河北省工业和信息化厅

关于印发《2024年工业企业信息安全综合

防护能力建设试点申报指南》的通知

各市（含定州、辛集市）工业和信息化局，雄安新区改革发展局：

为深入贯彻工业和信息化部《工业互联网企业网络安全分类分级管理指南（试行）》《工业和信息化领域数据安全管理办法》《工业和信息化部工业控制系统信息安全防护指南》有关要求，落实省政府《关于推动互联网与先进制造业深度融合加快发展工业互联网的实施意见》相关工作部署，提升我省工业企业信息安全综合防护水平，我厅制定了《2024年工业企业信息安全综合防护能力建设试点申报指南》，现印发给你们，请按照相关要求做好试点申报的组织工作。

　　　　　　　　　　　　　　　河北省工业和信息化厅

　　　　　　　　　　　　　　 2023年7月24日

2024年工业企业信息安全综合防护能力建设试点

申报指南

为深入贯彻工业和信息化部《工业互联网企业网络安全分类分级管理指南（试行）》《工业和信息化领域数据安全管理办法》《工业和信息化部工业控制系统信息安全防护指南》有关要求，落实省政府《关于推动互联网与先进制造业深度融合加快发展工业互联网的实施意见》相关工作部署，提升我省工业企业信息安全综合防护水平，决定开展2024年工业企业信息安全综合防护能力建设试点工作。为做好相关工作，特制定本申报指南。

申报条件

（一）在我省登记注册，具有独立法人资格的工业企业，且企业经营状况良好。

（二）企业两化融合发展水平达到单项应用阶段及以上，拥有专门的信息化支撑队伍。

（三）列入国家和省两化融合类试点示范的，取得省级以上信息技术创新成果或奖励的，开展两化融合管理体系贯标并通过评定的，同等条件下优先列为试点示范。

（四）优先考虑装备、钢铁、建材、石化、食品、医药等我省优势行业，工业控制系统广泛应用，工业控制信息安全基础较好的企业。

（五）所申报的试点内容须在试点建设期内完成。

（六）存在下列情形之一的不得申报：

1.违反国家相关法律和政策规定，在经营管理、企业诚信、节能减排等方面有不良记录的；

2.发生安全生产责任事故和重大信息安全事件的。

试点内容

（一）提升工业控制系统信息安全防护水平。试点企业按照《工业控制系统信息安全防护指南》要求，制定防护能力提升计划并组织实施，对企业工业控制系统信息安全防护设施进行加固和完善，进一步健全工控安全管理制度、机制，提升工业控制系统信息安全防护能力。

（二）搭建工业企业安全监测管理平台。试点企业结合行业特色，选取自动化程度相对较高的一条或多条产线，在第三方服务机构指导下，部署工业企业安全监测管理平台，并完成平台与省级工控信息安全态势感知和监测预警平台之间资产、拓扑、事件三类数据的交互对接。

（三）开展工业控制系统信息安全应急演练。试点企业要按照《工业控制系统信息安全事件应急管理工作指南》要求，编制企业工业控制系统信息安全应急预案，在第三方服务机构指导下开展工业控制系统信息安全应急演练，并配合本地工信部门在企业召开全市工业控制系统信息安全应急演练现场观摩会，为市县工信部门和本市重点工业企业提供现场参观服务。

（四）开展工业互联网企业网络安全分类分级管理。试点企业按照《关于开展工业互联网企业网络安全分类分级管理试点工作的通知》，组织开展自主定级并上报省工信厅，在第三方服务机构支持下，开展定级核查、生成核查报告，并根据防护意见落实安全防护措施。

（五）开展工业领域数据安全分级分类管理。试点企业按照《工业数据分类分级指南（试行）》《工业领域重要数据和核心数据识别规则（草案）》开展数据分类分级，在第三方服务机构支持下，制定重要数据和核心数据清单，开展数据安全评估并生成评估报告。

政策支持

优先推荐试点企业争取国家工业信息安全、工业互联网、新一代信息技术与制造业融合等两化融合类项目支持；优先支持试点企业申请省工业互联网创新发展、企业上云等省级项目。根据2024年省财政项目预算情况，对试点企业给予一定资金补助。组织省内企业到试点企业进行学习观摩、行业对标、经验交流等推广活动，提高和扩大企业影响力。

申报要求

（一）试点申报遵循政府引导、企业自愿原则，各市工业和信息化局要做好试点申报的组织和指导工作，将本通知及时转发到符合条件的工业企业。

（二）申报企业按要求填写提交《河北省工业企业信息安全综合防护能力建设试点申报表》、《河北省工业企业信息安全综合防护能力建设试点工作方案》（见附件），并附上企业两化融合评估报告（在线填报地址：http://hebeipg.cspiii.com，数据填报完成后，可在线生成评估报告）。企业对提交材料的真实性负责。

（三）各市请于2023年8月4日前将企业申报材料（一式三份）上报省厅，并将电子版拷至U盘或光盘一并上报。申报材料由申报企业填写并盖章；推荐单位一栏由各市工信局填写，并加盖公章。每个市（含定州、辛集市）和雄安新区申报企业数量不超过5个，已列为省工业控制系统信息安全试点单位的企业不得再次申报。

（四）联系方式

河北省工业和信息化厅软件产业处

联 系 人：李浩伟

联系电话：18032069673

电子邮箱：hbgkaq@163.com

邮寄地址：石家庄市和平西路402号

河北省工业和信息化厅邮政编码：050071

附件：1.河北省工业控制系统信息安全试点申报表

2.河北省工业控制系统信息安全试点工作方案

附件1

河北省工业企业信息安全综合防护能力建设试点申报表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 申报企业基本信息 | | 企业名称 | | |  | | | | | | |
| 法人代表 | | |  | | 组织机构代码 | | |  | |
| 注册地址 | | |  | | 单位性质 | | | □国有 □民营 □三资  □股份制 | |
| 联系地址 | | |  | | 邮政编码 | | |  | |
| 联系人 | | |  | | 电话及手机 | | |  | |
| 传 真 | | |  | | 电子邮箱 | | |  | |
| 截至上年末的  主营业务收入 | | |  | | 员工总数 | | |  | |
| 所属行业 | | |  | | | | | | |
| 信息化部门名  称 | | |  | | 部门人数 | | |  | |
| 申报试点的基本情况 | | 企业基本情况 | | | 填写企业主营业务、主要产品，生产经营情况等 | | | | | | |
| 企业信息化基本情况 | | | 填写企业基础网络、信息系统部署和使用情况等 | | | | | | |
| 企业工业信息安全建设情况 | | | 填写在工控系统、业务系统、数据系统、网络系统应用的总体情况，采取的安全防护措施等 | | | | | | |
|  | | 2024年工业信息安全工作主要打算 | | | （500字以内） | | | | | | |
| 进度安排 | | | （200字以内） | | | | | | |
| 试点预计投资情  况 | 投资  （万元） | | 预计总投资 | |  | 其中软硬件购置 | |  | |
| 其中安全服务 | |  | 其他 | |  | |
| 资金来源  （万元） | | 银行贷款 | |  | 自有资金 | |  | |
| 其他资金 | |  | | | | |
| 预期达到的经济和社会效益 | | | （200字以内） | | | | | | |
| 真  实  性  承  诺 | | 我单位申报的所有材料，均真实、完整，如有不实，愿承担相应的责任。  法定代表人签章： 公章：  年 月 日 | | | | | | | | | |
| 推  荐  单  位  意  见 | | 签章：  年 月 日 | | | | | | | | | |

填报说明：

1.表中文字叙述要重点突出，表述准确，实事求是。栏目不得空缺，无内容时填“无”。

2.申报单位名称需填写全称(并与银行开户的户名一致)。

附件2

河北省工业企业信息安全综合防护能力建设试点

工作方案

（方案应包含但不限于以下内容）

## 申报单位概况

主要包括企业基本情况、企业经营情况等。

两化融合情况

主要包括企业两化融合现状、重要信息系统部署和使用情况、两化融合主要成效、两化融合水平自评估结果（附两化融合评估报告）。

工业信息安全现状、问题和2024年工作打算

1.工业信息安全现状，包括在安全制度建设、安全设备部署、防范措施落实、应急体系建设等方面的工作。（附工控系统信息安全自查表，见附件）

2.企业工业信息安全技术防范和管理工作中存在的问题。

3.2024年工业信息安全工作打算。包括：根据《工业控制系统信息安全防护指南》的提升安全防护能力的具体计划；落实防护能力提升计划的具体措施；如何配合搭建工业企业安全监测管理平台；工控系统应急预案如何编制、工业控制系统信息安全应急演练的具体打算；举办应急演练现场观摩会的安排；网络安全和数据安全分级分类、数据安全分级分类工作打算。

组织实施

包括试点项目工作组织、经费投入计划、时间进度安排、风 险管控等。

附件

工业控制系统信息安全自查表

填 表 说 明

## 组成结构

本表包含四个分表：

（1）工业控制系统运营单位基本情况表

（2）工业控制系统运营单位自查情况汇总表

（3）工业控制系统信息安全自查表

（4）工业企业工业云信息安全自查表

填写对象

各分表填写责任人如下：

（1）工业控制系统运营单位基本情况表：由各工业控制系统运营单位指定专人负责填写。

（2）工业控制系统运营单位自查情况汇总表：由各工业控制系统运营单位指定专人负责填写。

（3）工业控制系统信息安全自查表：由工业控制系统运营单位的各工业控制系统负责人填写。

（4）工业企业工业云信息安全自查表：各工业企业指定专人负责填写

表 1 工业控制系统运营单位基本情况表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 单  位  信  息 | 单位全称 |  | | 法人代表 |  |
| 通讯地址 | 省 市 县（区） | | | |
| 单位网址 |  | | 邮政编码 |  |
| 所属行业 1 |  | | 销售收入 |  |
| 经济类型 | □国有事业单位 2  □国有及国有控制企业 3 （□中央 □地方）  □股份制企业 □外商及港澳台投资企业 4  □集体企业 □民营企业  □其他： | | | |
| 联  系  人 | 姓名 |  | | 职务 |  |
| 所属部门 |  | | 工作电话 |  |
| 电子邮件 |  | | 传真 |  |
| 工  控  系  统  基  本  情  况 | 工业控制系统总数量 | |  | | |
| 系统名称 | | 系统简介 | | |
|  | |  | | |
|  | |  | | |
|  | |  | | |
|  | |  | | |
| 工  业  安  全  管  理  情  况 | 应急预案演练情况 | 1.工控安全事件应急响应预案：  □已制定，包括：□应急计划策略和规程  □应急计划培训  □应急计划测试与演练  □应急处理流程  □事件监控措施  □应急事件报告流程  □应急支持资源  □应急响应计划  □其它：  □未制定  2.急预案演练情况：  □定期开展，演练周期：  □本年度已开展，演练时间：  □将演练情况报网络安全主管部门  □未将演练情况报网络安全主管部门  □应急演练结束后对应急预案进行了评估和适用性修订  □应急演练结束后未对应急预案进行了评估和适用性修订  □本年度未开展  □未定期开展 | | | |
| 落实责任情况 | 1.工控安全管理机制：  □已建立，包括：□建立了工业控制系统安全管理制度  □成立了工业控制系统信息安全协调小组  □明确了工控安全管理责任人  □其它：  □未建立 | | | |

**注1：**工控系统基本情况可另附表说明。

**注2：**此处工业控制系统的划分原则为1）具体的完整的工业控制系统：以企业工业自动化生产过程为基础，属于企业的一个自动化生产全过程或一个工业自动化生产装置；或者是2） 工业控制系统中相对独立的一部分：以企业工业自动化生产过程的局部环节为基础，属于企业的一个自动化生产全过程或一个工业自动化生产装置的工业控制系统中的相对独立的且物理边界清晰的某个安全区域或通信网络。

**注3：**每个工控系统均应填写1个工业控制系统信息安全自查表。

1.按照《国民经济行业分类》（GB/T4745-2011）规定填写。

2.按照《事业单位登记管理暂行条例》登记的，为社会公益目的、由国家机关举办或者其他组织组织利用国有资产举办的，从事教育、科技、文化、卫生等活动的社会服务组织。

3.按照《中华人民共和国企业法人登记管理条例》登记注册的三类经济组织：（1）全部资产归国家所有的（非公司制）国有企业；（2）全部资产归国家所有的国有独资有限责任公司；（3）由国有资本占控制地位的有限责任公司和股份有限公司，此处称国有控股公司，包括港、澳、台资本和其他地区外资资本投资设立的独资或控股的独资公司、有限责任公司和股份有限公司。

表 2 工业控制系统运营单位自查情况汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 运营单位名称 | |  | | |
| 基本情况 | 重要工业控制系统总数： 套 | | | |
| 系统构成情况 | 类型 | 设备 | 国内品牌 | 国外品牌 |
| 工业生产控制设备 | 可编程逻辑控制器（PLC） | 台 | 台 |
| 分布式控制系统（DCS） | 台 | 台 |
| 远程终端设备（RTU） | 台 | 台 |
| 数控机床 | 台 | 台 |
| 工业机器人 | 台 | 台 |
| 智能仪表 | 台 | 台 |
| 其它 | 台 | 台 |
| 工业网络通信设备 | 工业交换机 | 台 | 台 |
| 工业路由器 | 台 | 台 |
| 串口服务器 | 台 | 台 |
| 其它 | 台 | 台 |
| 工业主机设备 | 工业主机 | 台 | 台 |
| 组态软件& 数据采集与监控系统  （SCADA）软件 | 套 | 套 |
| 工业数据库 | 套 | 套 |
| 其它 | 台 | 台 |
| 工业生产信息系统 | 制造执行系统（MES） | 套 | 套 |
| ERP 管理系统 | 套 | 套 |
| 工业云 | 套 | 套 |
| 其它 | 套 | 套 |
| 工业网络安全设备 | 工业防火墙 | 台 | 台 |
| 工业网闸 | 台 | 台 |
| 主机安全防护设备 | 台 | 台 |
| 其它 | 台 | 台 |
| 安全软件选择与管理情况 | 1、安装防病毒软件或应用程序白名单软件的重要工业控制系统数量： 套  2、病毒库或白名单规则及时更新的重要工业控制系统数量： 套  3、定期对工业控制系统进行查杀的重要工业控制系统数量： 套  4、已建立防病毒和恶意软件入侵管理机制的重要工业控制系统数量： 套 | | | |
| 配置和补丁管理情况 | 1、已建立工业控制网络安全配置策略的重要工业控制系统数量： 套  2、已建立工业主机安全配置策略的重要工业控制系统数量： 套  3、已建立工业控制设备安全配置策略的重要工业控制系统数量： 套  4、已建立工业控制系统配置清单的重要工业控制系统数量： 套  5、定期对配置清单进行更新和维护的重要工业控制系统数量： 套  6、及时修复重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞的重要工业控制系统数量： 套 | | | |
| 边界安全防护情况 | 1、直接与企业网连接的重要工业控制系统数量： 套  2、与企业网进行物理隔离的重要工业控制系统数量： 套  3、直接与互联网连接的重要工业控制系统数量: 套  4、与互联网进行物理隔离的重要工业控制系统数量： 套  5、对工业控制系统进行安全区域划分的重要工业控制系统数量： 套  6、对工业控制系统安全区域实施逻辑隔离的重要工业控制系统数量： 套 | | | |
| 物理和环境安全防护情况 | 1、已明确划分重点物理安全防护区域并建立物理安全防护措施的重要工业控制系统数量： 套  2、拆除或封闭工业主机上不必要外设接口的重要工业控制系统数量： 套  3、使用外设安全管理技术手段管理外设接口的重要工业控制系统数量： 套 | | | |
| 身份认证情况 | 1、使用身份认证管理手段的重要工业控制系统数量： 套  2、以最小特权原则分配账户权限的重要工业控制系统数量： 套  3、未使用默认口令或弱口令的重要工业控制系统数量： 套  4、定期更新口令的重要工业控制系统数量： 套 | | | |
| 远程访问安全情况 | 1、面向互联网开通HTTP、FTP等网络服务的重要工业控制系统数量：套  2、使用数据单向访问控制等策略进行安全加固的重要工业控制系统数量： 套  3、无远程访问的重要工业控制系统数量： 套  4、使用VPN等远程接入方式的重要工业控制系统数量： 套  5、无远程维护的重要工业控制系统数量： 套  6、保留工业控制系统相关访问日志的重要工业控制系统数量： 套 | | | |
| 安全监测和应急预案演练情况 | 1、在工业控制网络部署网络安全监测设备的重要工业控制系统数量： 套  2、在重要工业控制设备前端已部署具备深度包分析和过滤功能防护设备的重要工业控制系统数量： 套  3、已制定工控安全事件应急响应预案的重要工业控制系统运营单位数量： 家  4、定期对应急预案进行演练的重要工业控制系统运营单位数量： 家  5、对应急响应预案进行修订的重要工业控制系统运营单位数量： 家 | | | |
| 资产安全情况 | 1、建立工业控制系统资产清单的重要工业控制系统数量： 套  2、对关键主机设备进行冗余配置的重要工业控制系统数量： 套  3、对网络设备进行冗余配置的重要工业控制系统数量： 套  4、对控制组件进行冗余配置的重要工业控制系统数量： 套 | | | |
| 数据安全情况 | 1、对静态存储的重要工业数据进行保护的重要工业控制系统数量： 套  2、对动态传输的重要工业数据进行保护的重要工业控制系统数量： 套  3、定期备份关键业务数据的重要工业控制系统数量： 套  4、对测试数据进行保护的重要工业控制系统数量： 套  5、无测试环境的重要工业控制系统数量： 套 | | | |
| 供应链管理情况 | 1、合同中已约定服务商在服务过程中应当承担的信息安全责任和义务的重要工业控制系统数量： 套  2、与服务商签订保密协议的重要工业控制系统数量： 套 | | | |
| 落实责任情况 | 1、建立工控安全管理机制的重要工业控制系统运营单位数量： 家 | | | |

表 3 工业控制系统信息安全自查表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 系统名称 |  | | | | | | |
| 负责人 | 姓名 | |  | | 职务 |  | |
| 所属部门 | |  | | 工作电话 |  | |
| 功能描述 | （描述该系统的功能、业务流程） | | | | | | |
| 业务互联 | （描述与其他工业控制系统、上层监控系统、MES 系统互联情况） | | | | | | |
| 系统组成结构 | （描述该工业控制系统的组成情况、网络拓扑图等） | | | | | | |
| 系统构成情况 | 类型 | | 设备 | 国内品牌 | | | 国外品牌 |
| 工业生产控制设备 | | 可编程逻辑控制器（PLC） | 台 | | | 台 |
| **其中：**  腾控科技： 台  和利时： 台  台达： 台  其它：  厂商： 数量： 台 | | | **其中：**  西门子： 台  施耐德： 台  GE： 台  AB（罗克韦尔）：  台  三菱： 台  欧姆龙： 台  菲尼克斯： 台 |
|  |  | |  |  | | | ABB： 台 |
| 其它：  厂商： 数量： 台 |
|  | 套 | | | 套 |
| 分布式控制系统  （DCS） | **其中：**  浙大中控： 套  和利时： 套  南京科远： 套  北京国电智深：  套  其它：  厂商： 数量： 套 | | | **其中：**  艾默生： 套  霍尼韦尔： 套  横河： 套  Foxboro： 套  西门子： 套  Invensys： 套  罗克韦尔： 套  ABB： 套 |
|  |  | | | 其它：  厂商： 数量： 套 |
|  | 台 | | | 台 |
| 远程终端设备  （RTU） | **其中：**  阿尔泰： 台  研华科技： 台 | | | **其中：**  艾默生： 台  sixnet： 台 |
|  | 其它：  厂商： 数量： 台 | | | 其它：  厂商： 数量： 台 |
|  | 台 | | | 台 |
| 数控机床 | **其中：**  齐二机床： 台  宝鸡机床： 台  沈阳一机： 台 | | | **其中：**  FAUNC： 台  三菱： 台  西门子： 台 |
|  | 其它：  厂商： 数量： 台 | | | 其它：  厂商： 数量： 台 |
|  | 台 | | | 台 |
| 工业机器人 | **其中：**  新松： 台  其它：  厂商： | | | **其中：**  库卡： 台  FAUNC： 台  ABB： 台  安川电机： 台 |
|  |  | |  | 数量： 台 | | | 那智不二越： 台  史陶比尔： 台  爱普生： 台  川崎： 台 |
|  | | | 其它：  厂商： 数量： 台 |
| 智能仪表 | 台 | | | 台 |
| 其它 | 台 | | | 台 |
|  | |  | 台 | | | 台 |
|  | | 工业交换机 | **其中：**  MOXA ：  台  研华科技： 台  东土科技： 台 | | | **其中：**  赫斯曼： 台  罗杰康： 台  西门子： 台  菲尼克斯： 台 |
|  | |  | 其它：  厂商： 数量： 台 | | | 其它：  厂商： 数量： 台 |
| 工业网络通信设备 | | 工业路由器 | 台 | | | 台 |
|  | 台 | | | 台 |
|  | | 串口服务器 | **其中：**  MOXA： 台  研华科技： 台  东土科技： 台  其它：  厂商： 数量： 台 | | | **其中：**  Perle： 台  sixnet： 台  其它：  厂商： 数量： 台 |
|  | | 其它 | 台 | | | 台 |
|  | | 工业主机 1 | 台 | | | 台 |
| 工业主机设备 | | 组态软件& 数据采集与  监 控 系 统  （SCADA）  软件 | 套 | | | 套 |
| **其中：**  组态王： 套KingSCADA： 套WebAccess： 套  三维力控： 套  紫金桥： 套 | | | **其中：**  Intouch： 套  GE iFix： 套  WinCC： 套  Citect： 套 |
|  |  | |  | MCGS： 套  世纪星： 套 | | | 其它：  厂商： 数量： 套 |
| 其它：  厂商： 数量： 套 | | |  |
|  | 套 | | | 套 |
|  | **其中：**  三维力控： 套  安捷： 套  亚控科技： 套 | | | **其中：**  霍尼韦尔： 套  PI： 套  InSQL： 套  Infoplus： 套  Proficy-Historian： 套  eDNA： 套  RSSQL： 套  西门子： 套  其它：  厂商： 数量： 套 |
| 工业数据库 | 其它：  厂商： 数量： 套 | | |
| 其它 | 台 | | | 台 |
|  | | 制造执行系统  （MES） | 套 | | | 套 |
| 工业生产信息系统 | | ERP 管理系统 | 套 | | | 套 |
| 工业云 | 套 | | | 套 |
|  | | 其它 | 套 | | | 套 |
|  | |  | 台 | | | 台 |
|  | | 工业防火墙 | **其中：**  威努特： 台  启明星辰： 台  海天炜业： 台 | | | **其中：**  赫斯曼： 台  Tofino： 台 |
| 工业网络安全设备 | |  | 其它：  厂商： 数量： 台 | | | 其它：  厂商： 数量： 台 |
|  | | 工业网闸 | 台 | | | 台 |
|  | | 主机安全防护设  备 | 台 | | | 台 |
| 其它 | 台 | | | 台 |
| 安全软件选择与管理情况 | 1.工业主机防护设备（如防病毒软件、应用程序白名单软件）：  □已安装，防护设备名称：  □未安装  2.及时进行恶意代码库或白名单规则库更新升级：  □是，目前库版本号：  □否，目前库版本号：  3.定期进行系统查杀：  □是，查杀时间间隔：  □未进行定期查杀  4.防病毒和恶意软件入侵管理机制：  □已建立，包括：□定期扫描病毒和恶意软件 □定期更新病毒库 □查杀临时接入设备（如临时接入U盘、移动终端外设）  □未建立 | | | | | | |
| 配置和补丁管理情况 | 1.工业控制网络安全策略配置：  □已建立，包括：□网络分区分域 □非必要端口禁用  □其它：  □未建立  2.工业主机安全策略配置：  □已建立，包括：□远程控制管理禁用 □关闭默认账户  □最小服务配置 □关闭非必要文件共享  □启用登录口令复杂度要求 □其它：  □未建立  3.工业控制设备安全策略配置：  □已建立，包括：□口令策略合规性 □其它：  □未建立  4.工业控制系统安全策略配置清单：  □已建立，包括：□设备名称 □设备编号 □配置策略  □配置时间 □其它：  □未建立  5.定期进行配置清单的更新和维护：  □是，维护时间间隔： 更新时间间隔：  □部分是，定期更新和维护的配置清单：  时间间隔：  □否  6.及时修复重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞：□是  □否 | | | | | | |
| 边界安全防护情况 | 1.直接与企业内网连接：  □是  □否，组网方式（单选）：□独立 □使用防护设备进行隔离，防护设备名称及生产厂商：  □其它：  □与企业网物理隔离  2.直接与互联网连接：  □是 | | | | | | |
|  | □否，组网方式（单选）：□独立 □使用防护设备进行隔离，防护设备名称及生产厂商：  □通过企业网连接 □其它：  □与互联网物理隔离  3.对工业控制系统网络进行安全域划分：  □是，划分原则：□安全域重要性 □业务需求 □其它：  □否  4.各安全域之间进行逻辑隔离：  □是，隔离措施：□防火墙 □网闸 □其它：  □否 | | | | | | |
| 物理和环境安全防护情况 | 1.物理安全防护区域防护措施：  □无 □门禁系统 □专人值守 □视频监控 □其它： 2.拆除或封闭工业主机外设接口：  □是  □否，未拆除或封闭的外设接口包括：□USB □光驱  □无线 □其它：  2.使用外设安全管理技术手段进行安全管理：  □是，方式：□主机外设统一管理设备（或软件）：  □隔离存放有外设接口的工业主机  □其它：  □否 | | | | | | |
| 身份认证情况 | 1.使用身份认证管理手段：  □是，包括：□口令密码 □USB-Key □智能卡 □生物指纹  □其它：  2.最小权限原则分配账户权限： □是 □否  3.工业控制系统口令使用：  □采用默认口令 □采用弱口令 □其它：*（口令策略要求）* 4.定期更新口令：  □是，更新周期：  □否 | | | | | | |
| 远程访问安全情况 | 1.面向互联网开通通用网络服务：  □是，包括：□HTTP □FTP □Telnet □其它：  □否  2.使用远程访问：  □是，安全加固策略：□无 □采用数据单向访问控制  □其它：  □否  □不使用远程访问  3.使用远程维护：  □是，安全加固策略：□无 □采用虚拟专用网络（VPN）  □其它：  □否  □不使用远程维护 | | | | | | |
|  | | 4.工业控制系统相关访问日志：  □留存，留存期：  □未留存 | | | | | |
| 安全监测情况 | | 1. 1.工业控制系统网络部署网络安全监测设备：   □是，网络安全监测设备型号及生产商：  □否  2.重要工业控制设备前端部署具备深度包分析和过滤功能的防护设备：  □是，防护设备型号及生产商：  □否 | | | | | |
| 资产安全情况 | | 1. 1.工业控制系统资产清单：   □已建立，包括：□设备名称 □设备编号 □设备型号  □设备类型 □生产厂 □设备重要程度/密级 □设备版本 □启用时间  □责任部门 □责任人 □使用状态  □其它：  □未建立   1. 2.关键主机设备是否进行硬件冗余：□是 □否 2. 3.网络设备是否进行硬件冗余：□是 □否 3. 4.控制组件是否进行硬件冗余：□是 □否 | | | | | |
| 数据安全情况 | | 1.对静态存储的重要工业数据进行保护：  □是，保护措施：□数据加密 □隔离存放 □访问权限控制  □其它：  □否  2.对动态传输的重要工业数据进行保护：  □是，保护措施：□数据加密 □数据隔离 □其它：  □否  3.定期备份关键业务数据：  □是，备份周期：  □否  4.对测试数据进行保护：  □是，保护措施：□数据加密 □数据销毁 □隔离存放  □访问权限控制 □其它：  □否  □无测试环境 | | | | | |
| 供应链管  理情况 | | 1.服务商在服务过程中应当承担的信息安全责任和义务：  □已约定，包括：  □未约定  2.服务商签订保密协议情况：□已签订 □未签订 | | | | | |

表 4 工业企业工业云信息安全自查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 企业名称 |  | | | | |
| 工业云应用  基本情况 | 1.企业是否使用云服务？ | | | | |
| □是 | | | | |
| □否 | | | | |
| 2.云部署模式： | | | | |
| □私有云 | | | | |
| □公有云 | | | | |
| 云服务商： | |  | | |
| □混合云 | | | | |
| 公有云服务商： | |  | | |
| 3.生产管理系统（ERP、MES 等）是否上云？ | | | | |
| □是 | | | | |
| □否 | | | | |
| 4.工业控制系统是否上云？ | | | | |
| □是 | | | | |
| □否 | | | | |
| 5.生产数据是否上云？ | | | | |
| □是 | | | | |
| □否 | | | | |
| 工业云安全情况 | **（以下内容由使用公有云、混合云的企业填写）** | | | | |
| 一、云服务商安全选择 | 1.所选云服务商是否为境外服务商 | | □是 | □否 |
| 2.云服务商是否通过政府安全审查或第三方机构的权威评估认证 | | □是 | □否 |
| 二、云服务安全运行监管 | 1.是否通过合同明确了云服务商的责任和义务 | | □是 | □否 |
| 2.是否建立云平台重大变更沟通机制 | | □是 | □否 |
| 3.是否与云服务商签订了保密协议 | | □是 | □否 |
| 4.是否要求云服务商提供必要的监管接口和日志查询功能 | | □是 | □否 |
| 5.是否定期对云服务开展风  险评估或安全检查 | | □是 | □否 |
| 三、企业安全管理与防护 | 1.是否配备云服务安全管理人员 | | □是 | □否 |
| 2.是否对云服务帐号进行安全管理 | | □是 | □否 |
| 3.是否对云服务客户端实施安全防护（如恶意代码防护、  浏览器版本及插件更新等） | | □是 | □否 |
| 4.是否对云服务的网络、操作系统实施安全配置管理 | | □是 | □否 |
| 5.是否对上云的重要业务系统和应用开展上线前安全测评 | | □是 | □否 |
| 6.是否对上云的数据进行分级分类管理 | | □是 | □否 |
| 7.是否建立安全事件应急处置机制 | | □是 | □否 |
| 8.是否配合云服务商开展应  急响应演练 | | □是 | □否 |
| **（以下内容由使用私有云的企业填写）** | | | | |
| 一、云平台开发与供应链安全 | 1.是否制定系统开发与供应链安全策略（包括采购策略） | | □是 | □否 |
| 2.是否在规划系统建设时考虑了系统的安全需求 | | □是 | □否 |
| 3.是否明确生命周期内各信息安全角色的责任 | | □是 | □否 |
| 4.是否明确外部服务提供商  的安全分工与责任 | | □是 | □否 |
| 5.是否制定了信息系统、组件  或服务的设计规范和安全架构 | | □是 | □否 |
| 6.是否在信息系统、组件或服  务的设计、开发、实现、运行过程中实施了安全配置管理 | | □是 | □否 |
| 7.是否对所开发的信息系统、  组件或服务开展安全测试 | | □是 | □否 |
| 二、云平台系统与通信保护安全 | 1.是否制定系统与通信保护策略（如边界保护策略、移动  代码策略、虚拟化策略） | | □是 | □否 |
| 2.是否对连接外部系统的边界和内部关键边界进行监控、隔离防护 | | □是 | □否 |
| 3.是否在网络出入口以及系统中的主机、移动计算设备上  实施恶意代码防护机制 | | □是 | □否 |
| 4.是否对虚拟机平台实施资  源隔离 | | □是 | □否 |
| 5.是否为云平台中虚拟网络资源间的访问实施网络逻辑隔离，并提供访问控制措施 | | □是 | □否 |
| 6.是否对各用户所使用的虚拟存储资源之间进行逻辑隔离 | | □是 | □否 |
| 三、云平台访问控制 | 1.是否制定访问控制策略与  流程 | | □是 | □否 |
| 2.是否实施用户标识与鉴别措施 | | □是 | □否 |
| 3.是否对接入云平台的设备  实施唯一性标识与鉴别 | | □是 | □否 |
| 4.是否对用户帐号进行严格 | | □是 | □否 |
| 管理 | |  | |
| 5.是否限制信息流向境外 | | □是 | □否 |
| 6.是否采用措施保证远程访问的安全 | | □是 | □否 |
| 四、云平台配置管理 | 1.是否制定合理的安全配置客理策略（基线配置策略、软件使用与限制策略等） | | □是 | □否 |
| 2.是否按最小化原则，根据仅提供的必需功能进行配置 | | □是 | □否 |
| 3.是否按安全配置要求制定、记录并维护当前的基线配置 | | □是 | □否 |
| 五、云平台维护 | 1.是否制定了维护策略（包括  远程维护策略） | | □是 | □否 |
| 2.是否审批、控制并监视维护工具的使用 | | □是 | □否 |
| 3.是否对远程维护和诊断连接明确有关策略和规程，并进行审批和监视 | | □是 | □否 |
| 4.是否建立维护人员的授权  流程和管理规范 | | □是 | □否 |
| 六、云平台安全审计 | 1.是否建立审计管理和审计记录体系 | | □是 | □否 |
| 七、云平台风险评估 | 1.是否制定风险管理策略、风险评估策略、持续监控策略 | | □是 | □否 |
| 2.是否在建设云计算平台时进行了风险评估 | | □是 | □否 |
| 3.是否在系统出入口和网络中的设备上部署垃圾信息监测与防护机制 | | □是 | □否 |
| 八、云平台物理和环境安  全 | 1.是否建立物理安全和环境安全防护手段 | | □是 | □否 |
| 九、企业安全管理与防护 | 1.是否配备云服务安全管理人员 | | □是 | □否 |
| 2.是否对云服务帐号进行安全管理 | | □是 | □否 |
| 3.是否对云服务客户端实施安全防护（如恶意代码防护、  浏览器版本及插件更新等） | | □是 □否 | |
| 4.是否对云服务的网络、操作系统实施安全配置管理 | | □是 □否 | |
| 5.是否对上云的重要业务系统和应用进行上线前安全测评 | | □是 □否 | |
| 6.是否对上云的数据进行分级分类管理 | | □是 □否 | |
| 7.是否建立安全事件应急处置机制 | | □是 □否 | |