ICS 35.040
L 8[illegible]

信息安全技术 [illegible]

目　　次

前言 …… Ⅲ
1 范围 …… 1
2 规范性引用文件 …… 1
3 术[illegible]
4 概述 …… 2
4.1 [illegible]应用 …… 2
4.2 [illegible]基本要求等级[illegible] …… 3
5 通用要求 …… [illegible]
6 第一级密码应用基本要求 …… 4
6.[illegible]
[illegible] …… 5
7.1 物理和环境安全 …… 5

9.1 物理和环境安全 ……………………

9.2 网络和通信安全 …………………… 9

9.3 设备和计算安全 …………………… 9

9.4 应用和数据安全 ……………………

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的[illegible]可能涉及专利。本文件的发布机构不承担[illegible]

[illegible]股份有限公司、中国金融电子化公司、飞天诚信科技股份有限公司、[illegible]信息技术有限公司、[illegible]深圳市网安计算机安全[illegible]

[illegible]

本标准主要起草人：[illegible]、罗鹏、[illegible]刘健、叶长伟、[illegible]马原、郑[illegible]

全技术
密码应用基本要求

1 范围

本标准规

第一级到第四

本标准适用于

GB/T 37092 信息安全技术 密码模块安全要求

3 术语和定义

下列术语和定义

3.7

密钥管理　key management

根据安全策略，对密钥的产生、分发、存储、使 [illegible] 归档、撤销、备份、恢复和销毁 [illegible]

[illegible] 称身份的过程。

3.9

[illegible]

4　概述

4.1　信息系统密码应用技术框架

4.1.1　框架概述

本标准从信息系统的物理和环境 [illegible]

4.1.2　密码应 [illegible]

1)　身份鉴别 [illegible]

3) [illegible]

[illegible]

——第二级，是在[illegible]

[illegible]

5 通用要[illegible]

第一级[illegible]

[illegible]

b) 可采用密码技术保证电子[illegible]

[illegible] 以上如采用密码服务[illegible]

[illegible]依法接受检测认证的，应经[illegible]

商用密码认[illegible]

[illegible]通信安全

[illegible]本级要求包括[illegible]

[illegible]

d) 可采用密码技术保证网络边界访问控制[illegible]息的完整性；

[illegible] 以上如采用密码服[illegible]

[illegible]

[illegible]安全

a) [illegible]

[illegible]检测认证[illegible]

商用密[illegible]

[illegible]

c) 可采用密码技术保[illegible]应用的重要数据在传输过程中的机密性；

d) 可采用密码技术保证[illegible]

[illegible]

g) 以上[illegible]

6.6 人员管理

使用[illegible]

[illegible]用方案；

c) 应按照密码应用方案实施建设；

d) 投入运行前可进行密码应用安[illegible]

c) 宜采用密码[illegible]

可采用密码技术保证[illegible]

[illegible]

商用密码认证机构认证合格

以上采用的密码产品，应达到GB/T [illegible] 一级及以上安全要求。

7.4 应用和数据安全

本级要求包括：

a) [illegible] 进行身份 [illegible]

[illegible]

d) 宜采用密码技术保证信息 [illegible]

e) [illegible] 采用密码技术保证 [illegible]

[illegible] 该密码服务应符合 [illegible] 的，应经商用密码认证机构认证合格 [illegible]

[illegible]

[illegible] 件及介 [illegible] 制度 [illegible]

b) 应根据 [illegible] 制定密钥管理规则 [illegible]

[illegible]

c) 应建立岗位责任 [illegible] 于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；

应建立关键人员保密 [illegible]

[illegible]

[illegible] 应按照 [illegible] 方案实施建设；

d) [illegible]前宜进行密码应用安全性评估。

7.8 应急处置

本级要求[illegible]

8 第三级密[illegible]

[illegible]

b) 宜 [illegible]

[illegible] 应采用密码技术保证 [illegible] 系统 [illegible]

1) [illegible]

[illegible] 接收行为的不可否认 [illegible]

f) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经 [illegible]

[illegible] 息系统应符合以下管理制度要求：

[illegible] 改进之 [illegible]

a) 相关人员应了解并遵守密码相 [illegible] 规、密码应用 [illegible] 理制度；

b) 应建立密码应用岗位责任制度，明确各 [illegible] 安全 [illegible]

c) 应建立上岗人员培训 [illegible]

d) [illegible]

[illegible]

[illegible] 物理和环境安全

[illegible]

e) 应采用 [illegible]

[illegible]

f) 以上如 [illegible]

[illegible] 信息的完整性：

[illegible]

g) 以上如果 [illegible]

商用密码认证 [illegible]

d) 应采用密码 [illegible]

[illegible] 规的相关要求 [illegible]

[illegible] 和操作规程的发布 [illegible]

2) 对关键岗位建立多人共管机制；

[illegible] 管理、密码安全审计、密码 [illegible] 人员职 [illegible]

[illegible] 应建立上岗人员培训制度，对于涉及 [illegible]

d) 应[illegible]对密码应用安全岗位人员进行[illegible]

附 录 A

（资料性附录）

不同级别密码应用基本要求汇总列表

第[illegible]四级密码应用基本要求[illegible]

表 A.1（续）

管理制度	[illegible]	[illegible]	[illegible]	[illegible]
	定期修订安全管理制度	—	—	应
	明确管理制度发布流程	—	—	应
	制度执行过程记录留存	[illegible]	[illegible]	应

附　录　B

（[illegible]）

[illegible]

[illegible] 的访问、使用、泄露、修改 [illegible]

[illegible] 以下 [illegible]

[illegible] 有者、使用起始时间、使用终止时间 [illegible]

b)　密钥分发

[illegible]

[illegible] 上密钥 [illegible] 被非授权的访问或篡 [illegible]

[illegible] 略进行 [illegible] 更新。

[illegible] 间等。

g)　密钥 [illegible]

[illegible] 钥 [illegible] 应的 [illegible] 当 [illegible] 按需进行密 [illegible]

[illegible] 命的时间等。

i） 密钥恢复

可以 [illegible]

参 考 文 献

[illegible] GB/T 22239—2019 [illegible]