智慧矫正中心信息化管理制度

为规范信息化管理工作，社区矫正中心配备专职信息化工作人员，负责中心维护工作。为确保信息管理平台安全正常运行，制定以下管理制度：

一、指挥中心管理制度

1. 确保指挥中心设备安全和信息安全，工作环境和设备运行良好。

2. 指挥中心需配备专人进行管理维护工作，包括清洁卫生、信息化设备维护等。

3. 无关人员需审批同意后方可进入指挥中心。

4. 消防物品按规定位置摆放并随时检查情况是否正常，机房工作人员必须掌握消防技能。

5. 定期维护保养设备，并进行登记。

6. 增强保密意识，做好网络安全工作，不得向无关人员泄露相关账号密码。

二、设备管理以及操作规范

1. 操作人员必须严格按照规定进行设备操作，爱护计算机设备，保持工作环境和计算机设备的清洁。

2. 不得泄露系统登录口令；不得让无关人员使用计算机；不

得擅自让非专业技术人员修改计算机系统设置；

3.严禁利用计算机系统上网发布、浏览、下载、入传送反动、色情和暴力信息； 严禁利用计算机非法侵他人或其他组织的计算机信息系统。

4.任何科室和人员不得违反规定，对计算机信息系统存储、处理或者传输的数据和应用程序功能进行增加、删除、修改、干扰。

5.中心机房和监控指挥中心主机（系统服务器）、网络设备（路由器、交换机、防火墙）及其外围设备由操作人员每周进行一次例行检查和维护，尤其是设备供电、运行状态是否正常等要进行日常检查和维护。

三、软件系统管理制度

1.软件资料需定期进行维护备份。

2.操作人员应具备使用和维护技能。

3.配备应用软件的使用说明和操作指南。

4.确保数据安全、准确，对日常数据进行校验，并进行相应的数据处理。

5.为确保软件系统安全，加密移动硬盘应由专人管理，配备防火器具，确保防磁、防静电、防灰尘等，明确保管责任，遵守出入库制度。

6.保证各系统数据安全、准确，对日常数据要进行校验检查，如发现错误数据，应及时按审批流程进行上报，并根据审批意见

进行数据处理。

四、计算机病毒防范管理

1. 操作人员应具备病毒防范意识，定期进行病毒检测（特别是服务器），发现病毒应立即处理。

2. 采用国家许可的正版防毒软件并及时更新软件版本。

3. 未经领导许可，操作人员不得在服务器上安装新软件，若确需安装，安装前应进行病毒检测。

4. 经远程通信传送的程序或数据，必须经过检测确认无病毒后方可使用。

五、数据保密及数据备份

数据保密

1. 根据数据的保密规定和用途，确定数据使用人员的存取权限、存取方式和审批手续；严禁泄露、外借和转移专业数据信息。

2. 应制定业务数据的更改审批制度，未经批准不得随意更改已在局域网内公布的业务数据。

3. 与非政务网连接的计算机不得录入机密文件和涉密信息。

数据备份

1. 对本科室计算机内的重要数据应制作备份并异地存放，确保系统发生故障时能够快速恢复；数据备份不得更改。

2. 数据备份必须指定专人负责保管，由计算机信息技术人

员按规定的方法同数据保管员进行数据的交接。交接后的备份数据应在指定的数据保管室或指定的场所保管。

3. 数据备份保管地点应有防火、防热、防潮、防尘、防磁、防盗等设施。

六、矫正中心机房，指挥中心安全检查管理。

1. 机房和指挥中心安全是矫正工作安全的重要环节，因此必须坚持定期安全检查。

2. 机房和指挥中心每周最少进行一次巡检，并认真做好检查记录。

3. 对检查中发现的问题进行限期整改，整改后需由主管领导进行督查。

临淄区司法局