信息系统标准化管理 V1.1

工业 4.0、智能制造等被越来越多的人熟知。中国企业在 IT 管理上问题频频，互联网企业在安全上的投入每年都在增加，业务系统每年都在增加，增加的投入远没有带来相应收益，困扰这很多企业。

企业信息化管理标准同时存在违法的风险，《网络安全法》规定，网络问题没有按规定执行的，严重的吊销企业营业执照、责任人判处 2 年有期徒刑。

这里整理一份标准化的信息化管理，作为信息化的工作者，希望信息技术为中国的大国制造走出一条道路。

企业的信息化是为了什么？ 为了提高业务的效率，为了方便业务管理，为了准确的财务数据。

1. 企业 IT 系统
   - 1.1. 软件系统开发过程：包括开发文档控制、变更控制、用户基本控制。
   - 1.2. 软件系统运维：包括业务操作审计、系统变更、权限管理、流程可行性管理。
   - 1.3. 系统环境运维：包括操作系统、物理环境、网络环境。
   - 1.4. 基础设备运维：包括电脑运维、基础软件运维、设备接入控制。
2. 业务系统
   - 2.1. 业务系统标准功能介绍：
     - 2.1.1. 系统中所有操作要求有记录。运维人员根据实际情况，设定对应留存日志的天数，并可以提供证明。
     - 2.1.2. 系统中有安全策略：账户密码长度、密码复杂度、密码有效期、登陆超时、密码存储加密。
     - 2.1.3. 系统中必须有登陆记录：包括成功记录与失败记录。
     - 2.1.4. 软件系统必须有权限管理：有用户管理，角色管理，并可以导出所有权限清单、单个权限设置。
     - 2.1.5. 多用户软件系统必须有编辑冲突：多人对同一条数据进行操作必须有提示或者等待完成操作，以确保数据准确性。
     - 2.1.6. 主要流程说明：新业务系统需要有流程说明。
     - 2.1.7. 系统必须由正版授权的软件。
     - 2.1.8. 业务系统必须有完整测试环境。
     - 2.1.9. 系统使用第三方授权软件开发的，系统架构再不影响使用的情况下，使用第三方授权应采用最少量的方案。
   - 2.2. 业务系统运维
     - 2.2.1. 业务系统必须有变更审核记录：申请变更审批流程、测试内容、正式变更。正式变由运维人员变更，不得使用开发人员变更。并由变更台账。变更要由负责人的确认签字。
     - 2.2.2. 业务系统操作记录：对不常变更的数据，但是又很关键的数据变更要变更记录，也可以有审批记录，保证管理者对系统中的数据负责。定期对系统操作进行审计查询。
     - 2.2.3. 业务系统权限变更：系统使用者的权限变更要求有权限变更记录、并由管理者对其授权操作的审批。定期对系统权限进行审计查询。
     - 2.2.4. 业务系统问题处理：使用者出现系统问题，要有问题处理记录。并定期审计。
     - 2.2.5. 定期审计系统正版授权的资料，保证软件没有超出服务期限。

2.2.6. 定期审计系统安全策略设置。

2.2.7. 定期进行灾难测试: 系统影响业务程度、灾难汇报过程、业务相关责任人清单、灾难情况说明、业务恢复时间、数据校准方式方法。

3. 业务系统环境运维-服务器操作系统、数据库。

3.1. 操作系统、数据库标准：

3.1.1. 操作系统、数据库必须是正版授权软件。

3.1.2. 操作系统、数据库可更新。

3.2. 操作系统、数据库运维

3.2.1. 定期审计操作系统、数据库软件的正版情况与软件支持期限。 运维人员确认相关信息。

3.2.2. 定期审计操作系统、数据库软件安全策略：账户策略、密码规则、密码有效期、登陆超时、锁定设置。运维人员导出相关信息，由相应业务系统的责任人确认。

3.2.3. 定期审计操作系统、数据库的权限，运维人员导出相关信息，由相应业务系统的责任人确认。

3.2.4. 定期审阅操作系统、数据库的日志文件。运维人员确认相关信息对业务系统不构成影响。

3.2.5. 定期安全测试：操作系统中安装的软件清单、系统服务清单。运维人员确认相关信息对业务系统不构成影响，软件清单中不存在盗版软件。

3.2.6. 系统出现问题：问题有处理记录。

3.2.7. 备份：必须包括软件目录、数据库文件、操作系统。备份要有天、周、月、年留存要求。定期恢复测试，并由恢复数据的证据，保证备份的数据可用。备份要有异地距离。

4. 业务系统环境运维-物理环境

4.1. 物理环境标准

4.1.1. 机房内机柜整齐、不存在易燃易爆物品。

4.1.2. 机房空调：温度控制、湿度控制。

4.1.3. UPS 由电量显示。

4.1.4. 机柜布线：强电弱电尽可能分离。

4.1.5. 机房防火报警装置。

4.1.6. 机房防水报警装置。

4.1.7. 室内影像监控。

4.2. 物理环境运维

4.2.1. 机房外来人员及非运维人员进出入记录，外来人员机房内工作必须有相关运维人员陪同，并记录。运维人员变更须由相关管理人员确认。

4.2.2. 机房设备点检：包括服务器、交换机、路由器、UPS、存储、防火墙等设备运行正常，并做点检记录。

4.2.3. 定期对 UPS 检测，并留存记录，电量满足断电时长。

4.2.4. 定期对防火、防水进行测试，保证报警装置可用，灭火器材有效期可用。

4.2.5. 机房每日检查空调情况，并做好记录。

5. 业务系统环境运维-网络环境

5.1. 网络环境标准

5.1.1. 业务系统服务器与终端用户须使用可管理的交换机。

5.1.2. 业务系统访问互联网须有防火墙控制。

5.1.3. 网络设备需要 UPS 供电。

5.2. 网络环境运维

5.2.1. 网络设备配置审计：定期对网络设备账号、密码策略、进行审计。

5.2.2. 防火墙策略审计：定期对防火墙配置进行审计。

5.2.3. 防火墙策略变更记录：要有变更记录、原始配置备份。并定期审计

5.2.4. 定期对网络设备灾难进行恢复测试：系统影响业务程度、灾难汇报过程、业务相关责任人清单、灾难情况说明、业务恢复时间。

6. 业务系统基础设备访问控制

6.1. 基础设备标准：

6.1.1. 基础设备有：PC、笔记本电脑、PDA。（不包含手机）

6.1.2. 基础设备操作系统正版并在有效的支持期内。

6.1.3. 基础设备必须有安全控制软件。

6.1.4. 未知设备接入系统要有记录。

6.2. 基础设备运维

6.2.1. 基础设备问题处理要有记录，并定期审阅。

6.2.2. 基础设备安装软件清单定期审阅并由记录，确认没有盗版软件

6.2.3. 基础设备每日监控信息：系统补丁、安全软件、未知设备访问网络或者业务系统。统计相关数据，并处理相关问题。减少病毒的入侵的可能。

6.2.4. 基础设备变更：有设备申请记录、发放时间、责任人、设备配置信息。设备配置需要有标准，以满足生产经营要求。

7. IT 信息技术审计

7.1. 审计标准

7.1.1. IT 管理的过程标准制定，满足需求的标准。

7.1.2. IT 服务中的实施、验收标准。

7.1.3. IT 设备中配置标准：硬件配置最低标准（包括：电脑、打印机、服务器、交换机、路由器等）和软件系统配置策略（包括：账号密码、受控软件、安全软件等）。

7.2. 信息化审计

7.2.1. 审计信息化建设的标准文件，变更记录。

7.2.2. 审计业务过程中 IT 的记录留存。

以上是信息系统标准化管理内容。 根据信息化系统建全一份符合企业的标准化文件。

变更：V1.0 - > V1.1

新增：

2.1.9 系统使用第三方授权软件开发的，系统架构再不影响使用的情况下，使用第三方授权应采用最少量的方案。