

## 课后报告二

环境和实体的安全管理是指为了保证信息系统安全、可靠地运行，确保系统在对信息进行采集、传输、存储、处理、显示、分发和利用的过程中，不会受到人为的或自然因素的危害而使信息丢失、泄露和破坏，对安全区域、信息系统环境、信息系统设备以及存储媒介等所进行的安全管理。

在信息系统安全中，环境安全是基础。该企业的机房坐落在远郊地区，地处偏僻，配备了 1 位安全员。要保证信息系统有一个安全的物理环境，充分考虑各种因素对信息系统造成的威胁并加以规避。

应该划分物理安全边界，明确界定安全范围，信息处理设施入口都应该实施适当的保护，以防止未经授权者进入，实体和环境保护的范围应当尽可能涵盖信息系统所在的整个环境空间，应按照地方、国内和国际标准建立适当的入侵检测系统，并定期检测组织管理的信息处理设施应在物理上与第三方管理的设施分开。

控制安全区域，包括监视进出安全区域的访问者，严格控制对敏感信息及其存储和处理程序的访问，访问者佩带某种形式的可视标识，第三方支持服务人员应被授权并受到监视，对安全区域的访问权要定期地予以评审和更新。

标识敏感信息处理设施位置的目录和内部电话簿不要輕易被公众得到。避免在安全区域内进行不受监督的工作，未使用的安全区域在物理上要封闭并进行周期性的检查，保障信息系统安全的环境条件，温湿度适宜。该机房安全要按照 B 级要求建设，对计算机机房的安全有较严格的要求，有较完善的计算机机房安全措施。除了防水防火防自然灾害之外还需要防止其他物理安全威胁，如防电磁泄漏，在设备选型、设备检测设备购置与安装、设备登记、设备使用管理、设备维修管理、设备存放管理以及媒介安全管理方面要遵循各项安全标准，保证电子文档安全。

对设备的安全管理是保证信息系统安全的重要条件。该企业开发的机房管理系统，包含传感器数据分析子系统，机房状态日志子系统，安全管理人员操作日志子系统，安全管理人员值班登记日志子系统，来访人员登记子系统，监控备份子系统以及数据访问行为日志子系统。其中，监控备份子系统以及数据访问行为日志子系统包括监测单元和控制单元，监测单元与机房设备连接，用于监测和获取机房设备的实时运行数据和机房设备运行环境条件信息，发送给管理模块分析，控制单元一端与机房设备连接，一端与交互模块连接，用于从交互模块获取控制命令，并转换成机房设备能够识别的指令发送给机房设备执行；管理模块包括数据管理单元、告警管理单元、配置管理单元、安全管理单元、自我管理单元和档案管理单元，数据管理单元用于数据显示、数据存储、数据查询、数据备份和恢复、数据处理和统计，告警管理单元用于告警显示、告警屏蔽、告警过滤、告警确认、告警信息发送短信，配置管理单元用于参数配置、界面自定义、时间校对，安全管理单元用于机房管理系统、设备和人员的安全，用户管理、操作记录管理、远程控制的安全保障，自我管理单元用于对机房

管理系统进行维护和管理，机房状态日志子系统、安全管理人员操作日志子系统、安全管理人员值班登记日志子系统以及数据访问行为日志子系统用于对机房管理系统维护信息和设备信息的管理；交互模块包括人机交互单元和系统交互单元，人机交互单元用于机房管理系统和管理人员之间的信息交互，系统交互单元用于机房管理系统之间的信息交互。