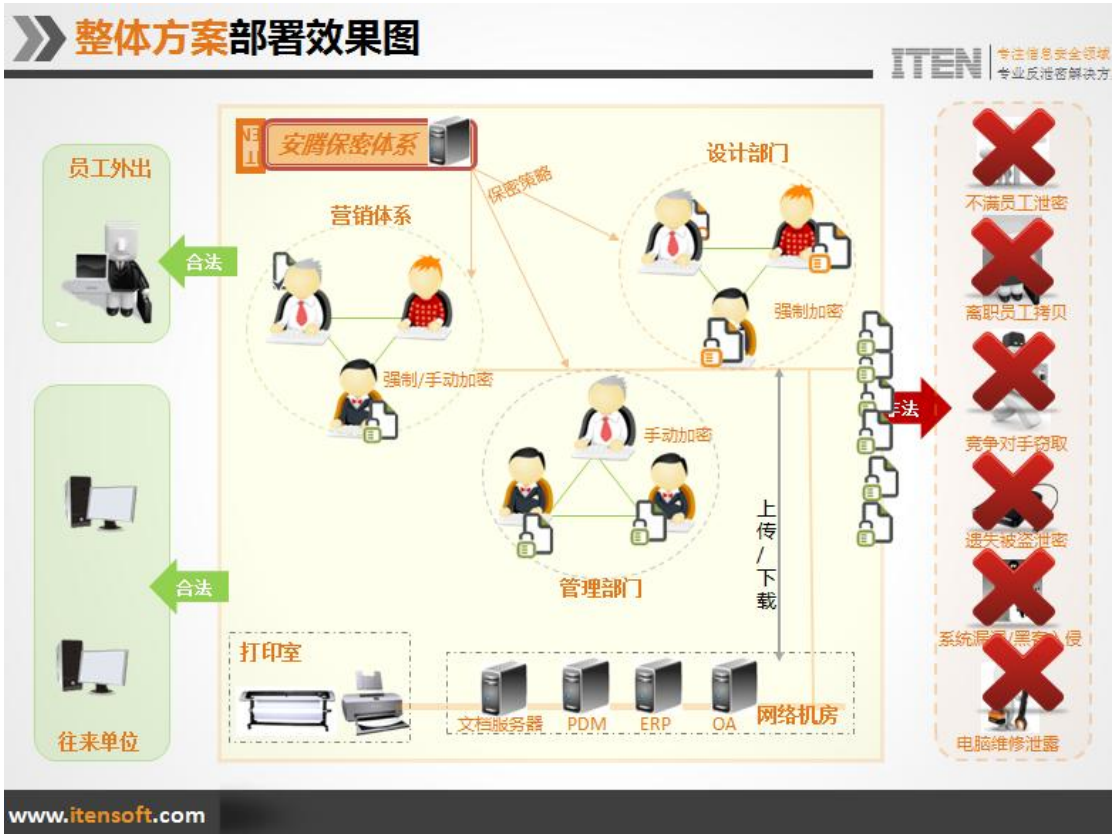
电力行业数据安全防控系统解决方案

电力系统信息安全是电力系统安全运行和对社会可靠供电的保障，结合电力工业特点，电力工业信息网络系统和电力运行实时控制系统，分析电力系统信息安全存在的问题，电力系统信息没有建立安全体系，购买了防病毒软件和防火墙，内部信息安全仍然存在着一些安全隐患，主要包括以下几个方面：



1.目前电力行业内的电脑数据都是明文保存，员工可以通过 QQ、MSN、Email 等网络传输工具随意将内部重要数据外发泄密；

2.电力企业和外部的单位都有着许多业务的往来，对外发的文件也是无法做到有效的控制，外发文档就像“放飞的风筝”一样，再也无法控制；

3.员工离职带走公司的重要资料，并格式化他们的电脑；

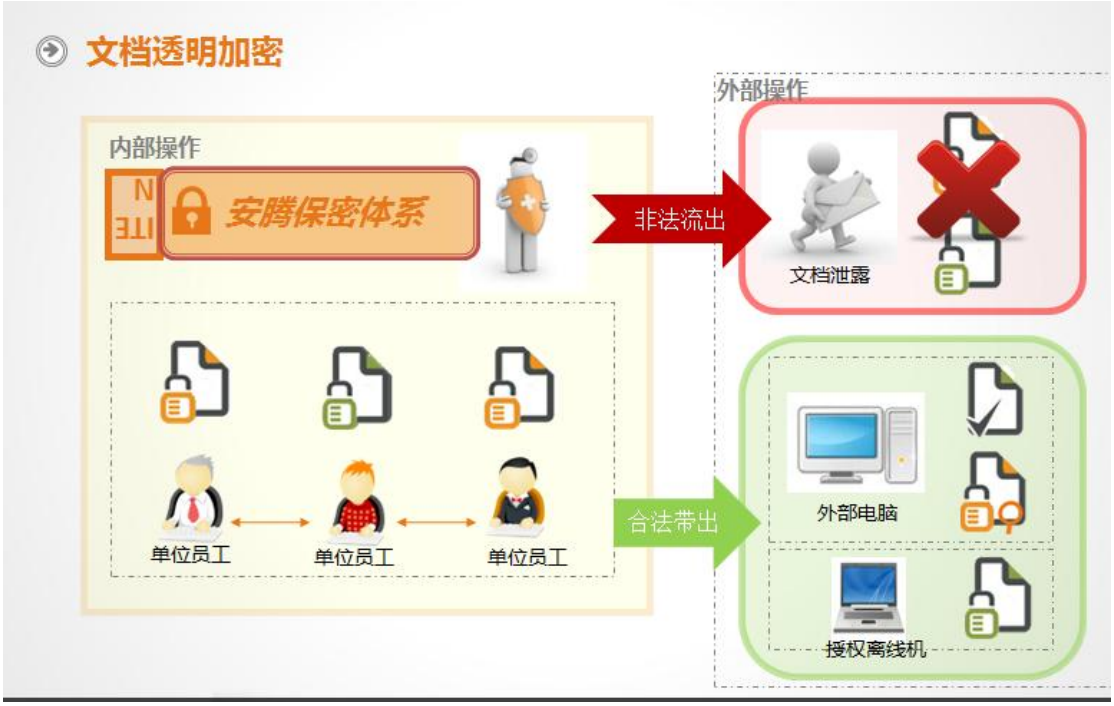
4.内部员工可以不经过公司相关领导审批，将内部重要文件外发给客户；

5.员工出差时无法对承载着公司大量重要数据的笔记本防止可能泄密；

6.员工外的计算机可以随意接入电力内网，造成数据泄密无法有效追踪其源头；

7.员工随意打印公司重要文件,无任何技术管理手段，给数据安全带来重大的安全隐患；

凤凰卫士数据防泄密加密系统解决方案：



1.防止电力数据离开办公环境泄密

凤凰卫士数据防泄密解决方案通过动态加解密技术，实现对电力所有电脑数据强制透明加密，员工无任何感觉，有效防止公司内部员工通过任意方式将数据泄密。即员工在创建、编辑文档时，一旦发出写硬盘的操作，文档会被自动加密存放在硬盘上，若发出读硬盘的操作，文档将被自动解密以明文的形式打开，防止作者故意或由于疏忽而造成泄密或对文件恶意破坏。

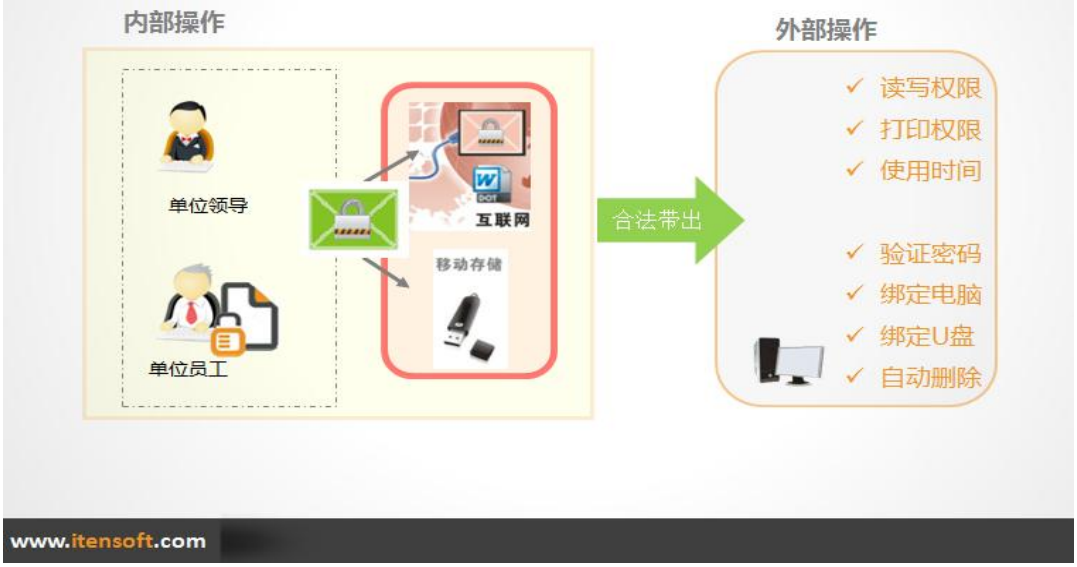
2. 防止电力机密文件在内部二次扩散

由于电力公司内部机密文件（比如：市场策略等，时效性、机密性要求高）访问，通常会因实际业务需要涉及到不同部门的相关人员，或者相关领导查阅。

3. 防止电力外发文件在外二次扩散

与外界进行频繁的信息沟通已成为公司必要的一种业务模式，这些交互的信息可能会涉

及企业核心信息，而这些信息一旦流出企业就面临着失控的风险。为了解决对外业务交互的后顾之忧，我们提供信息对外发布管理思路。



4. 防止电力员工在外办公导致数据泄密

短期外出：方便员工晚上回家或者周末在家也能正常加解密文件，不需要额外的操作

长期外出：在规定的期限内，携带笔记本在外也可以正常工作，超过期限，将无法打开加密文档。

永久外出：对在分公司或办事处用户，可使用永久离线，保证总部与分部之间的资料都是加密的，可以互相访问，又可以控制分部的资料，防止外泄。

5. 防止电力员工离职时带走技术资料泄密

员工在新建、编辑重要文件（如：CAD 文件、设计图纸等）时，到了指定时间服务器会自动对员工电脑重要文件备份到服务器指定目录下保存，避免员工离职时有意删除或格式化电脑，给企业带来损失；通过对公司电脑上的数据透明加密，带走了资料都是加密的，有效地避免了员工离职时，想带走几年下来大量重要的资料。

6. 对电力内部重要文件转化成纸质化泄密

打印外泄是常见的泄密途径。因为大多数单位内部人员可以随意使用打印机打印文件，

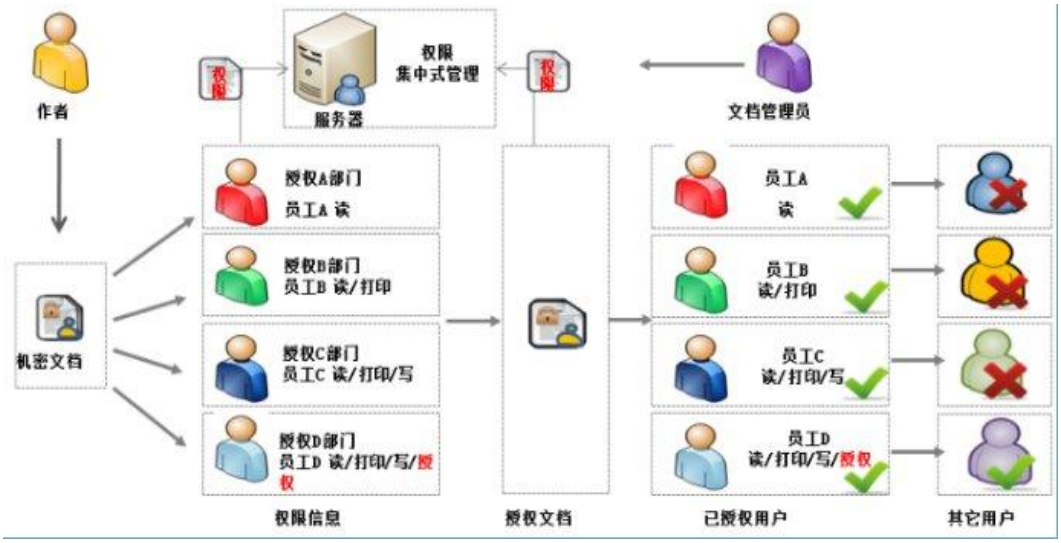
且无法进行监控和审计，直接影响着内部重要文档资料的安全。

凤凰卫士数据防泄密系统能够对内部员工的打印作业进行有效的监控和管理：

事前打印控制：是否可以打印？允许用哪台打印机？

事中打印警示：自定义水印内容，实现打印警示；

事后打印审计：什么时间、哪台电脑、打印什么内容。



7. 避开电力复杂服务器集群，保障服务器数据安全

安全隐患：无关人员和电脑，随意接入内部网络，访问服务器数据导致泄密，应该如何管控？如果要求终端数据上传到公司某些应用服务器（比如：ERP、OA）的数据是明文，该如何管控？应用服务器上明文数据下载该如何管控？

终端准入：只允许安装有数据防泄密系统客户端的终端用户正常接入应用服务器，非法用户禁止接入；上传下载：文件上传自动解密、下载自动加密；

数据加密安全通道：客户端用户在与公司内部服务器进行数据交换时，采用数据加密安全通道，保障数据在传输过程中不被窃取。

非法外联：安装有数据防泄密系统客户端的终端用户将禁止连接仿冒应用服务器，防止非法用户利用客户端上传自动解密机制进行非法外联泄密。

8. 对电力终端软硬件和网络办公环境，规范管理

对终端硬件使用规范管理：U 盘、刻录机、打印机等使用规范化管理；

对终端软件使用规范管理：规定企业不同的部门电脑统一安装哪些软件，部署规定的如软件才能打开公司加密的电子文档数据。

9. 为电力 IT 中心提供详细统计报表

泄密事件的发生，不再受人工审计难的困扰。我们全程监督、跟踪、记录所有员工的全部操作，实时回溯泄密全过程，提供详细审计报表。

凤凰卫士数据防泄密加密系统方案优势

1.凤凰卫士数据防泄密加密系统集成了先进安全技术，提出了一整套先进、完整、实用，完全满足电力行业需求的系统安全解决方案。

2.丰富的行业安全实施经验，基于 ISO 27001/20000 体系认证，为多个行业提供标准化的安全服务；

3.专业的项目管理能力，以卓越的信息安全资源整合能力，为您提供定制化的专业信息安全解决方案；

4.全方位的数据保护能力，通过对数据加密、访问控制、安全审计等多种技术，对涉密数据进行全生命周期的安全防护；

5.智能化的业务融合模型，基于业务的安全访问控制模型，与电力行业应用系统无缝结合。

行业案例：云南省玉溪市电力设计院、湘潭电力设计院、西安电力设计院、赣州宏远电力勘测设计院、黄石电力勘测设计有限公司、渭南电力设计院、江西智合电力设计有限公司、日照阳光电力设计有限公司、广州瑞景电力工程设计有限公司、福州电力设计院、景德镇昌南电力勘测设计有限公司、河南中油电力设计有限公司、福建中天电力、厦门成美电力勘察设计有限公司、华东电力设计院……