上联集团山东公司信息化升级
技术要求

2025.11

一、项目背景

为了迎合水泥行业绿色发展和全面推进水泥智能制造数字转型，完善水泥产业链生产管理，提高企业运营效率，所以实施本次信息化升级。目标是搭建业财税一体化管控平台和数智化工厂，实现OA办公系统、一卡通物流、ERP管理系统与生产管理系统的融合集成，建设成“绿色、环保、高效、低耗” 技术先进、成本领先，基于“平台+5G+应用”新一代“水泥智能工厂” 行业应用样板 。

二、项目目标

- 建成统一数据中心；
- 顺滑对接一卡通无人值守系统；
- 业务系统数据自动传递并自动生成记账凭证，提高财务工作效率；
- 与 OA 办公系统顺滑对接到 ERP 管理系统，数据实时共享；
- 实现生产管理信息系统与 ERP 系统数据顺滑对接；
- 实现业财一体化 ERP 管理系统；
- 实现 AI 智能分析和 BI 智能分析展示；
- 支持后期各种异构系统的融合；

三、项目范围

本次项目实施范围：先行实施山东联合王晁水泥有限公司、枣庄徕盛新型建材有限公司、山东上联水泥发展有限公司信息化系统整合。随后推进上海三家公司实施。

本项目涵盖范围及实现功能简介如下：

子系统	模块名称	功能简介
多组织特性	组织管理	支持多个组织业务处理及多组织间业务往来处理
	组织间结算	支持多组织，多组织架构下的多组织业务活动，即，需要在发生业务的组织之间进行内部结算。
工作流平台	工作流运行平台	顺滑对接联合王晁水泥公司现有的 OA 系统与 ERP 系统融合一体，实现合同审批、计划审批中的 OA 系统与 ERP 系统进行数据接口，流程办结完成后自动回传到 ERP 系统中相应系统模块，实现业务流程与单据自 动传递，提高流程处理的及时性和效率。
业务监控平台	业务监控平台	实现监控方案定时执行，并把满足条件的监控记录通过内部消息发送给接收人，实现对企业管理中采购、到货、付款、销售、发货、收款、库存管理等各主要业务环节的监控控制。

财务	总账	以凭证处理为中心，进行账簿报表的管理。通过智能会计平台与各个业务系统无缝连接，实现数据共享。提供账簿查询（总分类账、明细分类账多栏式明细账、核算维度明细账、数量金额、总账数量金额明细账）和财务报表（科目余额表、试算平衡表、摘要汇总表、核算维度余额表、核算维度与科目组合表、多账簿科目余额表），以及现金流量处理
	智能会计平台	智能会计平台自动生成凭证，实现业务数据与财务数据的一体化对接，并通过会计政策、会计核算体系的架构对业务进行财务监控、分类、记账
	报表	财务报表平台，基于类 EXCEL 报表编辑器，通过快速报表向导，灵活的取数公式，快速、准确地编制企业对外会计报表以及各类财务管理报表，支持对报表多维度的统计和查看
	应收款	应收款管理系统通过应收款确认、到期收款、应收收款核销、应收开票核销、期末处理、报表分析达到对应收款的精细化管理。其中应收款确认分为对销售应收的确认和对其他应收的确认
	应付款	应付款管理系统通过应付款确认、到期付款、应付付款核销、应付开票核销、期末处理、报表分析达到对应付款的精细化管理。其中应付款确认分为对采购应付的确认和对其他应付的确认
	出纳管理	出纳管理系统为企业出纳提供管理工具，管理企业资金、票据的收支业务，通过业务流程、权限、盘点作业、账表等保证企业资金收支业务的准确执行，确保资金安全

	银企直连	网上银行系统实现企业与银行的直联，企业通过网上银行系统直接完成与银行网银系统的所有提交以及查询动作。同时也可以实时下载银行的交易明细、电子对账单，以及查询银行账户余额。
	存货核算	存货核算系统面向企业成本会计人员，提供采购入库核算、入库成本维护、委外入库核算、出库成本核算、其他存货核算、成本调整以及报表分析等功能
	产品成本核算	产品成本核算系统面向企业成本会计人员，提供费用分配、自制半成品、产品、委外加工产品成本核算，以及成本计算报表分析等功能
	资产管理	资产管理系统以资产卡片管理为中心，从资产购入企业开始到资产退出的整个生命周期的管理，能针对资产实物进行全程跟踪、能够记录、计量资产的价值变化，能够记录资产的使用情况和折旧费用的分配情况。实现资产管理工作的信息化、规范化与标准化管理，全面提升企业资产管理工作的工作效率与管理水平。应考虑与设备管理软件的数据互通。
	税务平台	实现财务与税务数据联通，对发票进行统一接收、查验、管理，连接业务系统交易数据与税控软件开票，实现快速开票、统一管理。自动统计生成纳税申报表，并能实现电子申报。
管理会计	预算管理	费用预算模型搭建、费用预算编制、费用预算控制、费用预算调整、费用实际数据、费用预算分析等业务处理。支持财务、预算、企业报表数据整合，支持 ERP 端完整的预算编制流程。

供应链	采购管理	采购管理系统是通过采购合同、采购申请计划、采购订单、采购收料入库、采购退料等功能综合运用的管理系统，对采购业务全过程进行有效的控制和跟踪，实现完善的企业采购业务管理。结合公司现有的OA 系统。应考虑招采平台对接。
	销售管理	销售管理系统，是对销售报价、销售合同、销售订货、仓库发货、销售退货处理、客户管理、价格及折扣管理、订单管理、信用管理等功能综合运用的管理系统，通过对销售全过程进行有效控制和跟踪。如有特殊的业务流程需要，随需扩展。
	信用管理	信用管理系统，是通过信用检查规则、信用档案、信用特批权限、信用初始化、信用重算、信用状况查询、例外信息查询、业务单据中的信用查询和信用控制等功能的综合运用，对信用管理全过程进行有效控制和跟踪，从而建立完善的信用管理体系
	库存管理	通过提供采购、销售、生产经营过程中发生的出入库业务管理，提供库存在库业务管理，提供精细化的批号、有效期、序列号管理，自动生成库龄分析报表。
智能物流	无人值守地磅	集成现有无人值守计量系统，与金智捷一卡通物流系统实现顺滑对接，过磅数据与 ERP 贯通，实现业财一体化，有效支持正向及逆向业务处理，实现业务系统单据的自动流转，支持一单到底查询功能。
生产管理	生产管理	生产管理以生产订单为主线，实现了生产管理的核心业务流程，包括：生产订单管理（创建、审核、下达、结案等）、生产用料清单管理、完工汇报管理、生产入库管理、生产订单的变更管理等
	智慧	与生产线智能化系统对接

	车间	
HR 管理	s-hr 组织管理	行政组织管理可实现行政组织和职位的初始化导入、日常维护、行政组织调整，职务体系的搭建，多维编制管理、编制需求申请的发起等
	s-hr 员工管理	员工人数初始化、员工信息日常维护、员工全生命周期管理、员工人事事务处理、合同管理及员工明细查询和统计分析报表
	s-hr 薪酬核算	薪酬核算包含了员工薪酬档案管理、员工社保档案管理、员工薪酬向导式核算、变动员工薪酬精准核算、发放审批、银行代发、薪酬成本分摊，薪酬费用分配提交财务生成凭证，套打打印，员工自助查询工资条，薪酬报表查询和薪酬统计分析报表、社保及住房公积金缴纳计算和报表查询等功能
	s-hr 薪酬管理	薪酬管理包含了薪酬标准定义、定调薪业务设置和定调薪申请、场景化的激励薪酬申报管理、支持额度导入和预算管控的额度台账功能
	s-hr 报表查询	各类报表查询
	Apusic s-HR 专版	s-hr 必购基础模块

BI 分析	经营分析平台	自定义设计分析主题、分析模型，包括数据抽取、整理、优化，形成数据仓库
	分析主题	财务、采购、销售、仓库分析、生产分析（根据计划）
生态链扩展	互联网	信息采集、发布
数据中心	超融合数据中心	利用5G+新技术实现硬件、虚拟化、存储、网络、安全一体化集成管理，多资源池、多中心统一化管理、调度，实现异构、裸机服务器的统一化管理
云桌面	25	超融合平台融合的一体化终端，终端采用嵌入式操作系统，比如Android、Linux，支持终端准入检测，可根据用户接入的终端类型、操作系统版本、接入 IP 和时间、软件安装情况等条件设置接入访问策略

实施策略

本项目建设的原则是“总体规划，分步实施”。

本项目实施地点位于：台儿庄。

如果项目需要到上述实施地点之外的其他地点开展实施工作，另行安排。

1.超融合数据中心部署

技术要求

- 实现硬件、虚拟化、存储、网络、安全一体化集成管理
- 多资源池、多中心统一化管理、调度
- 实现异构、裸机服务器的统一化管理

部署方式

- 部署 3 台超融合一体机（aServer-X5-2105）承载现有及后续新增业务。
- 超融合一体机所能提供的资源分别为：

  CPU:2*16*2*2.9*3=556.8 HZ

  内存：4*32*3=384G

  存储：2*4*3=24T

安全性支持功能：

- 数据中心边界部署下一代防火墙，为数据中心提供全面、专业的安全防护能力，集传统防火墙、IPS、防病毒、应用管控等功能于一体。
- 根据业务系统数量部署主机版终端防护软件 EDR，为业务系统提供包括勒索病毒防护，弱密码防护，漏洞管理和微隔离在内的多种安全防护能力，保障业务的安全。

1.1 超融合交换机

1、不少于 12 个 10G SFP+光口，不少于 12 个千兆电口；交换容量≥1.28Tbps/12.8Tbps，

2、支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；包转发率≥480Mpps

3、支持终端识别、终端准入、安全防护及安全画像可视；

4、支持胖瘦一体化；

5、提供产品质保不低于三年;软件升级不低于三年;

1.2 云桌面（25 台）

1、CPU：四核、主频不低于 1.6GHz,内存不小于 1GB，内置存储器不小于 4GB；至少 6 个 USB 接口、1 个 VGA/HDMI 显示接口、1 个标准以太网口。

2、超融合平台融合的一体化终端，终端采用嵌入式操作系统，比如 Android、Linux，支持终端准入检测，可根据用户接入的终端类型、操作系统版本、接入 IP 和时间、软件安装情况等条件设置接入访问策略，如终端不满足安全检测要求则不允许接入。

3. 提供 3 年售后和硬件维保及软件升级服务。

1.3、范围及清单

序号	产品型号	产品名称	产品说明	购买数量	单位
1-1	超融合一体机	aServer	硬件参数：规格：2U，CPU：2 颗 Intel Xeon Silver 4510 CPU@2.4GHZ (12C)，内存：12*32GB DDR5 5600，系统盘：2*480GB SATA SSD，缓存盘：2	3	台

			个* 固态硬盘-1.92T-SATA-SSD;，数据盘：4 个* 机械硬盘 8T（X86 架构通用）； ，标配盘位数：12，电源：白金或钛金，冗余电源，接口：4 千兆电口+2 万兆光口。 aServer-X5-2105 标准产品,每台含： 2 套* 深信服虚拟存储软件 V3.0; 2 套* 深信服计算服务器虚拟化软件 V6.0（Base）； 2 套* 深信服网络虚拟化软件 V6.0（Base）； 2 套* 深信服云计算管理软件 V6.0 高级版; 3 年* 深信服 SDDC 基础运维软件 V1.0(一体机版)；		
1-2		深信服计算服务器虚拟化软件	服务器虚拟化，通过虚拟化技术将物理服务器虚拟化为一个逻辑计算资源池。开通后具备对虚拟机全生命周期管理的能力，可对虚拟机进行开关机、模板部署、克隆、导入导出等操作；具备 HA、动态资源调度、蓝屏重启等机制保证业务高可靠；具备对虚拟机资源监控、告警等功能。	6	套
1-3		深信服网络虚拟化软件	网络虚拟化，利用统一的管理平台对虚拟网络设备进行管理和配置。开通后实现”所画即所得“的网络部署，具备全局流量可视化、网络连通性检测等功能。为每个虚拟机提供一个 3-4 层的分布式防火墙和监控中心以及无限制的虚拟路由器和虚拟交换机，不开通只能创建 1 个虚拟路由器和 2 个虚拟交换机。	6	套

1-4		深信服虚拟存储软件	存储虚拟化，通过将硬盘资源池化提高资源利用率，利用智能条带化、分层、热点数据预测等技术提高存储性能。开通后支持创建虚拟存储卷，灵活配置存储策略（多副本、QoS 等）；具备磁盘故障重建、硬盘亚健康检测等功能。	6	套
1-5		深信服持续数据保护软件	CDP 功能必备模块。 支持无代理 CDP 技术，不需要在虚拟机内部安装任何代理软件，即可对虚拟机进行持续数据保护，CDP 不影响保护虚拟机的性能； 支持策略管理，最小提供 RPO 为秒级的数据保护； 支持业务虚拟机的快速恢复，可以指定策略覆盖原有虚拟机或者创建新虚拟机； 支持 CDP 备份任意时间点的数据克隆，通过克隆数据恢复虚拟机进行测试与验证； 支持通过 CDP 备份数据找回文件； 支持 CDP 功能升级扩展为异地 CDP 容灾能力； 支持提供 CDP 备份时间点图形化显示，并显示 CDP 时间点 IO 日志保存速率； 支持 CDP 日志丢失后的备份恢复容错能力。 开通后，默认送 25 台虚拟机的 CDP 授权基础包。	1	套

2	RS6300-24X-LI-12X	万兆SFP+光口≥12个；千兆电口≥12个；	1、万兆 SFP+光口≥12 个；千兆电口≥12 个； 2、支持双交流电源 1+1 冗余（非热插拔）； 3、Console 口≥1 个，Manage 口≥1 个； 4、交换性能≥1.28Tbps/12.8Tbps，包转发率≥360Mpps； 5、支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时在控制器平台灵活的进行切换；	2	台
3-1	配件	光纤线-多模-LC-LC-3M		9	条
3-2		万兆多模-850-300m-双纤	SFP+万兆多模光模块,速率:10Gb/s,波长:850nm，传输距离：0.3km，双 LC 接口	14	个
4	深信服下一代防火墙	AF-1000-FH1600B-1K	性能参数：网络层吞吐量：5G，应用层吞吐量：2G，防病毒吞吐量：650M，IPS 吞吐量：650M，全威胁吞吐量：550M，并发连接数：210 万，HTTP 新建连接数：7 万， 硬件参数：规格：1U，内存大小：4G，硬盘容量：	1	台

			128G SSD，电源：适配器，接口：8 千兆电口+2 千兆光口 SFP。 含： 深信服防火墙软件基础级(*1 套); 深信服云智订阅软件(*3 年); 深信服云威胁情报网关订阅软件(*3 年); 产品质保(*3 年); 软件升级(*3 年);		
5	桌面云 aDesk 瘦终端 +VDI 接入授权	aDesk-STD-220(VGA+HDMI)	硬件参数：CPU 型号：A55 1.6GHz，内存：2GB，硬盘容量：8GB（板载），接口：1 千兆电口，接口类型：1*VGA + 1*HDMI，USB：5*USB2.0+1*USB3.0（aDesk 5.5.2 及之后版本支持 USB3.0 速率）。 深信服 aDesk 瘦终端系统软件 深信服 VDI 接入授权（普通版）	25	点

2.ERP 系统部署

技术支持

- 系统所有模块应可工作于 SQL 2012R2 数据库。
- 服务器端主流操作系统（Windows SERVER 2012 R2）。
- 客户端支持 Windows 10/Windows 7、IE 11 浏览器、Google

Chrome 浏览器、手机端浏览应用。

部署方式

- 软件产品所构建的 ERP 管理平台支持公有云（移动云、华为云等）和本地私有云部署
- 软件产品所构建的 ERP 管理平台能够向公司外部用户提供 Internet 的访问与操作方式。

- ERP信息系统初始化配置。

安全性支持功能：

- 使用安全的授权方式；
- 最终用户客户端和 Web 服务器间能够使用安全的通信协议；
- Web 服务器同数据库间使用安全的通信协议；
- 数据采用安全的保护措施、设计安全的备份和恢复策略；
- 提供数据应急方案；
- 支持按角色、记录、属性设定业务与数据权限。

平台统一

- 同一业务角色在使用其可能用到的所有模块时，要实现统一入口登录。
- 用户工作界面具有灵活的配置能力。
- 一单到底，钻取式查询、分析。

流程支持

- 可以灵活配置工作流，并与业务流程紧密结合。

- 可以通过业务监控平台实现业务预警。
- 支持图形化的业务流程建模。
- 支持图形化的流程监控和流程效率统计分析。
- 定制支持
- 提供易于使用的报表定制工具。
- 提供易于学习的业务功能定制开发工具。

3.智能监控平台（根据计划安排）

技术要求

- 实现硬件、虚拟化、存储、网络、安全一体化集成管理
- 多资源池、多中心统一化管理、调度
- 实现服务器的统一化管理
- 客户端支持远程查看、移动手机查看。

部署方式

- 支持公有云（移动云、华为云等）和本地私有云部署
- 车间及厂区监控改造，替换更换网络数字高清摄像头
- AI 开放平台超脑(AIOP+HEOP)、泛智能超脑 iSecure Center 综合安防管理平台、iSecure Center 综合安防管理平台（视频监控）、iSecure Center 综合安防管理平台（AI 模型管理）

4.智慧车间、智能工厂（根据计划安排）

四、技术安全方案

4.1 安全体系

本项目中 ERP 相关系统要求采用为共享财务中心平台提供一个安全框架。该框架包括安全策略、安全管理、系统安全、安全合规、以及多种应用安全基础技术。安全策略包括企业需要对企业运行环境及使用者进行安全分析、并根据目标制定安全方案、对方案进行安全评估、进行关键风险的控制等；安全管理主要包括日常的与安全相关的工作，包括安全配置管理、补丁管理、系统监控等；系统安全包括数据和存储安全、服务器安全设置、应用安全设置、网络安全配置、以及各种端的安全等；安全合规性非常重要，是在标准产品、行业产品、本地化产品和产品定制开发时的重要内容；要求能够支持多种安全基础技术，包括 CA 认证、加密/解密、动态密码、USB Key、SSL、IPSec、VPN、https 等。

ERP 中心平台采用集中部署方式，安全架构包括应用、数据、主机、物理、网络、终端、安全运维和安全管理等八个方面的内容。

下文是指生产环境的安全设置。开发和测试环境，应和生产环境进行隔离。为了方便开发和测试，对于生产环境要求的数字证书登录等，可以简化。

4.1.1 安全建设规范

ISO/IEC 27001/27002，推动信息安全体系(ISMS)建立与实施，采用以风险管理为核心的方法管理公司和用户信息，保障信息的保密性、完整性及可用性；

符合等级保护基本要求：根据国家下发的《关于信息安全等级保护工作的

实施意见》、《信息安全等级保护管理办法》开展信息安全等级保护工作，主要是指对国家、法人和其他组织及公民的专有信息， 公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护,对信息系统中使用的信息安全产品实行按等级管理,对信息系统中发生的信息安全事件分等级响应与处置。

符合政策法规：根据国家信息安全相关法律、法规要求，设置与信息安全监控机构之间的联络员，制定实施程序，以确保系统符合国家关于知识产权相关法律和法规要求。通过定期检查识别、记录、评审保密协议中数据安全的相关控制要求(如访问控制、防泄露及完整性要求)，防止不正当披露、篡改和破坏数据。

4.1.2 流程和技术保障

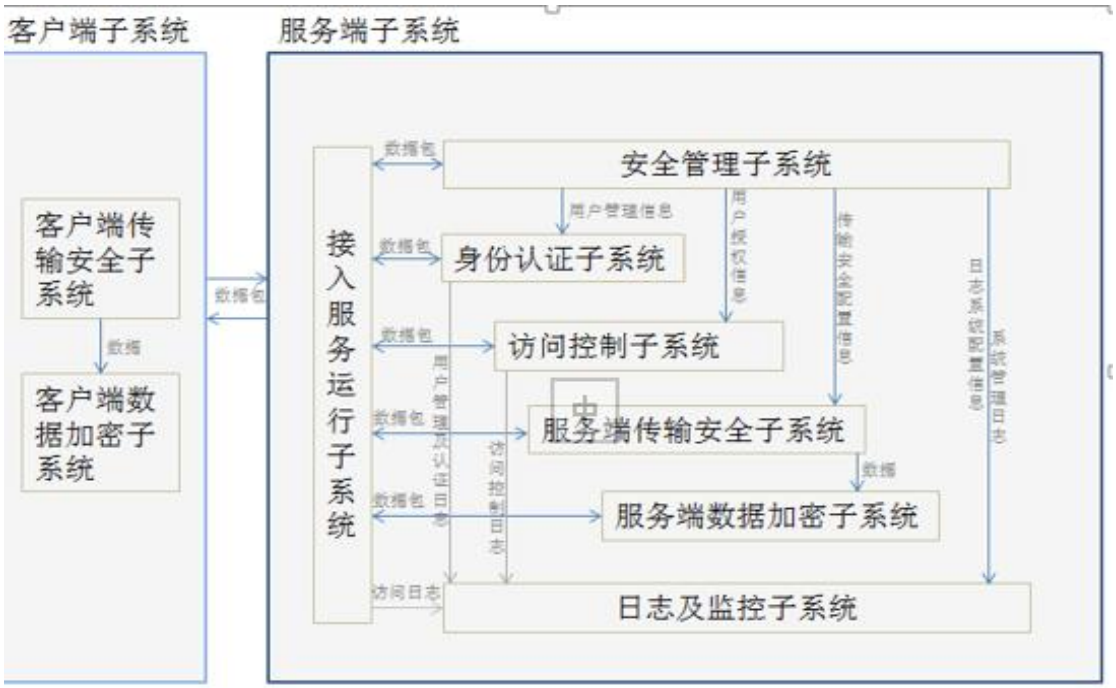
安全体系建设，从管理、运维到具体的技术保障，遵循业界的主流的框架和规范：

安全体系

4.2 应用安全

4.2.1 应用安全框架

应用安全框架是通过资源访问的控制、应用安全信息等级划分、系统调度、高强度的算法、安全终端机制保证应用服务器安全、集成应用安全、终端应用安全。



应用安全框架

4.2.2 应用级安全(身份认证/日志审计)

通过设置用户所能操作的资源即功能和数据的范围，从而达到对企业中各职位相关人员所使用系统权限的有效管控，使其各司其职，权责分明。

4.2.3 身份认证

用户登录及密码安全策略：

默认采用用户名+口令认证的身份认证方式，也可采用数字证书登录，可集成动态密码卡、IC 卡、USB 口的硬件认证设备；主要包括密码策略：初次登录，强制修改初始密码；密码强度、变更周期可以设置，在设置时低于信息安全规范要求不能生效；口令及数据采用加密的方式进行传输；设计统一错误提示，避免认证错误提示泄露信息。在认证失败时，向用户提供通用的错误提示信息，不区分是帐号错误还是密码错误，避免错误提示信息被攻击者利用。管理员登录系统时 IP 地址限制，为防止一个用户在一台计算机上以多个用户身分登录；同一计算机，限定只能有一个用户登录。并设置用户的访问时间。未在指定时间段访问的，不能登录；而且可以访问的客户端 IP 地址范围，符合才能登录系统等。

支持 CA 身份认证：为每个用户制作一个令牌（USB Key 或智能卡）用于存放用户标识，用户证书及用户私钥。访问令牌中的私钥需要提供口令。服务器端部署 KDC 和 CA 服务器。CA 服务器存放所有用户的证书。

会话安全：

轻量级会话安全采取如下措施：

在每次认证后打开一个新的会话：即使已经有与用户关联的会话标示符，在用户认证成功之后仍要重新建立一个会话；

强制执行一个会话最大空闲时间：用于缩短那些未能及时注销的用户暴露在外的时间，减少了可供攻击者猜解的会话 id 的平均数目。

强制执行一个会话最大生存周期：增加安全性和稳定性。只有在不超过会话 id 最大生存周期的时候，才允许一个会话不用再次进行对用户的认证。通过进行重新认证，可以防止攻击者窃取会话 id。

与服务会话是安全采取如下措施:

Token 算法使用强随机数，随机数由统一的获取随机数方法得到，提高加密强度。有重放攻击预防机制；

可以配置是否对单个账户的多重并发会话进行限制；

客户端 IP 地址绑定，是否绑定 IP 作为一个安全策略供选择是否启用。

4.2.4 日志审计

系统提供上机日志、业务日志和安全日志，通过日志对各个模块的运行情况和用户关键操作进行监控并跟踪记录。产品日志遵循 W7 原则，即记录谁、在什么时候、从什么地方、在什么地方、对什么对象做了什么事情、事情的结果是什么。支持记录所有访问控制校验失败的记录至系统 log。

系统级的日志在应用程序编译时刻就已经确定，使用的模块不会动态变化。该日志只有平台技术代码的代码使用，其它产品代码不准使用。

产品级日志是指日志系统所采用的模块在运行时刻随着程序的运行环境不断发生变化的的日志。

平台级日志是指日志系统所采用的模块在运行时刻随着程序的运行环境不断发生变化的的日志。主要不同之处为了确保产品的调试方便性，通过平台的日志保证代码放在平台配置的日志中。

上机日志

上机日志通过系统管理日志（system 的上机日志）、管理日志（管理员的上机日志）、普通业务日志（其他用户的上机日志）来分别记录用户进入或退出的某个功能节点及其时间。系统管理日志和管理日志是关键用户日志。

安全日志

安全日志记录发生了哪些与安全有关的活动，谁对这个活动负责。安全日志

的目的是追踪和记录发生在涉及安全对象上的事件。安全日志关注包括身份认证、登录，权限相关（权限管理、授权、权限访问控制）、访问控制、特权用户操作、安全配置变更、对关键功能的访问等等。安全日志默认打开并且不可关闭。

业务日志

业务日志记录用户对业务数据的有效操作内容。业务日志的记录配置支持记录到业务对象的操作和属性级，可以通过配置把敏感的业务对象的哪些操作和哪些属性记录业务日志，业务日志会记录这些属性的变化。对重要的业务对象，系统预置为必须记录业务日志，不可配置为不记录业务日志。

4.2.5 权限管理体系

通过设置用户所能操作的资源即功能和数据的范围，从而达到对企业中各职位相关人员所使用系统权限的有效管控，使其各司其职，权责分明。

4.2.6 用户管理

系统中的用户泛指能登录系统的账号，主要分为以下几种：普通用户、普通管理员、管理员、系统管理员、超级管理员（只有创建系统权限，无其他任何权限），对这些用户使用的安全策略的严格程度依次增强。

4.2.7 职责管理

职责即业务职能所具备的权限范围，是一组具有相关联的业务意义的功能节点，页签，和业务活动的集合。通常按企业相关职务的权限范围来建立职责并划分职责的功能范围，通过以职责为中间环节，为角色或用户分配功能权限。

4.2.8 角色管理

角色是相同岗位所拥有的一组权限的统称，在系统中体现为一些相关的职责，

以及数据权限的范围。用户通过扮演不同的角色来完成权限的控制。角色分为业务类角色和管理类角色，管理类角色只能分配管理类职责，业务类角色只能分配业务类职责。通过角色互斥系统管理员不做业务或业务人员不参与系统管理的情况下设置。

4.2.9 CA 安全体系

为了满足关键应用的信息传递的机密性、保障电子化信息交互的层面上双方（多方）行为的不可篡改和不可抵赖性、并且使电子化的数字签名和手写签名一样具有法律的效力，得到《中华人民共和国电子签名法》法律的保障。

（1）从技术层面上讲：信数字证书实现的数字签名技术可以通过目前最安全的 PKI 技术上实现以下功能：

数字签名：对关键业务数据进行签名，保证机密性、完整性和不可抵赖性。

安全访问：替换掉原有安全级别较低的“用户名/口令”方式，防止非授权用户的恶意攻击，同时不能破坏系统原有的权限管理机制。

信息加密：通过高强度的加密算法形成安全的 SSL 加密通道，防窃取。

（2）从法律层面上讲：第三方 CA 厂商率先获得了《电子认证服务许可证》，其所颁发的数字证书得到中华人民共和国《电子签名法》的认可和保护。

4.3 敏感数据加密存储策略

4.3.1 关键业务数据处理方案

针对企业员工工资等数据，系统利用数据加密算法等措施对这类敏感数据进行加密存储，具体描述如下所示：

利用 RSA+DES 算法进行数据加密，用 RSA 技术商讨密钥，DES 算法加密数据，无论对传送中的数据还是存储于数据库中的数据，均能保证其安全。

在传输层绑定各种协议，能够针对数据项、数据库表、操作功能进行不同层次的加密。

数据加密的密码和密钥采用非明文方式出现，在任何情况下不会暴露给第三方。

4.3.2 其他数据方案处理

有效防敏感信息不被泄露的保护措施是对该类数据进行加密，具体加密策略为：利用数据库的数据隐私技术中的高级安全插件：数据加密 TDE 和访问控制 Database Vault 这两种应用对数据库中存储的薪资、福利等敏感数据进行加密以及对访问数据库中的用户进行控制，防止敏感数据泄露，同时还运用操作监控对数据库运行过程进行事前监控预警以及事后跟踪查看据。

4.3.3 传输加密策略

数据在网络上传输时，为保证数据的安全，防止数据被窃取。数据报文加密可通过硬件加密或软件加密方法来实现，可根据数据处理量大小等因素选择硬件加密或软件加密。

所有加密设备和加密算法的选用应符合国家相关密码管理条例的规定。加密算法应选用国际通用的算法。

利用浏览器访问系统重要数据时，使用 HTTPS 协议。在浏览器与 WEB 服务器间建立安全的 SSL 通道，并对应用透明，做到了信息的秘密性。

4.4 安全算法体系

安全算法体系用于保证应用数据的加密安全和防止应用数据篡改，提供通用算法及用户定制算法的功能。安全算法体系由通用的安全算法框架、算法调用框架组成。

4.4.1 安全算法框架

安全算法框架是包含了有对称加密算如 DES、AES、不对称加密算法如 RSA 及不可逆加密算法等通用的标准加密算法实现，也包含数据唯一性的算法，也可以使用 JCA 包含的算法。同是还可集成用户自定义的安全算法。系统默认为 AES 加密。

4.4.2 算法调用框架

用户在系统登录及数据传输过程中选择使用的对应加密算法。改框架确保正确调用的算法，用已保证数据传输的安全。并减少代码的更改。

4.4.3 系统集成安全体系

集成应用安全体系是保障与其他服务器安全传输的的安全，保障数据的真实性、唯一性和抗抵赖性。如果数据在传输过程中，被非法的第三方通过非法手段进行截取修改。并可以加密，对通信进行保护。

集成应用安全体系通过安全中间件，收集服务器及其他集成应用服务器如网银适配器的生产环境信息；分别在服务器及其他集成应用服务器启程部署传输安全中间件；分别为服务器和其他集成应用服务器安装带有两者身份信息的服务器证书；每次由服务器发送的数据都添加签名和加密处理保障数据的安全性、唯一性。

4.4.4 系统级安全

平台的稳定性是保障应用服务和提高运营效率的重要保证，安全系统平台能够达到 7*24 小时可用，年系统可用率要达到 99.99%，同时一旦有突发事件发生，系统应当能够提供良好的容灾备份手段，保证对用户端的应用不被中断，同时记录下用户日志，当系统恢复时，可以实现用户的不间断服务。

数据资源的可靠保存和业务应用系统的可靠运行是整个平台的基本要求。

4.5 数据安全

4.5.1 数据库系统安全性

系统要采用高性能的主流数据库产品，同时要注意数据库版本的先进性和可靠性。所采用的数据库系统应符合 SC 认证的 C2 级安全标准，应提供严格的数据库恢复和事务完整性保障机制，提供完整的角色管理和自主控制安全机制，要支持软、硬件容错，逻辑备份与恢复，物理备份与恢复，在线联机备份和恢复等功能，保证在发生故障和灾难后能够很好地恢复或重构数据库。

ORACLE 数据库支持关键数据项的列或表空间加密技术，实现有关敏感数据仅在指定操作界面及授权下可见，导出的备份数据离开系统界面后无法理解和解读，防范系统外部非法入侵以及操作人员的越级操作等安全风险。

数据库的安全性措施主要有以下几方面：

用户标识和鉴定

通过数据库系统的用户账号与口令鉴定用户的身份，这是系统提供的最外层安全保护措施，也是最常用的措施。

存取控制

合理设置数据库对象的授权粒度，认真研究并大力推行角色/权限管理机制，建议使用具有口令保护的角色，通过应用系统级的身份认证连接数据库，通过应用程序进行角色的口令输入、打开角色并激活角色开关，以避免用户绕过应用程序而直接调用 SQL 语句访问数据库资源。

视图机制

为不同用户定义不同的视图，通过视图机制把要保密的数据对无权存取这些数据的用户隐藏起来，从而自动地对数据进行保护。

审计

打开数据库系统的审计功能，以监视不合法行为。

数据的完整性

为保证数据的完整性，在服务器应用层对数据进行检验，对不完整的数据返回异常。同时采用事务，保证数据的一致性。在数据库充通过实体完整性、参照完整性的定义，使数据库系统拒绝接收不合语义的数据，从而保证数据的正确。对一些特别重要的信息应加密存储。

磁盘 RAID

ORACLE 数据库的数据文件存放在 RAID 磁盘上，采取 RAID6 对数据库的数据文件进行保护，才坏掉一块磁盘的情况下数据不会丢失。

群集技术

服务器集群技术，由于现有的所有硬件系统不能达到 100%的不间断运行，而单台服务器不能做容错，所以不具备高的运行安全可靠性，利用服务器集群技术，可以建立一套高可靠系统运行环境。

4.6 数据归档

数据归档是企业如何处理历史数据的问题。一方面不再频繁访问的历史数据占据了大量的存储空间，影响系统的响应时间和性能，无形中增加企业成本。另一方面，这些数据对企业仍具有价值甚至是宝贵资产，同时受法律、法规、规章要求需要企业存储关键数据。由于企业应用场景不同，数据归档策略也不相同。

4.6.1 数据备份管理

数据是一个企业的重要资源，为了很好地保护企业的重要数据，除了做好在线数据的存储管理外，还应该有一个良好的数据备份管理策略。主要包括以下内容：备份类型的选择（全备份、增量备份、差异备份）、备份窗口选择、确定存储介质保存时间、计算所需存储介质数量、备份介质的管理等等。同时注意不要将备份文件放在统一设备上。

4.6.2 灾难恢复策略

灾难恢复是指生产运行中任一环节、任一时刻出现故障而导致整个系统部分或全部不能正常工作时，所必需采用的相应的恢复手段及对生产系统可能造成的损失的评估。必须首先制订良好的备份策略，当灾难发生时才能有条不紊地快速恢复系统。

4.6.3 应用软件备份

应用软件的备份是为了保证在应用系统瘫痪时迅速恢复。应用软件的备份可通过操作系统和内置磁带机设备完成。考虑到应用软件版本更新、升级频繁，各部分程序模块经常会有程度不同的修改，需要保留以前的旧软件版本来保证应用软件的安全性和高可恢复性。

4.6.4 数据安全删除

当数据在其生命周期结束时，或者数据存储介质更换、报修时，企业需要考虑如何安全地删除敏感的或有价值的数据。这是因为计算机数据存储于磁介质（磁盘、磁带）或者电荷式介质（内存、固态硬盘）中，所以通过某些技术如内存冷冻、测定电磁残余等方法可以直接访问数据或者重建“不安全删除”的数据。或者更简单，对通过操作系统删除命令删除的文件，由于其文件的数据块并未被清除，可以使用工具软件轻易恢复被删除的文件。所以删除敏感的或者有价值的数据时，企业可以参考“Gutmann 法”或者“DoD 5520.22-M”安全删除方法，或者使用实现上述方法的工具软件安全地删除数据。对存储介质的销毁处理，除了使用先对介质上数据做安全删除然后再使用有效的物理或化学方法销毁的办法外，可以参考涉密存储介质处理相关办法。

4.7 备份恢复技术安全

4.7.1 存储

根据本项目管理要求，存储需求分为 2 方面内容

1、影像数据：主要有扫描文件，电子附件等文件，存储容量估算依据如下：

按每日最高处理业务单量 10 万的 30%计算，每日大约 3 万笔业务，每笔业务上传影像单据 5 个，每个影像大小预估 250KB，按照 2 年容量预估，需要存储空间 24TB

影像数据需要有效存储大约 24TB

2、NCC 数据库数据：主要存放各种共享服务相关业务数据，存储容量估算依据如下：

按每日最高处理业务单量 10 万的 30%计算，每日大约 3 万笔业务，每单数

据库占用 10K，按照 3 年预估需要 313GB 空间；对接业务系统数据导入容量预留，按与业务单量预估容量相同，需要 3130GB；本地数据库备份预留空间 300GB

4.7.2 备份和恢复机制

应用服务

应用服务器都是采用的集群化设计，保障系统不间断运行，可横向扩展，提供应用服务。

应用服务器可以进行横向扩展，即当发生应用服务器负载过大，导致整个系统的性能下降的情况时，可以再增加新的应用服务器，以分摊负载。

数据归档

数据库大表，效率查询慢等，可以将历史数据归档到单独一个历史表中，这些表的日常业务操作性能提升，查询时，如果不查询历史表的数据时，提升很大等。

4.8 主机安全

主机包括 WEB 服务器、数据库服务器、应用服务器、文件服务器等。操作系统均应达到 SC 认证的 C2 级安全等级。

主机相关安全措施：

4.8.1 主机登录与权限

关闭不必要的系统默认服务；

开启系统自带的日志审计功能；

linux 服务器设定禁止 root 用户远程登录；

linux 服务器修改默认的 Banner 信息；

检查并设置系统的重要配置文件、目录的权限、禁止所有人可以读写；

对服务器采取 IP 地址和 MAC 地址绑定措施，防止地址欺骗。

4.8.2 主机访问控制

依据安全策略控制用户对客体的访问；

自主控制的覆盖范围包括与信息安全直接相关的主体、客体及它们之间的操作；

由授权主体设置用户对系统功能操作和对数据访问的权限；

应用系统的设计采用三层结构，提供数据显示功能与数据处理功能在物理或逻辑上分离。

4.8.3 主机安全加固

选择相对安全的操作系统、中间件和数据库系统，对主机系统进行必要的加固；

限制对主机的访问权，对操作系统用户、中间件系统、数据库系统的用户进行有效管理，禁止缺省口令和弱口令。

4.8.4 主机入侵检测

对主机运行监视，包括监视主机的 CPU、硬盘、内存、网络等资源的使用情况；

设置资源报警阀值，一边在资源使用超过规定数值时发出警报；

进行特定进程监控，限制操作人员进行非法进程；

检测各种已知的入侵行为，记录入侵的源 IP、共计的类型、目的、时间，并在发生严重入侵事件时提供报警；

主机系统根据安全策略阻止某些指定的入侵事件；

检测重要程序完整性受到破坏，并在检测到完整性错误时采取必要的恢复策略。

4.8.5 病毒防范

安装主机防病毒软件，对服务器和桌面终端安装防病毒软件；

配置账户策略：更换管理员账户，杜绝 Guest 账户等

安全配置，关闭不必要的端口，并定期进行版本和病毒库的更新。

4.8.6 主机监控审计

进行主机运行监视，包括监视主机的 CPU、硬盘、内存和网络等资源的使用情况；

对系统的访问授权、操作记录、日志等方面进行有效管理；

严格管理运行过程文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，并确保文档的完整性和一致性；

定期或不定期对保密制度执行情况进行监督检查；

建立安全管理中心，对恶意代码、补丁和审计等进行集中管理。

4.8.7 备份恢复

提供自动备份机制实现数据实时本地备份；

提供恢复数据的功能；

提供重要网络设备、通信线路和服务器的硬件冗余；

资源控制

对最大并发会话连接数进行限制；

对一个时间段内可能的并发会话连接数进行限制；

根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

禁止同一用户账号在同一时间内并发登录；

当系统的服务降低到预先规定的最小值时，应能检测和报警；

根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的处理能力。

4.9 安全认证

ISO 27001

ISO 27001 信息安全管理体系国际认证是被广泛采用的全球安全标准，从数据安全、网络安全、通信安全、操作安全等各个方面证明用友产品履行的安全职责。

C-Star

C-STAR 是一项全新且有针对性的国际专业认证，同时也是全球认可的国内最高级别的云安全认证，将中国国家信息安全标准和云安全联盟的云控制矩阵相融合，是对云服务提供商极为严格的第三方评估。

可信云

获得该认证标志着云服务从服务协议(SLA)标准性、数据存储可靠性、用户数据私密性、业务可用性、功能完备性、运维系统完善性等多方面达到国内顶级云服务评测系统的认证标准。

EAL3+

该标准综合考虑产品的预期应用环境，通过对产品的整个生命周期包括技术，开发、管理，交付等部分进行全面的安全性评估和测试，验证产品的保密性、完整性和可用性程度，确定产品对其预期应用而言是否足够安全。

其他要求

交货日期：硬件产品 30 日内前全部交货，并完成项目施工。

质量承诺以及售后服务：

1、配套装修约15平方标准机房，要求防尘、防水、恒温，防静电。

2、供货时设备包装箱需为全新，可致电厂家 400 电话查询出厂时间，防止供应商用翻新或 OEM 代替。

3、售后服务与培训：

整个工程售后服务三年。每年巡检 6 次，出具巡检报告，并在甲

方处留有易损产品的备品备件。售后服务期满后，超融合软件免费终身升级服务，硬件以成本价进行提供。

施工完成后，组织现场培训不少以两次，调试文档、用户名、密码、工程图纸等材料统一整理进行交接。

4、财务凭证自动制证率≥99%。

5、要对原浪潮账务系统数据初始化，补录入新账务系统（自2021年以后的数据），之前年度数据备查，并可调出供分析使用。