|  |  |
| --- | --- |
| ICS | 35.020 |
| CCS | L04 |

中华人民共和国国家标准

GB/T XXXXX—XXXX



工业互联网企业网络安全 第2部分：平台企业防护要求

Industrial Internet Enterprise Cyber Security Part 2: Protection Requirements of Industrial Internet Platform Enterprise

(点击此处添加与国际标准一致性程度的标识)

XXXX - XX - XX发布

XXXX - XX - XX实施

`

目次

[前言 II](#_Toc104671585)

[引言 III](#_Toc104671586)

[1 范围 1](#_Toc104671587)

[2 规范性引用文件 1](#_Toc104671588)

[3 术语和定义 1](#_Toc104671589)

[4 缩略语 2](#_Toc104671590)

[5 工业互联网平台企业安全防护范围及内容 2](#_Toc104671591)

[6 工业互联网平台企业安全防护级别的确定 2](#_Toc104671592)

[7 工业互联网平台企业安全防护要求 3](#_Toc104671593)

[7.1 基本级防护要求 3](#_Toc104671594)

[7.2 增强级防护要求 17](#_Toc104671595)

[参考文献 27](#_Toc104671596)

1. 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》的规定起草。

本文件是GB/T xxx《工业互联网企业网络安全》的第3部分。

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会（SAC/TC485）归口。

本文件起草单位：中国信息通信研究院、国家工业信息安全发展研究中心、中国电子信息产业发展研究院、中国工业互联网研究院、中国电子技术标准化研究院、北京航空航天大学、上海宝信软件股份有限公司、海尔卡奥斯物联生态科技有限公司、腾讯云计算北京有限责任公司、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、北京天融信网络安全技术有限公司、南京中新赛克科技有限责任公司、国能大渡河流域水电开发有限公司、郑州信大捷安信息技术股份有限公司、北京珞安科技有限责任公司、富士康工业互联网股份有限公司、国网河南省电力公司、国网电商科技有限公司、北京六方云信息技术有限公司、北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、北京升鑫网络科技有限公司、西安热工研究院有限公司、上海电器科学研究所（集团）有限公司、北京信安世纪科技股份有限公司。

本文件主要起草人：

1. 引言

工业互联网企业数量众多、信息化发展程度不同且承载业务类型相异，所属行业网络安全防护规律差异化明显，现有网络安全防护要求无法满足工业互联网企业发展实际需求，因此要实施工业互联网企业网络安全分类分级管理并编制相关标准。

GB/T XXXXX-XXXX 《工业互联网企业网络安全》标准作为工业和信息化部开展工业互联网企业网络安全分类分级管理工作的重要支撑，针对应用工业互联网的工业企业、工业互联网平台企业、工业互联网标识解析企业及企业数据安全，提出不同级别的网络安全管理及安全防护技术要求，指导企业落实与自身级别相适应安全防护措施，加强网络安全能力建设。

GB/T XXXXX-XXXX 《工业互联网企业网络安全》标准拟由4部分构成：

第1部分：应用工业互联网的工业企业防护要求

第2部分：平台企业防护要求

第3部分：标识解析企业防护要求

第4部分：数据防护要求

本文件为工业互联网企业网络安全系列标准的第2部分。

本文件作为工业互联网企业网络安全分类分级管理支撑系列标准之一，面向工业互联网平台的建设和运营者，综合考虑安全技术和管理等各方面要求，提出了不同等级安全防护要求。协助有关部门掌握不同等级工业互联网平台企业业务现状以及面临的安全风险，为主管部门开展分类分级工作提供依据，指导企业落实与自身级别相适应安全防护措施，为工业互联网平台企业建设、运营及强化网络安全防护能力奠定基础，提升工业互联网安全保障能力。

工业互联网企业网络安全 第2部分：平台企业防护要求

* 1. 范围

本文件规定了工业互联网平台企业网络安全防护的范围和内容，针对工业互联网平台企业提出不同等级安全防护要求，内容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、数据安全、安全管理以及物理和环境安全。

本文件适用于工业互联平台企业开展工业互联网企业网络安全分类分级防护工作。

* 1. 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 25069-2022 | 信息安全技术 术语 |
| GB 50174-2017 | 数据中心设计规范 |
| GB/T XXXXX-XXXX | 工业互联网企业网络安全 第4部分：数据安全防护要求 |

* 1. 术语和定义

GB/T 25069-2022、GB/T 22239-2019界定的以及下列术语和定义适用于本文件。

工业互联网平台企业 Industrial Internet platform enterprise

包括工业互联网平台的建设者和运营者。

安全防护 network security protection

通过技术和管理手段保护工业互联网平台企业相关系统的完整性、保密性、可用性免受外部破坏。

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 22239-2019，定义3.1]

工业APP industrial Internet application

工业APP是基于工业互联网，承载工业知识和经验，满足特定需求的开放给第三方进行下载、安装、卸载的工业应用软件，是面向工业产品全生命周期相关业务（设计、生产、实验、使用、保障、交易、服务等）的需求把工业产品及相关技术过程中的知识、最佳实践及技术诀窍封装成的应用软件。工业APP不包括工控系统、工业设备终端的嵌入式软件。

* 1. 缩略语

下列缩略语适用于本文件。

|  |  |  |
| --- | --- | --- |
| APP | 应用程序 | Application |
| API | 应用程序接口 | Application Programming Interface |
| CNVD | 国家信息安全漏洞共享平台 | China National Vulnerability Database |
| CVE | 公共漏洞和暴露 | Common Vulnerabilities & Exposures |
| CNNVD | 国家信息安全漏洞库 | Chinav National Vulnerability Database of Information Security |
| CNCVE | 中国国家通用漏洞披露 | China National Common Vulnerabilities and Exposures |
| CPU | 中央处理器 | Central Processing Unit |
| HTTP | 超文本传输协议 | Hyper Text Transfer Protocol |
| GRE | 通用路由协议封装 | Generic Routing Encapsulation |
| PKI | 公钥基础设施 | Public Key Infrastructure |
| IP | 网际互连协议 | Internet Protocol |
| SSL | 安全套接层 | Secure Socket Layer |
| VLAN | 虚拟局域网 | Virtual Local Area Network |
| VxLAN | 虚拟扩展局域网 | Virtual Extensible Local Area Network |

* 1. 工业互联网平台企业安全防护范围及内容

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：主要指针对网关等接入设备提出安全防护规范，包括接入设备安全、接入层网络安全等方面。
2. 基础设施层安全防护：包括计算环境安全、网络安全、虚拟化安全等方面。
3. 平台层安全防护：包括微服务组件安全、平台应用开发环境安全、容器安全等方面。
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方面。
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方面。
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、安全运维管理等方面。
7. 物理和环境安全要求：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、电磁防护等方面。
   1. 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依据企业平台服务行业的网络安全影响程度、平台业务范围、平台业务规模、平台一旦发生网络安全事件的影响程度进行级别划分，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：

1. 三级工业互联网平台企业应采取增强级防护措施。
2. 二级工业互联网平台企业应采取基本级防护措施。
3. 一级工业互联网平台企业宜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。
   1. 工业互联网平台企业安全防护要求
      1. 基本级防护要求
         1. 接入层安全防护要求
            1. 接入设备安全防护要求

口令账号安全

口令账号安全要求包括：

1. 对于采用静态口令认证技术的设备，口令长度应至少8位，并包含数字、大写字母、小写字母、特殊字符4类中至少3类，且应与帐号无相关性，同时应定期更换口令，更换周期不大于90天；
2. 不应启用默认帐号，如遇特殊需要必须启用默认帐号，应将默认帐号的权限进行最小化限制；
3. 对于具备字符交互界面或Web管理界面的设备，应配置定时帐号自动登出；
4. 应删除或锁定与设备运行、维护等工作无关的帐号。

设备硬件安全

安全配置要求包括：

1. 设备应具备独立的安全运行区域，用于密钥的生成、存储、使用等，不与非安全运行区域共享存储空间，防止篡改或非法获取；
2. 应使用物理方式移除或覆盖硬件接口、敏感引脚等关键信息，避免硬件调试接口直接暴露在外；
3. 设备调试接口默认配置为禁用或设置密码，且密码应具有一定的复杂度。

身份鉴别

身份鉴别安全要求包括：

1. 接入设备应具备唯一标识符，应采用鉴别机制对接入工业互联网平台中的设备接入身份进行鉴别，确保接入设备为已授权的合法设备；
2. 应对设备远程管理设置身份认证措施。

访问控制

访问控制安全要求包括：

1. 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；
2. 应在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限；
3. 对于设备的远程管理过程，应使用加密协议，禁止使用明文传输；
4. 设备远程管理应设置访问控制权限，系统管理、安全审计等应为不同权限账户。

安全审计

安全审计要求包括：

1. 应配置日志功能，对用户登录设备的操作进行记录；
2. 审计范围应覆盖设备所有用户；
3. 审计内容应包括重要用户行为、重要操作命令的使用等重要安全事件的时间、主体标识、客体标识和结果等；
4. 应统一时钟，保证日志功能记录时间的准确性；
5. 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；
6. 审计记录留存时间不少于6个月。

入侵防范

入侵防范安全要求包括：

1. 应对非授权设备的接入行为进行告警；
2. 应定期对设备固件进行安全增强，对漏洞进行修复；
3. 设备应具备入侵防范措施，包括但不限于开启防火墙功能等。
   * + - 1. 接入层网络安全防护要求

访问控制

访问控制安全要求包括：

1. 应在网络边界对源地址、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；
2. 网络边界应配置安全访问控制，过滤已知安全攻击数据包；
3. 应删除多余或无效的访问控制规则，优化访问控制列表；
4. 应进行安全区域划分，根据平台不同服务的类型、功能及租户的不同划分不同的子网、网段或安全组；
5. 设备应关闭不需要的服务端口，避免开放高危端口，避免使用不安全的服务；
6. 应对短时间内会话连接次数进行限制，对非法登录等情况采取及时结束对话、自动退出等安全措施。

安全审计

安全审计要求包括：

1. 应对来自外网的所有流量进行安全审计，配置流量日志记录功能，记录通过安全设备的网络连接的信息；
2. 对于接入层边界安全防护设备应配置日志记录功能；
3. 应统一时钟，保证日志功能记录时间的准确性；
4. 审计记录应包括网络安全攻击事件的日期和时间、用户、事件类型及其他与审计相关的信息；
5. 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，审计日志应至少保存六个月。

通信安全

通信安全要求包括：

1. 设备与工业互联网平台及其他应用建立通信时，应使用双向身份鉴别的方式，防止未授权的访问；
2. 设备在网络通信过程中应使用加密的方式，保证传输数据的保密性。

恶意代码防范

恶意代码防范安全要求包括：

网络侧应具有恶意代码防护能力。

入侵防范

入侵防范安全要求包括：

1. 应具备检测网络攻击行为的能力，并过滤已知的网络攻击数据包；
2. 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及时告警。
   * + 1. 基础设施层安全防护要求
          1. 计算环境安全防护要求

身份鉴别

身份鉴别安全要求包括：

1. 应对计算环境的运维用户进行身份标识和鉴别；
2. 计算环境管理用户身份标识应具有不易被冒用的特点，口令应满足复杂度要求并定期更换；
3. 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；
4. 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；
5. 当对计算环境进行远程管理时，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

访问控制安全要求包括：

1. 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；
2. 应关闭服务器不使用的端口，防止非法访问；
3. 应基于白名单机制检测非法运行的进程或程序；
4. 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

安全审计要求包括：

1. 审计范围应覆盖到服务器上的每个用户；
2. 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；
3. 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；
4. 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；
5. 审计记录留存时间不少于6个月；
6. 应能够根据记录数据进行分析，并生成审计报表；

资源控制

资源控制安全要求包括：

1. 应根据安全策略，设置登录终端的会话数量；
2. 应根据安全策略设置登录终端的操作超时锁定；
3. 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

恶意代码防范安全要求包括：

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

入侵防范安全要求包括：

1. 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；
2. 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；
3. 应支持对数据库攻击行为进行检测和防护；
4. 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。

其他安全

其他安全防护要求包括：

应制定平台计算环境的安全基线，定期检查。

* + - * 1. 网络安全防护要求

网络拓扑结构安全

网络拓扑结构安全防护要求包括：

1. 应绘制与当前运行情况相符的网络拓扑结构图；
2. 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；
3. 应保证接入网络和核心网络的带宽满足业务高峰期需要；
4. 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；
5. 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

访问控制安全要求包括：

1. 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；
2. 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

安全审计要求包括：

1. 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；
2. 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；
3. 应保证所有网络设备的系统时间自动同步；
4. 应对审计记录进行保护，定期备份，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
5. 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

恶意代码防范安全要求包括：

1. 应能够检测到恶意代码的异常行为并及时阻断；
2. 应周期性地维护恶意代码库的升级和检测系统的更新。

网络设备安全

网络设备安全防护要求包括：

1. 应对登录网络设备的用户进行身份鉴别；
2. 应对网络设备的管理员登录地址进行限制；
3. 网络设备用户的标识应唯一；
4. 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

网络安全监测防护要求包括：

1. 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；
2. 应能够支持对持续大流量攻击进行识别、报警和阻断的能力；
3. 应能够监视对平台服务存在的以下攻击行为：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；
4. 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。
   * + - 1. 虚拟化安全防护要求

虚拟机安全

虚拟机安全防护要求包括：

1. 应支持虚拟机之间、虚拟机与宿主机之间的隔离；
2. 应支持虚拟机部署防病毒软件；
3. 应具有对虚拟机恶意攻击等行为的识别并处置的能力；
4. 应支持对虚拟机脆弱性进行检测的能力；
5. 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；
6. 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
7. 应支持发现虚拟机操作系统漏洞的能力，支持漏洞修复；
8. 应提供最新版本的虚拟机镜像和补丁版本。

虚拟机网络安全

虚拟机网络安全防护要求包括：

1. 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；
2. 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；
3. 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；
4. 应采用VxLAN、GRE等手段支持不同租户之间的网络流量隔离；
5. 可支持用户选择使用第三方安全产品。

虚拟化平台安全

虚拟化平台安全防护要求包括：

1. 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；
2. 应保证不同虚拟机之间的虚拟CPU指令隔离；
3. 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；
4. 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）；
5. 应对虚拟机的运行状态、资源占用等信息进行监控；
6. 应支持发现虚拟化平台漏洞的能力，支持漏洞修复；
7. 应支持平台内采用的PKI、SSL认证等各类数字证书实施统一管理，支持用户按需更换。
   * + 1. 平台层安全防护要求
          1. 微服务组件安全防护要求

身份鉴别

身份鉴别安全要求包括：

1. 应对管理微服务组件的用户进行身份标识和鉴别；
2. 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；
3. 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；
4. 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；
5. 应对微服务API接口设置安全的身份鉴别方式。

访问控制

访问控制安全要求包括：

1. 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；
2. 对配置文件及重要数据配置最小的访问控制权限。

安全审计

安全审计要求包括：

1. 审计范围应覆盖到使用微服务组件的每个用户；
2. 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；
3. 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；
4. 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；
5. 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。

安全传输

安全传输防护要求包括：

应使用安全的协议保证接口传输数据的保密性和完整性。

开放接口

开放接口安全防护要求包括：

1. 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；
2. 应对开放接口调用有认证措施；
3. 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。

* + - * 1. 平台应用开发环境安全防护要求

身份鉴别

身份鉴别安全要求包括：

1. 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；
2. 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；
3. 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；
4. 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；
5. 应采用加密方式存储用户的账号和口令信息。

访问控制

访问控制安全要求包括：

1. 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；
2. 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

安全审计要求包括：

1. 审计范围应覆盖到每个用户的关键操作；
2. 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；
3. 应保护审计记录，保证无法删除、修改或覆盖等；
4. 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

资源控制安全要求包括：

1. 具有登录超时处理功能，当登录连接超时自动退出；
2. 应能够对系统的最大并发会话连接数进行限制；
3. 应能够对单个账户的多重并发会话进行限制；
4. 应能够对系统服务水平降低到预先规定的最小值进行检测和报警。

信息保护

信息保护安全要求：

1. 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；
2. 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；
3. 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；
4. 应对通信过程中的敏感信息字段进行加密；
5. 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；
6. 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)进行必要的容灾备份；
7. 应对平台重要系统配置数据进行加密保护；
8. 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；
9. 应对源码进行分级和加密，做好监控和安全审计。

上线前检测

上线前检测要求包括：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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；
6. 对使用的第三方组件库进行漏洞隐患排查。
   * + - 1. 容器安全防护要求

构建安全

容器构建安全防护要求包括：

1. 应仅授予完成必要工作所需的最低权限，不安装没有必要的软件；
2. 使用第三方跟镜像，应考虑来源及其可信度、更新频率、默认安装的软件；
3. 切勿将任何硬编码密钥嵌入容器，应使用Kubernetes或其他密钥管理系统；
4. 应将镜像限制为二进制文件、库、配置文件，避免安装软件包管理器、Unix Shell、编译器和调试器。

分发安全

容器分发安全防护要求包括：

1. 应对镜像添加不可变标签，防止对不同版本的镜像重复使用；
2. 应通过镜像签名增强安全防护；

运行安全

容器运行安全防护要求包括：

1. 应使用自定义或第三方访问控制器来避免部署不安全的容器镜像；
2. 应尽量避免以root等最高权限运行容器，禁止使用特权容器；
3. 应确保主机设备不直接共享给容器；
4. 应确保容器的内存使用合理、正确设置容器上的CPU优先级；

维护安全

容器维护安全防护要求包括：

应定期对容器进行漏洞扫描，根据漏洞严重性、数量、是否有可用的补丁或修补程序、是否影响部署等因素确定漏洞管理标准。

* + - 1. 应用层安全防护要求
         1. 身份鉴别

身份鉴别安全要求包括：

1. 工业APP应提供专用的登录控制模块对登录用户进行身份标识和鉴别，用户身份标识唯一， 登录控制模块具有鉴别信息长度、复杂度检查、登录失败处理功能；
2. 应具备登录超时后的锁定或注销功能。
   * + - 1. 口令安全机制

若工业APP使用过程中涉及用户口令，则具体技术要求如下：

1. 在使用过程中不应以明文形式显示和存储；
2. 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。
   * + - 1. 访问控制

若工业APP涉及用户敏感数据，则应对访问用户提供有效的授权机制，具体技术要求如下：

1. 用户访问的内容不应超出授权的范围；
2. 应限制工业APP用户账号的多重并发会话。
   * + - 1. 安全审计

安全审计要求包括：

1. 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；
2. 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；
3. 应定期针对审计日志进行人工审计；
4. 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。
   * + - 1. 运行安全

运行安全防护要求包括：

1. 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；
2. 应具备安全机制防止程序被反编译、反调试；
3. 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个月及以上的中高危及以上的安全漏洞。
   * + - 1. 安装与卸载安全

安装安全

安装安全防护要求包括：

1. 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；
2. 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；
3. 宜对平台操作系统和其他应用软件的正常运行无影响。

卸载安全

卸载安全防护要求包括：

1. 工业APP卸载后，不应影响工业互联网平台的正常使用；
2. 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；
3. 删除用户使用过程中生成的数据时应有提示；
4. 应对工业互联网平台系统和其他应用软件的功能无影响。
   * + - 1. 其他安全

其他安全防护要求包括：

1. 不应在数据库或文件系统中明文存储用户敏感信息；
2. 不应在Cookie中保存明文口令；
3. 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；
4. 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；
5. 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。
   * + 1. 数据安全防护要求

应按照GB/T XXXXX-XXXX《工业互联网企业网络安全 第4部分：数据安全防护要求》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。

* + - 1. 安全管理
         1. 安全管理制度

安全管理制度安全要求包括：

1. 应依据工业互联网平台企业业务功能与监管单位要求建立安全管理制度；
2. 应制定安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等；
3. 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及时进行修订；
4. 应指定或授权专人负责安全管理制度的制定和修订，并通过正式流程进行发布和版本控制。
   * + - 1. 安全管理机构和人员要求

安全管理机构

安全管理机构安全要求包括：

1. 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；
2. 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，以及系统管理员、网络管理员、安全管理员等专职人员岗位，并明确部门、各负责人和专职人员的岗位职责；
3. 应根据各职能部门和相关岗位的职责，明确对应的授权审批事项、审批部门和批准人等；
4. 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；
5. 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

人员安全要求：

1. 应加强相关部门之间、不同安全管理岗位人员之间的协作沟通，定期召开协调会议；
2. 应加强与工业互联网平台安全主管部门、各类供应商、业界专家的合作与沟通；
3. 应对被录用的工业互联网平台管理人员及第三方人员的身份、背景、专业资格和资质等进行审查；
4. 应及时终止离岗员工的所有访问权限，并按照规范流程取回各种身份证件、钥匙、徽章等以及企业提供的软硬件设备；
5. 应定期对工业互联网平台管理人员及第三方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；
6. 应确保在外部人员物理访问受控区域或接入受控网络系统前先提出书面申请，批准后由专人全程陪同或由专人开设账户及分配权限和期限，并登记备案；
7. 外部人员离场后应及时清除其所有的访问权限。
   * + - 1. 安全建设管理要求

定级

定级要求包括：

1. 应明确本企业的安全等级；
2. 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

安全方案设计要求包括：

1. 应根据安全防护对象的安全防护需求进行安全方案设计；
2. 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

产品采购和使用安全要求包括：

1. 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；
2. 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

软件开发安全要求包括：

1. 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；
2. 应在软件开发过程中进行安全性测试；
3. 应在软件交付前进行缺陷和恶意代码等安全检测；
4. 应要求开发单位提供软件设计文档和使用指南；
5. 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

系统交付安全要求包括：

1. 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；
2. 应根据交付清单对所交接的设备、软件和文档等进行清点；
3. 应对负责运行维护的技术人员进行相应的技能培训；
4. 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

服务供应商选择安全要求包括：

1. 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；
2. 应在服务协议中规定具体服务内容和技术指标；
3. 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；
4. 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；
5. 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；
6. 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；
7. 应确保外包运维服务商的选择符合国家的有关规定；
8. 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。
   * + - 1. 安全运维管理要求

环境管理

环境管理安全要求包括：

1. 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；
2. 应不在重要区域接待来访人员。

资产管理

资产管理安全要求包括：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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）；
6. 应对工业互联网平台部署环境的评估方法作出明确规定；
7. 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；
8. 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；
9. 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

安全审计要求包括：

1. 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；
2. 应对审计记录进行保护，定期备份，避免未预期的删除、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；
3. 应确保审计记录的留存时间不少于6个月。

配置管理

配置管理安全要求包括：

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

安全事件处置要求包括：

1. 应建立网络安全事件监测手段，并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；
2. 应制定安全事件报告和处置管理制度，明确安全事件的报告和处置流程；
3. 应在安全事件报告和响应处理过程中，收集证据，记录处理过程，分析和鉴定事件产生的原因，总结经验教训。

应急工作

应急工作安全要求包括：

1. 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，原则上每年进行至少一次评估和修订；
2. 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。
   * + 1. 物理和环境安全要求
          1. 物理位置选择

物理位置选择安全要求包括：

1. 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；
2. 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。
   * + - 1. 物理访问控制

物理访问控制安全要求包括：

1. 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；
2. 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. 防盗窃和防破坏

防盗窃和防破坏安全要求包括：

1. 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；
2. 应将通信线缆铺设在隐蔽安全处，可铺设在地下或管道中；
3. 主机房或重要设备区域应安装必要的防盗报警设置。
   * + - 1. 防雷击

防雷击安全要求包括：

应将各类机柜、设施和设备等通过接地系统安全接地。

* + - * 1. 防火

防火安全要求包括：

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。

* + - * 1. 防水和防潮

防水和防潮安全要求包括：

1. 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；
2. 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. 防静电

防静电安全要求包括：

应采用防静电地板或地面并采用必要的接地防静电措施。

* + - * 1. 温湿度控制

温湿度控制要求包括：

应设置温湿度自动调节设施，使机房及工业互联网平台相关设备放置场地的温湿度的变化处于设备运行所允许的范围之内。

* + - * 1. 电力供应

电力供应要求包括：

1. 应在机房供电线路上配置稳压器和过电压防护设备；
2. 应提供短期的备用电力供应，保障设备在断电情况下仍正常运行。
   * + - 1. 电磁防护

电磁防护要求包括：

电源线和通信线缆应隔离铺设,避免互相干扰。

* + 1. 增强级防护要求
       1. 接入层安全防护要求
          1. 接入设备安全防护要求

口令账号安全

同基本级要求。

安全配置

除满足基本级的要求之外，还应符合以下要求：

1. 应设置单独的接入安全区域，同时分配已规划的地址空间。

身份鉴别

除满足基本级防护要求之外，还应符合以下要求：

1. 在关键边缘接入设备应提供符合国家密码管理法律法规要求的通信加密和签名验签；
2. 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。

访问控制

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 能够对非授权设备的接入行为进行告警和阻断。

安全审计

同基本级要求。

入侵防范

除满足基本级防护要求之外，还应符合以下要求：

能够对未知威胁进行分析和防范。

* + - * 1. 接入层网络安全防护要求

访问控制

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 对于有线和无线接入，确保通过受控的边界防护设备或者其上的指定端口接入网络；
3. 对接入网络数据进行深度包检测；
4. 采用白名单控制方式，只允许合法设备接入网络。

安全审计

除满足基本级防护要求之外，还应符合以下要求：

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

通信安全

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 应保证通信过程中使用的互联互通协议的可信性

恶意代码防范

同基本级要求。

入侵防范

同基本级要求。

* + - 1. 基础设施层安全防护要求
         1. 计算环境安全防护要求

身份鉴别

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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。

安全审计

除满足基本级防护要求之外，还应符合以下要求：

1. 应能够根据记录数据进行分析，并生成审计报表；
2. 应保护审计进程，避免受到未预期的中断。

资源控制

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

应支持对防恶意代码的统一管理。

入侵防范

除满足基本级防护要求之外，还应符合以下要求：

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。

* + - * 1. 网络安全防护要求

网络拓扑结构安全

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

应实现对MODBUS TCP、OPC UA等常用工业协议及HTTP等互联网协议 的访问控制。

安全审计

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

应周期性地维护恶意代码库的升级和检测系统的更新。

网络设备安全

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 应支持对违法和不良信息或非法域名的检测发现并告警；
3. 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；
4. 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。
   * + - 1. 虚拟化安全防护要求

虚拟机安全

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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；
3. 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；
4. 应提供最新版本的虚拟机镜像和补丁版本；
5. 应具备发现虚拟机操作系统漏洞的能力，进行漏洞修复。

虚拟网络安全

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 应对虚拟机网络出口带宽进行限制；
3. 可支持用户选择使用第三方安全产品。

虚拟化平台安全

同基本级要求。

容器安全

除满足基本级防护要求之外，还应符合以下要求：

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。

* + - 1. 平台层安全防护要求
         1. 微服务组件安全防护要求

同基本级要求。

* + - * 1. 平台应用开发环境安全防护要求

身份鉴别

除满足基本级防护要求之外，还应符合以下要求：

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

同基本级要求。

安全审计

同基本级要求。

资源控制

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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

除满足基本级防护要求之外，还应符合以下要求：

1. 与开发环境中的重要功能相关的数据应进行异址备份；
2. 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

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 业务应用与工业APP应避免使用含有己公开漏洞的开源第三方应用组件及代码（漏洞库可参考CNVD、CNNVD、CVE、CNCVE等）。
   * + - 1. 容器安全防护要求

同基本级要求。

* + - 1. 应用层安全防护要求
         1. 身份鉴别

除满足基本级防护要求之外，还应符合以下要求：

1. 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。
   * + - 1. 口令安全机制

除满足基本级防护要求之外，还应符合以下要求：

1. 不应默认保存用户上次的账号及口令信息；
2. 应具备口令强度、时效性检查机制。
   * + - 1. 访问控制

同基本级要求。

* + - * 1. 安全审计

除满足基本级防护要求之外，还应符合以下要求：

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。

* + - * 1. 运行安全

同基本级要求。

* + - * 1. 安装与卸载安全

同基本级要求。

* + - * 1. 其他安全

除满足基本级防护要求之外，还应符合以下要求：

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。

* + - 1. 数据安全防护要求

平台应按照GB/T XXXXX-XXXX《工业互联网企业网络安全 第4部分：数据安全防护要求》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。

* + - 1. 安全管理
         1. 安全管理制度

除满足基本级防护要求之外，还应符合以下要求：

1. 应建立针对工业互联网平台的安全监测和应急响应制度，健全监测、处置、应急、备份等流程规范性文件；
2. 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. 安全管理机构和人员要求

安全管理机构

同基本级要求。

人员

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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；
6. 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；
7. 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；
8. 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；
9. 对关键区域或关键系统不允许外部人员访问。
   * + - 1. 安全建设管理要求

定级

同基本级要求。

安全方案设计

除满足基本级防护要求之外，还应符合以下要求：

1. 应根据安全防护对象的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；
2. 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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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；
6. 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

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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；
3. 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. 安全运维管理要求

环境管理

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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；
6. 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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 应对审计进程进行保护，防止未经授权的中断；
3. 审计记录的留存时间应不少于6个月。

配置管理

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

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

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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；
3. 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。
   * + 1. 物理和环境安全要求
          1. 物理位置选择

除满足基本级防护要求之外，还应符合以下要求：

1. 在机房选址及设计时，满足GB 50174-2017的相关规定；
2. 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。
   * + - 1. 物理访问控制

除满足基本级防护要求之外，还应符合以下要求：

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。

* + - * 1. 防盗窃和放破坏

除满足基本级防护要求之外，还应符合以下要求：

应对机房设置监控报警系统。

* + - * 1. 防雷击

同基本级要求。

* + - * 1. 防火

除满足基本级防护要求之外，还应符合以下要求：

1. 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；
2. 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. 防水和防潮

除满足基本级防护要求之外，还应符合以下要求：

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。

* + - * 1. 防静电

除满足基本级防护要求之外，还应符合以下要求：

应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

* + - * 1. 温湿度控制

同基本级要求。

* + - * 1. 电力供应

除满足基本级防护要求之外，还应符合以下要求：

应设置冗余或并行的电力电缆线路为工业互联网平台企业相关系统供电。

* + - * 1. 电磁防护

除满足基本级防护要求之外，还应符合以下要求：

应对工业互联网平台关键设备实施电磁屏蔽。

参考文献

《工业互联网企业网络安全分类分级管理指南》（试行）