ICS 号:01.040.35

中国标准文献分类号:L73

团　　体　　标　　准

T/ZOSA 002-2018

中央企业移动办公
商业秘密保护安全技术要求

2018-08-03 发布　　2018-08-03 实施

中关村智能终端操作系统产业联盟发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中关村智能终端操作系统产业联盟提出并归口。

本标准起草单位：北京航星机器制造有限公司，中国航天科工集团第三研究院三〇四研究所，北京元心科技有限公司，航天云网科技发展有限责任公司，北京邮电大学

本标准起草人：王东明，高鹏，郭文龙，费廷伟，王波，史旭升，马敬，林明祥，邹仕洪，奚智，穆森，陆月明，史子旺

中央企业移动办公商业秘密保护安全技术要求

1 范围

1.1 背景

伴随企业越来越多的将办公系统迁移到移动网络，企业的商业秘密在无线网络和移动终端之间流动，为了保证企业商业秘密的安全，故制定此标准，规范移动办公系统安全防护建设。

1.2 范围

本标准基于中央企业商业秘密在移动办公中的安全风险，提出了中央企业移动办公商业秘密保护的整体安全框架，规定了移动终端安全、信道安全、移动接入安全、服务端安全应满足的技术要求。

本标准适用于中央企业商业秘密移动办公系统的安全设计、产品研发、工程实施和运行管理，也可作为对中央企业商业秘密移动办公系统进行安全测评的依据。涉密移动办公系统按照国家保密局的规定执行。

2 符合性声明

本标准遵从以下标准：

《信息系统等级保护基本要求》
《中央企业商业秘密安全保护技术指引》（国资委保密〔2015〕3 号）
《中央企业商业秘密安全技术保护实施指南》（国资委保密〔2016〕3 号）
《中央企业商业秘密安全技术保护风险评估细则》（国资委保密〔2016〕4 号）
《信息安全技术 信息安全风险评估规范》GB/T 20984-2007
《信息系统安全通用技术要求》GB/T 20271—2006
《网络安全基础技术要求》GB/T 20270—2006
《操作系统安全技术要求》GB/T 20272—2006
《信息安全技术　云计算服务安全能力要求》GB/T 31168-2014
《信息安全技术　云计算服务安全指南》GB/T 31167-2014
《移动终端信息安全技术要求》YD/T1699-2007

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 移动终端

便携式、可移动的计算设备。

注：移动终端包括智能手机、平板、笔记本电脑，具备无线上网功能。

3.1.2 移动办公

利用移动终端随时随地通过无线网络访问企业办公系统进行网上办公。

3.1.3 商业秘密

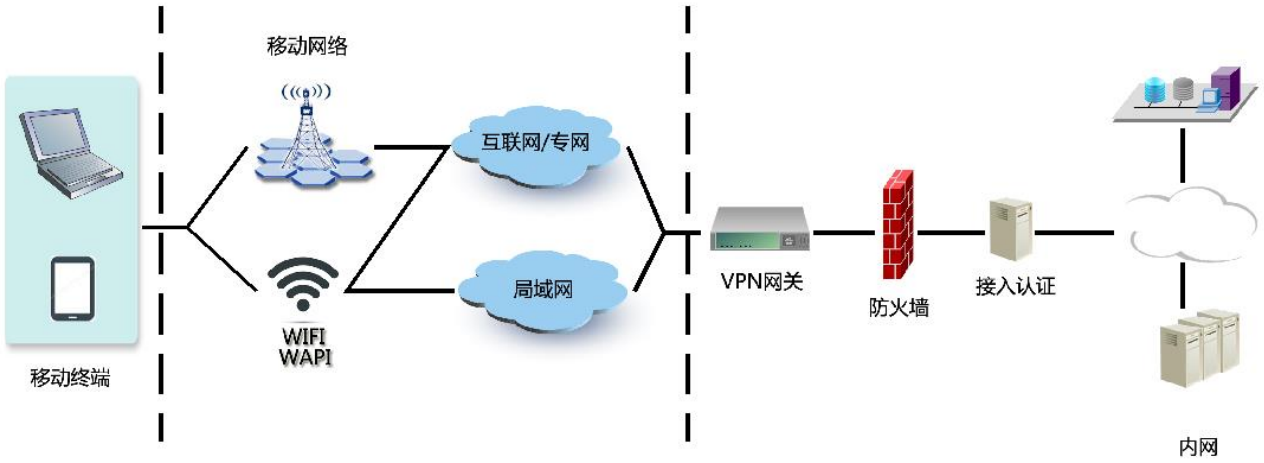
不为公众所知悉、能为企业带来经济利益、具有实用性并经企业采取保密措施的经营信息和技术信息。

4 总体设计

移动办公系统主要由三部分组成：位于用户侧的移动终端、移动网络、位于企业内网的办公系统服务

器。

图 1 移动办公网络拓扑图



本标准主要规范移动办公系统在移动终端侧的安全防护，以及移动网络中数据传输的安全防护。

5 移动终端安全功能要求

移动终端安全要求，包括：系统安全要求、应用安全要求、安全管控要求。

图 2 移动终端安全要求结构图

系统安全要求：针对承载移动办公应用的移动操作系统的安全要求。
应用安全要求：针对企业应用在部署、运行的安全要求。
安全管控要求：针对移动终端安全管控的要求。

5.1 系统安全要求

5.1.1 基本要求

（1）至少具备一个 SD 插槽或 USB 接口，支持硬件密码卡（如 TF/ Micro SD 卡）或 UKey 形式的数字证书；

5.1.2 独立的身份认证

a）应支持设置开机口令或利用生物特征识别，开启移动终端时进行身份认证；

b）应支持屏幕锁定口令，移动终端空闲时间达到设定阈值时锁定屏幕；解锁时应重新进行身份认证；
c）在限定时间段内多次连续尝试身份验证失败，应锁定系统；
d）认证信息应加密存储。

5.1.3 数据存储

（1）采用的加密算法应符合国家密码管理局的相关规定。

增强要求

（2）办公数据不应存储在手持式移动智能终端上，如手机和 PAD。

5.1.4 运行环境隔离

移动办公应用只允许通过 VPN 访问企业的商密网络，不允许访问互联网。

（1） 应采用隔离技术保证移动办公应用与个人应用运行环境的系统级隔离；
（2） 移动办公应用只能访问企业的商业网络，不能访问互联网。
（3） 应支持移动办公应用运行时防止截屏；

5.1.5 系统管理员权限管理.

系统中无具有所有权限的进程。

5.1.6 审计

（1）审计数据在本地加密存储，
（2）审计数据应定期上传，支持远程审计管理。
（3）只有管理员才有权限查看审计日志。

5.1.7 系统升级

（1）移动终端应支持通过 OTA 对系统进行升级。
（2）OTA 服务应部署在企业内部网络，终端通过商密网访问 OTA 服务，下载升级包进行升级更新。终端与 OTA 服务器之间需要进行 3 次以上的双向认证。
（3）升级时应对升级包进行安全性检测，只有经过身份认可的证书签名的升级包才被允许。

5.1.8 USB 连接

移动终端通过 USB 与 PC 连接时，应进行双向的身份认证，只有许可的 PC 才能连通。

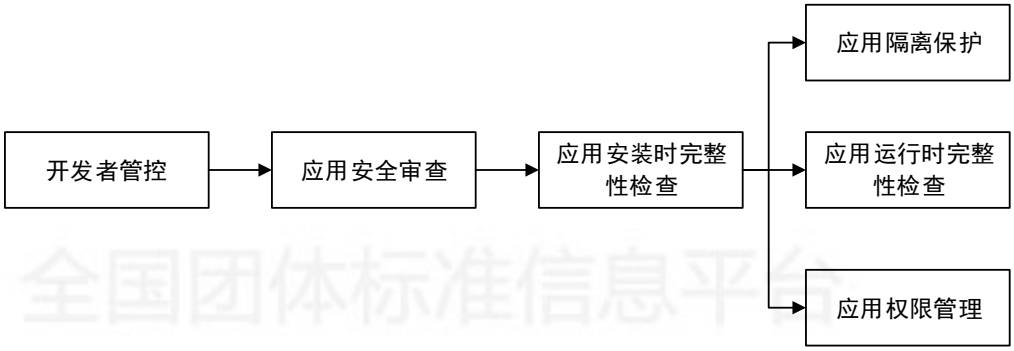
5.1.9 系统自检

（1）系统在开机时，应运行一套自检程序，证明系统自身的安全性。

5.2 应用安全要求

移动应用安全应采取如下要求

图 3 应用安全要求



5.2.1 应用开发者管控

对应用开发厂商进行详细的背景调查，在确信厂商安全可靠的前提下，向软件厂商提供软件开发资质授权、厂商身份标识证书、软件开发工具链，并对软件厂商根据资信程度，进行分级管理。

5.2.2 应用安全审查

软件厂商软件发布需要提交到商密网应用商店，企业应对应用进行全面的安全审查。审查方法主要包括：

（1）检查应用申请的权限是否合理，是否存在冗余的权限申请。

（2）对应用进行简单的测试，验证软件是否可用，是否存在应用崩溃等严重问题。

（3）采用静态安全检测方法，对应用进行反编译，检查应用对一些核心、关键函数调用情况。

（4）采用动态安全检测方法，在沙箱中运行应用，观测应用的行为。应用通过安全审查后，管理员应使用应用商店的证书对该应用进行签名，并发布到应用商店。

5.2.3 应用可信检查

（1）在终端上只允许通过预装的应用商店在线安装，不支持通过安装包的离线安装方式。

（2）应用安装过程中，应对应用进行完整性检查。

（3）应用在运行前，需要将执行文件、动态库加载到内存，在此过程中系统会对可执行的文件利用密码机制进行完整性验证，一旦发现文件被修改，则终止加载过程。

5.2.4 应用隔离保护

部署在系统中的应用之间是相互隔离的，不同应用之间，数据不能访问。

5.2.5 应用权限管控

在工作系统对应用权限应实施更加严格权限管控。

（1）系统中部分敏感（比如通话、SIM 卡通讯等），这些权限只会开放给系统应用。

（2）应用在安装时，系统的安装管理器会向用户显示告知应用所申请的权限，只有用户确认后才会安装该应用。

（3）应用运行过程中，用户可以动态调整应用申请的权限。

5.2.6 应用身份管理

为了保证应用生命周期安全，在工作系统上，对应用程序身份进行安全检测：

（1）采用身份认证机制，即为应用开发者颁发签名证书，应用开发者的整个开发生命周期内都必须使用这些证书才能完成应用的调试，发布。从而保证所有进入系统的应用程序都是经过身份认证的。

（2）为了保证应用运行的身份安全，系统在应用运行时也会校验应用身份，保证应用不被非法篡改。

（3）整个强认证机制采用的数字证书采用符合国家密码管理局规定的商用证书，其安全性和有效性是符合国内安全现状的要求的。

5.2.7 应用数据管理

为了防止企业商密网中的数据外泄：

（1） 访问企业商密网中，应本着先认证、再访问的原则；

（2） 在显示机密数据时，应用应在显示数据时，背景显示水印及要求系统禁止截屏。

5.2.8 应用商店

（1）应用下载过程，应采用安全加密传输，保证所有应用数据的安全。

（2）应用的安装包经过加密，签名，文件安全性校验性等相关处理，保证安装包的文件安全和身份合法。

（3）应用商店服务器部署在商密网内，安装后的应用放在沙箱内部运行，根据签名的级别不同，进行颗粒化的限权管理，保证系统相关数据的安全。

5.2.9 应用部署模式

为了保证安全，移动终端中的应用只能通过企业应用商店安装。应用商店作为工作系统唯一的应用安装来源，保证所有进入工作系统的应用的来源可控。所有终端用户只能通过工作系统的应用商店下载安装商密网应用。应用商店管理员负责审核，发布商密网内的可信应用。

5.3 安全管理要求

安全管控从用户、设备、应用三个维度来实现对移动终端的高效、安全的统一管理。

5.3.1 安全管理服务器部署

安全管理服务器应部署在企业内网，移动终端通过 VPN 网络与安全管理服务器进行通讯。

移动终端与安全管理服务器之间采用 HTTPS、TLS 等加密通讯协议，保证管控指令的传输安全。

5.5.2 用户管理

（1）支持用户的激活、锁定、挂失操作

（2）用户“激活”失败的次数是有 24 小时以内最多失败 20 次的限制的，如果 24 小时内失败 20 次后再激活失败，EMM 的激活界面就会变成激活限制界面 24 小时后才可恢复。

5.3.3 设备管理

（1）支持查看设备信息。

（2）支持设备激活、锁定、擦除数据等操作。

（3）设备的基本信息，其中包含了设备的 SN、SIM 卡信息、存储空间、OS 版本等，具体如下表：

表 1 设备基本信息

名称	描述
手机号	显示当前设备的手机号码
SIM 卡绑定状态	已绑定、未绑定,如果为“已绑定”状态，则用户私自更换 SIM 卡后，手机将不能开机使用
存储空间	设备内部存储空间\外部存储空间，如果没有外部存储则只显示内部存储空间大小
设备类型	phone、pad
OS 版本	系统版本号
SN	设备序列号：设备的唯一标识

MAC 地址	设备的网络物理地址

（4）外设统一管理，统一登记和配置属性参数，禁止使用没有登记外设。管控终端外设接口及访问权限，以防非安全外设访问，造成数据泄露。

（5）物理接口的监控，应可对各个物理接口进行接入安全控制：

a） 访问控制能力；

b） 指令许可性判断；

（6）应对外设接入行为进行审计。

5.3.4 应用管理

（1）应用管控是管理员可以通过管控界面，对于激活设备进行批量的安装和删除应用。

（2）应用的安装是静默安装，用户不需要手动的操作，以方便企业员工使用。

5.3.5 安全策略

终端安全管理应支持如下安全策略。

表 2 安全策略表

名称	策略描述
密码类型	强制要求用户设置较安全的密码类型。
摄像头合规时间	用户只能在该时间段内才可打开摄像头使用。
录音机合规时间	用户只能在该时间段内才可打开录音机使用。
设备远程锁定/解锁	用户可向本部门操作管理员申请锁定设备。
SIM 卡绑定状态	支持已绑定、未绑定两种状态。如果为“已绑定”状态，则用户在没有被授权更换 SIM 卡时，更换 SIM，终端将在 30 分钟内自动清除所有数据。
设置锁屏密码	用户可以向本部门操作管理员申请设置锁屏密码。
注销及擦除	终端设备执行注销命令，已经存在的数据需要全部清除。
数据离线擦除	手机离线断网 12 小时锁定手机无法使用，需管理员解锁，锁定后，断网时间达 24 小时且开机失常超过 30 分钟，提示用户进行一次身份认证，输入解锁密码，如不能正确输入则执行数据擦除动作，针对差旅人员可与本部门操作管理员申请延长离线时长（如乘坐飞机）。
数据远程删除	支持对远程终端上的文件内容进行管控、删除操作。

5.4 移动内容管理系统（MCM）客户端

5.4.1 客户端管理

应支持开机自动运行，支持自动更新升级。

5.4.2 文件监控

应支持对有安全策略的数据文件，进行信息收集并上报，如文件名称，格式，大小，版本，更新时间，所有者，以监控数据文件的创建、更新、分发条目、分发状况等。

5.4.3 文件管理

（MCM）客户端执行移动内容管理系统（MCM）下发的管理策略，对 PNG，JPG，GIF，BMP，PDF，DOC，DOCX，XSL，CSV，TXT，HTML 等格式数据文件进行分级标记管理。支持对不同安全级别的文件提供不同的管理策略。仅符合终端用户权限范围内的目录或数据文件，移动终端方可进行访问、处理和传输操作。

5.4.4 防卸载机制

支持防卸载机制，可与 MDM 客户端联动，当 MAM 客户端被卸载时，执行终端设备锁定或信息擦除策略。

5.4.5 数据安全

（1） 根据数据的安全级别，数据分为普通数据，私有数据，普通商业秘密（普通商密）数据、核心商业机密（核心商密）数据。

i. 普通数据，对安全没有影响的数据，对访问和存储没有要求。

ii. 私有数据，终端用户相关的个人数据，由用户决定其安全策略。

iii. 普通商业秘密数据、核心商业机密数据，必须根据不同的密级实行不同的安全策略，存储时必须要进行加密和完整性校验。

（2） 根据密级不同，提供不同级别的加密保护。

（3） 应提供数字签名、加密、数字水印等技术，防止数据被篡改或数据泄露。

（4） 根据密级不同，提供不同的访问控制策略。

（5） 应提供数据彻底删除功能，以保证被删除的文件不可再恢复出来。

5.4.6 安全域隔离

（1） 文件系统提供措施，对文件的存储空间进行统一管理。不同类型、不同密级、不同应用的文件，应支持存储在不同的分区或不同的目录文件上。支持加密文件系统，支持文件、目录、全盘不同级别加密。

（2） 支持虚拟机、容器等不同级别的隔离技术，根据具体情况、采取不同的隔离技术。

（3） 逻辑隔离采用隔离技术，普通商密数据、核心商密数据只能在自己隔离的运行环境中解密，并且防止拷贝、截屏等数据泄露行为。

6 端到端安全要求

6.1 系统接入安全

6.1.1 身份认证

（1） 传统身份认证：用户名+口令。

（2） 数字签名技术：第三方 CA、自建 CA。

（3） 其他认证技术支持 LDAP/AD、Radius、Dkey、短信认证、硬件特征码、动态令牌等单因素或多因素与或认证。

（4） 应同时支持两种以上身份认证方式。

6.1.2 客户端安全检测

支持对客户端的操作系统、文件、进程、登录 IP、接入线路 IP、使用终端、登录时间等因素，进行全方位的检查，避免风险终端接入。

6.2 数据传输安全

6.2.1 采用 VPN 技术

（1） 移动终端应采用 VPN 技术，接入到企业的内部网络。
（2） VPN 应支持国密算法。

6.2.2 采用安全的网络协议

（1） 采用安全的网络协议 SSL、HTTPS 等。
（2） 移动终端应与服务器基于安全传输层协议，进行数据传输。

6.2.3 数据完整性要求

应支持信息完整性校验机制，保证数据传输的完整性。

6.2.4 数据保护

根据数据的密级和数据类型提供不同的加密保护。

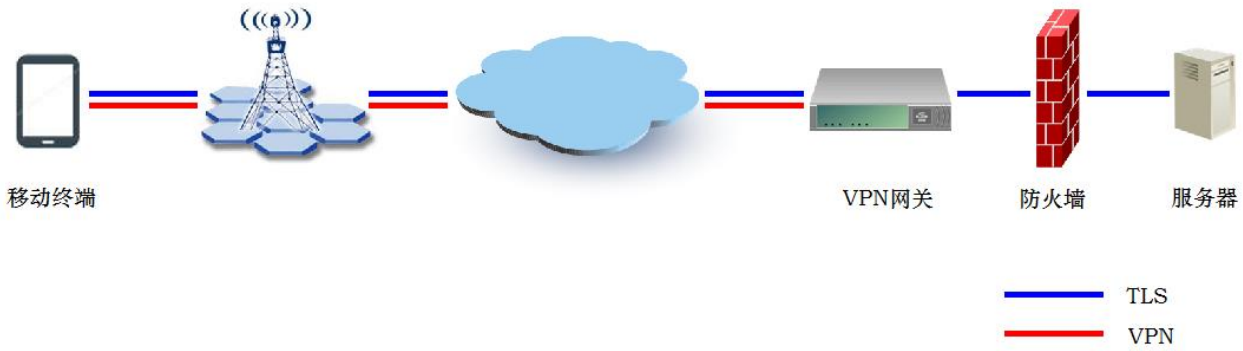
6.3 网络隔离

采用网络隔离技术通过逻辑划分，实现不同用户系统、网络和数据的安全隔离。

6.4 用户管理

（1） 细化访问权限，防止超级用户权限出现。
（2） 统一授权管理，结合用户身份关联相关资源，控制用户只能访问特定资源。
（3） 单点登录，将用户身份与权限内资源账户绑定。
（4） 主从账户绑定，保证用户输入的账户与绑定账户一致，避免账号密码失窃。
（5） 应支持对客户端访问实时监测，及时发现并隔离恶意终端访问。

图 4 移动网络安全要求



7 云端安全要求

7.1 云端安全能力要求

云端安全能力要求，参照国标 GB/T 31168-2014《信息安全技术　云计算服务安全能力要求》。

7.2 云端安全管理要求

云端安全管理要求，参照 GB/T 31167-2014 《信息安全技术　云计算服务安全指南》。

7.3 云端商业秘密存储和使用安全要求

7.3.1 存储中的数据保护

普通商密保护应符合：

（1） 文件服务器、应用系统和数据库应采取基于用户角色的授权访问控制，并且只赋予用户所需的最小权限；

（2） 文件服务器、应用系统和数据库中的商业秘密信息要有密级标识，并可通过有关系统为使用用户知悉；

（3） 与商业秘密相关的存储与备份设备、服务器，应确保其物理安全，防止介质丢失或信息的非法泄露；

（4） 存储介质的报废和销毁应集中由专人统一处理。

核心商密保护还应符合：

（1） 应用系统与数据库中核心商密数据的导出，应采取技术保护措施，未经审批授权无法将数据导出；

（2） 对以非结构化数据形式存储的核心商密数据，如保存于文件服务器上的文档，应采取技术保护措施，未经审批授权无法将数据导出；

（3） 对于因故障需要到外部机构维修的存储介质，应通过数据擦除工具/设备擦除介质中的数据，并确保被擦除的数据无法通过经检测认定的常规数据恢复工具得到恢复，再送出维修。介质的维修要进行登记；

（4） 存放核心商密的存储介质需要被带出工作环境时，须履行审批、登记程序，并对其中的信息进行加密存储。

7.3.2 使用中的数据保护

7.3.2.1 操作中的数据保护

普通商密保护应符合：

（1） 不同类别的商业秘密文档，应按照部门、项目组、指定用户名等方式设置阅读、编辑、删除、复制等权限。如：财务数据，只允许财务部具有编辑权限；董事长、总经理和相关人员具有阅读权限；其他有涉及商业秘密终端的人员没有阅读或编辑权限；

（2） 对商业秘密数据的管理和控制，须以不影响员工正常的文档编辑阅读、数据处理、数据交换、出差和在外办公为前提，并且不受到网络连通与否状况的影响。

核心商密保护还应符合：

（1） 在终端上使用核心商密数据时，须在终端屏幕上自动显示水印，水印位置、格式、透明度等可自定义，以防止通过拍照方式泄漏商业秘密；

（2） 对处理核心商密的终端上产生的工作文档和通过 C/S、B/S 方式从数据库或网络应用中获取的核心商密数据，应采取技术措施防泄漏，核心商密数据的外发，须经过审批授权，并对数据做集中式留档审计；

（3） 应用开发人员直接访问核心商密数据，须对其进行控制和管理，开发任务完成后应对相关的核心商密数据进行及时回收或转移；

（4） 应禁止任何未受控的终端通过网络访问有核心商密数据的应用、数据库和服务器。未受控的终端是指未正确安装管理控制软件或没有合法身份的终端。

7.3.2.2 数据打印保护

普通商密保护应符合：

应对包含商业秘密数据的文档的打印进行授权访问控制，并对打印行为进行控制和审计

核心商密保护还应符合：

（1） 应对包含核心商密数据的文档设置包含当前使用者相关信息的水印；

（2） 应对打印和复制核心商密数据的设备进行保密检查。

7.3.2.3 终端及外设上的数据保护

普通商密保护应符合：

（1） 应对处理商业秘密的终端进行文档打印、传真、光盘刻录等行为的审计和控制；

（2） 应对商业秘密数据文档的外发行为和在内部终端间的流转进行审计，审计记录必须上传到集中的服务器；

（3） 人员离职或转岗后，其所使用终端上的数据访问权限应及时回收或转移；

（4） 第三方人员在协作期间接触的商业秘密数据，应采取技术措施防止其泄露数据。合作任务完成后，其终端及存储介质上的商业秘密数据应及时回收或转移。

核心商密保护还应符合：

（1） 创建或保存含有核心商密信息的文档时，应加密并根据角色设置访问权限，并加上标识；

（2） 须对保存在终端、移动存储介质上的核心商密文档进行加密，并对加密数据做读写访问控制。加密时须保证每个文件使用不同的秘钥；

（3） 存放有核心商密文档的终端，未经授权不得做如下操作：使用网络应用程序向外部发送文档，使用终端上的红外、蓝牙等通信端口，使用未经授权的移动存储设备。对上述类型操作须就进行事前、事中、事后控制；

（4） 存放有核心商密文档的终端使用移动存储介质时应进行严格的授权访问控制，核心商密文档外发时，须审计文档内容；

（5） 通过外部终端访问核心商密数据时，应采用终端服务器或桌面虚拟化技术，防止核心商密数据保留在外部终端上；

（6） 涉及核心商密的终端的网络接入、操作系统登录、文档编辑阅读、数据处理，须用统一的基于数字证书的账号进行控制与保护；对核心商密数据，须采用基于硬件的数字证书和非对称加密算法进行保护。

7.3.3 数据安全审计、完整性、备份与恢复

普通商密保护应符合：

（1） 应对商业秘密数据的存储、传输、使用行为进行审计，审计记录集中保存；

（2） 审计内容应包括访问主体、被访问客体、访问方式、访问结果、日期及时间、访问所在服务器或终端的主机名、IP 地址、MAC 地址、用户等信息；

（3） 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

（4） 应提供商业秘密数据本地备份与恢复功能，完全数据备份至少每月一次，备份介质场外存放。

核心商密保护还应符合：

（1） 应定期对核心商密安全审计数据进行统计、查询、分析及生成审计报表；

（2） 应能够检测到核心商密数据在传输过程中完整性受到破坏，并采取必要的恢复措施；

（3） 应在国内异地进行数据和软件系统的完全备份，或在国内建立异地灾难备份中心。

附录

附录 A 自查表

企业可根据自身移动办公系统所采用的安全防护对照本标准，对各项安全技术要求进行自查、打分。

表 3 移动办公商业秘密安全保护自查表

类别	序号	安全技术要求	自查打分	满分
系统安全要求	1	基本要求		3
	2	独立的身份认证		4
	3	数据存储		3
	4	运行环境隔离		4
	5	系统管理员权限管理		3
	6	审计		2
	7	系统升级		2
	8	USB 连接		2
	9	系统自检		2
	合计			25
应用安全要求	1	应用开发者管控		2
	2	应用安全审查		2
	3	应用可信检查		2
	4	应用隔离保护		2
	5	应用权限管控		1
	6	应用身份管理		1
	7	应用数据管理		1
	8	应用商店		2
	9	应用部署模式		2
	合计			15
安全管理要求	1	安全管理服务器部署		3
	2	用户管理		3
	3	设备管理		4
	4	应用管理		3
	5	安全策略		2
	合计			15
内容管理要求	1	客户端管理		2
	2	文件监控		2
	3	文件管理		2
	4	防卸载机制		2
	5	数据安全		4
	6	安全域隔离		3
	合计			15
端到端安全要求	1	身份认证		2
	2	客户端安全检测		2
	3	采用 VPN 技术		5

	4	采用安全的网络协议		2
	5	数据完整性要求		1
	6	数据保护		5
	7	网络隔离		2
	8	用户管理		1
	合计			20
云端安全要求	1	云端安全能力要求		3
	2	云端安全管理要求		3
	3	云端商业秘密存储和使用安全要求		4
	合计			10
合计				100