ICS 35.040
L 80

中华人民共和国国家标准

信息安全技术

目　　次

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[redacted]。本文件的发布机构不承担[redacted]

[redacted]

[redacted]建、闾业龙、尚志仪、钟[redacted]刘

信息系统密码应用基本要求

…第和通信安全、设备和计算安全、应用和数据…会面提出了第一级到第四级的…
要求，并从管理制度、人员…

3.3

真实性 authenticity

一个实体是其所声…种特…和信息之类的实体。

3.4

不可否认…

3.7

密钥管理　key management

根据安全策略对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生存周期的管理。

3.8

身份鉴别　identity authentication

证实一个

3.9

[illegible]

[illegible]

[illegible]

对象或

应用场景描述如下

a) 机密性技术要求保护对象

使用

3） 日志记录；

4） 访问控制信息；

5） 重要信息资源安全标记；

6） 重要可执行程序；

7）

别；

程序的来源真实性保证；

6） 应用系统的异动用户类别；

1） 进入重要物理区域人员的身份

2） 通信双方的身份鉴别；

3） 网络各设备接入时的

4） 重要可执

5） 登录操作

逐级增强的要求，用一、二、三、四、五表示，信息

应级别的密码保障技术要

性的技术要求，

的基本安全保护能力要求，本标准提出密码保障能力

5 通用要[redacted]

第一级到第[redacted]

[redacted]

[redacted]

6.2 网络和通信安全

[redacted]

[redacted]的用户进行身份鉴别，保证用户身份的真实性；

b） 可采用密码技术保证系统资源访问控制信息[redacted]的完整性；

c） 可采用密码技术[redacted]

g) 以上九项[illegible]码服务，该密码服务应符合法律法规的相关要求，[illegible]
[illegible]经[illegible]商用密码认证[illegible]

6 [illegible]

b) 应及[illegible]

[illegible]离岗人员的[illegible]密码应用[illegible]

[illegible]

f) 以上采用的密码产品，应达到 GB/T 37092 一级及以上安全要求。

7.3 设备和计算安全

本级要求包括：

a) 宜采用密码

d) [illegible]宜进行密码应用安全性评估。

7.8 应急处置

本级要[illegible]

[illegible]

a) 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；

b) 宜采用[illegible]进出记录数[illegible]

[illegible]

c) 应采用密码技术保证通信过程中重要数据的机密性；

d) 宜采用密码技术保证网络边界访问控制信息的完整性[illegible]

e) 可采用密码技术对从外部连接到内部网络的[illegible]

[illegible]

程序进行完整性保护，并对其来源进行[illegible]

b) 宜采用密码技……保证信息系统应用的访问控制……完整性；

c) 应采用密……

……数据接收行为的不可否认性；

d) 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，应经商用密码认证机构……

……置、密码软硬件及介质管理等制度；

b) 应根据密码应用方案建立相应密钥管理规则；

c) 应对管理人员或操作人员执行的日常管理操作建立操作规程；

d) 应定期对密码应用安全管理制度和操作规程的合理性和适……

……系统的账号不得多人共用。

c) 应建立上岗人员培……

b) 应根据密码应用方案，确……涉及的密钥……

d) ……投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；

e) 在运行过程中……估及……攻防对抗演习，并根据评估结果进行整改……

8.8 应急处置

本……

……置情况

9 第四级密码应用……

9.1 物理和环境安全

本……

a) 应采用密码技术……

……要求包括：

……份鉴别，保证用户身份的真实性；

……远程管理设备时，应采用密码技术建立安全的信息传输通道……

c) 应采……

商用密码应

a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码使

4) 密码操作员

4) 相关设备

望和使用账号不得多

人共用；

密钥管理员、密码安全审计员、密码操作

d) 应定期对密码应用安全岗位人员进行

人员保密制度和调离制度

e) 应建立关键

建设运行

本级要求包括：

a) 应

附 录 A
（资料性附录）
不同级别密码应用基本要求汇总列表

第一级～第四级密码应用基本要求，见表 A.1，第五级略。

表 A.1 第一级～第四级密码应用基本要求汇总列表

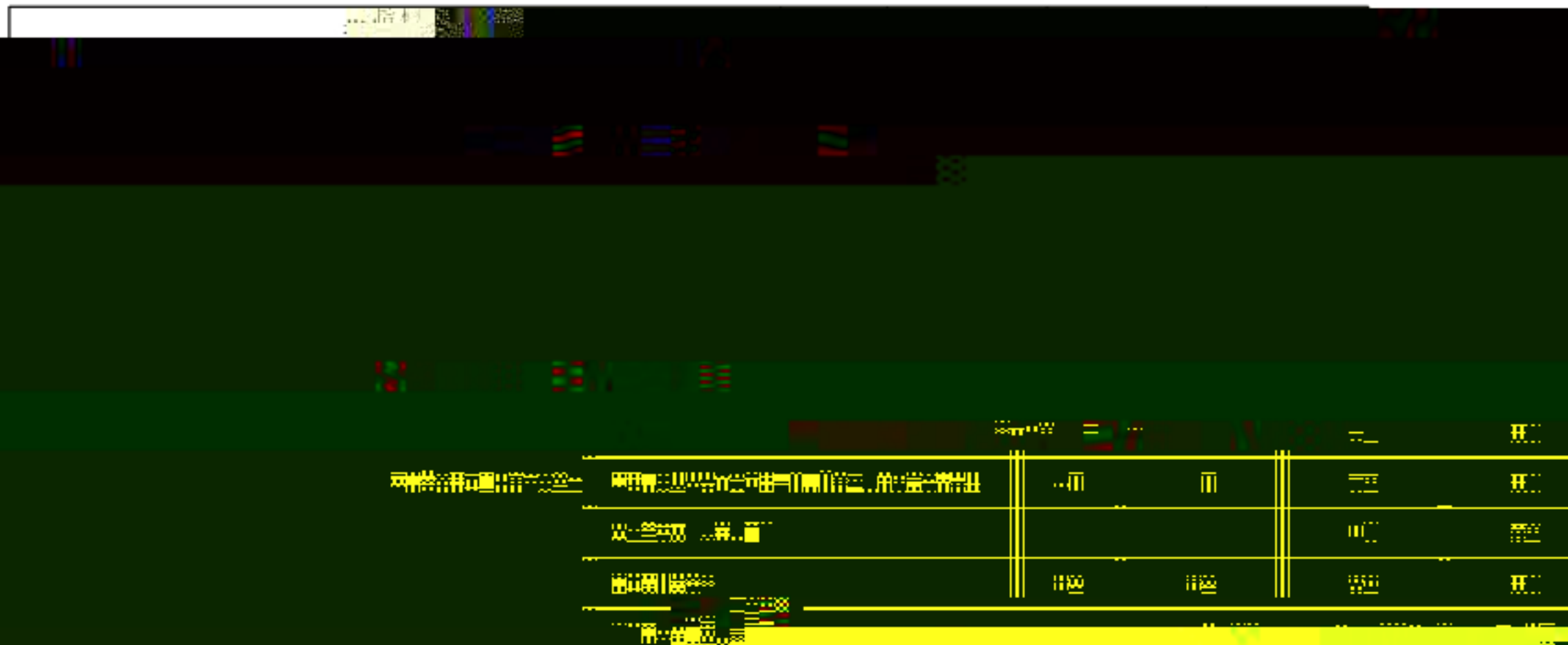

表 A.1（续）

			第一级	第二级	第三级	第四级
		具备密码应用安全管理制度	应	应	应	应
		[illegible]	[illegible]	[illegible]	[illegible]	应
		建立[illegible]	[illegible]	[illegible]	应	
	管理制度	[illegible]	[illegible]	[illegible]	[illegible]	
		定期修订安全管理制度	—	—	应	应
		明确管理制度发布流程	—	—	应	应
		制度执行过程记录留存	[illegible]	[illegible]	应	应
		了解并遵守密码相关法律法规和密码管理制度	应	应	[illegible]	应
		建立密码应用[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
应		[illegible]	[illegible]	[illegible]	[illegible]	应
应		向有关主管部门上报处置情况	—	—	—	应

附 录 B

（资

的密钥体系由业务系统根据密码应用需求在密码应用方案中明确，并在密码服务实

c） 密钥存储

密钥不以明文方式

i) 密钥恢复

可以支持用户密钥恢复和司法密钥恢[illegible]审计

信息，包括恢复的主体、恢复的时间等。

j) 密钥销毁

参 考 文 献

[1] GB/T 22239—2019