ICS 13.100
C 78

DB14

山　西　省　地　方　标　准

DB 14/T 2241—2020

应急管理信息化 应急管理业务软件系统安全设计规范

2020－12－08 发布　　2021－03－08 实施

山西省市场监督管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1-2020 《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由山西省应急管理厅提出并监督实施。

本文件由山西省安全生产标准化技术委员会归口。

本文件起草单位：山西省安全生产科学研究院。

本文件主要起草人：焦新华、陈泽宇、杨柯、王延辉、杨李根、刘艳、王刚、王洋、宋梅、张旭东、王波。

应急管理信息化　应急管理业务软件系统安全设计规范

1　范围

本文件规定了应急管理业务软件系统安全设计规范的术语和定义、基本内容、通用要求、研发管理以及安全运维等，本规范主要针对B/S架构。

本文件适用于指导山西省应急管理业务软件系统安全设计。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019　信息安全技术 网络安全等级保护基本要求

GB/T 30998-2014　信息技术 软件安全保障规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

安全设计

系统在设计阶段开展的结构分析、专项防护及方案评审等一系列活动的总称。

3.2

安全策略

业务系统中制定一系列规则，实现安全目标的总称。

3.3

系统级资源

系统级资源包括：文件、文件夹、注册表项、ActiveDirectory 对象、数据库对象、事件日志等。

3.4

前端

前端即网站前台部分，在浏览器上展现给用户浏览的网页。

3.5

后端

后端是负责与数据库的交互，实现相应的业务逻辑。

3.6

双因子认证

密码以及实物(SMS 手机、令牌等生物标志)两种或多种条件对用户进行认证的方法。

3.7

单向散列

是根据输入消息计算后，输出固定长度数值的算法，输出数值也称为“散列值”或“消息摘要”，其长度通常在 128～256 位之间。

3.8

反向代理

是指内部网络对 Internert 发出连接请求，需要制定代理服务将原本直接传输至 Web 服务器的 HTTP 发送至代理服务器中。

3.9

结构化异常处理

是可以使程序中异常处理代码和正常业务代码分离，保证程序代码更加优雅，并提高程序健壮性。

3.10

微服务架构

是一种将一个单一应用程序开发为一组小型服务的方法，每个服务运行在自己的进程中，服务间通信采用轻量级通信机制。

3.11

应用容器引擎

是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的容器中，然后发布到任何流行的机器上，也可以实现虚拟化。

3.12

渗透测试

是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

3.13

SQL 注入

是攻击者构造恶意的字符串， 欺骗业务系统用构造数据库语句并执行，从而达到盗取或修改数据库中存储的数据的目的。

3.14

跨站脚本攻击

是入侵者在 Web 页面的 HTML 代码中插入具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行，从而威胁用户浏览过程的安全。

3.15

回滚操作

是程序或数据处理错误，将程序或数据恢复到上一次正确状态的行为。

3.16

CA 认证

CA 认证，即电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。

数字证书的机构是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

3.17

RA 认证

RA（Registration Authority ），是数字证书认证中心的证书发放、管理的延伸。主要负责证书申请者的信息录入、审核以及证书发放等工作，同时，对发放的证书完成相应的管理功能。发放的数字证书可以存放于 IC 卡、硬盘或软盘等介质中。RA 系统是整个 CA 中心正常运营不可缺少的一部分。

4 业务软件系统软件研发周期

软件安全开发涵盖了软件的整个生命周期。软件安全周期是软件从产生到发布的生命周期，参考图1，包括项目启动、需求分析、原型设计、需求设计、研发设计、开发阶段、测试阶段、系统发布八个阶段，相关阶段产物参见附录A。业务软件系统研发单位同时也应按照GB/T 30998-2014，对研发过程进行规范管理，并记录相关过程和结果。

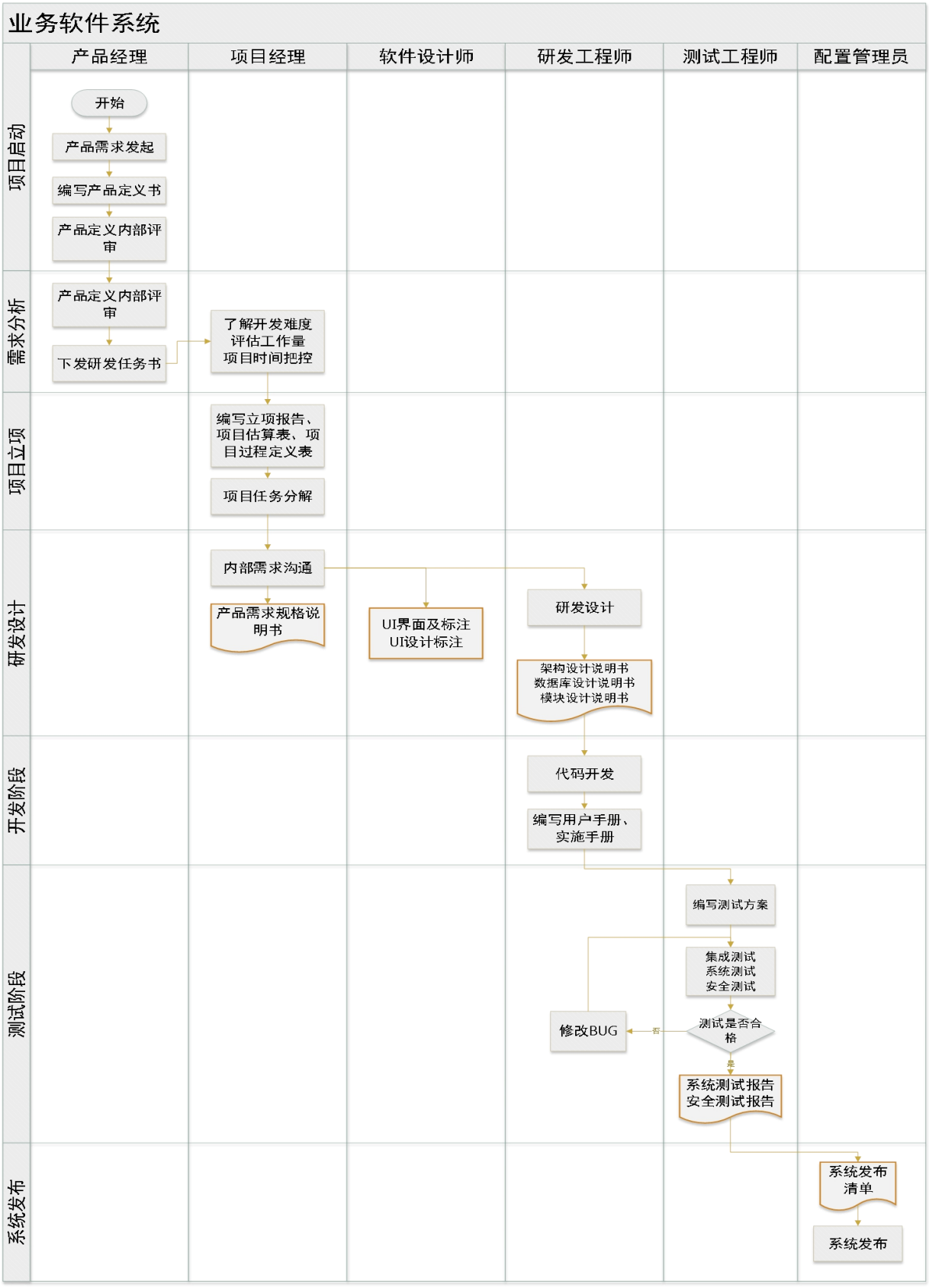

图 1　业务软件系统软件研发周期

5 软件系统安全设计的基本内容

5.1 设计要求

软件系统安全设计应按照GB/T 22239-2019，根据业务软件设计要求，进行网络安全等级保护。

5.2 身份鉴别

在身份认证方面，要求如下：

a) 可接入到统一认证中心（部级 CA 认证，省级 RA 认证）；
b) 应采用合适的身份认证方式，应采用双因子认证方式，认证方式如下：
   1) 用户名、口令认证；
   2) 动态口令认证、GA 认证；
   3) 证书认证，证书必须有载体，比如 USB KEY（注：生产环境中，应使用 USB KEY，不能私自导出证书）；
   4) 短信认证。
c) 应设计密码的存储和传输安全策略：
   1) 禁止在数据库中明文存储用户密码；
   2) 禁止在基于 HTML5 中 Session Storage、Local Storage、Cookie 中保存明文密码；
   3) 应采用单向散列加密技术在数据库中存储用户密码；
   4) 用户若忘记密码，应通过邮件验证，并使用手机号码及短信验证，找回密码；
   5) 用户若忘记密码，且邮件地址及手机号发生变更，应通过管理员进行密码找回。
d) 应设计密码使用安全策略，包括密码长度、复杂度、更换周期等，输入字符应可见；
   1) 弱密码：复杂度单一，长度小于 8 位，满足两项；
      中密码：复杂度三种类型，长度大于 8 位，满足其中一项；
      强密码：复杂度三种类型，长度大于 8 位，满足两项；
   2) 更换周期具体要求见附录 A；
e) 应设计图形验证码，增强身份认证安全，随机生成且包含字母、数字、字母数字组合或中文验证码的组合，具体详情见附录 A；
f) 应设计账号锁定功能限制连续失败登录，具体详情见附录 A；
g) 应根据系统设计限制重复登陆账号；
h) 对提供单点登录的分布式业务软件系统的用户应提供单点标识，且单点标识应具有与常规标识相同的安全性。

5.3 访问控制

在授权方面，要求如下：

a) 应设计资源访问控制方案，验证用户访问权限；
b) 电子政务外网等线上业务应设计后台管理控制方案：后台管理应采用白名单方式对访问的来源 IP 地址进行限制；
c) 应设计在后端实现访问控制，禁止仅在前端实现访问控制；
d) 授权粒度应根据业务软件系统的角色和功能分类进行限制。

5.4 安全审计

用户访问业务软件系统时，应对登录行为、业务操作以及系统运行状态进行记录与保存，保证操作过程可溯源、可审计，确保业务日志数据的安全。要求如下：

a) 日志记录事件应包含以下事件：
   1) 访问控制信息，比如：由于登陆失败超出尝试次数的限制而引起的账号锁定信息；
   2) 用户权限的变更；
   3) 用户密码的变更；
   4) 用户试图执行角色中没有明确授权的功能；
   5) 用户账户的创建、注销、锁定、解锁；
b) 审计日志应包含如下内容：
   1) 事件的日期、时间（时间戳）；
   2) 事件类型；
   3) 事件内容；
   4) 事件是否成功；
   5) 请求的来源（例如请求的IP地址）；
c) 审计日志应禁止包括如下内容（如必须包含，应做模糊处理）：
   1) 敏感信息（如密码信息等）；
   2) 隐私信息（如身份信息等）；
d) 应保证业务日志安全存储与访问：
   1) 日志应存储在数据库中；
   2) 日志保存期限可进行配置；
   3) 应支持与省部级独立的日志系统进行日志传输。

5.5 通信安全

5.5.1 接口方式安全设计

接口方式安全设计要求如下：

a) 与其他系统连接，禁止侵入式使用数据库；
b) 本系统前后端数据传输，可通过 Json 进行传输；
c) 本系统与其他系统连接进行身份认证，可通过 token 认证；
d) 本系统信息传输过程中，应注意防止中间人攻击，保障数据的可靠性和稳定性；
e) 对外接口设计必须有接口版本号，每次变更应考虑向下兼容性，基本原则：轻易不删除旧接口，新增接口要有版本号。

注：版本格式：主版本号.次版本号.修订号（例，1.0.0），版本号递增规则如下：

1) 主版本号：全盘重构时增加；重大功能或方向改变时增加；大范围不兼容之前的接口时增加；
2) 次版本号：增加新的业务功能时增加；
3) 修订号：增加新的接口时增加；在接口不变的情况下，增加接口的非必填属性时增加；增强和扩展接口功能时增加。

5.5.2 数据安全设计

数据安全设计要求如下：

a) 应使用加密技术对传输的敏感信息进行保护,敏感度信息判别见附录 A 表 A.4，加密方式选择见附录 A；

b） 应使用安全的传输协议（如:HTTPS、SFTP、SCP 等加密传输协议）来传输敏感度中度级别以上的文件；
c） 临时数据使用后需进行存储或销毁处理。

5.5.3 会话安全

在会话管理方面，要求如下：
a） 登录成功后应建立新得会话：
1） 在用户认证成功后，应为用户创建新的会话并释放原有会话，创建的会话凭证应满足随机性和长度要求，避免被攻击者猜测；
b） 应确保会话数据的存储安全：
1） 用户登录成功后所生成的会话数据应存储在后端，并确保会话数据不能被非法访问；
2） 更新会话数据时，应对数据进行严格的输入验证，避免会话数据被非法篡改；
c） 应及时终止会话：
1） 当用户登录成功并成功创建会话后，应在系统的各个页面提供用户退出功能；
2） 退出时应及时注销服务器端的会话数据；
d） 本系统消息会话类数据传输，可通过 ws、wss 进行连接；
e） 应设计合理的会话存活时间，超时后应销毁会话，并清除会话的信息；
f） 应能够对系统的最大并发会话连接数进行限制。

5.5.4 其他要求

除上述要求之外还应：
a） 应确保采用的安全协议不包含已公开漏洞；
b） 云端业务软件系统的外链业务应使用反向代理进行访问，Web 和数据库服务器建立连接访问，应使用内网域名进行访问，避免使用 IP 地址访问；
c） 通过互联网域名访问业务软件系统应考虑联通、电信、移动负载线路及 IPV4、IPV6 双站兼容。

5.6 容错设计

5.6.1 异常消息

异常消息一般包含了针对开发和维护人员调试使用的系统信息,这些信息将增加攻击者发现潜在缺陷并进行攻击的机会。要求如下：
a） 应使用异常处理机制；
b） 应使用通用错误信息：
1） 程序发生异常时，应重定向到特定网页；
2） 应向前端返回一般性错误消息；
a） 程序发生异常时，应终止当前业务，并对当前业务进行回滚操作。

5.6.2 其他要求

除上述要求之外还应：
a） 业务软件系统应分为调试和生产环境两个状态，在生产状态下产生的逻辑错误不应反馈给用户；
b） 业务软件系统对高并发接口，应采用微服务架构、Docker 容器技术等技术；

c) 业务软件系统应选取合适的部署操作系统，比如使用 Linux，可充分利用 I/O 多路复用，占用资源少、性能好的特性。

5.7 数据库安全

数据库安全包括：

a) 数据库的运行环境，应考虑单机部署以及分布式部署；
b) 数据库采用分布式部署方式应注意主键 ID 生成算法，例如采用雪花、uuid 等算法；
c) 数据库设计时，应注意业务逻辑不要过于复杂，应对索引优化；
d) 数据库设计时，使用查询应通过视图，报表展示应使用 map；
e) 数据库设计时，应考虑稳定性、安全性（多级安全）；
f) 数据库设计时，应读写分离，提升存取速度；
g) 数据库设计访问过程时，应以最小权限设计为主；
h) 数据库设计时，应考虑中间件对耗时语句的处理；
i) 数据库设计时，应减少使用存储过程；
j) 与数据库互联地址，如果为一台服务器，一台数据库，应采用 IPV4 私网地址，掩码根据具体服务器数量进行计算。

6 通用要求

6.1 安全原则

安全原则应包含：

a) 保护最薄弱的环节原则：保护最易受攻击影响的部分；
b) 纵深防御原则：不同层面、不同角度之间需要相互配合；
c) 最小权限原则：只授予执行操作所需的最小权限；
d) 最小共享原则：使共享文件资源尽可能少；
e) 权限分离原则：授予不同用户所需的最小权限，并在它们之间形成相互制约的关系。

6.2 输入和输入验证

要求如下：

a) 应设计多种输入验证的方法，包括：
   1) 应检查数据是否符合设定的类型；
   2) 应检查数据是否符合设定的长度；
   3) 应检查数值数据是否符合设定的数值范围；
   4) 应检查数据是否包含特殊字符；
   5) 应使用正则表达式进行检查；
b) 前后端都应进行输入验证：
   1) 应建立统一的输入验证接口，为整个系统提供一致的验证方法；
   2) 应将输入验证策略作为应用程序设计的核心元素；
c) 应对输入内容进行规范化处理后在进行验证，如文件路径、URL 地址等，规范化为标准的格式后再进行验证；
d) 根据输入目标的不同，应对输出数据进行相应的格式化处理。

6.3 配置管理

在配置管理方面，要求如下：

a) Web 目录使用配置文件，以防止可能出现的服务器配置漏洞导致配置文件被下载；
b) 应避免以纯文本形式存储重要配置，如数据库连接字符串或账户凭据。

6.4 参数操作

操作参数攻击是一种更改在Web应用程序发送的参数数据的攻击，包括查询字符串、cookie和HTTP标头。要求如下：

a) 应避免使用包含敏感数据或者影响服务器安全逻辑的查询字符串参数；
b) 应使用会话标识符来标识客户端，并将敏感项存储在服务器上的会话存储区中；
c) 应使用 HTTP POST 来代替 GET 提交窗体，避免使用隐藏窗体；
d) 应验证从客户端发送的所有数据。

7 软件开发管理

7.1 需求管理阶段

需求管理阶段应：

a) 确认安全需求规格说明，需求管理参见附录 B；
b) 项目经理、需求对接人员、软件架构工程师以及驻场开发人员，在深入调研系统需求前应签订保密协议；
c) 承保公司应以书面的方式提供管理制度、工作制度以及考核制度；
d) 第三方进行代码审计服务时，可验收时进行也可开发同步进行。

7.2 系统实现阶段

系统实现阶段应符合如下要求：

a) 项目安全管理要求：
   1) 软件研发开始前，应根据确认的需求，并提交项目立项报告，参见附录 B；
   2) 软件研发过程中，应对项目中出现的重大问题进行管控，并完成项目重大问题跟踪表，参见附录 B；
   3) 软件研发过程中，若出现意外情况，无法按期完成项目，应提交项目变更申请表，参见附录 B；
   4) 软件研发过程中，应对项目进度进行阶段性管控，完成项目进度报告，参见附录 B；
   5) 源代码的变更和版本发布进行统一控制，对程序资源库的任何修改、更新和发布都需经部门主管领导授权和批准，应记录在册，供验收时查验；
b) 开发环境安全管理要求：
   1) 软件系统开发、测试禁止在生产环境中进行；
   2) 开发环境中的使用的操作系统、开发软件等应进行统一安全配置，及时进行系统补丁升级和漏洞修复；
   3) 软件程序不得篡改应用软件所运行的环境或平台中任何安全配置、安全文件和安全程序；
c) 编码安全要求：
   1) 应按照安全编码规范以及安全设计方案进行系统开发；
   2) 应按照机密性要求，保护用户信息的机密性；
   3) 应按照异常处理机制，捕捉并处理程序异常，防止系统信息泄露；

4) 应按照代码脆弱性防范要求，严格处理输入输出验证、接口调用等，不应产生 SQL 注入、跨站脚本攻击等严重漏洞；

d) 开发流程安全要求：

1) 开发过程中应定期进行代码静态分析，使用代码审核工具对源代码进行检测，并报告源代码中存在的安全弱点；

2) 开发人员不得超越其规定权限进行开发，不得在程序中设置后门或恶意代码程序。

7.3 系统测试阶段

系统测试包括代码的安全测试和安全功能测试，包含以下要求：

a) 系统测试应按照业务软件系统安全设计基本要求进行测试，检查业务软件系统安全设计是否满足本规范；

b) 代码的安全测试是指使用代码测试工具或渗透测试来识别代码的安全脆弱性，并应按照其提供的修复建议进行修复，范围包括自己开发的代码以及引用的第三方控件代码；

c) 安全功能测试包括身份认证和访问控制的功能测试；

d) 测试系统环境应尽可能模拟生产环境并与生产环境进行安全物理隔离；

e) 真实数据不得直接在测试环境中使用，须进行适当修改或屏蔽，在测试完成之后须立即从测试应用系统清除运行信息；

f) 测试人员应编制安全测试方案；

g) 验收测试不得由开发人员兼岗；

h) 测试完成后应编写测试报告，参见附录 B。

7.4 系统发布阶段

系统发布阶段包含以下要求：

a) 配置管理员应妥善保管程序源代码及相关技术文档；

b) 应归档项目产品交付清单，包括开发文档、数据库设计文档、操作手册文档，参见附录 B；

c) 应对业务软件系统使用人员进行相关培训。

8 安全运维

8.1 备份方式规范

系统应提供有效的热备、冷备备份方式及备份策略，保障业务系统安全运行。

8.2 其他的安全防护规范

其他的安全防护应包含：

a) 针对 Web 保护与防御系统，应部署 Web 应用防火墙设备；

b) 对业务软件系统进行管理时，不允许公网直接访问，需通过 VPN 进行访问；

c) 可采用国密保密机保障数据的安全性。

8.3 备份对象规范

业务软件系统的备份对象应包含以下：

a) 系统数据的备份：数据库、文件服务器中的文件以及其他数据；

b) 系统的完全备份：应包括关键基础设施，通过 NAS 的完全备份，实现快速的灾难恢复；

c） 系统配置的备份：应包括关键路由器的配置、防火墙的配置、各类服务器操作系统的安全配置以及各类服务器中间件和容器的配置。

8.4 安全升级规范

业务软件系统的安全升级应按照以下要求：

a） 应提前在模拟生产环境中完成升级测试，保证系统升级的安全性；

b） 升级前应做好数据、程序、配置脚本等的备份，以防出现升级失败后能够立即快速恢复；

c） 升级过程中应保证一人执行一人监督，以防止升级过程中出现误操作；

升级完成后应进行升级验证测试，保障业务软件系统正常运行。

附 录 A
（资料性）
参考表

表A.1 阐述了业务软件系统研发周期及产物。

表 A.1 业务软件系统研发周期及产物表

研发周期	安全方面	产物
需求分析	明确安全需求	需求文档
需求设计、研发设计	分析攻击面	系统架构及接口设计文档
开发阶段	安全编码	安全编码手册、使用编程工具相关详细资料
测试阶段	自动化工具扫描、渗透测试、代码审计	测试用例及报告
系统发布	备份管理、应急处置、安全培训	备份方案、应急方案、安全培训方案

表A.2 阐述了更换密码周期。

表 A.2 更换密码周期表

角色	更换周期
超级管理员	30 天
一般用户	90 天

表A.3 阐述了验证码提示方案。

表 A.3 验证码提示及连续失败处理方案表

输入情况	提示验证码情况	处理方式
第一次输入错误	不提供验证码	不处理
第二次输入错误	字母、数字或字母数字的组合	不处理
第三次输入错误	中文验证码	记录 IP
第四次输入错误	中文验证码	记录 IP，通过邮件、短信通知系统管理员及账户使用者
第五次输入错误	中文验证码	记录 IP，通过邮件、短信通知系统管理员及账户使用者
第六次输入错误	中文验证码	屏蔽 IP，锁定账号 5 分钟，通过邮件、短信通知系统管理员，账户使用者

表A.4 阐述了敏感信息标识。

表 A.4　敏感信息标识表

敏感信息	敏感度	颜色标识
个人姓名、身份证号码、住址、电话、银行账号、密码、医疗信息、教育背景等信息	高	红色
企业人员信息、商业资料、财务信息等信息		
政府人员信息、坐标等信息		
个人公开的信息	低	黄色
企业公开的信息		
政府公开的信息		

表A.5 阐述了敏感信息加密方式。

表 A.5　敏感信息加密方式

敏感度	选取加密方式
高	非对称算法
低	不加密对称算法

附 录 B
（资料性）
业务软件系统验收大纲

表B.1 阐述了确认需求沟通表。

表 B.1 确认需求沟通表

项目名称	xxx 业务软件系统		
项目编号			
沟通地点		**沟通时间**	
沟通单位及人员			
确认需求	本次会议沟通，需确认需求 xxx 项，明确 xx 项，不一致 xx 项； 明确项，分别是： 1、…… 不一致项及问题分析如下： 1、……		
产品经理审批			
审批意见	（盖章） 年 月 日		
甲方单位审批			
审批意见	（盖章） 年 月 日		

表B.2 阐述了需求变更申请表。

表 B.2　需求变更申请表

项目名称			
需求名称			
影响分析人		**影响分析完成日期**	
影响分析			
变更内容说明	原 xxx 需求，由 xxx 提出，因 xxx 原因，需求变更为 xxx，由 xxx 进行修改。		
实现方案详细说明	xxx 方案说明		
实现前提	1、需对 xxx 功能进行重新设计，需要 xxx 工程师（产品经理）配合； 2、需对项目成员工作内容进行分配		
进度影响分析	可能增加项目交付时间		
风险分析	延期交付风险低		
产品经理审批			
审批意见	（盖章） 年　　月　　日		
甲方单位审批			
审批意见	（盖章） 年　　月　　日		

表B.3 阐述了需求变更一览表。

表 B.3 需求变更一览表

编号	项目名称	项目负责人	变更原因	变更内容	对项目造成的影响	申请人	申请时间	当前责任人	备注
1	xxx	xxx	增加功能	增加xxx功能	无	xxx	xx.xx.xx	xxx	

表B.4阐述了项目立项报告。

表 B.4　项目立项报告

<table>
<tr><td>项目名称</td><td colspan="4">（格式要求：项目名称-产品编号）</td></tr>
<tr><td>项目编号</td><td colspan="2"></td><td>版本号</td><td></td></tr>
<tr><td>项目经理</td><td colspan="2"></td><td>申请时间</td><td></td></tr>
<tr><td>项目开始日期</td><td colspan="2"></td><td>结束日期</td><td></td></tr>
<tr><td>项目范围</td><td colspan="4">xxx 项目包含以下系统功能模块:
……</td></tr>
<tr><td>可行性分析</td><td colspan="4">基于 xxx 进行开发，技术可行性已进行调研。</td></tr>
<tr><td>里程碑计划</td><td colspan="4">1、xx 月 xx 日完成项目立项
2、xx 月 xx 日完成需求分析、原型设计、架构设计、接口文档
3、xx 月 xx 日完成第一个迭代沟通的编码工作，包括功能模块如下：
xxx
4、xx 月 xx 日，完成实施手册，用户手册。
5、xx 月 xx 日，完成第一个迭代周期的测试工作
6、xx 月 x 日，V1.0.0 系统试运行
…</td></tr>
<tr><td rowspan="7">主要人员分配</td><td>参与人</td><td>职位</td><td>承担内容</td><td>计划投入人月</td></tr>
<tr><td>xxx</td><td>产品经理</td><td>需求沟通</td><td>x 人月</td></tr>
<tr><td>xxx</td><td>架构师</td><td>架构设计</td><td>x 人月</td></tr>
<tr><td>xxx</td><td>项目经理</td><td>项目管理、项目进度把控</td><td>x 人月</td></tr>
<tr><td>xxx</td><td>UI 设计</td><td>界面设计</td><td>x 人月</td></tr>
<tr><td>xxx</td><td>研发工程师</td><td>软件开发</td><td>x 人月</td></tr>
<tr><td>xxx</td><td>测试工程师</td><td>软件测试、安全测试</td><td>x 人月</td></tr>
<tr><td colspan="5">产品经理审批</td></tr>
<tr><td>审批意见</td><td colspan="4">（盖章）
年　　月　　日</td></tr>
<tr><td colspan="5">甲方单位审批</td></tr>
<tr><td>审批意见</td><td colspan="4">（盖章）
年　　月　　日</td></tr>
</table>

表B.5 阐述了项目重大问题跟踪表。

表 B.5 项目重大问题跟踪表

序号	问题描述	问题情况说明	问题分类	提出日期	责任人	计划解决日期	实际解决日期	对进度的影响分析	解决措施	当前状态
1	需求变更	xxx 功能需求变更	需求变更	xx. xx. xx	xxx	xx. xx. xx	xx. xx. xx	研发时间增加	待解决	研发

表B.6 阐述了项目计划变更申请。

表 B.6　项目计划变更申请

项目计划变更申请	
项目名称	
变更的内容及其理由	xxx 模块的设计不能满足项目需求，需重新设计，并对项目计划进行变更
变更类型	（设计变更、进度计划变更、重大不可抗拒事件的变更）
评估计划变更将对项目造成的影响	项目进度有影响，时间增长
项目经理签字	
变更申请的审批意见	
产品经理审批	（盖章） 年　　月　　日
变更申请的审批意见	
甲方单位	（盖章） 年　　月　　日

表B.7 阐述了项目进度报告。

表 B.7　项目进度报告

项目名称								
项目编号								
总体进展情况								
1、本周完成 xxx 功能 2、本周开始 xxx 功能测试 …								
工作内容与项目进度状况								
需求功能点	计划工作任务	主要成果	执行人	工作量(人/时)	已完成规模%	未完成原因	预计完成时间	对进度的影响
xxx 功能	完成 xxx	xxx 功能完成	xxx	x 人时	100%	无	无	无
下周工作计划								
需求功能点	计划工作任务	主要成果	执行人	开始时间	完成时间	备注		
xxx 功能	研发 xxx 功能	xxx 功能完成 30%	xxx	xx.xx.xx	xx.xx.xx			
问题及解决情况								
1）遗留问题								
序号	问题描述	问题情况说明	问题分类	提出日期	计划解决日期	解决措施		
1	BUG 修复	xxx 功能异常	解决 BUG	xx.xx.xx	xx.xx.xx	修改代码		
2）本周解决问题								

表 B.7 （续）

序号	问题描述	问题情况说明	问题分类	提出日期	计划解决日期	实际解决日期	解决措施
1	BUG 修复	xxx 功能异常	解决 BUG	xx.xx.xx	xx.xx.xx	xx.xx.xx	修改传送参数

风险监控				
序号	风险类别	具体描述	原因分析	缓解或纠正措施
1	软件兼容	软件开发兼容性问题	软件兼容性不佳	升级软件版本尝试

产品经理审批	
审批意见	（盖章） 年　　月　　日

甲方单位审批	
审批意见	（盖章） 年　　月　　日

表B.8 阐述了测试报告。

表 B.8 测试报告

项目名称	
项目编号	
测试时间	
测试单位及人员	
测试组	
测试项目	
模块一： 共测试 xxx 项，通过 xx 项，不通过 xx 项； 不通过原因分析： ……	
产品经理审批	
审批意见	（盖章） 年　　月　　日
甲方单位审批	
审批意见	（盖章） 年　　月　　日

表B.9 阐述了项目产品软件交付清单。

表 B.9　项目产品软件交付清单

项目名称		
项目编号		
软件版本号		
包括的产品	**对应的产品名称**	**版本号**
产品发布包	(前端)	
	(后端)	
产品支持包	mysql	x.x.x
	nginx	x.x.x
	….	….
开发手册	《xxxx 开发手册》	
实施手册	《xxxx 实施手册》	
测试报告	《xxxx 功能测试》	
	《xxxx 安全测试》	
开源报告	《xxxx 开源报告》	
产品经理审批		
审批意见	（盖章） 年　　月　　日	
甲方单位审批		
审批意见	（盖章） 年　　月　　日	