附件 2

工业互联网企业网络安全分类分级防护系列规范

（试行）

2-1 联网工业企业安全防护规范（试行）

目　　录

联网工业企业安全防护规范（试行）

1 联网工业企业安全防护范围及内容

1.1 联网工业企业安全防护范围

联网工业企业安全防护范围，包括联网工业企业应用工业互联网服务的各类信息系统安全及上述信息系统的安全管理。其中，联网工业企业应用工业互联网服务的各类信息系统的防护范围包括与应用互联网服务相关的各类软硬件基础设施、网络、数据、物理环境、工业App等。

1.2 联网工业企业安全防护内容

联网工业企业安全防护内容具体包括：

（1）设备安全防护：包括终端计算机安全、控制设备安全、存储介质安全等。

（2）控制安全防护：包括联网控制系统安全、组态软件安全、工业数据库安全、配置安全、运维安全等。其中，联网控制系统是指应用工业互联网服务的工业控制系统。

（3）网络安全防护：包括组网安全、架构安全、连接安全、网络设备安全、安全设备安全等。

（4）数据安全防护：包括研发域数据、生产域数据、运维域数据、管理域数据、外部域数据、个人信息域数据等。

（5）工业App安全防护：包括安装、卸载、身份认证、口令安全机制、访问控制、实现安全、升级安全、容错性、资源占用安全等。

（6）安全管理要求:包括安全管理制度、安全管理机构和人员、安全建设管理、安全运维管理等。

（7）物理和环境安全防护：包括物理位置选择、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、电磁防护等。

2 联网工业企业安全防护级别的确定

联网工业企业按照《工业互联网企业网络安全分类分级管理指南（试行）》的级别划分，采取不同程度的安全防护。联网工业企业的安全防护分为基本级防护和增强级防护两个级别：

三级联网工业企业建议采取增强级防护措施。

二级联网工业企业建议采取基本级防护措施。

一级联网工业企业参照基本级防护要求根据自身情况，自主落实安全防护措施。

3 联网工业企业安全防护要求

3.1 基本级防护要求

3.1.1 设备安全防护要求

3.1.1.1 终端计算机安全防护要求

a) 应规范软硬件使用，不应擅自更改软硬件配置，不应擅自安装软件；

b) 应加强账户及口令管理，使用具有一定强度的口令并定期更换；

c) 应关闭不必要的端口，停用不必要的服务；

d) 应安装恶意代码防护工具，及时对恶意代码库进行更新升级；

e) 应及时对服务器进行系统和补丁的离线更新升级；

f) 不应进行单台设备跨网使用（如一台终端计算机具有不同域的多个网卡）。

3.1.1.2 控制设备安全防护要求

a) 应加强账户及口令管理，合理分类设置账户权限，使用具有一定强度的口令并定期更换；
b) 应做好设备基本的安全策略配置（如口令策略合规性等），确保相关安全配置的有效性；
c) 应规范相关软硬件使用，不应擅自更改软硬件配置，不应擅自安装软件；
d) 应关闭不必要的端口，停用不必要的服务；
e) 建立安全策略配置清单，确保该清单满足控制设备安全可靠运行的需要。

3.1.1.3 存储介质安全防护要求

a) 应建立并严格执行存储介质安全管理制度；
b) 应建立相关资产台账（清单），对存储介质进行分类、分级标识；
c) 应对移动存储介质进行集中统一管理，记录介质领用、交回、维修、报废、销毁等情况。

3.1.2 控制安全防护要求

3.1.2.1 联网控制系统安全防护要求

a) 应建立联网控制系统防病毒和恶意软件入侵管理机制，确保该管理机制可有效规范防病毒和恶意软件入侵管理工作；
b) 应定期针对联网控制系统及临时接入的设备开展查杀，并留存详细查杀记录；
c) 应确保联网控制系统相关安全配置的有效性；
d) 应建立联网控制系统安全策略配置清单，确保该清单满足企业联网控制系统安全可靠运行的需要；
e) 禁止联网控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务；
f) 应保留联网控制系统相关访问日志（包括人员账户、访问时间、操作\内容等），并定期进行备份，以确保安全审计的有效开展；
g) 应建立联网控制系统资产清单（包括软件资产、硬件资产、数据资产等），确保联网控制系统资产信息可查、可追溯。

3.1.2.2 组态软件安全防护要求

a) 应为组态软件的登录账户设定足够强度的登录密码，并妥善管理，避免使用默认口令和弱口令，以降低对设备未授权登录和操作的可能性。定期更新口令；
b) 应跟踪组态软件的安全风险，及时更新最新补丁；
c) 应删除组态软件自带的非必要系统账户。

3.1.2.3 工业数据库安全防护要求

a) 应加强数据库账户及口令管理，使用具有一定强度的口令并定期更换；
b) 应关闭不必要的端口，停用不必要的服务；
c) 应定期对数据库存储数据进行备份。

3.1.2.4 配置安全要求

a) 应建立控制服务器等联网控制系统关键设备安全配置和审计制度，联网控制系统应提供为以下类别生成审计记录的能力：访问控制、请求错误、系统事件、备份和存储事件、配置变更、潜在侦查行为和审计日志事件，联网控制系统应提供时间戳用于生成审计记录；
b) 应严格账户管理，根据工作需要合理分类设置账户权限；
c) 应严格口令管理，及时更改产品安装时的预设口令，杜绝弱口令、空口令，应为所有用户提供实施口令的最小和最大有效期限制；

d) 应定期对账户、口令、端口、服务等进行检查，及时清理不必要的用户和管理员账户，停止无用的后台程序和进程，关闭无关的端口和服务，联网控制系统应具备对多次登录失败的账户进行锁定的功能。

3.1.2.5 运维安全要求

a) 应慎重选择运维服务商，在供货合同中或以其他方式明确供应商应承担的网络安全责任和义务，确保产品安全可控；

b) 应加强对技术服务的网络安全管理，在安全得不到保证的情况下禁止采取远程在线服务；

c) 应密切关注产品漏洞和补丁发布，严格软件升级、补丁安装管理，严防病毒、木马等恶意代码侵入，在联网控制系统软件升级、补丁安装前要请专业技术机构进行安全评估和验证。

3.1.3 网络安全防护要求

3.1.3.1 组网安全要求

a) 应根据承载业务的重要性对网络进行分区分域管理；

b) 应避免将重要网段部署在网络边界处；

c) 联网控制系统组网时要同步规划、同步建设、同步运行安全防护措施；

d) 应对非涉密信息系统与互联网及其他公共信息网络进行逻辑隔离。

3.1.3.2 架构安全要求

在纵深防御要求包括但不限于：

a) 联网控制系统网络拓扑结构应采用纵深防御思想进行概念设计，应将全网划分为不同的安全网络层级，例如包括企业管理层、制造执行层（MES）、集中监控层、过程控制层和现场设备层。

在网络边界划分要求包括但不限于：

a) 在网络边界定义方面，系统应定义明确的安全边界；

b) 在双重网络接口卡（NIC）使用方面，应严禁开启双重网络接口卡。

c) 在链路冗余要求包括但不限于：

d) 在网络带宽冗余方面，联网控制系统的网络带宽设计指标应大于网络带宽需求指标，网络带宽的大小应满足异常生产工况、突发业务需求、最大业务处理对联网控制系统网络带宽的实际要求。

在系统容错要求包括但不限于：

a) 在电源供应方面，联网控制系统应在不影响现有安全状态条件下实现与紧急电源之间的切换。

在网络安全架构要求包括但不限于：

a) 企业应对网络安全架构的开发和修改进行风险评估，在对联网控制系统的网络架构环境进行开发和修改时应考虑到这些修改潜在的安全影响。

3.1.3.3 连接安全要求

a) 应采取必要的技术措施对不同安全域之间实施访问控制；

b) 应建立互联网接入审批和登记制度，严格控制互联网接入口数量，加强互联网接入口安全管理和安全防护。

3.1.3.4 网络设备安全防护要求

a) 应采取访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范等措施，进行网络边界防护；

b) 应对网络监控日志进行管理，定期审计分析，发现安全风险或问题，及时进行处理；

c) 应对网络设备采取登录失败处理措施，如：结束会话、限制失败登录次数、当网络

登录连接超时自动退出等；

d) 应对网络设备的远程管理采取必要的安全措施，防止鉴别信息在传输过程中被窃取；

e) 不应在网络设备上使用弱口令、调试账号；

f) 应对网络设备日志进行管理，定期审计分析，发现安全风险或问题，及时进行处理。

3.1.3.5 安全设备安全防护要求

a) 应采取必要的技术措施，合理部署安全设备，对不同网络分区进行合理防护，应采用经国家相关部门认证的安全设备；

b) 应对安全设备采取登录失败处理措施，如：结束会话、限制失败登录次数、当登录连接超时自动退出等；

c) 应对安全设备的远程管理采取必要的安全措施，防止鉴别信息在传输过程中被窃取；

d) 不应在安全设备上使用弱口令、调试账号；

e) 应对安全设备日志进行管理，定期审计分析，发现安全风险或问题，及时进行处理。

3.1.4 数据安全防护要求

应按照《工业互联网企业数据安全防护规范（试行）》对联网工业企业所使用的数据进行分类分级，依据分级要求采取对应的数据安全防护措施。

3.1.5 工业 App 安全防护要求

应按照《工业互联网平台企业安全防护规范（试行）》中的工业 App 安全防护要求，结合联网工业企业的实际情况（去除不适用项），对联网工业企业所应用的工业 App 采取对应的安全防护措施。

3.1.6 网络安全管理要求

3.1.6.1 安全管理制度

a) 应对安全管理活动中重要的管理内容建立安全管理制度；

b) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

c) 应指定或授权专门的部门或人员负责安全管理制度的制定；

d) 安全管理制度应通过正式、有效的方式发布，并进行版本控制；

e) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

3.1.6.2 安全管理机构和人员要求

安全管理机构要求包括但不限于：

a) 应明确指定一个机构，具体承担网络安全管理工作，组织制定和落实网络安全管理制度，实施网络安全技术防护措施，开展网络安全宣传教育培训，执行网络安全监督检查等；

b) 应设立安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义部门及各负责人的职责；

c) 应设立系统管理员、网络管理员、安全管理员等岗位，配备一定数量的系统管理员、网络管理员、安全管理员等，并定义各个工作岗位的职责；

d) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

e) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；

f) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等。

人员要求包括但不限于：

a) 应加强各类管理人员之间、组织内部机构之间以及安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理安全问题；
b) 应加强与工业互联网安全主管部门、各类供应商、业界专家及的合作与沟通；
c) 应指定或授权专门的部门或人员负责人员录用；
d) 应对被录用人员的身份、背景、专业资格和资质等进行审查；
e) 应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
f) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
g) 应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
h) 外部人员离场后应及时清除其所有的访问权限。

3.1.6.3 安全建设管理要求

定级要求包括但不限于：

a) 应明确本企业的安全等级；
b) 应以书面形式说明企业确定为某安全等级的方法和理由。

安全方案设计要求包括但不限于：

a) 应根据安全防护对象的安全防护需求进行安全方案设计；
b) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用要求包括但不限于：

a) 工业控制系统、工业互联网平台或标识解析系统的重要设备及专用安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；
b) 应确保安全产品与服务的采购和使用符合国家的有关规定。

软件开发要求包括但不限于：

a) 应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
b) 应在软件开发过程中进行安全性测试；
c) 应在软件交付前检测其中可能存在的缺陷与恶意代码等；
a) 应要求开发单位提供软件设计文档和使用指南；
b) 应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

系统交付要求包括但不限于：

a) 应制订安全性测试验收方案，并依据测试验收方案实施验收，形成验收报告；
b) 应根据交付清单对所交接的设备、软件和文档等进行清点；
c) 应对负责运行维护的技术人员进行相应的技能培训；
d) 应提供建设过程中的文档和指导用户进行运行维护的文档。

服务供应商选择要求包括但不限于：

a) 应选择安全合规的设备、服务、工业互联网平台或标识解析系统供应商，其所提供的设备、平台系统等应为其所承载的业务提供相应的安全防护能力；
b) 应在服务协议中规定具体服务内容和技术指标；
c) 应在服务协议中规定供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
d) 应与选定的服务供应商签订相关协议，明确供应链各方需履行的安全相关义务；

e) 应在服务协议中规定服务合约到期时，完整地返还客户信息，并承诺相关信息均已在云计算平台、工业互联网平台或标识解析系统上清除；
f) 应确保供应链安全事件信息或威胁信息能够及时传达到客户；
g) 应确保外包运维服务商的选择符合国家的有关规定；
h) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

3.1.6.4 安全运维管理要求

环境管理要求包括但不限于：

a) 应对机房的安全管理做出规定，指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
b) 应不在重要区域接待来访人员。

资产管理要求包括但不限于：

a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
d) 应对各种设备（包括备份和冗余设备）、线路等定期进行维护管理；
e) 应记录工业互联网设备的状态（包括外观、电量、指示灯等信息），对工业互联网设备进行现场维护（除尘、充电、修理等）；
f) 应对工业互联网设备部署环境的评估方法作出明确规定；
g) 应对工业互联网设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
h) 应采用国家密码管理主管部门批准使用的密码算法和认证核准的密码产品；
i) 应明确资产变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

安全审计要求包括但不限于：

a) 应对重要设备、平台、系统等启用安全审计功能，对重要的用户行为和重要安全事件进行审计；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；
b) 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；审计记录中应避免明文记录敏感数据，如用户口令等；
c) 应确保审计记录的留存时间符合法律法规要求。

配置管理要求包括但不限于：

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

安全事件处置要求包括但不限于：

a) 应及时向工业互联网安全主管部门报告所发现的安全弱点和可疑事件；
b) 应明确安全事件的报告和处置流程，制定安全事件报告和处置管理制度；
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

应急要求包括但不限于：

a) 应制定网络安全事件应急预案，包括应急处理流程、系统恢复流程等内容，并根据实际情况适时进行评估和修订，原则上每年进行一次评估和修订；

b) 应定期开展网络安全事件应急预案宣贯培训，确保相关人员熟悉应急预案，并进行应急预案的演练。

3.1.7 物理和环境安全要求

1.1 3.1.7.1 物理位置选择

a) 机房场地及常规工业设备放置场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；

c) 室外工业互联网重要设备及控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中。

1.2 3.1.7.2 物理访问控制

a) 机房场地及工业设备放置场地出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；

b) 重要服务器、数据库、工程师站等核心工业互联网软硬件所在区域或工业互联网平台宜采取视频监控等手段。

1.3 3.1.7.3 防盗窃和防破坏

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b) 应将通信线缆铺设在隐蔽安全处，可铺设在地下或管道中；

c) 主机房或重要设备区域应安装比亚的防盗报警设置。

1.4 3.1.7.4 防雷击

a) 应将各类机柜、设施和设备等通过接地系统安全接地。

1.5 3.1.7.5 防火

a) 机房及工业设备放置场地应设置灭火设备和火灾自动报警系统。

1.6 3.1.7.6 防水和防潮

a) 应采取措施防止雨水通过机房或场地窗户、屋顶和墙壁渗透；

b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

1.7 3.1.7.7 防静电

应满足 YD/T 1754-2008 中 3.2.7 的相关要求。

1.8 3.1.7.8 温湿度控制

应满足 YD/T 1754-2008 中 3.2.8 的相关要求。

1.9 3.1.7.9 电力供应

应满足 YD/T 1754-2008 中 3.2.10 的相关要求。

1.10 3.1.7.10 电磁防护

a) 应满足 YD/T 1754-2008 中 3.2.11 的相关要求；

b) 室外工业互联网重要设备及控制设备放置应远离强电磁干扰、强热源等环境，如无法避免，应及时做好应急处置及检修保证设备正常运行。

3.2 增强级防护要求

3.2.1 设备安全防护要求

1.11 3.2.1.1 终端计算机安全防护要求

a) 应采用集中统一管理方式对终端计算机进行管理，统一软件下发，统一安装系统补丁，统一实施病毒库升级和病毒查杀，统一进行漏洞扫描；

b) 应对接入互联网的终端计算机采取控制措施，包括实名接入认证、IP 地址与 MAC 地址绑定等；

c) 应定期对终端计算机进行安全审计，并及时对发现的问题进行处置；

d) 不应用非涉密计算机存储和处理国家秘密信息。

3.2.1.2 控制设备安全防护要求

a) 根据自身情况，明确重要控制设备清单，并根据实际需要部署深度报分析和经过检测的安全设备；

b) 应对接入互联网的控制设备采取控制措施，包括实名接入认证、IP 地址与 MAC 地址绑定等；

c) 定期对控制设备安全配置进行核查审计，避免因调试或其它操作导致配置变更后，未及时更新配置清单。

3.2.1.3 存储介质安全防护要求

a) 应配备必要的电子信息消除和介质销毁设备，对变更用途的存储介质进行信息清除，对废弃的存储介质进行销毁；

b) 应严格存储阵列、磁带库等大容量存储介质的管理，采取技术措施防范外联风险，确保存储数据安全；

c) 不应在非涉密移动存储介质上存储涉及国家秘密的信息，不应在非涉密计算机上使用涉密移动存储介质；

d) 应在将移动存储介质接入本部门计算机和信息系统前，进行病毒、木马等恶意代码查杀。

3.2.2 控制安全防护要求

3.2.2.1 联网控制系统安全防护要求

a) 应定期自行对联网控制系统安全配置进行核查审计，避免因调试或其它操作导致配置变更后，未及时更新配置清单；

b) 应针对联网控制系统的开发、测试和生产分别提供独立环境，避免开发、测试环境中的安全风险引入生产系统；

c) 应部署具备对联网控制系统与网络进行状态监测、日志采集与事件管理、流量采集与行为分析、异常告警及关联分析等功能的网络安全监测设备，及时发现、报告并处理包括设备状态异常、恶意软件传播、异常流量、异常诊断日志、端口扫描、暴力破解等网络攻击或异常行为。

3.2.2.2 组态软件安全防护要求

同 3.1.2.2 基本级防护要求。

3.2.2.3 工业数据库安全防护要求

a) 应对服务器日志进行管理，定期审计分析，发现安全风险或问题，及时进行处理；

b) 应做好数据加密，使用协议加密，确保数据传输安全。

3.2.2.4 配置安全要求

a) 应具备恶意代码防护、服务器口令、服务器安全审计、服务器补丁更新、网络设备和安全设备口令、终端计算机接入控制及统一防护方面的策略。

3.2.2.5 运维安全要求

a) 在不影响正常生产运行情况下，联网控制系统应能支持识别和定位关键文件、并有能力执行用户级和系统级备份（包含系统状态信息），联网控制系统应提供可配置频率的自动实现上述功能的能力。

3.2.3 网络安全防护要求

3.2.3.1 组网安全要求

a) 应采取虚拟专用网络（VPN）、线路冗余备份、数据加密等措施，加强对联网控制系统远程通信的保护；

b) 应对无线组网采取严格的身份认证、安全监测等防护措施，防止经无线网络进行恶意入侵，尤其要防止通过侵入远程终端单元（RTU）进而控制部分或整个联网控制系统，对参与无线通信的所有的用户（人、软件进程或设备）、联网控制系统提供标识和认证的能力，对联网控制系统的无线连接应依据普遍接受的安全工业实践进行授权、监视和限制。

3.2.3.2 架构安全要求

纵深防御要求包括但不限于：

a) 在不同网络层级之间安全防护方面，系统各个层级之间应部署访问控制设备、入侵检测与防护设备、安全隔离设备以及安全审计设备；

b) 在横向分区方面，联网控制系统不同横向分区应依据安全性需求的不同而设置不同安全等级，并根据相应的安全等级采取不同的安全防护措施。

链路冗余要求包括但不限于：

a) 在网络组件冗余方面，联网控制系统的核心网及骨干网应建设冗余链路，确认冗余链路采用不同的网络方式构建，电力供应、现场控制站、工程师服务器、历史数据库服务器、实时数据库服务器、HMI 服务器、核心交换机等应进行硬件冗余；

b) 在网络故障诊断与恢复方面，当网络故障时系统切换到另一路通信网络的时间应满足实际需求，当网络故障时可保证业务不中断继续运行，数据不丢失。

系统容错要求包括但不限于：

a) 在关键软件容错方面，联网控制系统的历史数据库、实时数据库、组态软件、监控软件等应采取容错措施。

自主可靠要求包括但不限于：

a) 确认控制器、组态软件、数据库、监控软件、核心交换机、重要服务器等联网控制系统关键设备，或安全仪表系统、紧急停车系统、安全防护系统等联网控制系统采用国产设备，或经检测无安全漏洞的国外设备，联网控制系统运营单位应具备对联网控制系统的二次开发能力，并具备自主开展联网控制系统漏洞防护的能力。

3.2.3.3 连接安全要求

a) 对确实需要的连接，系统运营单位要逐一进行登记，采取设置防火墙、单向隔离等措施加以防护，并定期进行安全风险评估，不断完善防范措施；

b) 入侵检测设备和入侵防御设备应定期更新检测规则库，设备在部署前应先进行检测，设备的部署须不影响联网控制系统的正常运行，访问控制设备应阻断非授权访问，安全审计设备应对网络访问情况进行分析审计并保护审计记录。

3.2.3.4 网络设备安全防护要求

a) 应实现设备的最小服务配置，并对配置文件进行定期离线备份；

b) 应及时对网络设备进行系统更新升级和打补丁，并提前对重要文件进行备份；

c) 应定期对网络设备系统进行漏洞扫描，对发现的安全漏洞进行及时处理。

3.2.3.5 安全设备安全防护要求

a) 应实现安全设备的最小服务配置，并对配置文件进行定期离线备份；

b) 应及时对安全设备进行系统、恶意代码库和补丁更新升级，并提前对重要文件进行必要的备份；

c) 应定期对安全设备系统进行恶意代码检查和漏洞扫描，对发现的恶意代码和安全漏洞进行及时处理。

3.2.4 数据安全防护要求

同 3.1.4 基本级防护要求。

3.2.5 工业 App 安全防护要求

同 3.1.5 基本级防护要求。

3.2.6 网络安全管理要求

1.12 3.2.6.1 安全管理制度

除包括 3.1.6.1 基本级防护要求之外，还应包括但不限于：

a) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

1.13 3.2.6.2 安全管理机构和人员要求

除包括 3.1.6.2 基本级防护要求之外，还应包括但不限于：

安全管理机构要求包括但不限于：

同 3.1.6.2 基本级防护要求。

人员要求包括但不限于：

a) 应成立指导和管理安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
b) 应配备专职安全管理员，不可兼任，关键事务岗位应配备多人共同管理；
c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
d) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
e) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
f) 应从内部人员中选拔从事关键岗位的人员；
g) 应对被录用人员所具有的技术技能进行考核，应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
h) 人员离岗时，应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
i) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，应定期对不同岗位的人员进行技能考核；
j) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；对关键区域或关键系统不允许外部人员访问。

1.14 3.2.6.3 安全建设管理要求

除包括 3.1.6.3 基本级防护要求之外，还应包括但不限于：

定级要求包括但不限于：

同 3.1.6.3 基本级防护要求。

安全方案设计要求包括但不限于：

a) 应根据安全防护对象的安全防护需求及与其他防护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
b) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用要求包括但不限于：

a) 应预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；
b) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

软件开发要求包括但不限于：

a) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
b) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
c) 应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；

d) 应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
e) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；
f) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

系统交付要求包括但不限于：

安全测试报告应包含密码应用安全性测试相关内容。

服务供应商选择要求包括但不限于：

a) 应定期评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；
b) 应与选定的服务供应商签署保密协议，要求其不得泄露客户数据和业务系统的相关重要信息；
c) 应保证供应商的重要变更及时传达到客户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

1.15 3.2.6.4 安全运维管理要求

除包括 3.1.6.4 基本级防护要求之外，还应包括但不限于：

环境管理要求包括但不限于：

a) 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等；
b) 应加强对工业互联网设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

资产管理要求包括但不限于：

a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
b) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；
c) 应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；
d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；
e) 应建立资产变更的申报和审批程序，依据程序控制所有的变更，记录变更实施过程；
f) 应建立中止资产变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

安全审计要求包括但不限于：

a) 应能对远程访问企业内部网络的用户行为进行行为审计和数据分析；
b) 应对审计进程进行保护，防止未经授权的中断；
c) 审计记录的留存时间应不少于 6 个月。

配置管理要求包括但不限于：

a) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

安全事件处置要求包括但不限于：

a) 对造成业务中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

应急要求包括但不限于：

a) 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
b) 应定期开展网络安全应急演练，检验应急预案的可操作性，并结合应急演练结果，

对应急预案进行评估和适用性修订；

c) 应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。

3.2.7 物理和环境安全要求

1.16 3.2.7.1 物理位置选择

同 3.1.7.1 基本级防护要求。

1.17 3.2.7.2 物理访问控制

除包括 3.1.7.2 基本级防护要求之外，还应包括但不限于：

a) 拆除或封闭工业主机上不必要的 USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

1.18 3.2.7.3 防盗窃和防破坏

除包括 3.1.7.3 基本级防护要求之外，还应包括但不限于：

a) 应对机房设置监控报警系统。

1.19 3.2.7.4 防雷击

同 3.1.7.4 基本级防护要求。

1.20 3.2.7.5 防火

a) 机房及工业设备放置场地应设置灭火设备和火灾自动报警系统，能够自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

1.21 3.2.7.6 防水和防潮

除包括 3.1.7.3 基本级防护要求之外，还应包括但不限于：

a) 应安装对水敏感的检测仪表或元件，对机房及工业设备放置场地进行防水检测。

1.22 3.2.7.7 防静电

应满足 YD/T 1754-2008 中 3.3.7 的相关要求。

1.23 3.2.7.8 温湿度控制

同 3.1.7.8 基本级防护要求

1.24 3.2.7.9 电力供应

应满足 YD/T 1754-2008 中 3.3.10 的相关要求。

1.25 3.2.7.10 电磁防护

同 3.1.7.10 基本级防护要求。

2-2 工业互联网平台企业安全防护规范（试行）

目　　录

工业互联网平台企业安全防护规范（试行）

1 工业互联网平台企业安全防护范围及内容

1.1 工业互联网平台企业安全防护范围

工业互联网平台企业安全防护范围，包括企业对外提供服务的工业互联网平台安全。其中，工业互联网平台安全防护范围，包括工业互联网平台的接入层安全、基础设施层安全、平台层安全、应用层安全等。

1.2 工业互联网平台企业安全防护内容

工业互联网平台企业安全防护内容具体包括：

（1）接入层安全防护：包括网络架构安全、传输保护、边界防护、访问控制、入侵防范、安全审计、安全基线检查等。

（2）基础设施层安全防护：包括服务器安全、存储安全、网络安全、虚拟化安全等。

（3）平台层安全防护：包括数据分析服务安全、微服务组件安全、平台应用开发环境安全等。

（4）应用层安全防护：包括面向各类工业应用场景的业务应用安全等。

（5）数据安全防护：包括工业互联网平台相关数据全生命周期安全等。

（6）安全管理要求：包括安全管理制度要求、安全管理机构和人员要求、安全建设和管理要求、安全运维管理要求等。

（7）物理和环境安全要求：包括物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、电磁防护等。

2 工业互联网平台企业安全防护级别的确定

工业互联网平台企业按照《工业互联网企业网络安全分类分级管理指南（试行）》的级别划分，采取不同程度的安全防护。工业互联网平台企业的安全防护分为基本级防护和增强级防护两个级别：

三级工业互联网平台企业建议采取增强级防护措施。

二级工业互联网平台企业建议采取基本级防护措施。

一级工业互联网平台企业参照基本级防护要求根据自身情况，自主落实安全防护措施。

3 工业互联网平台企业安全防护要求

3.1 基本级防护要求

3.1.1 接入层安全防护要求

3.1.1.1 网络架构

网络架构要求包括但不限于：

a) 应设置单独的接入安全区域，并分配已规划的地址空间。

3.1.1.2 传输保护

传输保护要求包括但不限于：

a) 应保证通信过程中的数据完整性；

b) 应保证通信过程中的关键信息的保密性。

3.1.1.3 边界防护

边界防护要求包括但不限于：

a) 工厂内部网络与工厂外部网络的边界应该具有隔离措施；

b) 应采用鉴别机制对接入工业互联网平台中的设备身份进行鉴别，确保数据来源于真实的设备；
c) 能够对非授权设备的接入行为进行告警。

3.1.1.4 访问控制

访问控制要求包括但不限于：

a) 接入网络边界网关只开放接入服务相关的端口；
b) 应在网络边界根据访问控制策略设置访问控制规则，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目最小化；
c) 边界安全网关通过 ACL 检测机制对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据进出；
d) 应通过制定安全策略如访问控制列表，实现对接入工业互联网中设备的访问控制。

3.1.1.5 入侵防范

入侵防范要求包括但不限于：

a) 能够检测到信令风暴等在终端设备接入平台过程中出现的海量信令认证问题；
b) 能够检测接入设备发起的 DDoS 等网络攻击行为；
c) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应能够告警。

3.1.1.6 安全审计

安全审计要求包括但不限于：

a) 应对接入用户的重要安全事件和重要行为进行审计；
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) 审计日志应至少保存六个月。

3.1.1.7 安全基线检查

安全基线检查要求包括但不限于：

a) 应对接入层基础设施和平台计算环境进行安全基线制定；

3.1.2 基础设施层安全防护要求

3.1.2.1 服务器安全防护要求

身份鉴别认证要求包括但不限于：

a) 应对登录服务器的用户进行身份标识和鉴别；
b) 服务器管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
c) 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施；
d) 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用。

访问控制要求包括但不限于：

a) 应采用技术措施对允许访问服务器的终端地址范围进行限制；
b) 应关闭服务器不使用的端口，防止非法访问；
c) 应基于白名单机制检测非法运行的进程或程序；
d) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

安全审计要求包括但不限于：

a) 审计范围应覆盖到服务器上的每个用户；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件；
c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
d) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
e) 审计记录留存时间不少于 6 个月。

资源控制要求包括但不限于：

a) 应根据安全策略，设置登录终端的会话数量；
b) 应根据安全策略设置登录终端的操作超时锁定。

恶意代码防范要求包括但不限于：

a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

入侵防范要求包括但不限于：

a) 所使用的操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新；
b) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
c) 应支持对数据库攻击行为进行检测和防护。

3.1.2.2 网络安全防护要求

网络拓扑结构要求包括但不限于：

a) 应绘制与当前运行情况相符的网络拓扑结构图；
b) 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
c) 应保证接入网络和核心网络的带宽满足业务高峰期需要；
d) 应根据平台服务的类型、功能及租户的不同划分不同的子网、网段或安全组。

访问控制要求包括但不限于：

a) 应在（子）网络或网段边界部署访问控制设备并启用访问控制功能，或通过安全组设置访问控制策略；
b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力。

安全审计要求包括但不限于：

a) 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行日志记录；
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) 应保证所有网络设备的系统时间自动保持一致；
d) 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

恶意代码防范要求包括但不限于：

a) 应对恶意代码进行检测和清除。

网络设备防护要求包括但不限于：

a) 应对登录网络设备的用户进行身份鉴别；
b) 应对网络设备的管理员登录地址进行限制；
c) 网络设备用户的标识应唯一；
d) 身份鉴别信息应具有复杂度要求并定期更换。

网络安全监测要求包括但不限于：

a) 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行监测，识别和记录异常状态；
b) 应根据用户需求支持对持续大流量攻击进行识别、报警和阻断的能力；

c) 应监视是否对平台服务存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

3.1.2.3 虚拟化安全防护要求

虚拟机安全要求包括但不限于：

a) 应支持虚拟机之间、虚拟机与宿主机之间的隔离；
b) 应支持虚拟机部署防病毒软件；
c) 应具有对虚拟机恶意攻击等行为的识别并处置的能力；
d) 应支持对虚拟机脆弱性进行检测的能力；
e) 应支持虚拟机的安全启动。

虚拟机网络安全要求包括但不限于：

a) 应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机与外部网络之间的安全访问控制；
b) 应支持采用 VLAN 或者分布式虚拟交换机等技术，以实现网络的安全隔离；
c) 应采用 VxLAN、GRE 等手段支持不同租户之间的网络流量隔离；
d) 应支持东西向网络引流、网络安全编排、网络流量可视化。

虚拟化平台安全要求包括但不限于：

a) 应保证每个虚拟机能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机；
b) 应保证不同虚拟机之间的虚拟 CPU 指令隔离；
c) 应保证不同虚拟机之间的内存隔离，内存被释放或再分配给其他虚拟机前得到完全释放；
d) 应保证虚拟机只能访问分配给该虚拟机的存储空间（包括内存空间和磁盘空间）；
e) 应对虚拟机的运行状态、资源占用等信息进行监控；
f) 应支持发现虚拟化平台漏洞的能力，支持漏洞修复；
g) 应支持平台内采用的 PKI、SSL 认证等各类数字证书的统一管理，支持用户按需更换。

容器安全要求包括但不限于：

a) 定期开展容器镜像的安全性检查（包括镜像内部的程序、lib 和配置可能存在的缺陷等）；
b) 对容器镜像进行完整性校验，定期使用镜像扫描工具扫描镜像。

3.1.3 平台层安全防护要求

3.1.3.1 数据分析服务安全防护要求

数据挖掘要求包括但不限于：

a) 针对不同接入方式的数据挖掘用户，应采用不同的认证方式。需要检查使用数据的合法性和有效性；
b) 挖掘算法在使用前，必须申报算法使用的数据范围、挖掘周期、挖掘目的、以及挖掘结果的应用范围等内容。算法提供者必须对算法的安全性和可靠性提供必要的验证与测试方案；
c) 在数据挖掘过程中，应对挖掘算法使用的数据范围、数据状态、数据格式、数据内容等进行监控；
d) 禁止挖掘算法对数据存储区域内的原始数据进行增加、修改、删除等操作，以保证

原始数据的可用性和完整性；

e) 禁止将挖掘算法产生的中间过程数据与原始数据存储于同一空间，以防数据使用的混乱、加大数据存储的管理难度。同时，应周期性的检查用户操作数据的情况，统一管理数据使用权限；

f) 不同应用之间应进行数据关联性隔离，防止不同应用之间的 ECA 分析，产生数据泄露；

g) 应对挖掘内容、过程、结果、用户进行安全审计。主要包括挖掘内容的合理性、挖掘过程的合规性、挖掘结果的可用性，以及挖掘用户的安全性；

h) 应对源数据和挖掘结果进行签识，防止数据被恶意删除、随意篡改、无约束的滥用；

i) 如需将收集到的信息共享给第三方应用，应对信息进行脱敏处理，严格保护用户隐私不被泄露。

数据共享要求包括但不限于：

a) 数据共享要求按照《工业互联网企业数据安全防护规范（试行）》中数据共享要求。

3.1.3.2 微服务组件安全防护要求

身份鉴别要求包括但不限于：

a) 应对管理微服务组件的用户进行身份标识和鉴别；

b) 管理微服务组件的用户身份标识应具有唯一性，口令应有复杂度要求并定期更换；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用。

访问控制要求包括但不限于：

a) 在微服务组件权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

安全审计要求包括但不限于：

a) 审计范围应覆盖到使用微服务组件的每个用户；

b) 审计内容应包括重要用户行为、微服务组件资源的异常使用和重要操作命令的使用等重要的安全相关事件；

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

e) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

开放接口要求包括但不限于：

a) 微服务组件应有与外部组件或应用之间开放接口的安全管控措施，如对接口调用行为进行审计、通过黑/白名单等措施进行访问控制等；

b) 应对开放接口调用有认证措施；

c) 应对关键接口的调用情况进行技术监控，如调用频率、调用来源等；

d) 应制定开放接口管理机制和网络安全应急管理制度。

3.1.3.3 平台应用开发环境安全防护要求

身份鉴别要求包括但不限于：

a) 对保留用户个人信息或用户服务信息的业务，应对登录用户进行身份标识和鉴别；

b) 对要求提供登录功能的开发环境，应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

c) 对要求提供登录功能的开发环境，应提供并启用用户身份标识唯一检查功能，保证开发环境中不存在重复用户身份标识。应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用；

d) 应采用加密方式存储用户的账号和口令信息。

访问控制要求包括但不限于：

a) 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限；
b) 应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

安全审计要求包括但不限于：

a) 审计范围应覆盖到每个用户的关键操作；
b) 审计内容应包括对用户的重要行为、资源使用情况等重要事件；
c) 应保护审计记录，保证无法删除、修改或覆盖等；
d) 相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等，并且保留一定期限(至少 6 个月)。

资源控制要求包括但不限于：

a) 当用户和开发环境的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

信息保护要求包括但不限于：

a) 开发环境中各功能的提供、控制与管理过程应保护用户隐私，未经用户同意，不能擅自收集、修改、泄漏用户相关敏感信息；
b) 应保护相关信息的安全，避免相关数据和页面被篡改和破坏；
c) 应禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件；
d) 应对通信过程中的敏感信息字段进行加密；
e) 应对敏感信息(如用户信息、订单信息、应用软件下载路径等)进行加密存储；
f) 应对开发环境相关功能的关键数据(如业务数据、系统配置数据、管理员操作维护记录、用户信息、业务应用与 App 购买、下载信息等)应有必要的容灾备份；
g) 应能对诈骗、虚假广告等信息建立处理机制，防止类似信息的扩散。

上线前检测要求包括但不限于：

a) 开发环境应在业务应用与工业 App 上线前对其进行安全审核，以确保其不包含恶意代码、恶意行为等，经过安全审核后才能进行上线处理、正式发布；
b) 开发环境可提供用户数据同步功能，但开发环境同步的用户数据不应保存在位于境外的服务器上；
c) 开发环境应支持对工业 App 的移动代码签名机制，对 App 检测审核后，对 App 进行数字签名；移动终端在下载安装 App 之前，对经过签名的 App 进行签名验证，只有通过签名验证的 App 才能被认为是可信的，继而被安装到终端上；
d) 开发环境应对已经上线的业务应用与工业 App 进行拨测抽查，并记录拨测过程及结果，针对违规行为、可疑行为等进行相应的处理。业务应用与工业 App 拨测应采用自动拨测与人工拨测相结合的方式进行；
e) 开发环境应要求开发者在提交业务应用与工业 App 时声明其调用的 API，并对业务应用与工业 App 调用终端 API 的行为进行检测。业务应用与工业 App 不应调用与其业务功能无关的 API 以及在其声明范围之外的 API。

3.1.4 应用层安全防护要求

3.1.4.1 平台业务应用安全防护要求

身份鉴别要求包括但不限于：

a) 应采用两种或两种以上组合的鉴别技术来进行身份鉴别，，身份鉴别信息需要有一定的复杂度并定期更换；
b) 登录过程应提供并启用登陆失败处理功，多次登陆失败后应采取必要的保护措施。

访问控制要求包括但不限于：

a) 应严格限制用户的访问权限，按安全策略要求控制用户对业务应用的访问；
b) 应严格限制应用与应用之间相互调用的权限，按照安全策略要求控制应用对其他应用里用户数据或特权指令等资源的调用。

安全审计要求包括但不限于：

a) 审计范围应覆盖到用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
b) 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
c) 应定期针对审计日志进行人工审计；
d) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

资源控制要求包括但不限于：

a) 应限制对应用访问的最大并发会话连接数等资源配额；
b) 应提供资源控制不当的报警及响应；
c) 应在会话处于非活跃一定时间或会话结束后终止会话连接。

应用漏洞扫描要求包括但不限于：

a) 应针对所有上线的网络应用，进行上线前的应用漏洞扫描。

3.1.4.2 工业 App 安全防护要求

安装要求包括但不限于：

a) 应包含可有效表征供应者或开发者身份的签名信息、软件属性信息；
b) 安装时应提示终端操作系统用户对其使用的终端资源和终端数据进行确认；
c) 宜对平台操作系统和其他应用软件的正常运行无影响。

卸载要求包括但不限于：

a） 应能删除安装和使用过程中产生的资源文件、配置文件和用户数据；
b） 删除用户使用过程中生成的数据时应有提示；
c） 应对工业互联网平台系统和其他应用软件的功能无影响。

身份认证要求包括但不限于：

a) 在用户访问应用业务前，工业 App 应对其身份进行鉴别，并提供鉴别失败处理措施；
b) 应具备登录超时后的锁定或注销功能。

口令安全机制要求包括但不限于：

a) 在使用过程中不应以明文形式显示和存储；
b) 应支持口令强度检查机制；
c) 修改或找回口令时，应具备验证机制，如短信验证、邮箱验证等；
d) 应支持用户登录输入口令的键盘防劫持机制。

访问控制要求包括但不限于：

a) 用户访问的内容不应超出授权的范围；
b) 应限制工业 App 用户账号的多重并发会话；
c) 应支持用户权限分配和互斥机制。

实现安全要求包括但不限于：

a) 不应设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口；
b) 应具备安全机制防止程序被反编译、反调试；
c) 宜确保不存在漏洞发布平台/机构（例如 CNVD、CNNVD、CVE、CNCVE）公开发布了 6 个月及以上的高危安全漏洞。

升级安全要求包括但不限于：

a) 应支持软件的更新，且应至少采取一种安全机制（如身份认证），保证升级的时效

性和准确性；

b) 应对升级包的完整性进行校验。

容错性安全要求包括但不限于：

a) 应支持数据输入内容、长度容错能力。

资源占用安全要求包括但不限于：

a) 应支持前台、后台运行状态资源合理占用；

b) 应支持未运行状态释放资源占用。

其他安全要求包括但不限于：

a) 不应在数据库或文件系统中明文存储用户敏感信息；

b) 不应在 Cookie 中保存明文密码；

c) 应采取会话保护措施保障工业 App 与服务器端之间的会话不被窃听、篡改、伪造和重放；

d) 如使用开源第三方应用组件及代码，应对已公开安全漏洞及时更新补丁；

e) 应保证工业 App 运行稳定性，包括但不限于前后台切换操作无异常、锁屏截屏操作无异常、应用系统中断后无异常、强制终止后无异常等。

3.1.5 数据安全防护要求

应按照《工业互联网企业数据安全防护规范（试行）》对平台所使用和存储的数据进行分类分级，依据分级要求采取对应的数据安全防护措施。

3.1.6 安全管理

3.1.6.1 安全管理制度

a) 应对安全管理活动中重要的管理内容建立安全管理制度；

b) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

c) 应指定或授权专门的部门或人员负责安全管理制度的制定；

d) 安全管理制度应通过正式、有效的方式发布，并进行版本控制；

e) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

3.1.6.2 安全管理机构和人员要求

安全管理机构要求包括但不限于：

a) 应明确指定一个机构，具体承担网络安全管理工作，组织制定和落实网络安全管理制度，实施网络安全技术防护措施，开展网络安全宣传教育培训，执行网络安全监督检查等；

b) 应设立安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义部门及各负责人的职责；

c) 应设立系统管理员、网络管理员、安全管理员等岗位，配备一定数量的系统管理员、网络管理员、安全管理员等，并定义各个工作岗位的职责；

d) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

e) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；
应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等。

人员要求包括但不限于：

a) 应加强各类管理人员之间、组织内部机构之间以及安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理安全问题；

b) 应加强与工业互联网安全主管部门、各类供应商、业界专家及的合作与沟通；

c) 应指定或授权专门的部门或人员负责人员录用；
d) 应对被录用人员的身份、背景、专业资格和资质等进行审查；
e) 应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
f) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
g) 应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
h) 外部人员离场后应及时清除其所有的访问权限。

3.1.6.3 安全建设管理要求

定级要求包括但不限于：

a) 应明确本企业的安全等级；
b) 应以书面形式说明企业确定为某安全等级的方法和理由。

安全方案设计要求包括但不限于：

a) 应根据安全防护对象的安全防护需求进行安全方案设计；
b) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用要求包括但不限于：

a) 工业互联网平台的重要设备及专用安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；
b) 应确保安全产品与服务的采购和使用符合国家的有关规定。

软件开发要求包括但不限于：

a) 应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
b) 应在软件开发过程中进行安全性测试；
c) 应在软件交付前检测其中可能存在的缺陷与恶意代码等；
d) 应要求开发单位提供软件设计文档和使用指南；
e) 应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

系统交付要求包括但不限于：

a) 应制订安全性测试验收方案，并依据测试验收方案实施验收，形成验收报告；
b) 应根据交付清单对所交接的设备、软件和文档等进行清点；
c) 应对负责运行维护的技术人员进行相应的技能培训；
应提供建设过程中的文档和指导用户进行运行维护的文档。

服务供应商选择要求包括但不限于：

a) 应选择安全合规的设备、服务、工业互联网平台供应商，其所提供的设备、平台系统等应为其所承载的业务提供相应的安全防护能力；
b) 应在服务协议中规定具体服务内容和技术指标；
c) 应在服务协议中规定供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
d) 应与选定的服务供应商签订相关协议，明确供应链各方需履行的安全相关义务；
e) 应在服务协议中规定服务合约到期时，完整地返还客户信息，并承诺相关信息均已在云计算平台、工业互联网平台系统上清除；
f) 应确保供应链安全事件信息或威胁信息能够及时传达到客户；

g) 应确保外包运维服务商的选择符合国家的有关规定；

h) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

3.1.6.4 安全运维管理要求。

环境管理要求包括但不限于：

a) 应对机房的安全管理做出规定，指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b) 应不在重要区域接待来访人员。

资产管理要求包括但不限于：

a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；

d) 应对各种设备（包括备份和冗余设备）、线路等定期进行维护管理；

e) 应记录工业互联网平台相关设备的状态（包括外观、电量、指示灯等信息），对设备进行现场维护（除尘、充电、修理等）；

f) 应对工业互联网平台部署环境的评估方法作出明确规定；

g) 应对工业互联网平台相关设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；

h) 应采用国家密码管理主管部门批准使用的密码算法和认证核准的密码产品；

i) 应明确资产变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

安全审计要求包括但不限于：

a) 应对重要设备、平台、系统等启用安全审计功能，对重要的用户行为和重要安全事件进行审计；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；

b) 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；审计记录中应避免明文记录敏感数据，如用户口令等；

c) 应确保审计记录的留存时间符合法律法规要求。

配置管理要求包括但不限于：

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

安全事件处置要求包括但不限于：

a) 应及时向工业互联网安全主管部门报告所发现的安全弱点和可疑事件；

b) 应明确安全事件的报告和处置流程，制定安全事件报告和处置管理制度；

c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

应急工作要求包括但不限于：

a) 应制定网络安全事件应急预案，包括应急处理流程、系统恢复流程等内容，并根据实际情况适时进行评估和修订，原则上每年进行一次评估和修订；

b) 应定期开展网络安全事件应急预案宣贯培训，确保相关人员熟悉应急预案，并进行应急预案的演练。

3.1.7 物理和环境安全要求

3.1.7.1 物理位置选择

a) 机房场地及工业互联网平台相关设备放置场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；

3.1.7.2 物理访问控制

a) 机房场地及工业互联网平台相关设备放置场地出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；

b) 重要服务器、数据库、工程师站等核心工业互联网软硬件所在区域或工业互联网平台宜采取视频监控等手段；

3.1.7.3 防盗窃和防破坏

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b) 应将通信线缆铺设在隐蔽安全处，可铺设在地下或管道中；

c) 主机房或重要设备区域应安装比亚的防盗报警设置。

3.1.7.4 防雷击

a) 应将各类机柜、设施和设备等通过接地系统安全接地。

3.1.7.5 防火

a) 机房及工业互联网平台相关设备放置场地应设置灭火设备和火灾自动报警系统。

3.1.7.6 防水和防潮

a) 应采取措施防止雨水通过机房或场地窗户、屋顶和墙壁渗透；

b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

3.1.7.7 防静电

应满足 YD/T 1754-2008 中 3.2.7 的相关要求。

3.1.7.8 温湿度控制

应满足 YD/T 1754-2008 中 3.2.8 的相关要求。

3.1.7.9 电力供应

应满足 YD/T 1754-2008 中 3.2.10 的相关要求。

3.1.7.10 电磁防护

应满足 YD/T 1754-2008 中 3.2.11 的相关要求。

3.2 增强级防护要求

3.2.1 接入层安全防护要求

3.2.1.1 网络架构

除包括3.1.1.1基本级防护要求之外，还应包括但不限于：

避免接入设备与重要信息系统直接互连，可通过信息交换系统或者共享系统来进行数据的交互。

3.2.1.2 传输保护

除包括3.1.1.2基本级防护要求之外，还应包括但不限于：

a) 在关键边缘接入设备应提供满足国家密码管理法律法规的通信加密和签名验签；

b) 应保证通信过程中使用的互联互通协议的可信性。

3.2.1.3 边界防护

除包括3.1.1.3基本级防护要求之外，还应包括但不限于：

a) 能够对非授权设备的接入行为进行告警和阻断；

b) 对于有线和无线接入，确保通过受控的边界防护设备或其上的指定端口接入网络。

3.2.1.4 访问控制

除包括3.1.1.4基本级防护要求之外，还应包括但不限于：

a) 对接入网络数据进行深度包检测；

b) 采用白名单控制方式，只允许合法设备接入网络；

c) 采用 IP-MAC 绑定、802.1x、证书、标识码等技术对接入的 PC 机、便携机、智能终端等设备进行注册认证；

d) 终端接入后，限制该终端的访问权限，并限制其他设备与该终端的非授权通信；

e) 在一个非活动时间周期后，可以通过自动方式或者手动方式终止用户远程连接。

3.2.1.5 入侵防范

除包括3.1.1.5基本级防护要求之外，还应包括但不限于：

a) 能够对未知威胁进行分析和防范。

3.2.1.6 安全审计

除包括3.1.1.6基本级防护要求之外，还应包括但不限于：

a) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

3.2.1.7 安全基线检查

除包括 3.1.1.7 基本级防护要求之外，还应包括但不限于：

a) 每年度根据业务和平台实际运行水准进行基线优化。

3.2.2 基础设施层安全防护要求

3.2.2.1 服务器安全防护要求

除包括3.1.2.1基本级防护要求之外，还应包括但不限于：

身份鉴别认证要求包括但不限于：

a) 当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取。

访问控制要求包括但不限于：

同3.1.2.1基本级防护要求。

安全审计要求包括但不限于：

a) 应能够根据记录数据进行分析，并生成审计报表；

b) 应保护审计进程，避免受到未预期的中断。

资源控制要求包括但不限于：

a) 应对重要服务器进行性能监测，包括服务器的 CPU、硬盘、内存、网络等资源的使用情况，发现异常情况提供告警，并进行相应处置。

恶意代码防范要求包括但不限于：

a) 应支持对防恶意代码的统一管理。

入侵防范要求包括但不限于：

a) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

3.2.2.2 网络安全防护要求

除包括 3.1.2.2 基本级防护要求之外，还应包括但不限于：

网络拓扑结构要求包括但不限于：

应按照用户服务级别协议的高低次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护高级别用户的服务通信。

访问控制要求包括但不限于：

a) 应实现对 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。

安全审计要求包括但不限于：

a) 应能够根据记录数据进行分析，发现异常能及时告警，并生成审计报表。

恶意代码防范要求包括但不限于：

a) 应周期性地维护恶意代码库的升级和检测系统的更新。

网络设备防护要求包括但不限于：

a) 当对网络设备进行远程管理时，应采取加密等措施防止鉴别信息在网络传输过程中被窃取；

b) 应对网络设备进行分权分域管理，限制默认用户或者特权用户的权限，做到最小授权。

网络安全监测要求包括但不限于：

a) 应周期性地对攻击、威胁的特征库进行更新，并升级到最新版本；

b) 应支持对违法和不良信息或非法域名的检测发现并告警；

c) 应支持对攻击行为进行分析，明确攻击目标范围，并协助回溯到攻击源头；

d) 应在网络边界处部署异常流量和对未知威胁的识别、监控和防护机制，并采取技术措施对网络进行行为分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

3.2.2.3 虚拟化安全防护要求

除包括3.1.2.3基本级防护要求之外，还应包括但不限于：

虚拟机安全要求包括但不限于：

a) 应保证虚拟机迁移过程中数据和内存的安全可靠，保证迁入虚拟机的完整性和迁移前后安全配置环境的一致性；

b) 应确保虚拟机操作系统的完整性，确保虚拟机操作系统不被篡改，且确保虚拟机实现安全启动；

c) 应对虚拟机镜像文件进行完整性校验，确保虚拟机镜像不被篡改；

d) 应提供最新版本的虚拟机镜像和补丁版本；

e) 应支持发现虚拟机操作系统漏洞的能力，支持漏洞修复。

虚拟网络安全要求包括但不限于：

a) 应支持对虚拟网络的逻辑隔离，在虚拟网络边界处实施访问控制策略；

b) 应对虚拟机网络出口带宽进行限制；

c) 可支持用户选择使用第三方安全产品。

虚拟化平台安全要求包括但不限于：

同3.1.2.3基本级防护要求。

容器安全要求包括但不限于：

a) 对容器服务进行访问控制，避免不必要的权限升级，对容器镜像进行数字签名及签名验证。

3.2.3 平台层安全防护要求

3.2.3.1 数据分析服务安全防护要求

同3.1.3.1基本级防护要求。

3.2.3.2 微服务组件安全防护要求

同3.1.3.2基本级防护要求。

3.2.3.3 平台应用开发环境安全防护要求

除包括3.1.3.3基本级防护要求之外，还应包括但不限于：

身份鉴别要求包括但不限于：

a) 需要登录访问的开发环境，应对用户访问和操作的有关环节（如注册、登录、操作、管理、浏览等）提供有效的保护措施（如对用户注册口令进行强度检查、用户检测和账号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连接等）。

访问控制要求包括但不限于：

同3.1.3.3基本级防护要求。

安全审计要求包括但不限于：

同3.1.3.3基本级防护要求。

资源控制要求包括但不限于：

a) 根据需要对用户与开发环境之间相关通信过程中的全部报文或整个会话过程提供必要的保护（如进行通信数据加密），并提供对相关访问、通信等数据的防抵赖功能；

b) 定义服务水平阈值，能够对服务水平进行监测，并具备当服务水平降低到预先规定的阈值时进行告警的功能。

信息保护要求包括但不限于：

a) 与开发环境中的重要功能相关的数据应进行异址备份；

b) 开发环境应提供数据自动保护功能，当发生故障后应保证开发环境能够恢复到故障前的业务状态。

恶意代码防范要求包括但不限于：

a) 应提供有效的恶意代码检测和过滤技术手段，对开发环境向用户提供的各类信息（如用户发布和上传的文件、资源站点可供下载的立件、即时通信用户间传送的文件、电子邮件附件）进行必要的安全检查和过滤。

上线前检测要求包括但不限于：

a) 业务应用与工业 App 在上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善；

b) 业务应用与工业 App 应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）。

3.2.4 应用层安全防护要求

3.2.4.1 平台业务应用安全防护要求

除包括 3.1.4.1 基本级防护要求之外，还应包括但不限于：

身份鉴别要求包括但不限于：

a) 应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证一种身份鉴别机制是不易伪造的；

b) 应具备防范暴力破解等攻击的能力。

访问控制要求包括但不限于：

同3.1.4.1基本级防护要求。

安全审计要求包括但不限于：

a) 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能；

b) 应具备自动化审计功能，监控明显异常操作并响应；

c) 应能汇聚服务范围内的审计数据，支持第三方审计。

资源控制要求包括但不限于：

同3.1.4.1基本级防护要求。

应用漏洞扫描要求包括但不限于：

a) 规范公司内广泛认定的应用漏洞分级要求；

b) 每年至少进行两次应用漏洞扫描，并且出具相应报告。

3.2.4.2 工业 App 安全防护要求

除包括3.1.4.2基本级防护要求之外，还应包括但不限于：

安装要求包括但不限于：

a) 工业 App 的安装需得到明确授权，其安装过程仅能运行在特定环境中且不能破坏其运行环境，应对终端操作系统和其他应用软件的正常运行无影响。

卸载要求包括但不限于：

同3.1.4.2基本级防护要求。

身份认证要求包括但不限于：

a) 工业 App 在访问敏感数据、关键业务或系统配置前，应对用户身份进行二次鉴别。

口令安全机制要求包括但不限于：

a） 不应默认保存用户上次的账号及口令信息；

b） 应具备口令强度、时效性检查机制。

访问控制要求包括但不限于：

同3.1.4.2基本级防护要求。

实现安全要求包括但不限于：

a） 工业 App 应保证程序自身的安全性，应确保不存在漏洞发布平台/机构（例如 CNVD、CNNVD、CVE、CNCVE）公开发布了 6 个月及以上的高危安全漏洞；

b） 应支持程序反编译、反调试机制。

升级安全要求包括但不限于：

同3.1.4.2基本级防护要求。

容错性安全要求包括但不限于：

a） 应支持数据输入类型、一致性、规则等的容错能力。

资源占用安全要求包括但不限于：

同3.1.4.2基本级防护要求。

其他安全要求包括但不限于：

a) 不应在服务器端日志中记录用户敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理；

b) 应确保服务器端日志数据的安全存储，并严格限制日志数据的访问权限。

3.2.5 数据安全防护要求

平台应按照《工业互联网企业数据安全防护规范（试行）》对平台所使用和存储的数据进行分类分级，依据分级要求采取对应的数据安全防护措施。

3.2.6 安全管理

3.2.6.1 安全管理制度

除包括3.1.6.1基本级防护要求之外，还应包括但不限于：

a) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

3.2.6.2 安全管理机构和人员要求

除包括3.1.6.2基本级防护要求之外，还应包括但不限于：

安全管理机构要求包括但不限于：

同 3.1.6.2 基本级防护要求。

人员要求：

a) 应成立指导和管理安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
b) 应配备专职安全管理员，不可兼任，关键事务岗位应配备多人共同管理；
c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
d) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
e) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
f) 应从内部人员中选拔从事关键岗位的人员；
g) 应对被录用人员所具有的技术技能进行考核，应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
h) 人员离岗时，应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
i) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，应定期对不同岗位的人员进行技能考核；
j) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；对关键区域或关键系统不允许外部人员访问。

3.2.6.3 安全建设管理要求：

除包括 3.1.6.3 基本级防护要求之外，还应包括但不限于：

定级要求包括但不限于：

同 3.1.6.3 基本级防护要求。

安全方案设计要求包括但不限于：

a) 应根据安全防护对象的安全防护需求及与其他防护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
b) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用要求包括但不限于：

a) 应预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；
b) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

软件开发要求包括但不限于：

a) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
b) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
c) 应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；
d) 应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
e) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；
f) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

系统交付要求包括但不限于：

a) 安全测试报告应包含密码应用安全性测试相关内容。

服务供应商选择要求包括但不限于：

a) 应定期评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；
b) 应与选定的服务供应商签署保密协议，要求其不得泄露客户数据和业务系统的相关重要信息；
c) 应保证供应商的重要变更及时传达到客户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

3.2.6.4 安全运维管理要求

除包括 3.1.6.4 基本级防护要求之外，还应包括但不限于：

环境管理要求包括但不限于：

a) 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等；

b) 应加强对工业互联网设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

资产管理要求包括但不限于：

a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

b) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；

c) 应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；

d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；

e) 应建立资产变更的申报和审批程序，依据程序控制所有的变更，记录变更实施过程；

f) 应建立中止资产变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

安全审计要求包括但不限于：

a) 应能对远程访问企业内部网络的用户行为进行行为审计和数据分析；

b) 应对审计进程进行保护，防止未经授权的中断；

c) 审计记录的留存时间应不少于 6 个月。

配置管理要求包括但不限于：

a) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

安全事件处置要求包括但不限于：

a) 对造成业务中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

应急工作要求包括但不限于：

a) 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b) 应定期开展网络安全应急演练，检验应急预案的可操作性，并结合应急演练结果，对应急预案进行评估和适用性修订；

c) 应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。

3.2.7 物理和环境安全要求

3.2.7.1 物理位置选择

a) 在机房选址及设计时，满足 GB 50174 的相关规定；

b) 确保工业互联网平台服务器及运行关键业务和数据的物理设备位于境内。

3.2.7.2 物理访问控制

除包括 3.1.7.2 基本级防护要求之外，还应包括但不限于：

a) 应对机房划分区域并在不同区域之间设置物理隔离装置，在重要区域前设置交付或

安装等过渡区域。

3.2.7.3 防盗窃和防破坏

除包括 3.1.7.3 基本级防护要求之外，还应包括但不限于：

a) 应对机房设置监控报警系统。

3.2.7.4 防雷击

同 3.1.7.4 基本级防护要求。

3.2.7.5 防火

a) 机房及工业互联网平台相关设备放置场地应设置灭火设备和火灾自动报警系统，能够自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

3.2.7.6 防水和防潮

除包括 3.1.7.6 基本级防护要求之外，还应包括但不限于：

a) 应安装对水敏感的检测仪表或元件，对机房及工业互联网平台相关设备放置场地进行防水检测。

3.2.7.7 防静电

应满足 YD/T 1754-2008 中 3.3.7 的相关要求。

3.2.7.8 温湿度控制

同 3.1.7.8 基本级防护要求

3.2.7.9 电力供应

应满足 YD/T 1754-2008 中 3.3.10 的相关要求。

3.2.7.10 电磁防护

同 3.1.7.10 基本级防护要求

2-3 工业互联网标识解析企业安全防护规范（试行）

目　　录

工业互联网标识解析企业安全防护规范（试行）

1 工业互联网标识解析企业安全防护范围及内容

1.1 工业互联网标识解析企业安全防护范围

工业互联网标识解析企业安全防护范围，包括企业提供工业互联网标识注册服务、解析服务等的标识解析系统。其中，标识解析系统的安全防护范围，包括构成标识解析的系统的相关基础设施安全、网络安全、应用安全、数据安全、安全管理和物理和环境安全。

1.2 工业互联网标识解析企业安全防护内容

工业互联网标识解析企业安全防护内容具体包括：

（1）基础设施安全防护：包括主机安全、存储安全、云安全、身份认证与访问控制、防病毒等。

（2）网络安全防护：包括网络与边界的划分隔离、访问控制、机密性与完整性保护、异常监测、入侵防范、防DDoS攻击等。

（3）应用安全防护：包括标识解析系统及应用的访问控制、攻击防范、入侵防范、行为管控、协议安全、API安全等。

（4）数据安全防护：包括数据分级分类、数据脱敏加密、完整性保护、数据备份恢复、数据安全销毁等。

（5）安全管理要求：包括安全管理制度要求、安全管理机构和人员要求、安全建设和管理要求、安全运维管理要求等。

（6）物理和环境安全：包括物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、电磁防护等。

2 工业互联网标识解析企业安全防护级别的确定

工业互联网标识解析企业按照《工业互联网企业网络安全分类分级管理指南（试行）》的级别划分，采取不同程度的安全防护。工业互联网标识解析企业的安全防护分为基本级防护和增强级防护两个级别：

三级工业互联网标识解析企业建议采取增强级防护措施。

二级工业互联网标识解析企业建议采取基本级防护措施。

一级工业互联网标识解析企业参照基本级防护要求根据自身情况，自主落实安全防护措施。

3 工业互联网标识解析企业安全防护要求

3.1 基本级防护要求

3.1.1 基础设施安全防护

3.1.1.1 主机安全

标识解析系统相关主机安全防护要求包括但不限于：

a) 应遵循最小安装的原则，仅为标识解析系统相关设备安装需要的组件和应用程序；

b) 关闭设备中不需要的端口与服务；

c) 应能及时发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

d) 应能检测升级软件的真实性和完整性；

e) 主机应安装主流防病毒软件并具备及时升级能力。

3.1.1.2 身份认证与访问控制

身份认证与访问控制安全要求包括但不限于：

a) 应支持对标识解析服务器身份的真实性进行核验；
b) 应通过制定安全策略如访问控制列表，实现对接入标识解析系统中用户终端的访问控制；
c) 应采取相应技术手段，确保身份认证在不同层级间的节点互信、标识源的真实性验证、用户终端与企业标识解析节点间的互信等方面不被窃听或攻击；
d) 应通过防伪、标识绑定等技术措施防止被动及主动标识载体中的标识编码被篡改、伪造；
e) 应采取相应技术手段防止标识客户端被破坏，避免其身份被篡改、伪造和恶意利用；
f) 应对登录系统进行运维的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；
g) 对于登录设备进行运维的过程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；

3.1.1.3 云安全

云安全要求包括但不限于：

采用云计算部署方式的标识解析系统，除满足上述主机安全要求之外，还应具备云主机之间东西向隔离防护功能。

3.1.1.4 冗余和备份恢复安全

冗余备份恢复安全包括但不限于：

标识解析系统关键主机应支持冗余或负载分担功能，在设备运行状态异常时，可通过启用备用部件防范安全风险。

3.1.2 网络安全防护

3.1.2.1 区域划分与隔离

区域划分与隔离安全要求包括但不限于：

标识解析系统内部网络应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

3.1.2.2 网络边界访问控制

网络边界访问控制安全要求包括但不限于：

a) 应在网络边界根据访问控制策略设置访问控制规则，保证跨越网络边界的访问和数据流通过边界防护设备提供的受控接口进行通信，默认情况下受控接口拒绝所有通信；
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；
c) 应根据网络边界访问控制规则，通过检查数据包的源地址、目的地址、源端口、目的端口、协议等，确定是否允许该数据包通过该区域边界；
d) 系统内部网络与外部网络之间应采用访问控制机制，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
e) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

3.1.2.3 网络异常监测

网络异常监测安全要求包括但不限于：

应对网络通讯数据、异常访问、异常流量等进行监测，发生异常进行报警。

3.1.2.4 网络入侵防范

网络入侵防范安全要求包括但不限于：

a) 应在关键网络节点处部署端口扫描、木马后门等入侵防范措施，对针对这些节点的入侵行为进行检测，并在发生严重入侵事件时提供报警；

b) 应在关键网络节点处部署防 DDoS 攻击措施，对针对这些节点的 DDoS 攻击流量进行检测和清洗，保障系统正常运行，并在发生攻击事件时提供报警；

c) 应对进出标识解析关键系统的数据信息进行过滤，并能根据系统能力对网络流量及并发数进行限制，对关键入侵行为进行阻断。

3.1.2.5 安全监测审计

安全审计要求包括但不限于：

应对标识解析系统网络流量信息等进行记录，并对记录进行留存和保护，防止篡改和未授权访问。

3.1.3 应用安全防护

3.1.3.1 身份认证与访问控制

身份认证与访问控制安全要求包括但不限于：

a) 应对使用标识解析应用的用户和终端身份进行标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

b) 应使用密码技术对身份认证数据进行保密性和完整性保护；

c) 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；

d) 应提供访问控制功能，对使用应用程序的用户分配账户及相应的访问操作权限。

3.1.3.2 协议安全

协议安全要求包括但不限于：

a) 应支持对标识解析客户端和应用的双向身份认证，确保访问请求来自可靠的签名证书或可靠渠道；

b) 应确保各级节点间、客户端与服务器端间通信过程，对主体身份、消息进行安全认证；

c) 标识解析协议支持基于 TLS 等安全加密协议承载，节点内外部均不采用明文传输数据。

3.1.3.3 应用资源控制

应用资源控制要求包括但不限于：

a) 应能够对应用的最大并发会话连接数进行限制；

b) 应能够对单个用户、终端、IP 地址的多重并发会话进行限制；

c) 应能够对用户或进程对终端设备系统资源的最大使用限度进行限制，防止终端设备被提权。

3.1.3.4 攻击防范

攻击防范要求包括但不限于：

能够防范标识解析反射/放大攻击、地址劫持、递归攻击等攻击行为。

3.1.3.5 应用程序检测

应用程序检测要求包括但不限于：

应在应用程序上线前对其安全性进行测试，对可能存在的缺陷与恶意代码等进行检测。

3.1.4 数据安全防护

数据安全防护要求包括但不限于：

a) 标识解析企业应保证本节点的数据安全，建立身份认证机制；具有数据流向监控能

力等；

b) 标识解析企业应采取技术手段确保标识注册数据、标识解析数据和日志数据在数据采集、传输、存储、使用和销毁等全生命周期流转过程中不被窃取、篡改、丢失，确保相关隐私数据不被泄露等；

c) 标识解析企业应按照《工业互联网企业数据安全分级防护要求（试点）》对标识解析系统所使用和存储的数据进行分类分级，依据分级要求采取对应的数据安全防护措施。

3.1.5 安全管理

3.1.5.1 安全管理制度

a) 应对安全管理活动中重要的管理内容建立安全管理制度；

b) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

c) 应指定或授权专门的部门或人员负责安全管理制度的制定；

d) 安全管理制度应通过正式、有效的方式发布，并进行版本控制；

e) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

3.1.5.2 安全管理机构和人员要求

安全管理机构要求包括但不限于：

a) 应明确指定一个机构，具体承担网络安全管理工作，组织制定和落实网络安全管理制度，实施网络安全技术防护措施，开展网络安全宣传教育培训，执行网络安全监督检查等；

b) 应设立安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义部门及各负责人的职责；

c) 应设立系统管理员、网络管理员、安全管理员等岗位，配备一定数量的系统管理员、网络管理员、安全管理员等，并定义各个工作岗位的职责；

d) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

e) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；

f) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等。

人员要求包括但不限于：

a) 应加强各类管理人员之间、组织内部机构之间以及安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理安全问题；

b) 应加强与工业互联网安全主管部门、各类供应商、业界专家及的合作与沟通；

c) 应指定或授权专门的部门或人员负责人员录用；

d) 应对被录用人员的身份、背景、专业资格和资质等进行审查；

e) 应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

f) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

g) 应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

h) 外部人员离场后应及时清除其所有的访问权限。

3.1.5.3 安全建设管理要求

定级要求包括但不限于：

a) 应明确本企业的安全等级；

b) 应以书面形式说明企业确定为某安全等级的方法和理由。

安全方案设计要求包括但不限于：

a) 应根据安全防护对象的安全防护需求进行安全方案设计；

b) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用要求包括但不限于：

a) 工业互联网标识解析系统的重要设备及专用安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；

b) 应确保安全产品与服务的采购和使用符合国家的有关规定。

软件开发要求包括但不限于：

a) 应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

b) 应在软件开发过程中进行安全性测试；

c) 应在软件交付前检测其中可能存在的缺陷与恶意代码等；

d) 应要求开发单位提供软件设计文档和使用指南；

e) 应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

系统交付要求包括但不限于：

a) 应制订安全性测试验收方案，并依据测试验收方案实施验收，形成验收报告；

b) 应根据交付清单对所交接的设备、软件和文档等进行清点；

c) 应对负责运行维护的技术人员进行相应的技能培训；
应提供建设过程中的文档和指导用户进行运行维护的文档。

服务供应商选择要求包括但不限于：

a) 应选择安全合规的设备、服务、工业互联网标识解析系统供应商，其所提供的设备、平台系统等应为其所承载的业务提供相应的安全防护能力；

b) 应在服务协议中规定具体服务内容和技术指标；

c) 应在服务协议中规定供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

d) 应与选定的服务供应商签订相关协议，明确供应链各方需履行的安全相关义务；

e) 应在服务协议中规定服务合约到期时，完整地返还客户信息，并承诺相关信息均已在云计算平台、工业互联网标识解析系统上清除；

f) 应确保供应链安全事件信息或威胁信息能够及时传达到客户；

g) 应确保外包运维服务商的选择符合国家的有关规定；

h) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

3.1.5.4 安全运维管理要求

环境管理要求包括但不限于：

a) 应对机房的安全管理做出规定，指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b) 应不在重要区域接待来访人员。

资产管理要求包括但不限于：

a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
d) 应对各种设备（包括备份和冗余设备）、线路等定期进行维护管理；
e) 应记录工业互联网标识解析系统相关设备的状态(包括外观、电量、指示灯等信息)，对设备进行现场维护（除尘、充电、修理等）；
f) 应对工业互联网标识解析系统部署环境的评估方法作出明确规定；
g) 应对工业互联网标识解析系统相关设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
h) 应采用国家密码管理主管部门批准使用的密码算法和认证核准的密码产品；
i) 应明确资产变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

安全审计要求包括但不限于：

a) 应对重要设备、平台、系统等启用安全审计功能，对重要的用户行为和重要安全事件进行审计；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；
b) 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；审计记录中应避免明文记录敏感数据，如用户口令等；
c) 应确保审计记录的留存时间符合法律法规要求。

配置管理要求包括但不限于：

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

安全事件处置要求包括但不限于：

a) 应及时向工业互联网安全主管部门报告所发现的安全弱点和可疑事件；
b) 应明确安全事件的报告和处置流程，制定安全事件报告和处置管理制度；
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

应急要求包括但不限于：

a) 应制定网络安全事件应急预案，包括应急处理流程、系统恢复流程等内容，并根据实际情况适时进行评估和修订，原则上每年进行一次评估和修订；
b) 应定期开展网络安全事件应急预案宣贯培训，确保相关人员熟悉应急预案，并进行应急预案的演练。

3.1.6 物理和环境安全

3.1.6.1 物理位置选择

a) 机房场地及工业互联网标识解析相关设备放置场地应选择在具有防震、防风和防雨等能力的建筑内；
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；

3.1.6.2 物理访问控制

a) 机房场地及工业互联网标识解析系统相关设备放置场地出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；
b) 重要服务器、数据库、工程师站等核心工业互联网软硬件所在区域或工业互联网标识解析系统宜采取视频监控等手段；

3.1.6.3 防盗窃和防破坏

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b) 应将通信线缆铺设在隐蔽安全处，可铺设在地下或管道中；

c) 主机房或重要设备区域应安装比亚的防盗报警设置。

3.1.6.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

3.1.6.5 防火

机房及工业互联网标识解析系统相关设备放置场地应设置灭火设备和火灾自动报警系统。

3.1.6.6 防水和防潮

a) 应采取措施防止雨水通过机房或场地窗户、屋顶和墙壁渗透；

b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

3.1.6.7 防静电

应满足 YD/T 1754-2008 中 3.2.7 的相关要求。

3.1.6.8 温湿度控制

应满足 YD/T 1754-2008 中 3.2.8 的相关要求。

3.1.6.9 电力供应

应满足 YD/T 1754-2008 中 3.2.10 的相关要求。

3.1.6.10 电磁防护

应满足YD/T 1754-2008中3.2.11的相关要求。

3.2 增强级防护要求

3.2.1 基础设施安全防护

3.2.1.1 主机安全

同3.1.1.1基本级防护要求。

3.2.1.2 身份认证与访问控制

除包括3.1.1.2基本级防护要求之外，还应包括但不限于：

a) 应对工业互联网标识解析涉及的多主体对象的身份权限进行统一管理，对用户访问过程实行严格的权限控制；

b) 应对登录设备进行运维的用户分配账户和权限；

c) 应重命名或删除默认账户，修改默认账户的默认口令；

d) 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；

e) 应对登录设备进行运维的用户授予其所需的最小权限，并实现对不同类型运维用户的权限分离；

f) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

3.2.1.3 云安全

同 3.1.1.3 基本级防护要求。

3.2.1.4 冗余和备份恢复安全

同 3.1.1.4 基本级防护要求。

3.2.2 网络安全防护

3.2.2.1 区域划分与隔离

除包括3.1.2.1基本级防护要求之外，还应包括但不限于：

应对标识解析核心系统（如标识解析节点服务系统）内部网络环境经由受控边界与外部网络连接。

3.2.2.2 网络边界访问控制

除包括3.1.2.2基本级防护要求之外，还应包括但不限于：

应在标识解析系统关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。

3.2.2.3 网络异常监测

除包括3.1.2.3基本级防护要求之外，还应包括但不限于：

应能够对系统内部网络中的用户或网络设备非授权连接到外部网络或因特网的行为进行限制或检查，并对其进行有效阻断。

3.2.2.4 网络入侵防范

除包括3.1.2.4基本级防护要求之外，还应包括但不限于：

a) 应在关键网络节点处检测、防止或限制从节点内外侧发起的网络攻击行为；
b) 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；
c) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

3.2.2.5 安全监测审计

除包括3.1.2.5基本级防护要求之外，还应包括但不限于：

a) 应对标识解析系统网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
b) 应对分散在各个网络设备上的审计数据进行收集汇总和集中分析；
c) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
d) 应能对网络中发生的各类安全事件进行识别、报警和分析。

3.2.3 应用安全防护

3.2.3.1 身份认证与访问控制

除包括3.1.3.1基本级防护要求之外，还应包括但不限于：

a) 应重命名或删除默认账户，修改默认账户的默认登录口令；
b) 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。

3.2.3.2 协议安全

除包括3.1.3.2基本级防护要求之外，还应包括但不限于：

采用高强度加密算法进行数据加密，保障数据传输的机密性。

3.2.3.3 应用资源控制

同 3.1.3.3 基本级防护要求。

3.2.3.4 攻击防范

同 3.1.3.4 基本级防护要求。

3.2.3.5 应用程序检测

同3.1.3.5基本级防护要求。

3.2.4 数据安全防护

同3.1.4基本级防护要求。

3.2.5 安全管理

3.2.5.1 安全管理制度

除包括 3.1.5.1 基本级防护要求之外，还应包括但不限于：

a) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

3.2.5.2 安全管理机构和人员要求

除包括 3.1.5.2 基本级防护要求之外，还应包括但不限于：

安全管理机构要求包括但不限于：

同 3.1.5.2 基本级防护要求。

人员要求包括但不限于：

a) 应成立指导和管理安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
b) 应配备专职安全管理员，不可兼任，关键事务岗位应配备多人共同管理；
c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
d) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
e) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
f) 应从内部人员中选拔从事关键岗位的人员；
g) 应对被录用人员所具有的技术技能进行考核，应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
h) 人员离岗时，应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
i) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，应定期对不同岗位的人员进行技能考核；
j) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；对关键区域或关键系统不允许外部人员访问。

3.2.5.3 安全建设管理要求

除包括 3.1.5.3 基本级防护要求之外，还应包括但不限于：

定级要求包括但不限于：

同 3.1.5.3 基本级防护要求。

安全方案设计要求包括但不限于：

a) 应根据安全防护对象的安全防护需求及与其他防护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
b) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用要求包括但不限于：

a) 应预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；
b) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

软件开发要求包括但不限于：

a) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
b) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
c) 应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；
d) 应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
e) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；
f) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

系统交付要求包括但不限于：

a) 安全测试报告应包含密码应用安全性测试相关内容。

服务供应商选择要求包括但不限于：

a) 应定期评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；

b) 应与选定的服务供应商签署保密协议，要求其不得泄露客户数据和业务系统的相关重要信息；

c) 应保证供应商的重要变更及时传达到客户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

3.2.5.4 安全运维管理要求

除包括 3.1.5.4 基本级防护要求之外，还应包括但不限于：

环境管理要求包括但不限于：

a) 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等；

b) 应加强对工业互联网设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

资产管理要求包括但不限于：

a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

b) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；

c) 应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；

d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；

e) 应建立资产变更的申报和审批程序，依据程序控制所有的变更，记录变更实施过程；

f) 应建立中止资产变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

安全审计要求包括但不限于：

a) 应能对远程访问企业内部网络的用户行为进行行为审计和数据分析；

b) 应对审计进程进行保护，防止未经授权的中断；

c) 审计记录的留存时间应不少于 6 个月。

配置管理要求包括但不限于：

a) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

安全事件处置要求包括但不限于：

a) 对造成业务中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

应急要求包括但不限于：

a) 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b) 应定期开展网络安全应急演练，检验应急预案的可操作性，并结合应急演练结果，对应急预案进行评估和适用性修订；

c) 应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感

信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。

3.2.6 物理和环境安全要求

3.2.6.1 物理位置选择

a) 在机房选址及设计时，满足 GB 50174 的相关规定；

b) 确保工业互联网标识解析服务器及运行关键业务和数据的物理设备位于境内。

3.2.6.2 物理访问控制

除包括 3.1.6.2 基本级防护要求之外，还应包括但不限于：

a) 应对机房划分区域并在不同区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

3.2.6.3 防盗窃和防破坏

除包括 3.1.6.3 基本级防护要求之外，还应包括但不限于：

应对机房设置监控报警系统。

3.2.6.4 防雷击

同 3.1.6.4 基本级防护要求。

3.2.6.5 防火

a) 机房及工业互联网标识解析系统相关设备放置场地应设置灭火设备和火灾自动报警系统，能够自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

3.2.6.6 防水和防潮

除包括 3.1.6.6 基本级防护要求之外，还应包括但不限于：

应安装对水敏感的检测仪表或元件，对机房及工业互联网标识解析系统相关设备放置场地进行防水检测。

3.2.6.7 防静电

应满足 YD/T 1754-2008 中 3.3.7 的相关要求。

3.2.6.8 温湿度控制

同 3.1.6.8 基本级防护要求

3.2.6.9 电力供应

应满足 YD/T 1754-2008 中 3.3.10 的相关要求。

3.2.6.10 电磁防护

同 3.1.6.10 基本级防护要求

2-4 工业互联网企业数据安全防护规范（试行）

目　　录

工业互联网企业数据安全防护规范（试行）

1 工业互联网企业数据安全防护范围及内容

1.1 工业互联网企业数据安全防护范围

工业互联网企业数据安全防护的范围包括联网工业企业、工业互联网平台企业、工业互联网标识解析企业等企业，在工业互联网这一新模式新业态下产生或使用的数据。

同一工业互联网企业可能存在不同级别的数据，需要在网络安全防护的基础上，专门针对数据开展分级安全防护。

1.2 工业互联网企业数据安全防护内容

工业互联网企业数据安全防护内容具体包括：

（1）工业互联网企业数据分类：包括联网工业企业数据分类、工业互联网平台企业数据分类、工业互联网标识解析企业数据分类等。

（2）工业互联网企业数据分级：包括一、二、三级工业互联网数据的分级方法等。

（3）工业互联网企业数据通用安全防护要求：包括安全管理制度和机构、人员管理、系统与设备安全管理、供应链安全管理、安全评估、日志留存、安全审计、应急处置等。

（4）一级工业互联网数据安全防护要求：包括一级数据采集、传输、存储、处理、交换共享与公开披露、归档与销毁等全生命周期安全防护要求。

（5）二级工业互联网数据安全防护要求：在一级数据安全防护的基础上，从数据采集、传输、存储、处理、交换共享与公开披露、归档与销毁等全生命周期提出安全防护要求。

（6）三级工业互联网数据安全防护要求：在二级数据安全防护的基础上，从数据采集、传输、存储、处理、交换共享与公开披露、归档与销毁等全生命周期提出安全防护要求。

2 工业互联网企业数据分类

联网工业企业结合研发设计、生产制造、运维、管理等环节，工业互联网平台企业与工业互联网标识解析企业结合服务运营模式，分析梳理各类企业的工业互联网相关业务流程和系统设备，考虑行业要求、业务规模、数据来源和用途等实际情况，对工业互联网数据进行分类识别，形成工业互联网数据分类清单。

2.1 联网工业企业数据分类

联网工业企业结合研发设计、生产制造、运维、管理等环节，对数据进行分类，包括但不限于研发域数据、生产域数据、运维域数据、管理域数据、外部域数据等数据类型。

2.1.1 研发域数据

a) 研发设计数据：研发设计过程中产生的数据，包括但不限于研发知识数据、产品模型、设计图纸、协同研发数据等；

b) 开发测试数据：开发测试过程中产生的数据，包括但不限于开发代码、测试用例、功能性能测试数据、安全测试数据等。

2.1.2 生产域数据

a) 控制信息：工业互联网环境下与生产控制过程相关的系统及设备所产生的各类数据，包括但不限于 SCADA、DCS、PLC 等系统及设备的计算或分析结果、控制指令、告警信号等；

b) 工况状态：与工业现场设备的实时运行状态相关的各类数据，包括但不限于设备运行监测数据、设备故障数据等；
c) 工艺参数：完成工业互联网业务所需工艺的一系列基础数据或者指标，包括但不限于温湿度、压强、电流、电压、功率、高度、速度、位置等；
d) 系统日志：工业现场设备、应用系统运行过程中所产生的日志数据，包括但不限于设备登录日志、运维操作日志、故障告警日志等。

2.1.3 运维域数据

a) 物流数据：物品从供应地向接收地的实体流动过程中，根据实际需要在物流过程中产生的数据，包括但不限于交通数据、物流公司数据、贸易信息、物品流转路径信息、每日运价指数等；
b) 产品售后服务数据：产品出售以后所提供的各种运维等服务活动产生的数据，包括但不限于维修服务数据、售后咨询数据、售后服务评价数据等。

2.1.4 管理域数据

a) 系统设备资产信息：应用系统、设备等资产登记入库信息及其正常运行所需的配置数据，包括但不限于资产库信息、系统使用的 IP 地址与端口号、系统账号信息等；
b) 产品供应链数据：产品上下游供应链中所涉及的数据，包括但不限于供货商数据、制造商数据、仓储商数据、运输商数据、分销商数据、零售商数据、服务商数据、终端客户数据等；
c) 业务统计数据等：企业相关业务的统计数据，包括但不限于用户数量、联网设备数量、服务行业数量、设备运行效率、产能统计数据等。

2.1.5 外部域数据

与其他企业交互的数据：包括但不限于本企业与其他企业进行交换、共享、交易等相关数据。

2.2 工业互联网平台企业数据分类

工业互联网平台企业结合平台相关服务运营模式对数据进行分类，包括但不限于平台运营域数据和企业管理域数据等数据类型。

2.2.1 平台运营域数据

a) 物联采集数据：工业互联网平台通过工业互联网通信协议采集的来自其他企业的数据，包括但不限于从工业现场所采集的各类数据、企业上云数据等；
b) 知识库模型库数据：为指导或保证工业互联网业务正常或最优运行所需要的各类知识与模型数据，包括但不限于标准政策、专家知识库、计算分析模型、地理信息数据、气象数据等。

2.2.2 企业管理域数据

a) 客户与产品信息：业务运营过程中所采集、使用的与客户、产品相关的数据，包括客户信息、用户身份鉴别信息、产品手册等；
b) 业务合作数据：为满足业务运营需要及支撑业务运行的各类合作相关数据，包括但不限于企业基础信息、合作内容、合作业务信息等；
c) 人事财务数据：人力资源信息、财务状况和经营业绩等相关数据，包括但不限于人员招聘考勤信息、人员教育培训信息、人员薪酬、合同、财政收支等。

2.3 工业互联网标识解析企业数据分类

工业互联网标识解析企业结合标识解析相关服务运营模式对数据进行分类，包括但不限于标识解析运营域数据和企业管理域数据等数据类型。

2.3.1 标识解析运营域数据

a) 标识数据：标识编码本身的数据，包括但不限于 Handle 体系中的前缀/后缀、DNS 体系中的域名等；
b) 标识运营数据：标识解析服务过程中所产生的数据，包括但不限于标识运营服务数据等；
c) 标识解析数据：标识解析过程中单个标识编码关联的数据，包括但不限于每个标识对应的属性值等。

2.3.2 企业管理域数据

同 2.2.2 防护要求。

3 工业互联网企业数据分级

a) 企业应根据不同类别工业互联网数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益、国家安全等带来的最大后果影响，将工业互联网数据分为一级、二级、三级共 3 个级别，三级数据的安全防护要求最高；
b) 企业应在数据产生阶段确定数据的类别和级别。对拟定为二级、三级的数据，企业应组织专家评审数据分类分级情况，并对评定为二级、三级的数据，做好企业基本信息、数据分类分级结果、数据安全防护措施、数据流动路径等相关情况的记录；
c) 企业应定期复查工业互联网数据分类分级情况，出现企业生产经营重大变化、系统改建等导致数据管理情况、数据流动情况、数据级别发生变化的，应及时更新数据分类分级清单和相关情况记录。

3.1 一级数据

指一旦遭泄露、丢失、滥用、篡改或未经授权共享、销毁等，可能对工业生产运营、社会稳定、经济发展等造成较小影响或无影响的数据。

3.2 二级数据

指一旦遭泄露、丢失、滥用、篡改或未经授权共享、销毁等，可能对工业生产运营、社会稳定、经济发展等造成严重后果的数据。

3.3 三级数据

指一旦遭泄露、丢失、滥用、篡改或未经授权共享、销毁等，可能对工业生产运营、社会稳定、经济发展等造成特别严重后果的数据，或者影响国家安全的数据。

工业互联网企业数据分级判定条件详见附件 A。工业互联网企业数据分类分级清单示例详见附件 B。

4 工业互联网企业数据安全防护要求

4.1 工业互联网数据通用安全要求

4.1.1 安全管理制度和机构

a) 应制定工业互联网数据安全相关管理制度规范，并及时根据法规政策要求、数据安全防护需求等，定期更新修订制度规范；
b) 应明确工业互联网数据安全管理责任部门，负责统筹开展数据安全管理工作，包括制定数据安全管理制度规范、制定年度数据安全工作计划、协调数据安全管理相关

部门建立数据安全防护措施、组织开展数据安全评估、提出数据保护的对策建议、监督检查数据安全管理制度规范执行落实情况等；

c) 应根据数据安全管理相关部门和岗位的职责，明确数据安全授权审批事项、审批部门和审批人等。

4.1.2 人员管理

a) 应明确企业数据安全管理责任人，负责指导数据安全管理责任部门、协调各相关部门开展数据安全工作；

b) 应在数据安全管理责任部门和相关部门配备数据安全专职人员，负责数据安全管理制度执行落实、资产管理、安全审计、应急处置等工作；

c) 应在人员录用、调离等过程中，对涉及数据安全工作的人员身份、背景、专业资质、涉密情况等开展审查，录用时应对其技术技能进行考查；

d) 应定期开展数据安全宣传教育与技能培训，提高人员数据安全意识和专业技能。

e) 应根据人员角色（包括内部人员、外部合作人员、运维人员等），加强对数据的访问控制；

f) 应对数据安全关键岗位（如权限审批、安全审计、开发测试等）设立双人双岗。

4.1.3 系统与设备安全管理

a) 系统设备（服务器、交换机等）接入前，需由安全管理机构对设备的涉密情况、基本配置情况、用途、安装的软件、使用的端口和服务、MAC 地址等登记备案并进行安全审核，合格后方可入网与处理信息；

b) 系统设备应根据业务需求和安全级别设置用户访问控制策略，用户权限应执行分类分级、权限最小化、权限执行一致性等原则；

c) 系统设备的用户口令应按照安全管理规定设置，并定期修改；

d) 应定期进行漏洞扫描，及时修补发现的系统安全漏洞；

e) 应采用边界防护、入侵防范、身份鉴别、安全审计等措施，加强承载工业互联网数据的系统与设备安全，并对系统与设备定期开展安全检测与运维管理。

4.1.4 供应链安全管理

a) 应制定供应链安全管理方案，并明确供应链涉及的数据的安全风险控制措施；

b) 应在选择工业互联网规划、设计、建设、运维等服务商时，以合同等方式明确服务商应承担的安全责任和义务，以保密协议等方式要求服务商做好保密工作，防范敏感数据外泄。

4.1.5 安全评估

a) 应建立数据安全评估相关制度规范，定期开展数据安全评估，评估的内容包括但不限于数据管理能力、数据安全能力、数据安全防护能力等情况，分析数据被未经授权的访问、控制、处理或数据被泄露、窃取、篡改、滥用等风险，并形成相应的数据安全评估报告；

b) 应在新业务上线，数据迁移、数据出境、数据开放共享等重大操作行为，涉及第三方管理等情况下，启动数据安全评估工作，分析可能存在的风险、造成的问题和影响等，并形成相应的数据安全评估报告；

c) 应及时整改数据安全评估中发现的风险隐患和问题。

4.1.6 日志留存

a) 应对数据采集、迁移、跨境、开放共享、销毁等环节实施日志留存管理；

b) 日志记录信息应包括执行时间、操作账号、处理方式、授权情况、登录信息等，并确保日志记录完整、准确；
c) 日志的留存时间应满足国家相关法律法规要求，不低于 6 个月；
d) 应对日志操作进行权限控制，配备日志审计员加强日志访问和处理管理。

4.1.7 安全审计

a) 应建立数据安全审计相关制度，明确审计目的、审计对象、审计操作规程、审计频度、审计内容、审计结果规范等；
b) 应明确数据安全审计工作涉及部门和人员的权限、责任以及相关权限的授予规程。
c) 应明确数据安全审计的内容，包括但不限于企业内部权限控制、企业数据流动跟踪情况、数据安全事件、数据安全防护措施有效性等；
d) 应在数据安全审计过程中准确记录对数据的操作时间、操作地点、操作人、操作方式、操作的数据内容等信息，以及审计发现的相关安全事件；
e) 应记录并形成数据安全审计报告，并及时整改审计发现的问题。

4.1.8 应急处置

a) 应制定数据安全相关应急管理制度，建立数据安全应急处置工作机制；
b) 应在网络安全相关应急预案中明确数据安全事件应急措施，并在相关应急演练中有针对性的开展数据安全应急演练；
c) 应在发生数据安全事件时及时按照应急管理制度和应急预案采取应急措施；
d) 应在发生重大数据安全事件时，立即启动应急响应机制并进行处置。

4.2 一级工业互联网数据全生命周期安全要求

4.2.1 数据采集安全

a) 数据采集应符合“合法正当、权责一致、目的明确、最小够用”原则；
b) 根据数据采集需求，数据采集者应与数据所有者明确采集目的、方式、数量、用途、获取源、接收方、范围、频率和周期等，确立数据采集规则，保障采集数据的安全可用；
c) 数据采集时应标记数据的级别。

4.2.2 数据传输安全

a) 必要情况下，采用密码技术、数据脱敏、校验技术、数字签名等技术，保证传输数据的保密性、完整性、可用性；
b) 在数据迁移前对数据进行本地备份和安全评估，保证数据迁移不影响业务应用的连续性；
c) 在数据迁移、上云、跨境等传输过程中，开展数据安全监测。

4.2.3 数据存储安全

a) 应根据存储数据量、数据重要性、数据敏感程度等因素，选择合适的存储介质，实施数据存储介质安全管控或数据碎片化存储；
b) 应能够检测到数据在存储过程中保密性、完整性、可用性受到破坏，防止数据被泄露、篡改、删除、插入等操作。在数据受到破坏时，应向授权用户提供可察觉的告警信息；
c) 实施分类分级存储，对确需加密的数据可采用加密技术、数字签名、校验技术等技术，实现存储数据的保密性、完整性和可用性；
d) 必要情况下，提供数据本地灾难备份与恢复功能。备份数据应与原数据具有相同的

访问控制权限和安全存储要求；

e) 对存储数据的使用进行身份鉴别和访问控制。

4.2.4 数据处理安全

a) 应对数据的处理使用进行授权和验证；

b) 应建立数据导入导出过程保护和回退机制，在导入导出过程中发生问题时应能够有效还原和恢复数据。

4.2.5 数据交换共享与公开披露安全

应在数据交换共享与公开披露前对数据进行安全评估，并根据评估情况采取相应的防护措施，确保数据交换共享与公开披露安全。

4.2.6 数据归档与销毁安全

a) 应对访问频率极低的数据进行归档，建立归档数据保护机制，防止数据被篡改和删除；

b) 应采用硬盘格式化等技术手段，确保数据销毁；

c) 数据归档与销毁日志的留存时间不少于 6 个月。

4.3 二级工业互联网数据全生命周期安全要求

4.3.1 数据采集安全

除包括 4.2.1 安全防护要求外，还应包括但不限于：

在数据采集前，应对数据采集所涉及的软硬件工具、设备、系统、平台、接口以及采集技术等，采取必要的测试、认证、鉴权等措施，确保数据采集的合规性和执行上的一致性。对数据采集行为进行监控与审计，一旦发现异常行为需及时告警。

4.3.2 数据传输安全

除包括 4.2.2 安全防护要求外，还应包括但不限于：

a) 采用密码技术、数据脱敏、校验技术、数字签名等技术，保证数据在传输过程中的保密性、完整性、可用性；

b) 应能够检测到数据在传输过程中保密性、完整性、可用性受到破坏，并在检测到数据被破坏时，采取必要的恢复措施；

c) 应采用 SSL、TLS 等安全协议进行数据传输；

d) 应在数据迁移前对数据开展本地备份及恢复相关工作，做好数据迁移安全评估与安全控制，防止迁移过程中因突发状况导致数据丢失，避免影响业务应用的连续性；应在数据迁移、上云、跨境等传输过程中，开展数据安全监测，能够对网络流量行为、攻击威胁、数据泄露或篡改等进行分析和研判。

4.3.3 数据存储安全

除包括 4.2.3 防护要求外，还应包括但不限于：

a) 应实施分类分级存储，采用加密技术等方式，实现存储数据的保密性、完整性和可用性；

b) 应能够检测到数据在存储过程中保密性、完整性、可用性受到破坏，在检测到数据被破坏时，及时进行告警并采取必要的恢复措施；

c) 应提供有效的虚拟机镜像文件加载保护机制，保证即使虚拟机镜像被窃取，非法用户也无法直接在其计算资源上进行挂卷运行；

d) 应建立数据本地及异地灾难备份与恢复机制，定期开展全量数据、增量数据备份。

定期对数据进行恢复测试，确保能够及时、完整、准确地恢复数据。

4.3.4 数据处理安全

除包括 4.2.4 防护要求外，还应包括但不限于：

a) 应采用恶意代码检测、身份鉴别、访问控制等技术手段保障处理数据的平台、系统、工具、APP 等安全；
b) 应在不影响数据加工与分析的情况下，对数据脱敏后再进行处理；
c) 应对数据的处理使用进行审计，并形成审计日志。

4.3.5 数据交换共享与公开披露安全

除包括 4.2.5 防护要求外，还应包括但不限于：

a) 应建立数据交换共享安全监控措施，对交换共享的数据及数据交换共享行为等进行监控，确保交换共享的数据合理规范使用，未超出授权范围；
b) 应采用数据标注、水印等溯源技术，对数据流经节点及共享流转过程中的篡改、泄露、滥用等行为进行溯源；
c) 应根据交换共享或公开披露的数据特点、应用场景等选择合适的脱敏方法，并对数据脱敏有效性进行评估，保证数据脱敏完全以及脱敏后数据的可用性。

4.3.6 数据归档与销毁安全

除包括 4.2.6 防护要求外，还应包括但不限于：

a) 应建立数据销毁审批机制，设置数据销毁相关监督角色、监督操作过程等；
b) 应采用硬盘格式化、多次擦写、消磁等技术手段，确保数据完全销毁，不留痕迹，不能恢复；
c) 应完全清除数据导入导出通道中的数据，并在数据存储空间被释放或重新分配前完全清除数据，防止数据被恶意恢复。

4.4 三级工业互联网数据全生命周期安全要求

4.4.1 数据采集安全

同 4.3.1 防护要求。

4.4.2 数据传输安全

除包括 4.3.2 防护要求外，还应包括但不限于：

a) 应采用密码技术、数据脱敏、校验技术、数字签名等技术，保证数据在传输阶段的保密性、完整性、可用性。必要情况下，应采用隔离技术等手段进行单向数据传输；
b) 应采用 SSL、TLS 等安全协议进行数据传输，必要情况下，采用 VPN 或物理专网传输数据。

4.4.3 数据存储安全

除包括 4.3.3 防护要求外，还应包括但不限于：

a) 应建立数据本地及异地灾难备份与恢复机制，全量数据备份至少每周一次，增量数据备份至少每天一次，备份数据应与原数据具有相同的访问控制权限和安全存储要求；
b) 应定期对数据进行恢复测试，确保能够及时、完整、准确地恢复数据。

4.4.4 数据处理安全

除包括 4.3.4 防护要求外，还应包括但不限于：

a) 应在不影响数据加工与分析的情况下，对数据脱敏后再进行处理，支持数据处理使

用过程中的动态脱敏；

b) 应在不影响数据加工与分析的情况下，对需要用到的知识机理、数字化模型、算法、工具等进行测验分析，确保数据处理结果的准确性和安全性。

4.4.5 数据交换共享与公开披露安全

原则上不允许交换共享与公开披露，确需交换共享与公开披露的数据应严格控制知悉范围，并满足 4.3.5 中的数据安全防护要求。

4.4.6 数据归档与销毁安全

除包括 4.3.6 防护要求外，还应包括但不限于：

应采用粉碎、拆解等方式，实现物理销毁存储介质，并在保证数据完全删除后，再销毁废弃存储介质，确保以不可逆的方式销毁数据。

附件 A：工业互联网企业数据分级判定条件

在工业互联网数据分级时，应判断数据保密性、可用性、完整性任一属性遭破坏后，对客体造成的后果影响程度，采用“就高不就低”原则，将数据分为一级、二级、三级共3个安全级别，三级数据的安全防护要求最高。客体包括国家安全，公民生命健康安全，国民经济、社会秩序和公共利益，企业核心商业秘密，工业生产运营安全，公民、法人和其他组织的合法权益等。

1.后果影响符合下列条件之一的，数据安全级别定为三级数据：

1）数据保密性遭到破坏，使数据信息泄露或丢失，威胁国家安全；造成大量企业核心商业秘密泄露或丢失，对企业运营造成特别严重影响；

2）数据可用性遭到破坏，使数据访问受限或不可用，对工业控制系统及设备、工业互联网平台、通信网络、标识解析网络等的正常运行造成特别严重损害，引发大面积网络瘫痪或系统平台崩溃事件；

3）数据完整性遭到破坏，使数据被篡改，引发特别严重的生产安全事故，威胁公民生命健康安全甚至造成人员伤亡；

4）数据保密性或可用性或完整性遭到破坏，对国民经济、社会秩序、公共利益等造成特别严重损害，会造成5000万元以上的直接经济损失，难以恢复工业互联网运行或消除负面影响。

2.后果影响符合下列条件之一的，数据安全级别定为二级数据：

1）数据保密性遭到破坏，造成企业核心商业秘密泄露或丢失，对企业运营造成严重影响；

2）数据可用性遭到破坏，使数据访问受限或不可用，对工业控制系统及设备、工业互联网平台、通信网络、标识解析网络等的正常运行造成严重损害，引发小范围网络瘫痪或系统平台崩溃事件；

3）数据完整性遭到破坏，使数据被篡改，引发严重的生产安全事故，对公民生命健康安全构成的威胁较小；

4）数据保密性或可用性或完整性遭到破坏，对国民经济、社会秩序、公共利益等造成严重损害，会造成1000万元以上5000万元以下的直接经济损失，恢复工业互联网数据或消除负面影响的难度较大；对公民、法人和其他组织的合法权益造成严重损害，受影响的数量多、范围大、持续时间长，会引发级联效应。

3.后果影响符合下列条件之一的，数据安全级别定为一级数据：

1）数据保密性遭到破坏，造成非企业核心商业秘密泄露或丢失，对企业运营影响较小；

2）数据可用性遭到破坏，使数据访问受限或不可用，对工业控制系统及设备、工业互联网平台、通信网络、标识解析网络等的正常运行的影响较小；

3）数据完整性遭到破坏，使数据被篡改，会造成生产安全隐患，但未引发生产安全事故；

4）数据保密性或可用性或完整性遭到破坏，对国民经济、社会秩序、公共利益等造成严重损害，会造成一定的经济损失，恢复工业互联网数据或消除负面影响的难度较小；对公民、法人和其他组织的合法权益造成损害较小。

附件 B：工业互联网企业数据分类分级示例

责任主体	数据类别	数据子类分类参考	数据分级参考
工业企业	研发域数据	研发设计图纸文档	三级研发设计图纸
			二级研发设计图纸
			一级研发设计图纸
		产品模型文件	三级产品模型文件
			二级产品模型文件
			一级产品模型文件
		开发测试代码	三级开发测试代码
			二级开发测试代码
			一级开发测试代码
工业企业	生产域数据	生产监控数据	三级生产监控数据
			二级生产监控数据
			一级生产监控数据
		工业控制信息	三级工业控制信息
			二级工业控制信息
			一级工业控制信息
		工况状态	三级工况状态
			二级工况状态
			一级工况状态
		工艺参数	三级工艺参数
			二级工艺参数
			一级工艺参数
		系统日志	三级系统日志
			二级系统日志
			一级系统日志
工业企业	运维域数据	物流数据	二级物流数据
			一级物流数据
		产品售后运维服务数据	二级产品售后运维服务数据
			一级产品售后运维服务数据
工业企业	外部域数据	外部交换数据	三级外部交换数据
			二级外部交换数据
			一级外部交换数据
工业企业、工业互联网平台企业、工业互联网标识解析企业	管理域数据	规划与制度规范文件	二级规划与制度规范文件
			一级规划与制度规范文件
		固定资产信息	二级固定资产信息
			一级固定资产信息
		财务数据（合同、财政收支）	二级财务数据

			一级财务数据
		人力与客户信息	二级人力与客户信息
			一级人力与客户信息
		资源管理与业务统计数据（订单、仓储、排产）	三级资源管理与业务统计数据
			二级资源管理与业务统计数据
			一级资源管理与业务统计数据
		供应链数据	三级供应链数据
			二级供应链数据
			一级供应链数据
工业互联网平台企业	平台运营域数据	物联采集数据	三级物联采集数据
			二级物联采集数据
			一级物联采集数据
		知识库模型库数据	三级知识库模型库数据
			二级知识库模型库数据
			一级知识库模型库数据
		平台运行与服务数据	三级平台运行与服务数据
			二级平台运行与服务数据
			一级平台运行与服务数据
工业互联网标识解析企业	标识运营域数据	标识数据	三级标识数据
			二级标识数据
			一级标识数据
		标识解析数据	三级标识解析数据
			二级标识解析数据
			一级标识解析数据
		标识运营数据	三级标识运营数据
			二级标识运营数据
			一级标识运营数据

注：工业互联网企业应根据自身实际情况开展数据分类分级，并定期更新数据分类分级清单。