安全保护和系统定级的关系

- 定级指南要求按照“业务信息”和“系统服务”的需求确定整个系统的安全保护等级
- 定级过程反映了信息系统的保护要求

安全等级	信息系统保护要求的组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4

2022/5/12

不同级别系统控制点的差异

安全要求类	层面	一级	二级	三级	四级
技术要求	物理安全	7	10	10	10
	网络安全	3	6	7	7
	主机安全	4	6	7	9
	应用安全	4	7	9	11
	数据安全及备份恢复	2	3	3	3
管理要求	安全管理制度	2	3	3	3
	安全管理机构	4	5	5	5
	人员安全管理	4	5	5	5
	系统建设管理	9	9	11	11
	系统运维管理	9	12	13	13
合计	/	48	66	73	77
级差	/	/	18	7	4

2022/5/12

各级系统安全保护要求-物理安全

- 物理安全主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。
- 具体包括：**物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等十个控制点。**

各级系统安全保护要求-物理安全

控制点	一级	二级	三级	四级
物理位置的选择		*	*	*
物理访问控制	*	*	*	*
防盗窃和防破坏	*	*	*	*
防雷击	*	*	*	*
防火	*	*	*	*
防水和防潮	*	*	*	*
防静电		*	*	*
温湿度控制	*	*	*	*
电力供应	*	*	*	*
电磁防护		*	*	*
合计	7	10	10	10

2022/5/12

各级系统安全保护要求-物理安全

- **一级物理安全要求**：主要要求对物理环境进行基本的防护，对出入进行基本控制，环境安全能够对自然威胁进行基本的防护，电力则要求提供供电电压的正常。
- **二级物理安全要求**：对物理安全进行了进一步的防护，不仅对出入进行基本的控制，对进入后的活动也要进行控制；物理环境方面，则加强了各方面的防护，采取更细的要求来多方面进行防护。
- **三级物理安全要求**：对出入加强了控制，做到人、电子设备共同监控；物理环境方面，进一步采取各种控制措施来进行防护。如，防火要求，不仅要求自动消防系统，而且要求区域隔离防火，建筑材料防火等方面，将防火的范围增大，从而使火灾发生的几率和损失降低。
- **四级物理安全要求**：对机房出入的要求进一步增强，要求多道电子设备监控；物理环境方面，要求采用一定的防护设备进行防护，如静电消除装置等。

各级系统安全保护要求-网络安全

- 网络安全主要关注的方面包括：网络结构、网络边界以及网络设备自身安全等。
- 具体的控制点包括：**结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等七个控制点。**

各级系统安全保护要求-网络安全

- **一级网络安全要求**：主要提供网络安全运行的基本保障，包括网络结构能够基本满足业务运行需要，网络边界处对进出的数据包头进行基本过滤等访问控制措施。
- **二级网络安全要求**：不仅要满足网络安全运行的基本保障，同时还要考虑网络处理能力要满足业务极限时的需要。对网络边界的访问控制粒度进一步增强。同时，加强了网络边界的防护，增加了**安全审计、边界完整性检查、入侵防范**等控制点。对网络设备的防护不仅局限于简单的身份鉴别，同时对标识和鉴别信息都有了相应的要求。
- **三级网络安全要求**：对网络处理能力增加了“优先级”考虑，保证重要主机能够在网络拥堵时仍能够正常运行；网络边界的访问控制扩展到应用层，网络边界的其他防护措施进一步增强，不仅能够被动的“防”，还应能够主动发出一些动作，如报警、阻断等。网络设备的防护手段要求两种身份鉴别技术综合使用。
- **四级网络安全要求**：对网络边界的访问控制做出了更为严格的要求，禁止远程拨号访问，不允许数据带通用协议通过；边界的其他防护措施也加强了要求。网络安全审计着眼于全局，做到集中审计分析，以便得到更多的综合信息。网络设备的防护，在身份鉴别手段上除要求两种技术外，其中一种鉴别技术必须是不可伪造的，进一步加强了对网络设备的防护。

2022/5/12

各级系统安全保护要求-主机安全

- **一级主机系统安全要求：**对主机进行基本的防护，要求主机做到简单的身份鉴别，粗粒度的访问控制以及重要主机能够进行恶意代码防范。
- **二级主机系统安全要求：**在控制点上增加了**安全审计和资源控制**等。同时，对身份鉴别和访问控制都进一步加强，鉴别的标识、信息等都提出了具体的要求；访问控制的粒度进行了细化等，恶意代码增加了统一管理等。
- **三级主机系统安全要求**：在控制点上增加了**剩余信息保护**，即，访问控制增加了设置敏感标记等，力度变强。同样，身份鉴别的力度进一步增强，要求两种以上鉴别技术同时使用。安全审计已不满足于对安全事件的记录，而要进行分析、生成报表。对恶意代码的防范综合考虑网络上的防范措施，做到二者相互补充。对资源控制的增加了对服务器的监视和最小服务水平的监测和报警等。
- **四级主机系统安全要求**：在控制点上增加了**安全标记和可信路径**，其他控制点在强度上也分别增强，如，身份鉴别要求使用不可伪造的鉴别技术，访问控制要求部分按照强制访问控制的力度实现，安全审计能够做到统一集中审计等。