公司网络安全工作计划

篇1：公司网络安全工作计划

202*年互联网网络安全形势严峻，企业信息、商业机密、客户信息等信息安全保护工作十分重要。为了更好地落实网络安全相关工作，增强网络安全防护意识，强化网络与信息安全管理能力，现将网络安全相关工作安排如下：

一、组织机构调整为有效贯彻落实工信部、自治区通信管理局、市委网信办、区公司等上级单位网络安全工作要求，为分公司网络安全管理工作的顺利开展，切实落实“单位法人是网络安全第一责任人，分管网络安全的负责人是直接责任人”的责任要求，做好两部委网络与信息安全责任考核、网络安全自查等专项工作，分公司进一步调整完善网络安全领导小组、工作组成员及职责。

（一）领导小组领导小组主要负责在区公司与相关部门的指导下，全面强化对本单位网络安全工作的管理、指导，切实抓好工作落实，督促各单位网络安全工作实施，做到保质保量按时完成各项工作。组长：总经理副组长：分管网络副总经理、分管市场副总经理、分管综合副总经理成员：网络部、市场部、集团客户部、渠道运营中心、客户响应中心、工程建设部、综合部、财务部等各部门总经理、各旗县分公司总经理。

（二）工作组领导小组下设工作组：组长：分管网络副总经理副组长：网络部总经理、综合部总经理、市场部总经理、客户响应中心总经理、集团客户部总经理成员：网络部综合维护中心总经理、网络部网络优化中心总经理、市场部业务支撑中心总经理及分公司各部门分管网络安全副总经理。主要职责：贯彻落实区公司相关工作要求及分公司网络安全领导小组的工作要求，配合通管局、两部委、市委网信办、公安开展各项网络安全检查工作，统筹协调相关单位实施信息安全统筹规划、不良信息治理、客户信息保护、网络安全专家团队建设、安全培训和技术研究等各项网络安全相关工作，全力推进网络安全责任考核及防范打击通讯信息诈骗等工作的常态化管理和落实。

二、各单位职责按照“谁主管谁负责”的原则，各责任单位负责本单位及业务管理、维护管理范围内的网络与信息安全工作，制定本单位网络与信息安全工作要求及相关制度规章，并组织学习宣贯。同时还应负责以下工作：网络部：全面负责网络安全相关工作。制定网络安全工作全年工作计划；对相关文件、规章及工作要求进行组织学习宣贯；定期开展网络部维护设备的安全及风险防控工作，并对发现问题进行相关整治工作；推进“金库模式”应用工作；监督涉及其他单位的网络与信息安全风险整治；制定网络安全威胁处置流程，并按要求进行工作处理；配合公安部门做好问题号码、IP地址的查询工作，以及“伪基站”打击治理工作。市场部：负责牵头开展客户信息安全防护专项工作；负责开展深化“金库模式”应用工作，用户信息模糊化管理，落实客户信息保护工作要求，落实电信业务实名制；负责网络安全类投诉的分析与处置；通过手机短、彩信向用户发送防范通信信息诈骗预警类、提醒类消息。集团客户部：负责本部门相关业务的实名制落实工作及白名单管理；全面负责专线出租业务、“一号通”“400”业

务等集客相关业务的规范管理；负责集客主管业务产生的网络与信息安全举报受理工作。渠道运营中心：负责管理社会营销渠道代理资质审核、代理行为监管；落实电信业务实名制；利用营业厅张贴电信网络诈骗犯罪预警提示；负责到厅或网厅渠道产生的网络与信息安全举报受理工作。客户响应中心：负责本部门维护范围内客户设备、终端等信息安全漏洞及风险进行清理整改。推进“金库模式”应用工作；负责对MAS机开展日常安全风险排查整改；综合部：负责公众教育及对外宣传，积极营造网络与信息良好社会舆论环境；负责通过制作播放视频材料、悬挂警示标语、张贴防范提示、发放宣传资料等方式，普及法律知识，提高公众对各类电信网络诈骗的鉴别能力和安全防范意识。旗县市区分公司：负责本单位维护范围内专线及家庭宽带客户设备、终端等信息安全漏洞及风险进行清理整改；落实客户信息保护工作要求，落实电信业务实名制；负责集客业务实名制落实及白名单管理；对垃圾短信投诉进行处置；负责在管辖区域向公众发布电信网络诈骗犯罪预警提示；利用营业厅张贴电信网络诈骗犯罪预警提示；负责本地区举报投诉处理；配合网络部做好“伪基站”打击治理。

三、202*年网络安全工作内容

（一）网络安全自查工作牵头部门：网络部责任部门：网络部、市场部、集团客户部、客户响应中心、工程建设部、综合部及旗县分公司。配合上级单位开展202*年网络安全检查及做好网络安全工作责任落实情况、网络安全防护情况开展自查。对自有关键信息基础设施的数量、分布情况、网络安全管理机构、运维机构等情况进行梳理。定期对分公司重要信息系统进行漏洞扫描、合规配置检查，在网络安全检查中“零”隐患上报；对2018年网络安全检查中发现问题的整改效果进行自查，做到整改有效，确保202*年全年不出现网络安全重大问题。

（二）持续提升网络与信息安全技术手段建设牵头部门：网络部责任部门：网络部、市场部、集团客户部、客户响应中心、工程建设部、综合部与旗县分公司。信息系统建设必须符合“三同步”与配套保障工作要求，开展“三同步”实施情况自查工作，发现问题第一时间整改；确保承载网站专线100%接入IDC/ISP系统并进行备案，发现漏备或未接入系统的专线，立即整改；加强网络威胁监测，针对异常流量、敏感漏洞、病毒做好防范工作，做到全年不出现网络安全重大事故；做好日志留存工作；按照有关规定要求，做好特殊通信技术接口配备和系统建设工作。加强人员培训，提升维护人员网络威胁监测能力。

（三）数据安全管理工作牵头部门：市场部责任部门：网络部、市场部、集团客户部、客户响应中心、工程建设部、综合部与旗县分公司。完善数据安全组织保障体系，建立健全数据安全制度，有效落实数据安全管理责任，责任落实到个人，加强数据安全和用户个人信息保护。根据区公司有关指导文件建立完善数据安全管理制度开展客户侧数据安全防护工作。与此同时开展对外合作数据安全防护工作，对外合作项目做到100%签订安全协议，明确合作方的数据使用权限、期限、安全保护责任、必要的安全保护措施以及违约责任和处罚条款。

（四）网络环境治理工作牵头部门：网络部、市场部责任部门：网络部、市场部、集团客户部、客户响应中心、工程建设部、综合部以及旗县分公司。做好防范治理电信网络诈骗专项工作，重视投诉、加强号码监管、对通报诈骗号码、诈骗短信、诈骗网站第一时间处

理，做好封停工作，积极配合上级单位及有关部门进行溯源工作；加大伪基站打击力度；加强网络安全威胁的监测，保证发现网络威胁后在规定时限内按要求采取相关处置措施；定期开展网络安全加固工作，减小网络安全威胁影响范围。由市场部牵头开展用户实名制登记工作，从入网把关，确保新入网用户100%实名登记。四、考核与处罚网络安全按“谁主管谁负责”的原则，对网络安全责任落实不到位，职责履行不到位的，产生网络安全风险及漏洞，造成管辖范围内发生重大安全隐患，造成社会不良影响甚至造成公司损失的，将对责任部门及责任人按照《公司网络数据安全管理实施细则》中第六章要求进行考核与处罚。

四、重点工作要求

（一）分公司各单位每月6日前要以OA邮件方式反馈网络暴露面资产新增情况、APP软件开发上线情况、管辖区域内网络安全工作自查情况等进行上报（附件2、3）。报表要由单位总经理签字盖章（单位）后扫描作为附件上传。

（二）网络部将每半年组织各部门进行一次网络与信息安全检查，各部门做好配合工作。

（三）各部门严格按照《公司202*年网上“扫黄打非”工作方案》《关于进一步做好防范治理电信网络诈骗重点工作的通知》《公司关于配合做好网络安全执法检查工作的通知》中要求完成相关工作。

（四）各部门需要对使用我公司网络数据及客户数据的第三方公司签订保密协议（附件6）。以上要求，请各单位认真落实到实际工作中，做好职责范围内的网络安全风险防控工作，完善网络安全防护措施，不断提升业务及网络的安全性，确保网络安全不出现重大安全事故。

篇2：公司网络安全工作计划

一、前言

随着互联网的快速发展，网络安全问题也日趋复杂。各种黑客攻击、病毒入侵、恶意代码等网络安全威胁层出不穷，给企业、个人甚至国家的信息安全带来巨大威胁。为此，本文将从现状分析、目标规划、工作重点和实施措施四个方面制定网络安全工作计划，以提高企业的网络安全水平，保障信息安全。

二、现状分析

目前企业在网络安全方面存在的问题主要有以下几个方面：

1.缺乏安全意识：很多员工缺乏对网络安全的认识和关注，对于网络安全的重要性没有充分认识，缺乏必要的安全意识，极大地增加了企业遭受网络攻击的可能性。

2.信息系统安全设施不完善：企业信息系统的安全设施存在不足，无法全面保障信息的安全。软件、硬件设施的安全性有欠缺，容易遭受黑客攻击。

3.无法有效监测网络安全状态：企业无法有效监测网络安全状态，不能及时发现、处理网络威胁，缺乏信息安全事件应对和处置的能力。

4.缺乏紧密合作机制：企业内部各部门在信息安全方面缺乏紧密的合作机制，难以共同应对网络安全威胁，缺乏联防联控能力。

以上问题对于企业的信息安全构成了极大的威胁，因此，我们需要通过有效的网络安全工作计划，有效地应对这些问题，保证企业网络安全。

三、目标规划

为了应对以上存在的问题，我们目标规划如下：

1.提高员工安全意识：通过组织安全培训、安全宣传等方式，提高员工的安全意识，让员工充分认识到网络安全的重要性，防止人为因素造成的安全漏洞。

2.提升信息系统安全设施：完善和加强企业信息系统的安全设施，增强网络安全防护能力，构建可信的安全体系。

3.加强网络安全监测治理：建立有效的网络安全监测机制，实时监测网络安全状况，及时发现、拦截网络威胁，及时应对安全事件。

4.提高部门合作能力：建立紧密的部门合作机制，推动各部门各职能部门之间的协同配合，优化整个企业的安全体系，提高联防联控能力。

四、工作重点

以下是我们将重点部署的几个方面：

1.加强安全意识的宣传：通过安全政策、安全宣传等渠道，提高员工的安全意识，让员工充分认识到网络安全的重要性和自身在信息安全中的重要作用。

2.完善网络安全设施：加强对公司各类信息系统和网络设备的安全管理和控制，对所有终端设备、网络线路等进行安全配置和监控，强化互联网接入点的安全防护措施，提高企业的网络安全防御能力。

3.建立网络安全异常监测与处置体系：建立强大的网络威胁监测系统，对网络攻击、网络入侵、恶意代码等威胁进行实时监测和分析，提供快速的处置方案和措施。

4.推进网络安全体系建设：在整个企业内，推进网络安全体系建设，加强部

门之间的协作，从建立安全策略、建立安全规范、制定安全应急预案等多个方面提升网络安全能力。

五、实施措施

为了顺利完成以上目标和工作重点，我们将给出以下实施措施：

1.在员工教育和培训中强调安全意识的重要性，让员工知道什么是网络安全，如何在工作中避免安全风险，定期开展网络安全知识培训和技术演示等活动。

2.加强对信息系统设施的管理和控制，对所有使用信息系统的设施进行安全配置和监控，加强安全权益管理，确保数据的安全性、完整性和可用性。

3.建立网络威胁监测与处理中心，进行实时的网络安全事件检测、分析、处置和回溯，周期性的演练安全攻击和事故应急演习。

4.定期召开网络安全会议，宣传和部署公司的安全策略和安全规范，加强部门之间的沟通和配合，确保各项网络安全措施得到有效执行。

以上实施措施可能需要根据企业实际情况调整和修改，但是这些方案必须在企业的网络安全管理中重要的组成部分。

六、综述

针对当前网络安全形势，我们提出了一份实用且可行的网络安全工作计划。它不仅能有效地提高员工的安全意识、加强网络安全设施，并建立网络安全监测与治理机制。通过集中整合资源和力量，优化建立可靠安全体系，既可以提高企业的竞争优势，也可以保护客户和企业的合法权益，最终实现企业的可持续发展和信息安全的保障。

篇3：公司网络安全工作计划

为加强本单位的网络安全工作，经局领导班子研究，制定本局2019年网络安全工作计划。

一、加强考核，落实责任

结合质量管理体系建设，建立健全信息化管理和考核制度，进一步优化流程，明确责任，与各部门重点涉密岗位签订《网络安全及保密责任书》。

加大考核力度，将计算机应用及运维情况列入年度考核中，通过考核寻找信息安全工作存在的问题和不足，认真分析原因，制定切实可行的预防和纠正措施，严格落实各项措施，持续改进信息安全工作。

二、做好信息安全保障体系建设

进一步完善信息安全管理制度，重点加强用户管理、变更管理、网络安全检查等运行控制制度和数据安全管理、病责防护管理等日常网络应用制度；加强入侵检测系统应用，通过桌管系统、控制台密切关注各移动存储介质（移动硬盘、U盘、CD光驱）等设备运行情况；在业务分析需求的基础上，合理设置安全策略，充分利用局域网优势，进一步发挥技术防范措施的作用，从源头上杜绝木马、病毒的感染和传播，提高信息网络安全管理实效；

进一步完善应急预案，通过应急预案演练检验预案的科学性、有效性，提高应对突发事件的应变能力。

三、加强各应用系统管理

进一步作好政府信息公开网站后台管理系统、OA等业务系统应用管理。加强与各部门勾通，收集使用过程中存在的问题，定期检查系统内各模块使用情况及时反馈给相关部门，充分发挥系统功能；完善系统基础资料，加大操作人员指导力度，确保系统有效运行，切实提高信息安全水平。

篇4：公司网络安全工作计划

网络安全工作计划为了保障企业网络安全，我制定了如下工作计划：

一、加强网络基础设施安全.对公司内部所有服务器进行全面检查，确保安全性，防止黑客攻击和恶意软件感染。

1.更新服务器操作系统和应用程序，修复已知的安全漏洞，提高安全性。

2.加强网络设备的管理和维护，定期更新固件和配置，确保设备安全可靠。

3.加强对内外网的访问控制管理，限制用户的网络权限，减少网络攻击的风险。

二、加强内部信息安全管理.加强对企业内部敏感信息的管理和保护，对数据进行分类处理，实施访问控制和审计。

1.建立内部安全审计机制，对网络访问日志进行定期审计，及时发现异常情况。

2.加强对员工的安全教育和培训，使其具备网络安全意识和基本防护知识。

3.对重要数据备份进行定期测试，确保备份的可靠性和安全性。三、加强对外部威胁的应对能力.建立紧急事件响应机制，对网络攻击和恶意软件感染等事件进行快速应对和处理。

4.加强对第三方软件和服务的管理和审查，避免存在安全风险的软件和服务对企业造成威胁。

5.定期进行安全评估和漏洞扫描，及时发现并修复漏洞，提高网络安全水平。

四、加强安全监控和日志管理.加强网络监控和报警机制，及时发现异常情况，采取相应措施。

1.建立安全日志管理体系，对网络日志进行集中、存储和分析,为安全事件的调查和溯源提供支持。

以上是我的网络安全工作计划，希望能够为企业的网络安全保障提供有效的措施，降低安全性风险，保障企业的信息安全。

篇5：公司网络安全工作计划

一、计划目标与范围

网络安全工作计划的核心目标是建立一个全面、系统的网络安全管理体系，以保护组织的信息资产，确保数据的机密性、完整性和可用性。计划将涵盖网络安全的各个方面，包括风险评估、技术防护、人员培训、应急响应和合规管理等。通过实施这一计划，旨在提升组织的网络安全防护能力，降低潜在的安全风险，确保业务的持续性和稳定性。

二、背景分析与关键问题

随着信息技术的快速发展，网络安全威胁日益严重。近年来，网络攻击事件频发，给组织带来了巨大的经济损失和声誉损害。当前，组织面临的主要网络安全问题包括：

1.网络攻击的多样性：黑客攻击手段不断演变，常见的攻击方式包括钓鱼攻击、勒索软件、DDoS攻击等。

2.内部安全隐患：员工的安全意识不足、操作失误或恶意行为可能导致信息泄露和数据损坏。

3.合规压力：各类法律法规对数据保护的要求日益严格，组织需要确保合规性以避免法律风险。

4.技术更新滞后：部分组织在网络安全技术的投入不足，导致防护措施不够完善。

三、实施步骤与时间节点

1.风险评估与分析

进行全面的网络安全风险评估，识别潜在的安全威胁和漏洞。评估内容包括：

资产识别：列出所有信息资产及其重要性。

威胁分析：识别可能的攻击者及其攻击手段。

漏洞评估：检查现有系统和应用程序的安全漏洞。

时间节点：计划在实施后的第一个季度完成风险评估报告。

2.制定安全策略与标准

根据风险评估结果，制定网络安全策略和标准，明确安全管理的基本原则和要求。策略应包括：

数据保护政策：明确数据分类、存储和传输的安全要求。

访问控制政策：规定用户访问权限的管理和审计流程。

应急响应计划：制定应对网络安全事件的流程和责任分配。

时间节点：在风险评估完成后的第二季度内制定并发布安全策略。

3.技术防护措施的实施

根据制定的安全策略，部署必要的技术防护措施，包括：

防火墙和入侵检测系统的配置与优化。

数据加密技术的应用，确保敏感数据的安全。

定期进行系统和应用程序的安全更新与补丁管理。

时间节点：在第三季度内完成技术防护措施的部署。

4.人员培训与意识提升

开展网络安全培训，提高员工的安全意识和技能。培训内容包括：

网络安全基础知识：介绍常见的网络安全威胁及防范措施。

钓鱼攻击识别：教导员工如何识别和应对钓鱼邮件。

应急响应演练：模拟网络安全事件的处理流程，提高员工的应急反应能力。

时间节点：在技术防护措施实施后的第四季度内完成培训。

5.定期审计与评估

建立定期审计机制，评估网络安全管理的有效性。审计内容包括：

安全策略的执行情况。

技术防护措施的有效性。

员工安全意识的提升程度。

时间节点：每半年进行一次全面的网络安全审计。

四、数据支持与预期成果

在实施网络安全工作计划的过程中，将收集和分析相关数据，以评估计划的有效性。数据支持包括：

网络攻击事件的发生频率及其影响评估。

员工安全培训的参与率和反馈。

安全审计中发现的漏洞数量及其整改情况。

预期成果包括：

网络安全事件发生率降低30%。

员工安全意识提升，培训参与率达到90%以上。

安全审计中发现的重大漏洞整改率达到100%。

五、总结与展望

网络安全工作计划的实施将为组织提供一个系统的安全管理框架，提升整体的网络安全防护能力。通过风险评估、技术防护、人员培训和定期审计等措施，确保组织的信息资产得到有效保护，降低潜在的安全风险。未来，组织将持续关注网络安全领域的新技术和新威胁，及时调整和优化