

信息安全学习总结 (精选4篇)

篇1：信息安全学习总结

今年以来，全市从落实各项安全管理制度和规范入手，积极有效地开展了政府信息安全工作，主要完成了以下五项工作：

1. 落实信息安全规范。全市范围内逐步推行《苏州市电子政务网信息安全规范》，所有接入苏州电子政务网系统严格遵照规范实施，按照七个区、五个下属市、市级机关顺序，我委定期组织开展安全检查，确保各项安全保障措施落实到位。

2. 组织信息安全培训。面向全市政府部门CIO及信息安全技术人员进行了网站渗透攻击与防护、病毒原理与防护等专题培训，提高了信息安全保障技能。

3. 加强政府门户网站巡检。定期对政府部门网站进行外部web安全检查，出具安全风险扫描报告，并协助、督促相关部门进行安全加固。

4. 狠抓信息安全事件整改。今年，省通信管理局通报了几起我市政府部门主机感染“飞客”蠕虫病毒、木马受控安全事件，我市高度重视，立即部署相关工作，向涉及政府部门发出安全通报，责令采取有力措施迅速处置，并向全市政府部门发文，要求进一步加强政府门户网站安全管理。

5. 做好重要时期信息安全保障。采取一系列有效措施，实行24小时值班制及安全日报制，与重点部门签订信息安全保障承诺书，加强互联网出口访问实时监控，确保世博会期间信息系统安全。

信息系统安全检查工作开展情况及检查效果

按照省网安办统一部署，我市及时制定了《XX年度苏州市政府信息系统安全检查工作方案》，五市七区及市级机关各部门迅速展开了自查工作，**家单位上报了书面检查报告，较好地完成了自查工作。在认真分析、总结前期各单位自查工作基础上，9月中旬，市发改委会同市国密局、市公安局和信息安全服务公司抽调21名同志组成联合检查组，分成三个检查小组，对部分市和市级机关重要信息系统安全情况进行抽查。检查组共扫描了**个单位门户网站，采用自动和人工相结合方式对**台重要业务系统服务器、**台客户端、**台交换机和**台防火墙进行了安全检查。

检查组认真贯彻“检查就是服务”理念，按照《工作方案》对抽查单位进行了细致周到安全巡检，提供了一次全面安全风险评估服务，受到了服务单位欢迎和肯定。检查从自查情况核实到管理制度落实，从网站外部安全扫描到重要业务系统安全检测，从整体网络安全评测到机房物理环境实地勘查，全面了解了各单位信息安全现状，发现了一些安全问题，及时消除了一些安全隐患，有针对性地提出了整改建议，并出具了18份书面检查报告，督促有关单位对

照报告认真落实整改，工作总结《信息安全工作总结》。通过信息安全检查，使各单位进一步提高了思想认识，完善了安全管理制度，强化了安全防范措施，落实了安全问题整改，全市安全保障能力显著提高。

全市信息状况总体评价

综合信息系统安全自查和抽查情况看，我市信息系统安全工作整体情况良好，尤其在组织机构、制度建设和日常管理方面，比较完善规范，个别单位还通过了ISO9001质量管理认证，采取了有效安全防护措施，信息安全工作得到了各单位领导普遍重视。但在风险评估、等级保护、应急演练以及经费保障上面都有待于加强。

主要存在问题

经过本次信息安全自查，对照检查标准，主要存在以下一些问题：

1. 部分单位规章制度不够完善，未能覆盖信息系统安全所有方面。
2. 少数单位工作人员安全意识不够强，日常运维管理缺乏主动性和自觉性，存在规章制度执行不严、操作不规范情况。
3. 存在计算机病毒感染情况，特别是U盘、移动硬盘等移动存储设备带来安全问题不容忽视。
4. 信息安全经费投入不足，风险评估、等级保护等有待加强。
5. 信息安全管理人員信息安全知识和技能不足，主要依靠外部安全服务公司力量。

整改措施

针对上述发现问题，我市积极进行整改，主要措施有：

1. 对照要求，要求各单位进一步完善规章制度，将各项制度落实到位。
2. 继续加大对机关全体工作人员安全教育培训，提高信息安全技能，主动、自觉地做好安全工作。
3. 加强信息安全检查，督促各单位把安全制度、安全措施切实落实到位，对于导致不良后果安全事件责任人，要严肃追究责任。
4. 继续完善信息安全设施，密切监测、监控电子政务网络，从边界防护、访问控制、入侵检测、行为审计、防毒防护、网站保护等方面建立起全方位安全防护体系。
5. 加大应急管理工作推进力度，在全市信息安全员队伍基础上组建一支应急

支援技术队伍，加强部门间协作，完善应急预案，做好应急演练，将安全事件影响降到最低。

信息系统安全检查是一项非常有效、非常重要工作方式，能够督促我们及时发现问題，解决问题。但是，信息安全保障是一项长期工作，过去安全不等于现在安全，现在安全不等于将来安全，需要建立长效机制，加强日常管理。

要做好信息安全工作，思想是保障，制度是根本，坚持是关键。强化信息安全意识提高，高度重视信息安全，规范日常操作，是做好信息安全工作重要保障；不断完善各项信息安全制度，做到有章可循，有章必循，严格按照制度来执行，用制度管好人，用人管好技术，信息安全工作才能取得预期效果；信息系统安全维护管理工作必须持之以恒，常抓不懈，以高度负责态度把各项安全工作认真落到实处。

信息安全工作必须坚持统一规划、统筹管理、分步建设原则。全市信息安全工作整体一盘棋，在科学、统一信息安全规划指导下，按照《苏州市电子政务网信息安全规范》(以下简称安全规范)要求，进行统筹管理，根据“重点保护、分等级保护、同步建设”原则分步建设，做到成本和安全间动态平衡，反对把信息安全问题绝对化、静止化、夸大化。苏州电子政务外网分成根区域、节点区域、叶子区域三种区域，每个区域有着不同安全要求，采取不同安全策略，重点关注区域间互联，对区域边界进行安全控制，来隔离区域间安全风险，阻断区域间风险传递。

必须强化电子政务项目安全管理职能。按照同步建设原则，各部门在信息化项目立项时要确定安全等级，项目验收时将安全审计作为重要内容之一，安全防护措施未达到相应安全等级，不予通过验收。

针对检查中发现一些主要问题，我们将加大信息安全投入力度，将信息安全经费列入单位年度预算，对重要单位、重要信息系统强制配备必要信息安全设备；加大信息安全检查力度，将信息安全检查工作纳入单位工作考评体系，定期、不定期对各单位信息安全实行检查，提高信息安全检查工作力度和效率；加大信息安全培训力度，对各单位信息安全主管和人员定期进行培训，使得负责信息安全人员能够具有一定安全知识，掌握必须安全技能，胜任信息安全工作。

篇2：信息安全学习总结

一、20XX年信息安全工作情况

〔一〕重点工作开展状况公司坚持“安全第一、预防为主、综合治理”的信息安全方针，全面加强“人防、制防、技防、物防”的“四防”工作，细化安全治理、深化技术督查、建立健全信息安全治理体系，加大信息安全根底设施建设投入，强化信息系统运维治理工作，坚持信息安全“八不准”，实现了“三个不发生”的安全目标，保障了全年信息安全。

细化信息安全治理为加强信息安全保密治理工作，编制了《重庆市电力公司

员工信息安全与保密手册》、《重庆市电力公司计算机治理方法》等规章制度，并将保密手册印刷成册，做到每个员工人手一册。增加了员工的信息安全保密意识，标准了员工的信息安全行为，使公司计算机设备治理更加标准化。

乐观开展信息安全技术督查

1)建立信息安全督查工作常态化机制在深入开展信息安全保障工作根底上，成立了重庆市第一支企业化的信息安全督查队，将信息安全督查工作常态化、固定化、流程化。制定了《重庆市电力公司信息安全督查治理方法》，依据该治理方法，公司先后开展了“春节及两会专项督查”、“供电公司信息安全督查”、“迎世博信息安全督查”等多项工作。5月21日至22日，通过了国网公司督查组对重庆公司的信息安全专项督查并获得良好评价。

2)开展信息安全反违章专项行动为努力实现“三个不发生”根本安全目标，根治违章顽疾，消退事故隐患，全面提高信息系统“可控、能控、在控”水平，公司编印了《重庆市电力公司开展信息安全“反违章”专项活动方案》下发到公司各单位。通过开展信息安全“反违章”专项活动，组织全员学习《信息安全反事故基线措施》，进展信息安全宣传教育；重点督查了信息安全“八不准”、隐患消缺机制落实等状况，并准时对公司邮件系统和应用系统觉察的弱口令进展了整改。

加强应急演练和专项安全保障

1)组织应急演练公司首次成功举办了由信通公司、江北供电局、杨家坪供电局和超高压局参与的信息广域网联合应急演练。转变了广域网故障排除以前大家各自为阵的局面，取而代之的是先进的远程统一指挥协作。通过本次演练，为今后信息系统突发性故障远程统一指挥、协同处置供给了的模式。

2)保障迎峰度夏和世博会期间的信息安全为确保迎峰度夏和世博会期间的网络与信息安全，公司开展了以下三方面的工作，一是完善信息系统应急处理机制。二是开展了安全区域、分区防护、终端安全接入等方面的划分工作，强化业务应用系统与核心设备的综合防护，加大互联网出口和对外效劳系统的安全巡检与防恶意攻击。三是强化运维值班制度，尤其是在重要、特别时期的值班治理。

信息安全人才梯队建设

1)举办公司首届信息化技能竞赛在全公司组织开展了首届信息化技能竞赛。公司直属单位、控股供电公司共计40家单位参与竞赛。本次竞赛的开展对建设信息化高技能人才队伍、优秀信息运维队伍、进一步提高全公司信息化建设水平具有重要意义。

2)开展进大学生信息安全培训坚持从源头抓信息安全教育，不断创信息安全教育培训工作。每年对进大学生开展信息安全学问培训，使每位大学生在正式走上工作岗位前就深刻领悟信息安全的重要性，敲响安全警钟，结实树立信息安全意识，在今后的工作中严格遵守

信息安全和保密相关规章制度。

〔二〕工作的突破和创：信息安全标准化体系建设参照ISO27001标准建立了公司信息安全标准化治理体系。已梳理原有11方面共计64个信息安全规章制度，编了24个制度、修订了20个制度，保证了公司信息安全治理体系的先进性和完整性。

二、形势分析和重要问题争论

〔一〕面临的形势随着国网公司SG186工程的不断深入，越来越多的系统投入运行，信息系统安全运行工作的重要性更加凸显。SG186工程对于国网公司，乃至对于整个电力行业都是一个跨时代的大事，通过建立“纵向贯穿、横向集成”的一体化企业级信息集成平台，公司系统实现了上下信息畅通传输和数据共享，由于SG186工程主要是大集中模式，使得信息安全大事已成为一个全局性的、能影响整个公司的较大威逼。因此必需建立有效的觉察、报告、处理、解决信息安全工作机制。

公司作为公共效劳行业之一，假设信息安全得不到有效保障，在患病恶意攻击等破坏行为的状况下，可能造成局部或整个系统瘫痪，影响公司正常生产业务和对外效劳。在加快推进公司信息化建设的同时，必需全面提高信息安全的整体防范力量，加强系统运行维护工作。

〔二〕需要着力解决的重要问题及措施公司要建立健全信息安全保障、监视体系，乐观防范和综合防范信息技术风险，增加信息系统安全预警、应急处理和灾难恢复力量，保证网络和信息系统功能正常发挥，不断提高信息系统安全稳定运行水平。

强化信息安全意识目前还有个别员工使用信息内网终端直接连接互联网，给公司带来巨大信息安全隐患，甚至可能造成信息泄露大事。这些行为充分说明个别员工的信息安全意识仍旧淡薄，需进一步强化员工信息安全意识。

健全信息系统运维体系健全信息系统运维体系，人员保障是根本。依据国网公司工作部署，公司2022年建立了“两级三线”信息运维体系。但目前由于信息系统建设、运行、治理工作呈现点多面广的局面，加之个别单位未建立专业的信息化机构，运维人员极其缺乏，很难连续深入细致地开展信息化工作。

三、2022年信息安全工作思路和重点工作安排

〔一〕工作思路20xx年信息安全坚持“安全第一、预防为主、综合治理”的工作方针，以确保信息系统运行安全和信息内容安全为目标，全面加强“人防、制防、技防、物防”的“四防”工作，落实安全责任。以“制度完善”为根底，以“体系健全”为关键，以“措施强化”为手段，以“队伍建设”为保障，进一步完善公司信息系统运维体系，严峻安全运行纪律，深化安全治理，加强技术手段应用。全面深化应用信息运行综合监管系统〔IMS系统〕，着力加强信息系统运行监控，变被动处理为主动防范，持续提升信息系统运维安全保障水平，为公

司两个转变和智能电网五大体系建设供给支撑。

〔二〕重点工作1.强化信息安全责任制，坚决做到信息安全“八不准”，确保“三个不发生”信息安全关系到公司电网安全，关系到国家安全。一是各单位要坚持将信息安全纳入公司安全生产治理体系中，将信息安全纳入信息化工作中，将信息系统等级保护纳入信息安全日常治理工作中。二是要依据“谁主管谁负责、谁运行谁负责、谁使用谁负责、谁督查谁负责”的原则，抓好信息安全责任落实。抓安全生产必需抓信息安全，抓保密工作必需抓信息安全。三是完善以各单位要成立一把手任组长的信息化领导小组和分管领导任组长的信息安全领导小组，落实信息安全组织机构、编制、人员等方面工作，贯彻执行国家和公司发布的各项信息安全规章制度，把安全责任和安全措施落实到每个环节、每个岗位和每位员工。四是健全信息化治理运维部门及人员配置，完善本单位的信息化运维考核治理方法，确保责任到位、治理到位、措施到位、执行到位。

建立健全信息安全制度体系建立健全信息安全过程治理的制度、流程、标准体系，实行信息系统安全规划、打算、实施、运行、督查的全过程管控。对信息安全制度、标准进展滚动式修订，持续夯实公司信息安全标准化治理根底。

持续强化信息安全根底治理

一是强化信息安全教育培训，引入信息安全仿真培训平台，将原有单次现场培训调整为通过网络屡次、周期化培训，按季度、半年滚动进展，不断强化和提高员工信息安全意识和行为标准；

二是深化现有信息安全防范体系建设，加强信息外网安全防护，对信息外网终端进展标准化治理，提高信息外网对DDos攻击防护力量。推广实施信息安全接入平台及安全终端、非法外联监测系统、身份认证〔RA〕系统、文档保护系统、统一漏洞补丁治理系统；

三是推广实施信息安全综合治理体系，主要包括合规掌握、风险掌握、治理掌握等方面；四是推动智能电网信息系统安全接入，依据国家电网公司统一坚强智能电网信息安全总体方案要求，争论重庆公司用电采集系统、输电线路监测系统、仓库治理系统和车辆治理系统的安全接入工作。

切实提高信息系统运行水平

一是依据电网安全生产和运行治理的要求强化信息系统运行治理，建立一套先进的信息调度运行体系。进一步将全部信息系统纳入公司统一信息运行队伍，严峻安全运行纪律，严格运维监控、运行维护、打算检修、故障通报处理等环节。

二是开展运维操作标准化建设。制定信息系统运行《标准作业指导书》，实施标准化作业流程〔SOP〕，对操作前、中、后三个环节执行严格治理。严格执行工作票制度，严格故障处理、升级和配置变更、投运与停运等操作流程的审批；

通过安全审计系统对全部操作进展全程记录，实现对运行操作从审批、执行到检查、审核各主要环节的全过程管控。运行操作人员实行持证上岗操作制度，重要操作必需两人在场，有人监护执行。加强运行现场工作的科学治理，标准运行操作标准，提高系统运维质量。

三是加强“三同步”工作。确保信息安全措施与SG-ERP各业务建设的同步规划、同步实施、同步投运，使信息系统全生命周期安全治理贯穿信息系统规划、设计、实施、运维、废弃五个阶段，明确界定各涉及部门责任要求。建立信息系统安全评审制度，搭建应用系统工程管理平台，从安全治理、安全技术方面对信息系统进展安全管控。

深化信息安全督查工作

一是通过完善信息安全技术督查队伍的装备、工具，建设信息安全试验室等手段逐步完善信息安全督查队伍的硬件设施，提高技术检查的准确性和准确度。

二是贯彻“全员参与、全员合格、全员保安全”的宗旨，结合电监会和国网公司培训、技术沟通等形式，开展信息安全督查人员持证上岗培训，提高信息安全督查队员的业务技能，推动信息安全督查工作标准化、规范化，打造一流的信息安全技术督查队伍。

三是建立督查挂牌“消缺”制度，加强督查觉察问题的整改工作机制。深化日常、专项督查工作，开展信息安全高级督查。加强督查通报，建立公司督查标杆，推广督查典型阅历。整合并扩大督查工具功能，搭建安全督查工作平台，通过安全督查专家分析，提高督查工作效率，标准督查工作。

大力培育信息系统运维人才推广运维队伍持证上岗工作，拓展运维人员视野，适应信息技术日新月异进展的潜在要求，提升运维人员监测、响应和主动觉察威逼的力量，产品技术掌控力量，风险准时觉察处置力量，建立一支高素养的信息运行维护人才队伍，确保公司信息系统安全稳定牢靠运行。

篇3：信息安全学习总结

跟着计算机网络技术的快速发展，信息技术正以惊人的速度浸透到金融行业的各个领域。可是，信息技术又是一把“双刃剑”，它为银行经营管理带来巨大发展机会的同时，也带来了严重的挑战，网络信息的安全性变得愈来愈重要。特别是好像瘟疫般的计算机病毒以及危害公共安全的歹意代码的宽泛流传，波及到计算机的犯法案件快速增加，造成的损失也愈来愈大。基于此，对于初入建行的我们而言，学好银行信息安全知识显得尤其重要。下午，个金部的周经理给我们详尽解说了一些有关银行的信息安全知识，并介绍了建行的邮件都办公系统的使用方法，周经理的解说深入浅出，让我们在较短的时间内对建行职工在信息安全方面应当掌握的知识有了一个比较全面的认识，也为我们此后正式走上工作岗位确立了基础。

经过下午的学习，我们认识到了一些常犯的信息安全方面的错误，比方：开

着电脑走开，就像走开家却忘掉关灯那样;轻易相信来自陌生人的邮件，好奇翻开邮件附件;使用简单猜想的口令，或许根本不设口令;事不关己，高高悬起，不报告安全事件等等。也知道了在此后的工作中我们在信息安全方面该怎样要求自己：1、成立对信息安全的敏感意识和正确认识2、清楚可能面对的威迫微风险3、恪守各项安全策略和制度4、在平时工作中养成优秀的安全习惯。

信息安全对于金融机构特别是银行来说是至关重要的，只需出现一点问题，不单会对公司造成严重的损失，还会对人民的财富造成威迫。所以，作为金融机构一定成立一个完好的信息安全系统。而对于我们建行职工而言，一定学好银行信息安全知识，能正确辨别有关风险并及时报告，防微杜渐，努力提高自己的信息安全水平。

篇4：信息安全学习总结

通过学习计算机与网络信息平安，使我更加深刻的理解网络信息平安的重要性。网络信息平安是爱护个人信息的完好性和保密性的重要条件，只有明白了网络信息平安的基础学问，我们才能更加的了解网络信息平安在如今信息化时代的重要性！

如今信息化的时代，我们每个人都需要跟着时代的步伐，那么我们不缺乏使用电脑信息工具，那么我们需要了解网络的好处和风险，利弊都有，我们需要把弊端降到最低，把利处合理利用，使我们在网络时代不会落后；如今我们每个人的信息都会在网络上面，只是看你如何爱护自己的信息呢？你的个人电脑会不会被黑客攻击？你注册的会员网站会不会泄露你的信息呢？等等！全部这些，都可视为网络信息平安的一部分。

经过学习我才更加的熟悉到网络平安的重要性，由于我们每个人都基本在使用电脑，个人电脑有没有被黑客攻击，病毒侵害呢？每个人的个人电脑都会存储好多个人信息和重要文本文件，那么我们为了保障这些文本信息的平安不被篡改，我们就需要更加深刻的熟悉网络信息平安的重要性，并不断学习和提高自己的'网络平安技能，可以爱护好自己的网络信息平安。比方我们的个人电脑大家估量在不经意间已经把自己的好多重要文件给共享了，你其实不想让大家知道你的隐秘文件的，却不知道怎么都把这些文件给共享给大家了，好多黑客可以很简单侵入到你的个人电脑的，所以我们需要更多的了解网络平安的基本学问。

另外我们每天的新闻都会有好多网络犯罪案件，这些都是个人信息的泄露，不是个人网上银行密码被盗，就是网络个人信息泄露犯罪，所以这些呢都是需要我们重视的，如今第三方支付平台和网上零售等的不断进展我们更是需要提高对计算机网络信息平安的熟悉，特殊是对计算机类专业的学习，更是提出了一个新的要求，那就是我们必需拥有丰富的网络信息平安的学问，我们仅仅知道文本等的加密那是完全不够的，时代在进步我们更需要进步，所以我们需要在了解计算机网络平安基础学问的同时，进一步提高自己的信息平安学问。

网络信息平安需要简洁的熟悉到文件的加密解密，病毒的防护，个人网络设置，加密解密技术，个人电脑的平安防护，生活中的网络泄密和不经意间的个人信息泄露，等等；有时候我们个人的信息是自己泄露的，只是我们没有留意，我们的生疏人可以简洁的通过你的个人主页，你的网络言论中分析得到你的个人资料，你会不经意间说明你的所在的城市小区等等

，这都是不经意间消失的，那么你的不留意有可能就被另外一些人所利用了，所以我们需要留意在网络信息时代的用词和个人信息的爱护，提高防护意识！