需要考虑的数据库相关安全政策 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/143/2021_2022__E9_9C_80_E8_A6_81_E8_80_83_E8_c102_143735.htm 在能够真正影响每个行业的所有的政府和行业规则中，总有一天会出现这么一条，要你真正地应用一些信息安全政策。你也许已经对密码和数据备份有了一些基本政策。但是还有更多内容。所以，如果你的企业现在才刚刚把它的安全政策放在一起，或者你已经意识到了是时候需要更新一些东西了，那么这里有几个你需要了解的数据库安全相关的问题。 从技术上来说，为了准确判断需要哪个安全政策，你需要执行信息风险评估。然而，我理解，现实情况经常会导致其它内容。就是说，我可以考虑得很少，如果有的话，但是几乎很少有不再要求我思考如下数据库相关安全政策的环境出现： 可接受的利用率什么可以/不可以在数据库服务器上完成，例如网络浏览和安装/卸载中间件，以及个人防火墙保护，还有MSDE, SQL Server Express 2005，以及其它非服务器系统上的数据库软件的安装。 认证控制对于数据库，以及有关应用程序和操作系统来说，包括密码的要求，多种成分的使用等。 业务合作应对外部承包人、审计人员、寄存提供者商等，包括合同规定和应用的服务级别的协商。 业务连续性灾难恢复和/或业务连续性计划要求可以帮助你的数据库保持运转状态，可以访问。 变更管理记录谁、为什么、在什么时候，如何，以及所有相关的拆除过程。 数据备份什么，什么时候，以及使用的方法。 数据保持和破坏什么，为什么，使用的方法和时间线。 加密不仅覆盖了静止的数据，例如加密特定的行，还覆盖了传输的

数据，例如数据库服务器和网络应用程序之间的TLS。数据备份也是覆盖的一部分。 信息分类为信息贴上公共、内部、机密等标签。 物理安全构建，数据中心和服务器的安全。 财产的删除服务器，驱动，磁带，和其它财产。 安全测试和审计什么，如何，什么时候，以及谁执行的测试，用的什么工具。 职责的分隔用户，数据库管理员，安全审计员，以及其它与数据库管理有关的人的角色/职责。 系统维护打补丁，系统清理/清楚和中间件的更新。 系统监控和意外事件的响应谁，为什么，什么时候，以及如何进行实时监控和记录审计日志，还有为了维护正式的意外响应计划所需要的特殊需求。 用户授权添加/删除用户，授予谁，为什么，什么时候，多长时间的管理权限。 我认为这里有几个关键点需要与数据库中心的安全政策相关。首先，如果管理层没有明确表示他们的支持(例如，他们将会接受并强制政策的执行)，你兴许也只能一起放弃这个计划。所以首先要把他们也拉上船。其次，尽可能地把你的政策提到最高级别上，这样你就可以最大化覆盖的部门和系统。最大化规则的数量，你可以真正地实施它。换句话说，如果你可以帮助它，不在你的数据库中发生以上所有的政策，并且在无线网络、存储系统等等中拥有另一套规则。同样，至少也要理解你的企业对解决PCI, GLBA, HIPAA, SOX等问题上的规则上的调整需求。这一点在你有一个依从性或者IT管理委员会来审视和现实安全政策的时候，可以带来最好的帮助。如果你能帮助它的话，你不会想要你自己管理一套政策。 