

信息系统授权及审批规范

一、 总则

1. 目的

为规范信息安全管理各环节的审批流程和审批责任人，特制订本规范。

2. 范围

本管理制度适用于公司内部信息系统相关的所有授权和审批事项，明确各相关管理环节授权和审批的部门和责任人。

3. 职责

信息安全局负责监督管理，相关部门和相关人员参照执行。

二、 管理细则

1. 内部人员授权管理办法

(1) 根据信息安全领导委员会的主要职责，信息安全各小组组长由信息安全领导委员会授权后生效。信息安全工作小组直接对信息安全领导委员会负责。

(2) 根据信息安全工作小组的主要职责，信息安全各安全岗位的负责人员由信息安全工作小组授权后生效。各信息安全岗位管理人员对信息安全工作小组负责。

(3) 根据信息安全工作小组的主要职责，各业务信息系统的经办人员由各业务单元的相关部门提名产生，最终由信息安全工作小组授权后生效，各业务经办人员对信息安全工作小组负责。

2. 外包人员审批管理办法

(1) 外包运维人员对信息系统每个环节的参与均需要信息安全工作组组长的审批，或者由信息安全工作组组长授权信息安全工作小组成员进行相关审批。

(2) 对于没有经过正式授权的，临时的、紧急的、需要即时审批的信息系统维护需求，可由信息安全工作组组长电话审批同意，但过后需要补充审批记录。

3. 变更审批办法

(1) 变更分类与审批的一般原则：

- a) 信息系统变更主要分两大类：功能优化类变更和系统完善类（bug 修订，补丁修复）变更。
 - b) 功能优化类变更的发起人为业务部门人员。
 - c) 系统完善类变更的发起人为业务经办人员、系统管理人员或系统运维外包厂商人员。
 - d) 两类变更的审批办法和流程基本一致，原则是需要有效识别各类系统变更的风险，并严格按照审批程序有效规避风险、落实相关责任方。
- (2) 变更审批流程：
- a) 变更由上述变更发起人发起，根据变更的具体内容填写相关的变更管理表单。
 - b) 功能优化类变更审批的第一级部门是业务部门，因为不直接牵涉到信息系统的变更，该部分变更由业务经办部门审批，最后一个审批人须是业务经办部门的部门领导或者更高一级的主管领导，具体由业务经办单位自行决定。
 - c) 功能优化类变更审批的第二级审批部门是信息技术部，由信息技术部安排专人评估变更的风险和可行性，评估结果可行后，有信息安全工作组组长审批，信息安全工作组组长审批后交由系统运维人员具体实施，完成系统变更。
 - d) 系统完善类变更可能会涉及到系统的内核，影响系统运行的稳定性。此类变更一般由系统管理员发起，要求系统管理员在发起变更的同时需要就本次变更的潜在风险和风险规避措施进行描述后报请信息安全工作组组长进行审批，信息安全工作组组长审批后由系统管理员进行具体实施，完成系统变更。

4. 关键活动的授权和审批

- (1) 在系统运维过程中，对信息系统的访问、变更等授权给运维管理人员。具体为机房管理员负责机房相关事务的授权和审批；网络管理员负责网络相关事务的授权和审批；主机管理员负责主机相关事务的授权和审批；应用系统管理员负责应用相关事务的授权和审批。
- (2) 授权审批流程：
- a) 由工作组组长判断职责、然后授权给相应的管理员；
 - b) 由外包服务机构申请，相应的管理员进行授权、审批；
 - c) 填写授权审批表。

- (3) 组织信息中心相关人员每季度审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，保存审批文档。

5. IT 设备采购审批办法

IT 设备的采购过程按照《采购管理制度》规定执行，牵涉到信息中心部门审批的环节，均需要信息技术部总经理签字审批认可。IT 设备采购审批的最后一个环节按照公司现有办法，由总务处负责采购执行。

6. 其他审批办法

- (1) 物理访问、系统接入等其他对信息系统（包括 关键业务网、主机房、各业务信息系统）的访问和修改操作，均由信息安全工作组组长授权的信息中心其他人员负责审批并监督后续的访问过程。
- (2) 重要操作，如业务系统功能上的重大调整、重大升级变更、网络架构大的调整，均需要由信息安全工作组组长召集相关人员论证后初审，初审的结果报信息安全领导小组做最后审批后进行。

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。