数据管理平台安全管理方案

目　录

1.1.1 安全管理体系建设的目标.....3

1.1.2 信息安全管理原则.....3

1.1.3 安全管理总体框架.....4

1.1.4 安全管理体系技术.....5

1.1.5 安全管理体系内容建设.....7

1.1.6 安全管理体系措施.....7

1.1.6.1 物理环境安全防护.....7

1.1.6.2 通信网络安全防护.....7

1.1.6.3 区域边界安全防护.....8

1.1.6.3.1 边界防护.....8

1.1.6.3.2 访问控制.....9

1.1.6.3.3 入侵防范.....10

1.1.6.3.4 恶意代码防范.....11

1.1.6.3.5 安全审计.....12

1.1.6.4 计算环境安全防护.....13

1.1.6.4.1 身份鉴别.....13

1.1.6.4.2 访问控制.....14

1.1.6.4.3 安全审计.....16

1.1.6.4.4 入侵防范.....17

1.1.6.4.5 恶意代码防范.....18

1.1.6.4.6 数据完整性 19
1.1.6.4.7 数据保密性 19
1.1.6.4.8 数据备份和恢复 19
1.1.6.5 应用信息安全防护 21
1.1.6.5.1 信息应用身份认证 21
1.1.6.5.2 访问控制 22
1.1.6.5.2.1 账号权限范围 22
1.1.6.5.2.2 账号安全认证 22
1.1.6.5.2.3 账户风险控制 23
1.1.6.5.3 安全审计 26
1.1.6.5.4 剩余信息保护 27
1.1.6.5.4.1 敏感信息保护 27
1.1.6.5.4.2 数据分级分类 29
1.1.6.6 物联网安全防护 30
1.1.6.6.1 接入控制 30
1.1.6.6.2 入侵防范 31
1.1.6.6.3 感知节点设备安全防范 31
1.1.6.6.4 网关节点设备安全防范 31
1.1.6.6.5 抗数据重放 32
1.1.6.6.6 数据融合处理 32
1.1.6.6.7 感知节点设备运维管理 32
1.1.7 安全管理策略建设 33

1.1.8 安全组织体系建设.....35
1.1.9 安全教育和培训.....35

管理是网络中安全得到保证的重要组成部分，是防止来自内部网络入侵必须的部分。责权不明，管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。

1.1.1 安全管理体系建设的目标

安全管理是安全系统的重要组成部分，没有健全的安全管理，系统的安全性是很难保证。任何网络系统仅在技术上无法达到完整的安全。为此，需要建立一套科学、严密的网络安全管理体系。

通过有效的安全管理体系的建设，最终要实现的目标是：采取集中控制、分级管理的模式，建立由专人负责安全事件定期报告和检查制度，从而在管理上确保全方位、多层次、快速有效的网络安全防护。

1.1.2 信息安全管理原则

1、 多人负责原则

每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。

以下各项是与安全有关的活动：

（1） 信息处理系统使用的媒介发放与回收；

（2） 处理保密信息；

（3） 硬件和软件的维护；

（4） 系统软件的设计、实现和修改；

（5） 重要程序和数据的删除和销毁等。

1、 任期有限原则

一般地讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假策略，并规定对工作人员进行轮流培训，以使任期有限策略切实可行。

2、 职责分离原则

在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。

出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

（1） 敏感资料的接收和传送；

（2） 安全管理和系统管理；

（3） 应用程序和系统程序的编制；

（4） 计算机操作与信息处理系统使用媒介的保管等。

1.1.3 安全管理总体框架

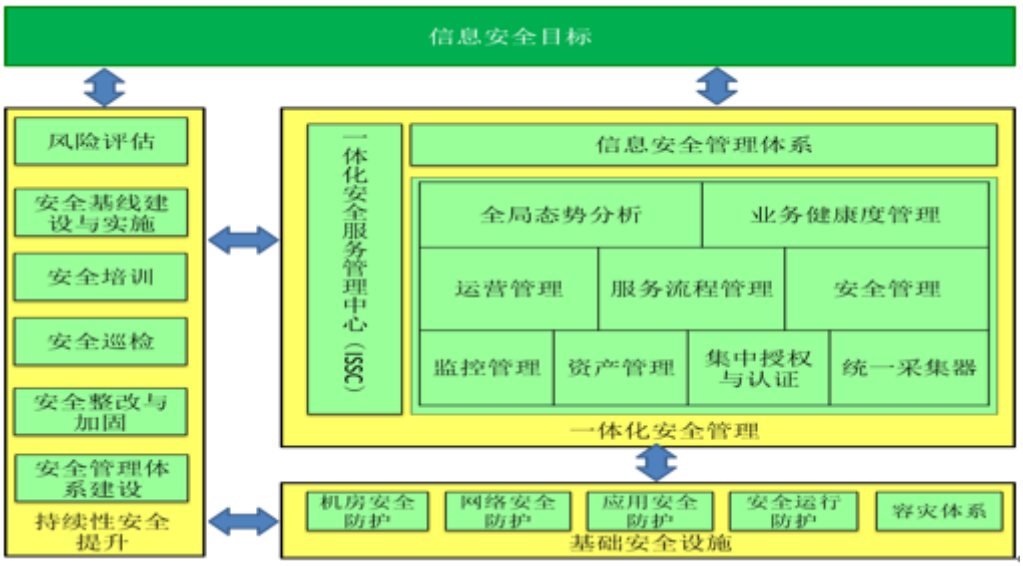
按照安全体系总体框架，结合前期的工作，应在三个架构的三个层次分别开展信息安全建设，确保信息安全体系均衡发展，有效提高投资回报率。

通过对研究所信息化系统的网络和应用现状、安全现状、面临的安全风险的分析，根据安全保障目标模型，设计了研究所信息安全体系框架，制定该框架的目的在于从宏观上指导和管理信息安全体系的

建设和运营。

本框架由一组相互关联、相互作用、相互弥补、相互推动、相互依赖、不可分割的信息安全保障要素组成。一个系统的、完整的、有机的信息安全体系的作用力远远大于各个信息安全保障要素的保障能力之和。在此框架中，以安全目标为指导，融会了基础安全设施、一体化安全管理和持续性安全提示三个安全核心，达到系统可用性、可控性、抗攻击性、完整性、保密性的安全目标。

研究所信息安全体系框架的总体结构如下图所示：



研究所信息安全总体框架

1.1.4 安全管理体系技术

平台在安全性设计上遵循中国现行信息安全技术网络安全标准，平台安全性包括南向接入安全、北向对接安全、门户访问安全、数据存储安全、数据容灾、数据传输安全、数据访问安全以及网络安全等。

- **南向接入安全**

平台支持用户名密码认证、设备序列号认证、应用平台标识认证、IP 地址认证、证书认证等多种接入方式认证，来保证平台接入的安全性。

■ **北向对接安全**

平台和上层应用平台或第三方订阅平台支持双向认证机制，即平台对其他平台身份进行认证和其他平台对平台身份进行认证。

■ **门户访问安全**

平台提供自服务门户和运营管理门户，门户访问具备必要的安全保障措施，包括统一登录页面、短信验证码认证、强密码机制、严格的访问权限控制。

■ **数据存储安全**

数据存储过程中，及时缓存内容到支持层，保证数据完全写入不丢失。同时，通过磁盘阵列、分布式存储系统对数据进行冗余备份，保证节点异常时候数据不丢失。

■ **数据传输安全**

通过客户端和平台之间使用 SSL 安全连接，保证传输过程中的数据被加密，可以防止中间人攻击。使用双向安全认证客户端带证书连接平台，可以防止非法设备接入网络。

■ **数据访问安全**

1）使用 OAuth2.0 进行统一登陆授权，引入了授权服务器做为中间件隔离，客户端和应用之间不会进行私密信息的直接传输和交互，保证用户认证信息的安全性和伪造性。

2）基于角色的用户权限系统设计。系统分为资源、角色、用户三层概念，可以方便的分级、分域、细粒度的进行权限控制。

3）资源自身的认证体系。每个资源被请求访问的时候，均会判断请求者的合法性，只有拥有相应权限的请求者才能得到正常的资源服务，非法的请求直接被拒绝服务。

1.1.5 安全管理体系内容建设

通过规划安全策略、确定安全机制、明确安全管理原则和完善安全管理措施，建立安全管理机制，制定各种规章、制度和准则，合理地协调法律、技术和管理三种因素，实现对系统安全管理科学化、系统化、法制化和规范化，达到保障网络系统安全的目的。

1.1.6 安全管理体系措施

1.1.6.1 物理环境安全防护

政务外网云计算平台在物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和带电磁防护等方面都满足三级等保要求。

1.1.6.2 通信网络安全防护

网络安全域划分是落实访问控制策略、建立纵深安全防护、执行安全管理政策的物理基石。根据等级保护要求，并依据信息系统实际情况分析，划分互联网接入区、公用网络区等安全域。

1、 互联网接入区

- 边界网络：网络边界是安全防护重点区域，部署防火墙、IPS、WEB 应用防火墙等安全设备。
- 骨干网络：提供全网网络交换，部署交换机等。

- 服务器：部署应用服务器、数据库服务器等。
- 终端接入：接入互联网有线终端和无线终端等设备。

2、 公共网络区

- 骨干网络：提供全网网络交换，部署交换机等。
- 服务器：部署应用服务器、数据库服务器等。
- 安全管理中心：从功能、重要级别角度考虑，建立安全管理中心，承担保障网络运行、安全、维护的工作。安全管理中心内部署堡垒机、日志审计系统、数据库省级、防病毒系统等。

1.1.6.3 区域边界安全防护

1.1.6.3.1 边界防护

通过防火墙系统进行网络边界的安全防护，保障跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，满足等保三级建设安全区域边界——边界防护要求。

子项	等保要求	防护措施
边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	防火墙
	b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；	

	c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；	

1.1.6.3.2 访问控制

参照等级保护要求在相关边界部署防火墙系统进行访问控制，通过安全加固服务配置实现进出网络的数据流实现基于应用协议和应用内容的访问控制,将所有不安全的或不符合安全规则的数据包屏蔽，除允许通信外受控接口拒绝所有通信，杜绝越权访问，防止各类非法攻击行为。

子项	等保要求	防护措施
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	安全策略加固
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	安全策略加固
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	安全策略加固

	d）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	防火墙

1.1.6.3.3 入侵防范

在各安全域之间,根据安全策略在网络层判断数据包的合法流动。但面对越来越广泛的基于应用层内容的攻击行为，需要其他具备检测新型的混合攻击和防护的能力相互配合，共同防御来自应用层到网络层的多种攻击类型，建立一整套的安全防护体系，进行多层次、多手段的检测和防护。入侵防御措施就是安全防护体系中重要的一环，它们能够及时识别网络中发生的入侵行为并实时报警并且进行有效拦截防护。

子项	等保要求	防护措施
入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	IPS
	b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	
	c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；	

	d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。	

1.1.6.3.4 恶意代码防范

通过防病毒网关系统，对夹杂在网络交换数据中的各类网络病毒进行过滤，对网络病毒、蠕虫、混合攻击、端口扫描、间谍软件、P2P软件带宽滥用等各种广义病毒进行全面的拦截。阻止病毒通过网络的快速扩散，将经网络传播的病毒阻挡在外，可以有效防止病毒从其他区域传播到内部其它安全域中，截断了病毒通过网络传播的途径，净化了网络流量。

子项	等保要求	防护措施
恶意代码防范	a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	防病毒网关
	b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	

1.1.6.3.5 安全审计

通过日志审计系统针对设备以及主机日志进行统一的收集与审计，审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。满足《网络安全法》要求“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

子项	等保要求	防护措施
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	日志审计系统
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	
	d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	

1.1.6.4 计算环境安全防护

主要是对资源的有效性进行控制，管理和控制不同等级用户对信息资源和服务资源具有什么权限，其安全性策略包括用户和服务器间的双向身份认证、信息和服务资源的访问控制和访问资源的加密，并通过审计和记录机制，确保服务请求和资源访问的防抵赖。针对本项目的信息资源的安全级别的特点，其安全策略主要包括统一的身份认证、权限管理、日记审计等。

1.1.6.4.1 身份鉴别

用户端进行登录认证时，根据用户设备信息、系统版本、终端类型、终端版本等相关信息进行组合并通过加密算法生成的唯一密钥，合法授权后下发登录令牌 Token。整个数据交互过程加密，同时发起授权与登录的过程间隔时间服务器严格控制,不管登录成功还是失败，授权码当次有效，保证登录过程不被攻击。

通过安全服务加固的方式对用户鉴别信息复杂度、时效性进行加固，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出进行配置，并采用两种或以上组合的鉴别技术对用户身份进行鉴别，加强用户身份管理。

本项目需采用安全服务中主机加固服务来满足等保三级建设安全计算环境——身份鉴别要求。

子项	等保要求	防护措施

身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	主机加固

	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	

1.1.6.4.2 访问控制

通过安全服务主机加固进行有效的计算环境主机访问控制，保障计算环境安全，加固内容包括但不限于：

（1）对登录的用户分配账户和权限；

（2）重命名或删除默认账户，修改默认账户的默认口令；

（3）及时删除或停用多余的、过期的账户，避免共享账户的存在；

（4）授予管理用户所需的最小权限，实现管理用户的权限分离；

（5）由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

（6）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

（7）对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

本项目需采用主机加固服务来满足等保三级建设安全计算环境——访问控制要求。

子项	等保要求	防护措施
访问控制	a）应对登录的用户分配账户和权限； b）应重命名或删除默认账户，修改默认账户的默认口令； c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； d）应授予管理用户所需的最小权限，实现管理用户的权限分离； e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	主机加固

1.1.6.4.3 安全审计

计算环境安全审计主要从主机安全审计以及数据库系统安全审计两方面来设计。