# 关于2025年网络安全工作计划【三篇】

来源：网络 作者：紫芸轻舞 更新时间：2025-04-12

*报告使用范围很广。按照上级部署或工作计划，每完成一项任务，一般都要向上级写报告，反映工作中的基本情况、工作中取得的经验教训、存在的问题以及今后工作设想等，以取得上级领导部门的指导。以下是小编为大家收集的关于20\_年网络安全工作计划【三篇】，...*

报告使用范围很广。按照上级部署或工作计划，每完成一项任务，一般都要向上级写报告，反映工作中的基本情况、工作中取得的经验教训、存在的问题以及今后工作设想等，以取得上级领导部门的指导。以下是小编为大家收集的关于20\_年网络安全工作计划【三篇】，仅供参考，欢迎大家阅读。[\_TAG\_h2]20\_年网络安全工作计划篇1

　　为加强本单位网络与信息安全保障工作，经局领导班子研究，制定xx县工业商务和信息化局20\_年网络与信息安全工作计划。

　　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《网络与信息安全及保密责任书》。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。

　　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、瑞星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。

　　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。

　　利用局域网、oa系统，通过宣传栏等形式，加大信息安全宣传力度，不断提高员工对信息安全重要性的认识，努力形成“广泛宣传动员、人人积极参与”的良好气氛；着力加强信息化工作人员的责任意识，切实增强做好信息化工作的责任感和使命感，不断提高服务的有效性和服务效率。

**20\_年网络安全工作计划篇2**

　　我单位高度重视网络安全工作，成立了由主要领导任组长，技术分管领导任副组长，全体干部为组员的网络安全领导小组，领导小组下设办公室，办公室设在技术部办公室。同时针对网络安全人员的配备及责任落实情况做了明确要求(附件一：《\*\*日报网络传媒中心网络安全人员及相关责任登记表》)，为确保网络安全工作顺利开展，我单位要求全体干部充分认识网络安全工作的重要性，认真学习网络安全知识，都能按照网络安全的各种规定，正确使用计算机网络和各类信息系统，并制定了《\*\*日报网络传媒中心网络安全规划方案》(附件五)。

　　我单位目前共有内网线路1条，即中国电信宽带网，由光纤接入办公室，共连接非涉密计算机244台;政务内网1条、档案专线1条，涉密计算机2台。上述所有电脑都配备了杀毒软件，能定期杀毒与升级。对涉密计算机的管理，明确了一名分管领导具体负责，并制定专人从事计算机保密管理工作。对非涉密计算机的管理，明确非涉密计算机不得处理涉密信息。对于计算机磁介质(软盘、u盘、移动硬盘等)的管理，采取专人保管、涉密文件单独存放，严禁携带存有涉密内容的磁介质到上网的计算机上加工、储存、传递处理文件。

　　另外，我单位在电信托管有7台服务器，维护\*\*市市委、市政府、市直部门及党群单位网站共计30余个(附件六：《\*\*市市委、市政府、市直部门及党群单位登记表》)，在日常进行安防、备份等方面的维护工作方面，能做到对网站和应用系统的程序升级、账户、口令、软件补丁、查杀病毒、外部接口以及网站维护等方面的问题逐一进行清理、排查，能及时更新升级的更新升级，进一步强化安全防范措施，及时堵塞漏洞、消除隐患、化解风险。

　　为确保计算机网络及服务器安全，实行了\*\*日报网络传媒中心技术部工作职责(附件二)、idc机房管理制度(附件三)及突发事件应急处理预案(附件四)等以有效提高管理员的工作效率。同时我室结合自身情况制定安全自查工作制度，做到四个确保：一是系统管理员于每周五定期检查计算机系统，确保无隐患问题;二是制作安全检查工作记录，确保工作落实;三是实行领导定期询问制度，由系统管理员汇报使用情况，确保情况随时掌握;四是定期组织相关人员学习有关网络知识，提高计算机使用水平，确保预防。

　　为了构筑科学严密的制度防范体系，不断完善各项规章制度，规范计算机及其网络的安全保密管理，确保计算机及其网络安全管理工作各项规定制度的落实，我单位采取自查与抽查相结合，常规检查与重点检查相结合，定期检查与突击检查相结合等方式，对计算机及其网络管理制度的落实情况、涉密网络的管理和使用情况、防范措施的落实情况进行检查。今年以来，我单位对所有计算机及其网络的安全情况进行了一次全面的检查，通过检查，查找到计算机及其网络安全工作中存在的管理漏洞，并整改到位。我单位主要采取了以下几项措施：一是认真贯彻执行上级保密部门文件的有关规定和要求，不断增强依法做好计算机保密管理的能力;二是对处理信息类别进行了明确规定;三是定期对非涉密网络开展保密检查，严格涉密信息流转的规范性，弥补管理上存在的空档;四是针对信息发布存在的不规范等问题，及时对照《政府信息公开保密审查制度》进行整改，要求对上网信息严格审查、严格控制、严格把关，从制度上杜绝泄密隐患，做到上网信息不涉密、涉密信息不上网。

　　通过此次自查，我单位网络安全工作能做到制度到位、管理到位、检查到位，并做到以下几点：

　　1、安装了专业杀毒软件，加强了在防篡改、防病毒、防攻击、防瘫痪、防泄密等方面的有效性。

　　2、网络安全领导小组工作人员负责保密管理，相关的用户名和开机密码为其专有，且规定严禁外泄。做到禁止在未采取防护措施的情况下，涉密信息系统与非涉密网络及其他公共信息网络之间进行信息交换。

　　3、领导小组要求对网站所要发布内容一律要通过分管领导审核同意后才能够发表、删除、修改。做到信息公开坚持先审查、后公开和一事一审原则。

　　(1)在发布信息的权威、一致性方面规定了网站发布、转载有关信息须依据国家有关规定执行，内容加入或更新不得出现有关法律、行政法规禁止的内容，不得有不宜公开的内容;(2)在网站信息处理和人员落实方面规定了栏目的内容及相应的信息提供实行各科室分工负责制，网站领导小组负责网站信息的分类、整理、更新、发布。(3)在网站涉密信息方面明确了要严格遵守上网不涉密，涉密不上网的规定，确保党和国家秘密的绝对安全。

　　通过此次自查也发现存在一定的问题和不足，主要是计算机防范技术有待学习提高，二是专业技术人员较少，信息系统安全方面可投入的力量有限;三是应急机制初步建立，但还不完善;四是网站发布信息的时效性不强。

**20\_年网络安全工作计划篇3**

　　通过召开专题会议、发送微信通知，及时将上级的文件精神传达给每位干部职工，让全体党员干部充分认识到做好当前网络信息安全保障工作的重要性和必要性，并作为当前的一件头等大事来抓，确保网络安全。

　　为进一步完善网络信息安全管理机制，严格按照“谁主管谁负责、属地管理”的原则，明确了第一责任人和直接责任人，加强对本单位的内部办公网及其它信息网站的监督管理，防范黑客的入侵。严禁传播、下载、发表一切不利于党和国家的信息资料，坚决制止违纪违规行为发生，确保网络信息安全。按照上级要求，迅速成立了网络安全工作小组，负责网络安全应急工作，组织单位有关方面做好应急处置工作，组织开展局域网络安全信息的汇集、研判，及时向县网信办报告。当发生重大网络安全事件时，能及时做好应急响应相关工作。由办公室负责本区域网络安全事件的监测预警和应急处置工作，分管副局长为网络安全工作小组的副组长，负责办公室。建立了本单位计算机信息网络系统应用管理岗位责任制，明确主管领导，落实责任部门，各尽其职，常抓不懈，并按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，切实履行好网络信息安全保障职责。

　　1.积极响应上级领导的有关要求，实时观测本区域网络安全信息，努力做到有效应对网络安全事件，一旦发生重大安全网络事件及时向县网信办报送网络安全事件和风险信息，并及时上报相关部门，积极配合协同做好应急准备工作或处置。

　　2.积极建立健全本系统、本部门、本行业重大网络安全事件应急响应机制。应急处置时，需要其他部门、行业或技术支撑队伍支持的，一定及时报请县网信办协调，同时配合其他部门尽快解决。

　　办公室将对对全局的网络设备、计算机进行一次细致的排查。检查安装桌面终端安全管理系统和杀毒软件，确保桌面终端安全管理系统注册率和360杀毒软件覆盖率达百分之百。对于在检查中发现的问题或可能存在的安全隐患、安全漏洞和薄弱环节，立即进行整改。进一步完善相关应急预案，落实应急保障条件。杜绝出现违规“自选动作”，遇重大突发敏感事件，一律按统一部署进行报道。各科室要严把网上宣传报道导向关，严格规范稿源，不得违规自采，不得违规转裁稿件，不得擅自篡改标题。严格网上新闻报道审校制度，防止出现低级错误，同时加大了对新闻跟帖的管理，组织本单位网评员积极跟帖。

　　1.单位网络安全应急负责人、联系人要保持网络畅通，及时接收风险提示、预警信息和任务要求，并按要求报告相关情况。负责人、联系人名单或联系方式有调整的，及时函告县网信办。

　　2.值班期间，实行每日“零报告”制度，每日下午17：00前，报送当天本部门网络安全运行情况、受攻击情况和事件情况，一旦发生网络安全事件，立即启动应急预案，迅速应对，有效处置，并按规定程序及时报告有关情况。

　　（一）压实责任，强化组织领导。要严格落实属地管理责任和网站主体责任，持续开展网上安全检查，全面排查风险漏洞，强化改进工作措施，推进各项重点工作落实到位。要安排专人做好有害信息监看处置工作，严防出现重大网络安全事故。提前做好本单位重点人的工作，要求其规范网上言行。全面排查梳理薄弱环节和安全风险，进一步加强内容审核管理和过滤拦截，强化各类有害信息快速处置机制，筑牢网络安全堤坝。

　　（二）加强督导，完善奖惩机制。要加强对本单位网络专职人员的管理，加强对网站的的督导检查，深入排查整改，做到守土有责、守土负责、守土尽责。对网络建设表现突出的单位和个人，进行通报表扬；对落实管理责任不到位、服务保障不力的，给予严肃通报批评，并责令限时整改；对工作中存在失职、渎职行为，造成严重后果的，严肃追责问责。

本文档由028GTXX.CN范文网提供，海量范文请访问 https://www.028gtxx.cn