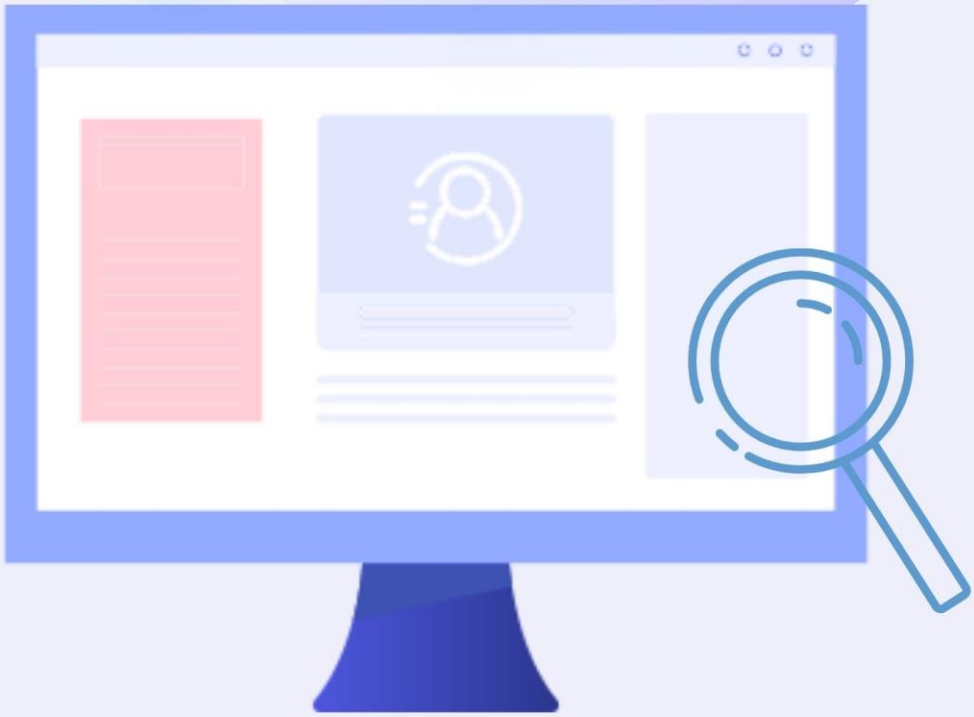
域智盾软件®

政府单位

上网行为管理解决方案



CONTENTS/目录

01 项目背景 ---------- 3

02 面临问题 ---------- 3

03 方案设计 ---------- 4

04 解决方案 ---------- 5

05 方案优势 ---------- 8

06 方案价值 ---------- 9

07 系统架构 ---------- 9

08 公司简介 ---------- 10

一、项目背景

2014 年 2 月 27 日总书记提出网络强国战略目标后，电子政务进入快车道，行政机关、事业单位的日常办公已基本依托政务外网与政务云平台完成。与此同时，政务信息的安全属性并未因载体变化而降低。电子公文、会议材料、财政与项目数据、执法与审批记录、群众诉求与个人事项信息，多具有内部性或敏感性。一份未公开的政策文稿在印发前外流，一份含群众身份信息的统计表被转发至互联网，都可能引发舆论与问责。

本方案面向区县以上党政机关、事业单位及其下属单位，围绕办公终端的上网行为与操作行为，提供一套与行政管理体系相配套的技术实现方式。

二、单位面临问题

从大量政务单位的安全检查与运行情况看，上网行为管理方面的困难集中在以下几个方面。

- 制度与技术之间存在断层

多数单位已有《办公终端使用管理规定》、《上网行为管理办法》，但制度条款停留在文本层面，缺少与之对应的技术动作，执行情况依赖个人自觉，检查时难以举证。

- 审计工作量大而有效信息不足

网络设备与安全设备各自留存日志，格式不一、周期不一。纪检与审计部门提出核查要求时，往往需要多部门人工比对，一份上网行为核查报告的形成周期以周计。

- 上网行为边界不清

办公终端在工作时间访问与公务无关的网站、运行与工作无关的程序，占用带宽并带来安全风险，但全面封禁又影响正常的政策查询、资料检索与业务办理。

- 公文流转环节存在失控风险

电子公文在起草、会签、印发各环节以明文形态在终端上存取，未经批准带离单位、通过个人邮箱发送、拷贝至移动介质的情形难以完全避免。

- 打印环节缺少事前控制

涉密与敏感材料打印无审批、无登记，打印件在科室之间流转，事后无法确认由谁在何时打印、打印了几份。

- 违规外联难以察觉

办公终端私接无线热点、加装无线上网卡、双网卡同时连接内外网的情形时有发生，破坏了内外网物理隔离的要求，且多在上报之后才被发现。

- 补丁与漏洞处置滞后

操作系统与办公软件的补丁长期不更新，上级通报的高危漏洞在本单位终端上仍有大量存量，处置靠逐台通知，闭环周期长。



三、方案设计

本方案以“上网行为可约束、公文流转可控制、终端操作可留痕”为出发点，从以下四个角度形成解决方案。

- **以制度条款为设计依据**

将单位现行的管理规定逐条转化为终端上可执行的技术规则。哪一类网站不得访问、哪一类文件不得外发、哪一级人员可以打印，均在系统中以策略形式落地，使制度具备可检查、可考核的执行载体。

- **以岗位职责为授权边界**

按领导、业务科室、综合办公、财务、执法、外包运维等岗位划分权限与策略。涉密与敏感岗位从严，一般岗位在保证办公效率的前提下适度放开，避免以统一标准处理差异化的岗位需求。

- **以事前、事中、事后为完整链条**

事前通过权限设置与准入校验减少风险来源；事中通过策略阻断与实时告警控制具体动作；事后通过审计记录与报表支撑核查与问责。三个环节相互衔接，避免只做事后归档而无实际约束。

- **以最小干扰为实施前提**

办公终端是公务人员的主要工作工具，任何管控措施均应以不影响办文、办会、办事为前提。加密与管控在系统层完成，办公自动化系统、业务系统的操作方式保持不变；策略上线分批推进，保留调整与回退通道。

四、解决方案

方案由八项能力构成，覆盖上网行为、数据流转、终端配置与接入秩序四个方面。

4.1 上网行为审计

系统按终端记录访问的网页地址、网页标题、搜索关键字、搜索引擎、起止时间与流量，形成按人、按科室、按时段可检索的行为档案。纪检与审计部门提出核查要求时，可按关键词、按时间区间直接提取，无需在交换机与代理服务器日志之间人工拼接。

注：系统仅记录上网行为，不采集通信内容与个人隐私数据，采集范围在制度中明确告知。

4.2 上网权限管控

按科室与岗位下发差异化策略：综合办公、政策研究类岗位放开政策查询与资料检索类站点；窗口服务岗位仅放行业务系统与必要查询地址；与公务无关的娱乐、购物、下载、网络游戏类站点在全部终端上予以拦截。

程序侧同步管控，未经批准的程序不得在办公终端上启动，包括各类下载工具、网络游戏、非办公类即时通信工具。拦截行为留存记录，便于说明策略执行情况，也为个别岗位的例外申请提供依据。



4.3 数据防泄密

功能定位在于降低公文与政务数据的失控风险，覆盖三个环节。

- 透明加密，降低公文失控风险

对电子公文、会议材料、统计报表、执法文书等指定类型文件在终端上自动加密。公务人员的操作习惯不变，文件被拷贝至移动介质、作为附件外发、通过即时通信工具传输时保持密文形态，脱离本单位授权环境后显示乱码。

- 打印事前控权，事后可追溯

打印作为独立环节管理，可按需设置打印审批，敏感材料打印须经科室负责人确认，审批通过后方可输出。同时，可以设置打印水印、打印机白名单、程序打印规则、打印操作审计，事后可按人按件核查。

- 对外交互可制作外发文件

对确需向外部单位提供材料的场景，可通过文件外发包功能处理。经办人提交申请，注明接收单位、用途与有效期限，经审批后系统对文件重新封装并附加接收方授权，接收方只能在约定时间、约定设备上查阅，到期自动失效，查阅过程留痕，减少以私人渠道传递材料的做法。

4.4 USB 外设管控

按科室与岗位设置 U 盘使用策略，可选权限包括禁止使用、仅读取、仅写入、允许使用等，确需使用的设备，可以提交使用申请，待领导审批同意后，方可正常使用，至于非登记设备插入后不可使用。

此外，手机连接数据线、无线网卡、红外、串口、并口、蓝牙、光驱刻录同样纳入管理范围。

4.5 违规外联报警

功能定位在于守住内外网隔离要求。

终端侧持续检测网络环境变化，判断是否出现新增网络接口、是否连接未登记的无线热点、是否加装无线上网设备、是否存在内外网同时连接的情形，一旦出现违规外联的情形，会弹出警告框、锁屏电脑屏幕、提示输入密码并记录告警信息，改变以往“事后听说、难以查证”的状况。

4.6 硬件和软件变化报警

对硬盘更换、内存加装、网卡新增、外设长期接入、软件安装与卸载、安全客户端被停用等变化实时上报，记录变更前后的具体信息。

4.7 补丁管理

支持按科室分批下发补丁，上级通报高危漏洞后，可据此快速确定受影响终端范围，定向推送补丁并在完成后形成闭环报告，改变以往逐台通知、逐台确认的做法。



4.8 设备准入控制

所有申请接入办公网络的设备，须先通过准入校验：是否安装客户端、客户端是否正常运行、补丁是否达标、是否存在违规软件、是否为登记设备。不满足条件的设备引导至修复区域，仅可访问补丁与修复资源，达标后按所属科室授予相应网络权限。

外来设备单独管理。上级检查、兄弟单位交流、参会人员、运维厂商的设备，由接待科室提交来宾接入申请，注明单位、事由、使用时长与可访问范围，经审批后限时放行，到期自动收回，全过程留痕。

五、方案优势

- 制度与技术同构：管理规定中的每一条要求都能在系统中找到对应的策略项，检查时可逐条对应、逐条举证，避免制度与执行两张皮。
- 兼顾效率与约束：策略按岗位差异化配置，敏感岗位从严、一般岗位适度放开，减少因管控过严引发的效率抱怨与变通做法。
- 审计成本下降：上网记录、文件操作、打印登记、外设使用集中留存、统一检索，核查报告的编制由人工比对转为系统导出。
- 不改变办公习惯：加密与管控在系统层完成，办公自动化系统与业务系统无需改造，公

务人员的办文流程保持不变。

- 合规口径明确：能力对齐等级保护对终端管控、边界防护、审计留存的要求，测评时可提供策略配置说明与审计记录作为支撑材料。

六、方案价值

（一）管理价值：让制度具备执行载体

把上网行为、公文流转、终端使用三方面的规定落到具体技术动作上，管理要求由“提倡”转为“可核查”，为作风检查与责任追究提供客观依据。

（二）安全价值：减少政务信息失控风险

公文与政务数据在终端侧受控，外发与打印走审批与留痕，移动介质与外来设备纳入管理，重要信息离开授权环境的可能性显著下降。

（三）审计价值：缩短核查响应周期

按人、按件、按时段直接提取记录，配合审计、纪检、上级检查时的材料准备由数日缩短至小时级，且口径统一、可重复核对。

（四）运行价值：减轻信息中心负担

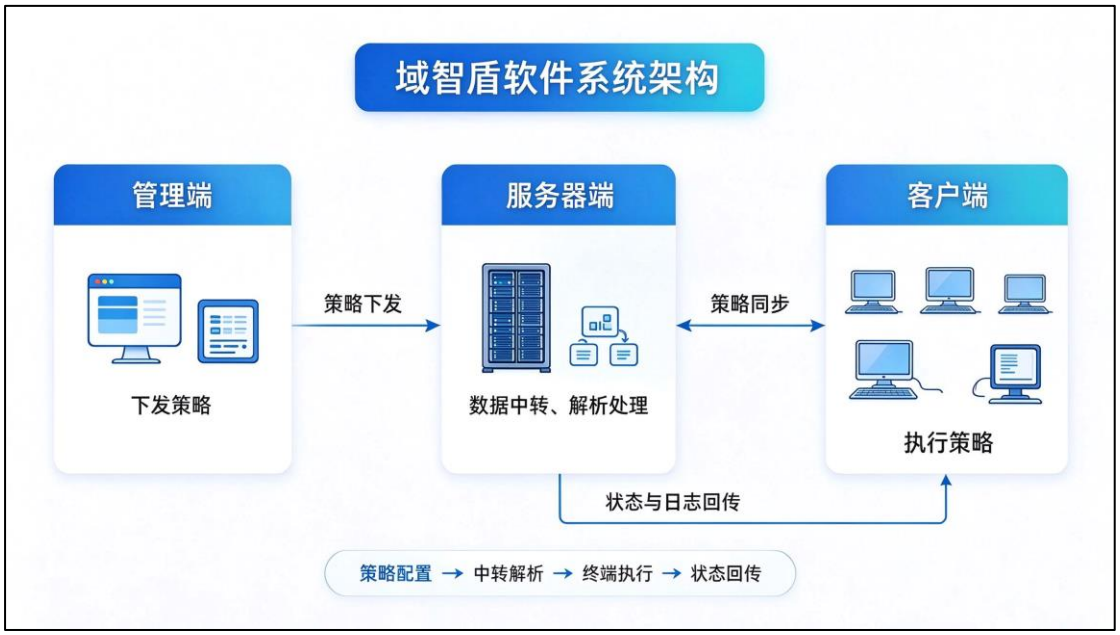
补丁分发、软件安装、资产盘点、终端维护由逐台处理转为批量执行，信息中心有限的人力可更多投入业务系统保障与项目建设。

（五）合规价值：支撑等级保护与专项检查

策略配置、审计记录、审批流水、处置过程形成完整材料链，可直接用于等级保护测评、政务信息系统安全检查与保密自查。

七、系统架构

系统按三层组织，各层职责清晰、数据贯通。



- 客户端：执行策略。
- 管理端：下发策略。
- 服务器端：数据中转解析。

八、公司简介

河北中视新研软件开发有限公司长期专注终端安全治理与数据防泄漏赛道，构建覆盖上网行为管理、终端管控、透明加密、外设管控、补丁分发、设备准入的完整产品矩阵，广泛服务党政机关、事业单位以及制造、医疗、金融等行业客户。

公司具备全生命周期项目交付体系，可提供从前期需求研判、定制化方案设计、试点验证部署到常态化上线运维的专业服务，协助客户完成等保测评、保密自查与专项检查相关技术支撑工作。服务热线：400-097-8770。

官方网站 yzdsaas.com

电话： 400-097-8770

地址： 河北省石家庄市

——以制度落地为要求，以留痕可查为标尺

域智盾软件®