**一、数据安全形势**

**1、攻击目标：**企业核心数据是吸引“黑客”攻击的最终目标，其中内鬼导致的数据外泄事件占比超过70%，而系统被攻陷后盗取数据事件占比低于30%。

**2、薄弱环节：**位于企业内部的核心数据安全防护等级高，外部盗取困难。但数据一旦流转到办公电脑后被拷贝、被盗取的机会就大很多，且追溯困难。

**总结：办公电脑的数据管控对企业数据安全管理意义重大。**

**二、数据安全防护思路**

**1、可信设备：**办公电脑（正版系统 + 防病毒 + 网络准入等）+ 数据防泄露工具。

**2、可信通道：**办公环境的基础分享工具，如OA、邮箱、仓库、VPN等。

**3、可信授权：**管理员给办工需要的人员分配系统账户、授予需要的最低权限等。

**总结：主流互联网企业都会在其办公电脑上安装终端数据防泄露工具。**

**三、数据防泄露工具**

**1、主动盗取：**工具可以感知其办公电脑所囤积的数据概况、实时监控数据使用行为、阻止数据滥用、追溯数据盗取行为等。

**2、被动盗取：**工具可以管理通过办公电脑外设、网络等渠道静默发生的数据外发动作，阻止数据盗取，追溯攻击者行为等。

**总结：无论是主动还是被动地盗取数据行为，数据防泄露工具都能很好地发挥作用。**

**四、数据防泄露管理**

**1、数据分离：**办公环境使用办公电脑，个人相关数据的操作不使用办公电脑，避免产生个人数据和公司数据的管理冲突和司法纠纷。

**2、三权分立：**部署终端数据防泄漏工具的部门可自行定制其数据审计策略、安全团队进行日常系统的运营、审计部门定期审计系统运营的动作监督其中敏感数据不被扩散。

**总结：明确数据管理的权责，形成完善的数据防护制度。**

**五、安装数据防泄露工具的影响**

**1、兼容问题：**数据防泄露工具安装在办公电脑上，一定会遇到软件和操作系统版本兼容问题。虽然我们的供应商有阿里巴巴、美团等这种5万个以上端规模的客户使用案例，但是不排除像操作系统版本更新带来的新的软件兼容性问题。目前在效能部门安装时发现的问题基本已经解决。一旦出现软件运行出错的情况，可以及时联系7000处理。

**2、性能下降：**数据防泄露工具会实时检测办公电脑上操作数据的内容和行为是否属于保密数据和异常外发动作，根据检测结果记录日志报警和阻断动作（可配置不阻断），这些会消耗一些系统的CPU、内存和存储等资源，配置低的办公电脑可能安装后有些卡顿感，如果排除软件bug则需升级电脑硬件配置解决，可联系运维部内部IT老师处理。

**3、违规监察：**安装数据防泄露工具以后，我们一定会发现一些用户违反安全红线的数据使用行为。如果我们没有做到事前宣贯，明确安全红线行为，并和用户达成一致，则追责可能会困难。所以我们制作了在线《办公电脑数据保护要求》视频课程和安排线上考试，安装了数据防泄露工具的员工需要学习完课程并通过考试。

**备注：**安全红线依据2019年6月28日发布的《集团信息安全红线和处罚规定》中关于信息安全红线的第十四条：将保密文档、数据等，例如：人力、财务数据报告、产品设计文档、源代码等泄露到非指定保管存储空间，如公共代码仓库或网络空间。

**总结：工具安装后会出现系统兼容或性能下降问题，处置违规行为前宣贯并达成共识。**

**附录：**

**1、DLP策略运营案例：**[https://ya](https://yach-doc-shimo.zhiyinlou.com/docs/890a1066f4df4c69)

**2、后台部门DLP关键字整理：**[https://y](https://yach-doc-shimo.zhiyinlou.com/sheets/kxTxVWKPy6VJDcHX/9JSfX)

**3、终端安全管理制度：**[https://ya](https://yach-doc-shimo.zhiyinlou.com/docs/01d16cfc860942a1)