 应划分业务安全域，对不同业务安全域进行隔离;

b) 应统一配置远程办公业务，最小化开放业务所需的服务和端口;

c) 应维护业务系统安全基线，确保相关安全补丁及时更新;

d) 宜持续对访问行为进行监控和分析，识别并及时阻断恶意用户和行为。

3.4 数据安全

使用方:

a) 应对数据进行分类分级;

b) 宜设置数据防泄漏策略;

c) 宜限制向用户自有设备传输使用方敏感数据;

d) 宜提供数据销毁方案。

3.5 个人信息保护

使用方应按照 GB/T 35273《信息安全技术 个人信息安全规范》要求保护个人信息。

3.6 通信安全

使用方:

a) 应使用安全协议，例如，传输层安全协议（TLS）、因特网安全协议（IPSec）等，保护业务系统传输的保密性和完整性;

b) 宜在通信过程中对设备的安全性进行持续验证。

3.7 安全审计

使用方应定期对办公系统进行安全审计，审计内容包括但不限于对敏感数据的操作、访问控制权限变更等。

（二）用户安全

1 概述

用户在开展远程办公时，应了解本实践指南第四章中的安全风险，遵守使用方制定的远程办公安全管理制度。

2 设备安全

用户:

a) 应确保用户自有设备安装了正版软件、安全防护软件，并及时更新;

b) 应确保用户自有设备采用了安全配置，例如，关闭共享文件、禁用不使用的账号等;

c) 应对下载的文件进行病毒查杀;

d) 不应使用公用设备进行远程办公;

e) 宜将用户自有设备在使用方登记。

3 数据安全

用户:

a) 应采用使用方指定的工具传输、存储、处理数据;

b) 宜减少从远程办公系统下载文件。

4 环境安全

在居家环境，用户:

a) 应使用路由器厂商提供的固件，并及时更新固件版本;

b) 宜在路由器中开启局域网防护等安全功能。

在公共场所，用户:

c) 在环境无法满足远程办公安全性要求时，应停止远程办公;

d) 不应在公共场所离开设备;

e) 不应使用不安全的网络,例如,无口令或公开口令的无线网络;

f) 宜防止设备屏幕被窥视，例如，使用防窥屏。

5 安全意识

用户:

a) 应使用强口令，并定期更新;

b) 应防范人员身份仿冒带来的风险;

c) 应使用办公邮箱，避免使用个人邮箱;

d) 不使用远程办公系统时，应及时退出;

e) 不应访问来源不明的链接、文档等;

f) 不应将存储使用方敏感数据的设备接入公用网络;

g) 不应将设备、账号信息等提供给他人使用;

h) 宜使用办公系统使用方提供的移动存储设备。