文档密级：

C

信息安全惩戒管理规范

一、 总则

1. 目的

为建立完整的惩戒处罚机制，对违反信息安全方针和程序的员工进行公正有效的惩戒处理，并作为对可能在其它情况下有意轻视信息安全方针和制度的员工的警示，强化全体员工的信息安全意识，特制定本规范。

2. 适用范围

本程序适用于对违反公司信息安全方针策略、制度规范标准、操作手册等行为，根据造成危害的程度、情节轻重及后果的严重程度给予行政、经济惩戒。

3. 职责

1）人力资源部

负责对违反信息安全相关制度文件的员工进行惩戒处理。负责组织安排员工的信息安全知识教育和信息安全培训等工作。

2）信息技术部

负责信息安全事件调查、分析、处理。

二、 管理细则

1. 对信息安全事件，信息技术部应按《信息安全事件管理规范》进行调查、分析、处理，并将结果报部门总经理。

2. 人力资源部应考虑自然因素、破坏的严重程度、对业务的影响、是初犯还是重复发生、责任人是否受到了适当的培训等其他因素，综合确定处罚结论，经公司分管领导批准后，由相关部门实施。

3. 处罚包括行政处罚和经济处罚，可同时实施，经济处罚不受经济责任制考评结果的影响与限制，具体的处罚方式，按照人力资源部发布的《员工手册》相关条款执行。

4. 如果属于故意行为导致重大信息安全事件，造成严重影响的，解除劳动合同并依法追究法律责任。

5. 员工和第三方用户在明显故意性的严重情况下，屡次违背公司信息安全

C

策略和标准以及进行其它安全破坏，公司可以立刻解除信息资源访问权限，并追究相关责任。

6. 对于故意制造、传播病毒，或使用电子邮件炸弹等黑客攻击手段，攻击信息系统，包括篡改、删除信息系统数据、程序及相关配置等行为，给公司经济和社会形象造成重大影响的，一经发现并查实，系内部人员的按本程序第3、4 条处理。

7. 对第三方用户违背我公司安全策略和程序以及进行其它安全破坏，按相关的法规、业务合同规定惩戒，公司保留追究经济和法律责任的权利。

8. 对于信息安全事故责任人的处理结果由处理部门在集团范围内予以通报。

三、 附则

1. 本制度由公司信息安全局负责解释和修订。

2. 本制度自发布之日起开始执行。