**XXX单位**

**数据安全管理规范**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479434019)

[2 适用范围 1](#_Toc479434020)

[3 数据库安全 1](#_Toc479434021)

[3.1 身份鉴别 1](#_Toc479434022)

[3.2 访问控制 1](#_Toc479434023)

[3.3 日志审计 1](#_Toc479434024)

[3.4 安全传输 2](#_Toc479434025)

[3.5 资源利用 2](#_Toc479434026)

[3.6 安全管理 2](#_Toc479434027)

[4 数据加密要求 3](#_Toc479434028)

[4.1 加密技术选择 3](#_Toc479434029)

[4.2 加密管理 3](#_Toc479434030)

[5 数据备份恢复 3](#_Toc479434031)

[5.1 数据管理 3](#_Toc479434032)

[5.2 数据备份实施 4](#_Toc479434033)

[5.3 数据恢复与演练 4](#_Toc479434034)

[5.4 备份存储管理 5](#_Toc479434035)

[6 附则 5](#_Toc479434036)

# 目的

为保障关键数据安全，修订本文档，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范。

# 适用范围

本文档适用于XXX单位信息系统数据管理。

# 数据库安全

## 身份鉴别

1）应对数据库系统中的用户进行标识，用户标识应遵守唯一性原则，并将用户标识与审计相关联。

2）应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

3）应在登录过程中确保鉴别信息是保密的，不易伪造的。

## 访问控制

1）应对数据库系统的访问设定访问控制规则，减少非授权访问。

2）数据库系统应按照最小权限原则对不同用户进行授权，保证各用户权限最小化。

3）数据库系统的安装目录和文件的访问权限应进行最小化设置，防止未授权用户访问相关资源。

## 日志审计

1）应为数据库系统建立独立的日志审计系统，定义与数据库安全相关的日志审计事件记录。

2）能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏。保护审计数据，严格限制未经授权的用户访问。

## 安全传输

1）对数据库系统进行管理时，应采取一定的安全机制，防止鉴别信息和管理数据在网络传输过程中被窃听。

2）数据库系统与第三方系统进行数据交互时，应采用加密措施保护数据信息传输安全。

## 资源利用

1）应对数据库系统的最大并发会话连接数进行限制，防止受到拒绝服务攻击。

2）应对数据库系统内单个帐户的多重并发会话进行限制，并对会话超时进行重鉴别控制。

3）应对数据库系统资源进行监视，并对系统的服务水平降低到预先规定的最小值进行检测和报警。

## 安全管理

1）设置数据库系统审计管理员、系统管理员角色、系统安全管理员角色，并且实现不同管理用户的权限分离，仅授予管理用户所需的最小权限，同时系统审计管理员角色与系统管理员角色、系统安全管理员角色不能是同一人担任。

2）数据库系统应定期进行系统版本更新和补丁更新。

# 数据加密要求

## 加密技术选择

在选择和应用加密技术时，应考虑以下因素：

1）必须符合国家有关加密技术的法律法规，包括使用和进出口限制。

2）根据风险评估确定保护级别，并以此确定加密算法的类型、属性，以及所用密钥的长度。

3）听取专家的建议，确定合适的保护级别，选择能够提供所需保护的合适产品，该产品应能实现安全的密钥管理。另外，还应听取与加密技术法律法规相关的法律建议。

## 加密管理

单位应采用基本的加密技术控制措施，包括：

1）加密策略必须经过审核批准。

2）重要信息在传输时必须加密。

3）当使用环境不允许加密时（例如法律禁止等），专用通信线路必须采用有线系统。

4）数据压缩技术不得代替安全手段。

# 数据备份恢复

## 数据管理

1）应设立数据备份与恢复工作管理岗位。

2）数据备份与恢复工作包括制定数据备份与恢复工作规划及实施方案，实施数据备份和恢复的具体工作。

3）应根据备份要求确定备份策略，备份策略内容包括备份方式（自动备份、手动备份等）、备份方法（例如全备份、增量备份、差异备份等）、备份技术、自动备份周期、备份介质、备份冗余、备份保留时间周期等。对核心应用系统的数据备份应保存两份以上，数据保留周期至少为两周。

## 数据备份实施

1）各地应根据实际情况制定相应的数据备份实施方案和操作手册。

2）备份工作要有记录，记录要素包括时间、参加人员、系统名称等。

3）对自动备份的系统，应对备份任务执行情况进行有效监控。

4）系统重大变更前，应对系统进行数据备份。

5）数据备份开始前要制定详细的计划、流程和回退方案，以保证业务的连续性、完整性。

6）数据备份结束后，应对数据备份集的完整性进行检查。

7）加强移动备份介质的安全管理，备份完成后，备份介质应及时归档。

8）数据备份在制作、传递、转移过程中，必须建立详细的交接登记记录，详细记载备份数据制作、传递、转移的全部过程与责任人。

9）备份的实施活动应尽量选择在非工作时间进行，以免影响业务的正常开展。

## 数据恢复与演练

1）应制定数据恢复方案，定期组织评审并结合实际环境持续改进。

2）数据恢复方案需经主管领导或运行维护负责人批准后，方可实施。

3）实施数据恢复时，应按照数据恢复方案执行，恢复过程要有记录，记录内容包括：执行人、执行时间、恢复步骤、恢复内容、恢复结果等。恢复过程中要保证双人上岗，一人负责实施，一人负责检查。数据恢复后，要组织相关人员对数据正确性进行验证。

4）定期（半年或一年）对备份数据在模拟环境下进行恢复演练，保证备份数据的可恢复性。无法进行恢复演练的系统，应定期对备份介质进行试读。

5）及时对恢复演练进行总结，并加以改进。

## 备份存储管理

1）备份存储介质应按照介质中存储信息的敏感程度进行管理，明确责任人以及存储日期。

2）备份存储介质应存放在安全环境中，并与原始文件分开存放。

3）借用备份存储介质时应进行登记，非授权人员借用时需经过相关领导的批准后方可借用。

4）超过保存时限的备份可进行销毁，并做好销毁记录。

5）对于需要永久保留的备份，应在明确标识，并单独存放。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。