

附件一：

温州市国有企业信息安全等级保护 推进工作实施方案

保护国有企业信息系统的安全稳定运行，对于促进企业健康发展，维护我市经济安全和社会稳定具有重要意义。为全面落实国家信息安全等级保护制度，进一步加强我市国有企业的信息安全工作，保障和促进企业的信息化发展，根据公安部、国务院国资委《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字〔2010〕70号）及浙江省公安厅、浙江省人民政府国资委《关于加快推进我省国有企业信息安全等级保护工作的通知》（浙公通字〔2011〕37号）精神，结合我市实际情况，制定本实施方案。

一、指导思想

以公安部、国务院国资委和省公安厅、省国资委有关加快推进国有企业信息安全等级保护工作的意见为指导，通过全面推行国有企业信息安全等级保护工作，切实将信息安全等级保护工作纳入国有企业信息化工作同步规划，提高我市国有企业信息安全的保障能力和防护水平，维护国家安全、社会稳定和公共利益。

二、工作目标

将信息安全等级保护工作纳入国有企业信息化工作，通过对我市国有企业信息系统实行等级保护工作，全面梳理摸清我市国有企业信息系统备案情况，完成国有企业信息系统的定级工作；同时在定级备案工作的基础上，开展信息安全等级保护等级测评和安全建设整改工作，规范国有企业信息安全等级保护管理，完善重要信息系统安全防护体系，确保信息系统安全保护能力达到等级保护要求。

三、组织分工

为加强信息安全等级保护工作的领导，成立由市公安局、市国资委组成的市国有企业信息安全等级保护工作协调小组（附件 1，以下简称：市协调小组），负责组织市属国有企业开展信息安全等级保护工作，并开展信息安全等级保护工作的宣传、培训、监督和先进经验推广工作，监督指导全市各地开展信息安全等级保护工作。

各县（市、区）也要参照成立由公安机关和国资监管部门组成的国有企业信息安全等级保护工作协调小组负责组织本地所属国有企业开展信息安全等级保护工作，并做好本地信息安全等级保护工作的宣传、培训、监督工作。

各国有企业要成立主管领导参加的信息安全等级保护工作领导小组，并确定职能部门负责本单位的信息安全等级保护工作，开展信息系统定级、备案、安全建设整改、

等级测评、自查等工作，并接受公安机关和主管部门对信息安全等级保护工作的监督、指导。

四、工作安排

（一）前期准备阶段（2011年7月1日至2011年7月30日）

1 各县（市、区）成立由公安机关和国资监管部门组成的国有企业信息安全等级保护工作协调小组，并建立工作协调小组与国有企业之间的信息安全等级保护联络员制度，以便沟通、交流和指导。联络员具体负责本单位等级保护工作的日常联系工作。

2 各协调小组组织所属国有企业开展全市国有企业开展信息安全等级保护的排查摸底工作，全面掌握重要信息系统的底数、承载的业务、系统结构等基本情况，为后续工作做好准备。

3 市县两级协调小组举办信息安全等级保护工作部署动员会，具体部署信息安全等级保护工作。

4 分批次召集市县两级国资监管部门下属国有企业具体负责本单位信息安全等级保护工作的人员进行相关业务知识培训。培训主要内容为信息安全等级保护有关法律法规、实施细则及具体工作步骤。

（二）组织实施阶段（2011年8月1日至2011年9月30日）

1、自主定级

在摸清信息系统定级备案情况后，对尚未开展信息系统定级的国有企业，应按照“企业自主定级、专家评审、主管部门审批、公安机关监督”的原则，抓紧开展信息系统自主定级工作，并将定级材料报送所属协调小组并由其初审，再由市协调小组汇总。定级材料包括：

1)信息系统信息安全保护等级备案登记表(以下简称：备案表)

2)信息系统信息安全保护等级自定级报告(以下简称：定级报告)

3)本单位信息系统安全组织的建立情况

4)本单位信息系统基本应用情况

5)本单位信息系统使用的主要设备、操作系统、数据库、防病毒软件以及网络拓扑图

6)其他与等级选定或者审定有关材料。

2 组织评审

市协调小组将汇总后的定级材料转送市信息办，由市信息办组织我市有关信息系统安全保护等级评审专家对其进行定级评审工作，并出具信息系统信息安全等级保护定级专家评审报告。

3 等级测评

在完成信息系统定级评审工作后，各国有企业要根据

企业特点，从《浙江省信息安全等级保护工作协调小组关于公布信息安全等级保护测评机构的通知》(浙等保〔2010〕9号)(详见附件2)中自行选择测评机构，对本企业信息系统开展等级测评，对于在等级测评工作当中发现的系统安全问题、漏洞和安全隐患，国有企业要及时制定方案开展整改，以符合安全保护等级要求。

4 书面备案

国有企业信息系统在经自主定级、评测、整改达到所定等级安全要求后，必须向公安机关补充提供以下有关材料：

1)本单位信息系统等级保护制度(含安全等级保护职责的责任部门和人员管理制度；信息安全等级保护系统建设运行维护制度、信息系统安全检查、检测和风险评估制度；安全教育和培训制度)

2)本单位信息系统安全保护整体需求分析及安全策略报告

3)本单位信息安全事件等级响应和处置预案

4)本单位信息系统信息安全等级评估报告

5)本单位信息系统信息安全等级保护建设方案

6)本单位信息系统信息安全等级保护工作验收报告

7)系统使用的信息安全产品清单及认证、许可证明。

公安机关收到备案材料后，应认真审核备案材料，对

定级合理、材料齐全的，应当完整准确记录和保存备案登记信息和登记材料，建立备案登记档案，对符合安全保护等级要求的，公安机关颁发信息系统安全等级保护备案证明。

（三）巩固完善阶段（2011年 10月 1日至 2011年 11月 30日）

信息系统信息安全等级保护备案工作完成后，各国有企业应当建立完善信息系统安全状况日常检测工作制度，加强对信息系统的日常维护和安全管理工作，及时消除安全隐患，确保信息的安全和系统的正常运行。各级公安机关根据有关规定对各国有企业信息安全等级保护工作进行监督检查。

五、工作要求

（一）提高认识，加强领导。信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。为此，县两级协调小组以及下属国有企业，要充分认识开展信息安全等级保护工作的重要性、必要性，切实增强政治责任感和工作紧迫感，全面贯彻落实中央、国务院和省、市政府的要求和部署，加强对下属国有企业的领导，督促其切实做好信息安全等级保护工作。

（二）动员部署，开展培训。市县两级协调小组要按照统一部署，广泛进行宣传动员，加强培训，指导下属国有企业按照信息安全等级保护工作的总体要求，分阶段、分步骤完成各项工作任务。市县两级协调小组还要就信息安全等级保护工作规范、标准等内容对国有企业进行相关培训。各国有企业要积极委派专职人员接受培训。

（三）认真落实，及时报送。各国有企业需认真填写《国有企业信息安全等级保护工作自查表》（详见附件 3）以便排查摸底和建立联络员制度，并于 2011 年 7 月 15 日前上报所属协调小组；再根据《信息系统安全等级保护定级指南》等技术标准开展定级工作，并参照样本（详见附件 4、5）撰写《定级报告》和《备案表》等材料按规定时间上报所属协调小组。待专家评审通过后，开展等级测评、安全整改及书面备案工作。在整个等级保护工作流程中，各国有企业要按照有关要求，向所属协调小组及时报送开展信息安全等级保护工作的有关情况和数据。