

泉州海洋职业学院 人员安全管理

制定： 安全管理员

审核： 信息安全办公室

批准： 信息安全领导小组

版本： V1.0

泉州海洋职业学院

二〇一八年六月

版本控制

| 时间 | 版本 | 说明 | 修改人 |
|------------|------|------|-------|
| 2018.06.12 | V1.0 | 报告建立 | 安全管理员 |
| | | | |
| | | | |
| | | | |
| | | | |

人员安全管理制度

1.1 安全人员组织管理原则

网络信息系统的安全管理的最根本核心是人员管理，提高安全意识，行于具体的安全技术工作中。为此，安全的人事组织管理主要基于以下三个原则。

（一）多人负责

每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，工作认真可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。

负责的安全活动范围包括：

1. 访问控制使用权限的发放与回收；
2. 信息处理系统使用的媒介发放与回收；
3. 处理保密信息；
4. 硬件和软件的维护；
5. 系统软件的设计、实现和修改；
6. 重要程序和数据的更新、删除和销毁等。

（二）任期有限

任何人最好不要长期担任与安全有关的职务，遵循任期有限原则，工作人员应不定期地循环任职，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

（三）职责明确

在信息系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非主管领导批准。

出于对安全的考虑，下面每组内的两项信息处理工作应当尽可能分开。

1. 系统管理与计算机编程；
2. 机密资料的接收和传送；
3. 安全管理和系统管理；
4. 访问证件的管理与其它工作；
5. 计算机操作与信息处理系统使用媒介的保管等。

1.2 安全人事组织管理的实现

信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制订相应的管理制度或采用相应的规范。具体工作是：

（一） 根据工作的重要程度，确定该系统的安全等级；

（二） 根据确定的安全等级，确定安全管理的范围；

对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理可采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记和管理。

（四） 制订严格的操作规程；

操作规程要根据职责明确和多人负责的原则，各负其责，不能超越自己的管辖范围；对工作调动和离职人员要及时调整相应的授权。

（五） 制订完备的系统维护制度；

对系统进行维护时，应采取数据保护措施，如数据备份等。维护时要首先经主管部门批准，并有安全管理人员在场，故障的原因、维护内容和维护前后的情况要详细记录。

（六） 制订应急措施。

要制订系统在紧急情况下，如何尽快恢复的应急措施，使损失减至最小。

1.3 安全管理人员的奖惩制度

泉州海洋职业学院将根据网络信息安全管理制度给予相应奖惩，具体如下

（一）奖励机制

安全管理人员全年无事故（“事故”指违反本制度相关安全规范要求），且当年度累计违规次数未超过1次者，信息安全办公室将在OA系统上公告表扬。

（二）处罚机制

计算机终端硬件、软件及网络按照“谁主管、谁负责”、“谁建设、谁负责”、“谁使用、谁负责”的原则进行管理，一经发现违反本制度的，由登记的责任人承担相应责任。

由信息安全办公室牵头信息公司应定期或不定期巡查学院各部门计算机终端硬件、软件及网络，对本制度的执行情况进行检查。

如发现违反本制度者，视情节轻重、所造成的影响和损失程度、是否初犯或累犯，可采取以下方

式之一进行处理：警告、通报所在小组负责人；通报所在部门分管领导；安全领导部门主管领导处理。违反法律法规构成犯罪的，还将移送司法机关处理。

1.4 安全管理人员教育培训制度

为进一步提高网络信息管理人员对网络信息安全重大意义的认识，增强遵守规章制度和劳动纪律的自觉性，避免网络信息安全事故的发生，确保各项工作顺利进行，特制订本制度。

(一) 定期组织管理员认真学习《中华人民共和国网络安全法》、《计算机信息网络国际互联网安全保护管理办法》、《网络安全管理制度》及《信息审核管理制度》，提高工作人员的维护网络安全的警惕性和自觉性。

(二) 负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《中华人民共和国网络安全法》《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。当存放物品的区域内部的门打开时，一定要保证外部的门是安全的。

(三) 对信息源接入单位进行安全教育和培训，使他们自觉遵守和维护《中华人民共和国网络安全法》、《计算机信息网络国际互联网安全保护管理办法》，杜绝发布违犯《中华人民共和国网络安全法》、《计算机信息网络国际互联网安全保护管理办法》的信息内容。

不定期地邀请公安机关有关人员进行信息安全方面的培训，加强对有害信息，特别是影射性有害信息的识别能力，提高防范能力。