文档密级：C

第三方人员管理规范

一、 总则

1. 目的

为加强对第三方人员的控制，减少安全风险，防范公司信息资产损失，特制定本制度。

2. 适用范围

适用于公司对第三方人员和供应商的管理活动。

3. 职责

（1） 行政部门

负责统一管理相关方和供应商在信息安全方面的控制活动。

（2） 信息技术部

a) 负责识别本部门的相关方，并与相关方签订保密协议；

b) 负责对相关方的服务进行信息安全控制；

c) 负责定期对相关方进行监督和评审；

d) 负责做好相关方的变更管理。

二、 管理细则

1. 管理对象

我公司的相关方、外包方包括以下团体或个人：

服务提供商：互联网服务提供商、电话提供商、IT 维护和支持服务提供商、软件产品和 IT 系统供应商、绿化服务提供商、打印机租赁方、设备供方。

外来人员：临时人员、实习学生以及其他短期工作人员、外包单位驻点人员、管理服务提供商、管理咨询、业务咨询、外部审核、公司客户。

2. 第三方的信息安全管理

（1） 相关部门应协调信息技术部识别外部相关方对信息资产和信息处理设施造成的风险，并在批准外部相关方访问信息资产和信息处理设施前实

施适当的控制。

（2） 相关部门应与外部相关方签署涉及物理访问、逻辑访问和工作安排条款和条件的《保密协议》，所有与外部相关方合作而引起的安全需求或内部控制都应在协议中反映，在未实施适当的控制之前不应该向外部相关方提供对信息的访问。

（3） 相关部门应识别外包供应商活动的风险，明确供应商活动的信息安全要求，在外包合同中明确规定信息安全要求或签署《保密协议》。

（4） 相关部门应确保外部相关方意识到其义务，并接受与访问、处理、交流或管理组织信息和信息处理设施相关的责任和义务。

3. 外来人员管理

（1） 外来人员主要有：实习人员、参观检查人员、外来技术人员等。

（2） 外来人员由使用部门全程陪同其在公司内的全部活动，如需接触公司非公开涉密信息，需与其签订《保密协议》。

（3） 外来人员的物理访问需遵守公司内部相关制度进行。

4. 供应商的管理

（1） 相关部门供应商选择时，特别是将设备、网络、系统、软件和信息安全等事项外包时，应明确供应商信息安全方面的内容和要求，对供应商提供服务的能力进行评定，

（2） 应确保供应商保持充分的提供服务的能力，并且具备有效的工作计划，即便发生重大的服务故障或灾难也能保持服务的连贯性。

（3） 供应商提供商需提供服务人员的姓名、技术能力评定、联系方式等信息，服务人员需持有效身份证明进入现场。临时服务人员由专业人员全程陪同。

（4） 供应商服务人员在现场或远程服务时，必须明确相关内容，包括时间、地点、联系人、工作安排、预期结果、观察期等。

（5） 对服务提供方技术人员在现场处理需要设备入网时，需选择公共 WIFI 通道，如果需要访问内部系统，需通过经信息技术部总经理同意后方可入网，对系统的巡检和维护需有本公司专业人员陪同，并对开放的权限和时效进行记录，在规定时间内关闭系统权限。如需延期，需要重新申请。

（6） 当服务提供方发生变更时，行政部应进行服务提供方变更登记，并进行服务、现有状态的评估。对变更后的服务提供方进行服务评估。

（7） 当服务内容发生变更时，综合部应进行服务内容变更登记，对服务变更后对现有系统进行评估，确保系统的安全性。

（8） 第三方应提供服务报告，行政部负责对供应商情况进行评价。对不符合要求的供应商提出整改意见，对因整改不符合要求或拒绝整改可能造成事件的供应商，做出限期整改、经济扣罚、终止合同等决定意见。

三、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。
2. 本制度由公司信息安全局负责解释和修订。
3. 本制度自发布之日起开始执行。