安全：10大方法减少内部人员安全风险 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_AE_89_E5_85_A8_EF_BC_9A1_c101_461734.htm 如今内部人员给公司的安全造成的威胁非同小可。近来的一些报告指出，内部人员对公司的损害在所有的危害事件中已从80% 上升为86% ，而且超过半数发生在雇员的终端。无疑，拥有访问公司系统权限的内部雇员极有可能被误导到那些欺诈性的或危险的链接上。而在所有的雇员中，IT工作人员拥有的这种访问权限最多。因此，IT审核应关注从多个方面确认风险。下面我们给出实施有关控制和减少工作人员对管理员欺诈的方法。 1.IT安全策略 管理人员应该审视那些能够管理特权账户（如域管理员账户、应用程序管理员账户、数据库管理员）的IT安全策略，要保障安全策略的存在，还要清楚存取访问是如何被处理、验证、证明的，要确保对这些策略定期进行审查。否则，基本上就不存在管理特权访问的基础了。在没有相关报告的情况下，管理特权账户的策略是不完整的。特权账户的口令审核报告经常要涉及到如下的问题：口令何时更新、更新失败有哪些，以及在一个共享账户下，个别用户如何执行任务等等。 制定的策略应具有这样的目标：能够终止明显的不可防御的用户活动。要确保所有的雇员、订约人和其它用户清楚其责任，从而与IT的安全策略、方法以及与其角色相适应的相关指导等。 2.“ 超级用户 ”账户和访问 了解公司与用户访问有关的暴露程度是很重要的。应该决定拥有访问特权的账户和用户的人员，并获得对网络、应用程序、数据和管理功能的访问有较高权力的所有账户列表。包括通常

被忽视的所有计算机账户。由此，要确保用户访问能够被检查，并确保其拥有恰当的许可。一个好方法是定期地审查用户访问，并决定数据和系统的“ 所有者 ”已经得到明确授权。 3.账户和口令配置标准 要保证所有的管理员账户能够根据策略更新。在特定设备上，不应存在默认的口令设置。对那些拥有足够的默认账户和口令资源的用户来说，其信息是很丰富的。有一些安全账户，其账户名就是口令，这简直是自寻烦恼。设置口令的期限也是很重要的，禁用某些明显的临时账户也是很聪明的作法。 4.对口令的受控访问 对权力有所提升的账户和管理员的口令存取要加以管理。其道理可能很明显，不过对口令的共享访问并非总能得到控制。离线的记录或开放性的访问，如包含口令的电子邮件，就不应当存在。即使一个加密的口令文件也是不足取的。在最糟的情形中，口令文件的口令并没有得到控制。 5.服务账户(“ 机器 ”账户) 服务器也可以被提升权限，并用于各种罪恶的目的。这些账户典型情况下并不分配给人类用户，并且也不包括在传统的认证或口令管理过程中。这些账户可被轻易地隐藏。管理员应该保障服务账户只拥有必要的访问权。这些账户应该定期检查，因为它们经常拥有超级用户的能力。这种用户的数量是很多的，而且还有许多不用的账户也需要注意。 6.高风险用户和角色 有一些公司积级地监视某些角色，这些角色对企业会造成极高的风险，企业的监视会发现其潜在的“ 不可接受 ”的行为。许多企业拥有一些风险极高的关键角色。例如，一位采购经理为谋求一个职位可能会将自己能够访问的敏感数据带到另外一家竞争公司那里去。这种情况下，其访问是被授权的，不过却存在着滥用的情况。岗位、职责的

轮换以及设定任命时间是对付高风险的一个重要方案。注意：IT安全专家通常都属于高风险角色的范围。 7.安全知晓项目 任何雇员或用户都可能造成一种威胁。贯彻执行一个可以处理上述所有要点的安全知晓项目，并能保证其强制实施势在必行。现在有许多方案能够确保所有的用户已经阅读并同意有关规则和政策。其中一种工具是在用户登录时要求其在一个警告消息上签名，要求用户确认其同意并选择窗口中的“ 接收 ”或“ 同意 ”复选框。 8.背景筛选 背景筛选就是要认真地问雇员一些措词严格的问题，以揭示其特定行为和态度的危险信号，例如： 违规的或异常的工作经历：离开工作的可疑理由、长期未被雇用的原因 欺诈：在某些事实上（例如教育、以前的雇佣关系）的虚伪陈述 人格/态度问题：与同事或管理人员的糟糕关系 挫败、威信问题、猜疑、无力接受改变等 9.事件记录 安全事件记录提供了实时使用和活动的透明度。精确而完整的用户及其活动的记录对于事件分析和制定额外的安全措施是至关重要的。获取访问的方法、访问范围和过去的活动是很重要的。为保证有充足的记录，应考虑改善对较高风险领域和服务的记录利用。 10.证据 管理人员应熟悉所使用的不同存储设备，如果有任何可疑迹象，还应具备“ 指纹 ”知识的足够知识水平。这可以是cookie数据、隐藏的操作系统数据等。从公司系统中获取关键文件并将其放置到闪速存储器上是很简单的事情，这些闪速设备可被伪装为数码相机、个人数字助理（PDA）或移动电话等。还有一些调查人员从移动电话中收集和分析信息，因为这种设备可包含语音邮件、正文消息、地址文件、电话号码和许多遗漏电话、已接电话等。如果有任何可疑的非法活动，就应保留相关

证据，直至最终决定其结果。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com