

1.网络与信息安全管理主管部门名称：技术部。

2.公司自系统搭建完成上线以来，公司便设立了以技术部为主的信息安全管理机构，以技术总监钟秋为负责人，以公司整个技术部门为主要实施执行团队，主要负责我公司网站、网络的信息安全工作。

3.公司将依照相关规定完善公司的网络与信息安全保障措施，切实落实安全责任，完善相关管理制度。

4.工作职责

(1) 制定信息安全管理责任制：建立信息安全管理机构，成员包括信息管理员、技术员，对信息安全提供预警、救援、恢复、监控和测评，负责网络与信息安全保障体系建设的规划、协调和监督，并对相关重大事项做出决定。同时要求所有人员在入职后，签订一份网络与信息安全责任书。

(2) 制定网络与信息安全管理年度工作计划：加强考核，落实管理责任制度，以文件形式明确各部门职责，将网络与信息安全工作与员工的日常考核挂钩。所有资料每天、每周、每月、每季度分别备份，保证在出现意外情况或业务中断时，能以最短的时间得到恢复。另外，公司网站每天产生的大量数据，公司会将所有的档案信息，按照每天、每周、每月、每季度、每年进行归档，以便后期可以使用或查找。

(3) 制定重大信息安全事件应急处置和报告制度：根据事件的影响程度等因素分为三个等级：

第三等级：特大信息安全事件，涉及国家和社会稳定，造成恶劣影响和严重后果。

第二等级：重大信息安全事件，涉及国家和社会稳定，造成较大社会影响和较严重后果。

第一等级：一般信息安全事件，造成一定社会影响的信息安全事件。

处理流程：一般信息安全事件发生时，向入侵者所在的网络管理员投诉。

重大信息安全事件及特大信息安全事件发生时，技术部及时保留证据，并立即向应急小组报告。应急小组接到报告后，立即对发生的事件进行调查核实、保留相关证据，确定事件等级，向上级主管部门上报。

报告流程：

第三等级，公司在 2 小时内做出口头报告，24 小时内做出书面报告，事件处理

结束后 5 日内做出专题书面报告。

第二等级，公司在 4 小时内做出口头报告，事件处理结束后 5 日内做出专题书面报告。

第一等级，公司在 2 日内做出专题书面报告。

（4）有害信息发现和过滤技术手段：在网关的设计中，须包含过滤的处理逻辑。设计一张记录信息匹配项的过滤表，网关在初始化时读入，处理每一条信息时，将信息内容和过滤项进行匹配，如果命中，则按规则将匹配的内容过滤或替换成提示信息，然后将原始信息保留到过滤历史记录表中备案。

（5）网络安全防护技术手段：

①在IP资源管理方面，采用IP+MAC捆绑的技术手段防止用户随意更改IP地址和随意更换交换机上的端口。

②在网络流量监测方面，使用网络监测软件对网络传输数据协议类型进行分类统计，查看数据、视频、语音等各种应用的利用带宽。

③ 服务器制定合理的备份策略，每周日晚上做一次完全备份，然后周一到周五晚上做增量备份或差额备份；定期对服务器备份工作情况进行检查。

④使用微软的SUS解决运行Windows操作系统的计算机免受病毒和黑客攻击，将需要升级的软件从Internet下载到公司Intranet的服务器上，为公司内的所有客户端PC提供自动升级，打上所有需要的“补丁”。

（6）监督检查：由网络与信息安全责任人实时监督检查网站信息，决定相应应急预案的启动，负责现场指挥，并组织相关人员排除故障，恢复系统。

网站检查：

①技术人员将公司网站设置为主页，每天上班则进行网站内容及信息检查。

②及时、准确、无误地填写运行记录，对网络异常现象进行反应。

③主动监测网络，随时发现问题，及时查清故障点。

公司内部流程检查：

①由技术部负责人每日对安全负责人员的工作日志进行检查。

②每周对网站所有负责人员对相关制度的执行情况进行检查。

③每个月以考试的形式检查所有人员的法规制度和技术学习执行情况。

④制定一套激励制度，充分调动管理人员积极性。