# 办公安全

## 理解

办公安全的保护对象，是公司的一切。内鬼行为，不安全的办公行为可能导致公司各方面的损失。

办公安全聚焦于日常办公的工作流及公司员工。对日常办公的相关事务进行保护。

理论上任何公司都需要办公安全。

高精尖高端制造业，如汽车、芯片等行业，办公安全的比重更强，因为其机密数据的存储及表现形式、其工作特征，本身就不会与互联网有过多接触，不像互联网公司的互联网应用一样，需要对公众提供服务，所以此类公司进行安全建设，其办公安全的比重是很大的。

办公安全的理念有零信任。但是零信任应用的前提条件是办公系统会被大量的非公司人士，非办公区人员访问。疫情时代所有公司都出现了大量的对应需求，零信任理念也随之大火，相关产品陆续出现。零信任对技术要求非常高，因此一般都只有大公司才能研发。另外零信任对相关办公系统的扩展能力要求很高。

因此进行办公安全建设可借鉴零信任理念，但要视公司具体情况做取舍，不可照搬，不可本本主义。

办公安全可拆分为办公环境安全、办公系统安全、办公工作流安全、员工安全、行为安全、身份权限安全。

环境安全包括办公终端安全及办公网络安全。

办公终端安全的对象是 员工个人终端及办公区内的机房服务器、交换机、公用主机、大屏主机等。

办公网络安全的对象是 办公区域内的网络，包括机房。

办公系统安全的对象是 员工通用系统（如oa，邮箱）及部门特定系统（如客服，git，Jenkins，财务系统）

办公工作流安全的对象是 各部门日常工作流，先从贴近业务或机密信息的部门人员开始梳理调研。

员工安全的对象是 公司员工。通用的安全意识培训，保密意识培训。特定部门可有相关的部门培训，如开发部门的安全开发培训。

行为安全的对象是 员工行为及自动化行为。

权限安全的对象是 员工身份权限，系统权限等。

## 人选要求

办公安全的工作流安全部分，对能力要求很高。需要人选有发现问题的能力，需要深入各部门的工作流程，发现其存在的安全隐患，对工作流程进行改善。编制新的工作流，相关制度文档，必要的话要提供相关系统以实现工作流，或对系统进行改造。

其他部分，有经验当然更好，但是没经验也没关系，有能力可以快速上手与学习。

## 落地

梳理：发现所有数据。建设数据发现机制跟能力。

状态调研：调研安全建设状态，评估完成度，高优先级的东西是否覆盖了。

决策工作内容：做不做，做什么，怎么做

一般是先进行纯技术体系的落地，然后是运营体系，然后是管理体系。

### 技术体系

办公区网络安全：AD域，网络准入，网络隔离划分

员工终端安全：EDR，防病毒，零信任终端软件，DLP等

服务器终端安全：特指办公区内的机房服务器、公用主机、大屏主机。可参考基础安全部分中的主机安全。

办公系统如oa，邮箱等系统安全。财务的ERP系统，运维的jenkisn，zabbix等系统。

权限安全：管理混乱忘记删除，IAM统一认证，软件硬件认证统一认证。专用设备。

操作审计，权限审计，弱口令，渗透测试，应用安全。安全配置，安全使用。系统升级，漏洞情报。

GitHub监控，gitlab操作审计。

工作流安全：偏安全管理，比如资产申请，权限申请。应有工作流规定，不能瞎搞。特别是对于自动化的工作流，要有审批节点，通过节点管控自动化进度。

工作流：权限申请，资源申请，数据申请工作流。异常发现及处理的工作流（应急）。

在信息化/it化建设中，在IT的边界，会存在线上行为及线下行为的过渡过程。

在过渡过程中出现办公安全问题。

工作流应是制度制定方面的工作多一些。主要解决先干什么后做什么。

再就是发现不合适的线上线下过渡行为。

通用场景，应设置钉钉审批流。

非特殊场景，邮件审批就可以了。

员工：安全意识培训，部门培训，系统使用安全培训

安全意识培训，解决办公安全问题。

保密，内鬼，内审内控，解决办公安全。

权限管理，IAM，权限最小化授权

上网行为审计

网络环境安全：纯净的网络环境，没有恶意用户接入，能发现恶意流量，阻止恶意流量。

办公系统安全：系统只有员工能使用，IAM，认证。系统安全配置。系统放在内网，服务用内网IP启动

权限安全：管理混乱忘记删除，IAM统一认证，软件硬件认证统一认证。专用设备。

办公终端安全：EDR，防病毒，零信任终端软件，DLP等

终端软件管理：

<https://www.ibm.com/cn-zh/topics/uem>

权限，行为，密码，审计。管理。

### 运营体系

安全问题的发现，处理，监控等

### 管理体系

制度，工作流改变