2023年全国行业职业技能竞赛——第二届全国工业和信息化技术技能大赛网络与信息安全管理员（工业互联网安全方向）赛项广东省选拔赛理论知识竞赛
命题方案及样题

理论赛题（样例）

2023年9月

2023年全国行业职业技能竞赛——第二届全国工业和信息化技术技能大赛网络与信息安全管理员（工业互联网安全方向）赛项广东省选拔赛理论知识竞赛命题方案

为了参赛选手更有效地备赛，以及确保竞赛组织的严密性和有效性，根据2023年全国行业职业技能竞赛——第二届全国工业和信息化技术技能大赛网络与信息安全管理员（工业互联网安全方向）赛项广东省选拔赛技术方案，对理论知识竞赛的命题工作作一个细化说明。

一、理论知识竞赛的范围及所占总分比例

理论知识竞赛的知识范围分6个模块，分别是：

工业互联网安全政策法规，占10%；工业互联网安全标准规范，占5%；工业互联网安全理论与基础知识，占15%；工业互联网安全技术，占25%；工业互联网安全管理，占20%；工业互联网安全运行，占25%。

二、试题类型和分值

试题全部是客观题，分别是：（1）单项选择题；（2）多项选择题；（3）判断题。竞赛试题由40道单项选择题、30道多项选择题、30道判断题组成，共计100道题目，题目总分100分，其中单项选择题每题1分、多项选择题每题1.5分、判断题每题0.5分。

三、理论知识竞赛时间

理论知识竞赛时间为1小时。

四、考试方式

采用计算机考试。

五、命题和组卷方式

命题采用专家命题，建立具有一定规模的竞赛题库，采用按比例随机组卷的方式生成理论知识竞赛试题。

六、复习参考书

供参考教材清单如下：

（1）魏毅寅，柴旭东. 工业互联网：技术与实践[M].北京：电子工业出版社，第2版。

（2）威廉·斯托林斯. 网络安全基础：应用与标准[M].北京：清华大学出版社，第6版。

（3）魏强，王文海，程鹏. 工业互联网安全：架构与防御[M].北京：机械工业出版社。

（4）闫怀志. 工业互联网安全体系理论与方法[M].北京：科学出版社。

七、每套赛卷各模块的题目类型和数量分配

根据每套赛卷的总量和各模块占比，综合计算，按如下方式分配题目数量。

表 1　每套赛卷的题目类型数量和理论知识模块对照表

序号	理论模块 题目类型	工业互联网安全政策法规	工业互联网安全标准规范	工业互联网安全理论与基础知识	工业互联网安全技术	工业互联网安全管理	工业互联网安全运行	小计
1	单项选择题	4	2	6	10	8	10	40
2	多项选择题	3	1	4	8	6	8	30
3	判断题	3	2	5	7	6	7	30
合计		10	5	15	25	20	25	100

八、各模块知识点（考核点）命题分解

表 2　工业互联网安全政策法规模块命题点分布

序号	知识点（考核点）	
	一级	二级
1	1-1 工业互联网安全相关法律	/
2	1-2 工业互联网安全相关法规	/
3	1-3 工业互联网安全相关政策	/

表 3　工业互联网安全标准规范模块命题点分布

序号	知识点（考核点）	
	一级	二级
1	2-1 工业互联网安全标准体系	/
2	2-2 工业互联网安全相关标准	2-2-1 工业互联网安全相关国际标准
		2-2-2 工业互联网安全相关国内标准

表 4　工业互联网安全理论与基础知识模块命题点分布

序号	知识点（考核点）	
	一级	二级
1	3-1 工业互联网相关基础知识	3-1-1 工业互联网的定义与内涵
		3-1-2 工业互联网发展历程
		3-1-3 工业互联网体系架构
2	3-2 工业互联网安全防护相关理论与模型	3-2-1 网络安全典型理论与模型

		3-2-2 工业互联网安全框架
3	3-3 工业互联网安全相关基础知识	3-3-1 密码学
		3-3-2 网络安全应用
		3-3-3 系统安全

表 5　工业互联网安全技术模块命题点分布

序号	知识点（考核点）	
	一级	二级
1	4-1 工业互联网物理安全	4-1-1 物理访问控制
		4-1-2 盗窃破坏保护
		4-1-3 环境变化保护
		4-1-4 电磁防护
2	4-2 工业互联网设备安全	4-2-1 工业现场设备安全
		4-2-2 智能设备安全
		4-2-3 智能装备安全
3	4-3 工业互联网控制安全	4-3-1 控制软件安全
		4-3-2 控制协议安全
4	4-4 工业互联网网络安全	4-4-1 企业内网络安全
		4-4-2 企业外网络安全
		4-4-3 标识解析系统安全
5	4-5 工业互联网应用安全	4-5-1 工业互联网平台安全
		4-5-2 工业应用程序安全
6	4-6 工业互联网数据安全	4-6-1 数据分类分级保护
		4-6-2 数据脱敏
		4-6-3 数据跨境传输监测
		4-6-4 个人信息保护

表 6　工业互联网安全管理模块命题点分布

序号	知识点（考核点）	
	一级	二级
1	5-1 工业互联网安全策略制度管理	5-1-1 策略制度体系
		5-1-2 策略制度制定与发布
		5-1-3 策略制度评审与修订
2	5-2 工业互联网安全组织机构管理	5-2-1 岗位设置管理
		5-2-2 人员配备管理
		5-2-3 权限授权与审批
		5-2-4 机构间沟通合作
		5-2-5 安全审核与检查
3	5-3 工业互联网安全人员管理	5-3-1 人员录用管理
		5-3-2 人员离岗管理
		5-3-3 人员教育与培训
		5-3-4 外部人员管理

4	5-4 工业互联网安全建设管理	5-4-1 安全方案设计
		5-4-2 产品采购与使用管理
		5-4-3 软件开发管理
		5-4-4 项目实施管理
		5-4-5 验收与交付管理
		5-4-6 供应商管理
5	5-5 工业互联网安全运维管理	5-5-1 环境管理
		5-5-2 资产管理
		5-5-3 介质管理
		5-5-4 设备维护管理
		5-5-5 漏洞和风险管理
		5-5-6 网络和系统安全管理
		5-5-7 恶意代码防范管理
		5-5-8 配置管理
		5-5-9 密码管理
		5-5-10 变更管理
		5-5-11 备份与恢复管理
		5-5-12 安全事件处置
		5-5-13 应急预案管理
		5-5-14 外包运维管理

表 7　工业互联网安全运行模块命题点分布

序号	知识点（考核点）	
	一级	二级
1	6-1 工业互联网安全风险评估	6-1-1 风险评估原理
		6-1-2 风险评估实施
		6-1-3 风险评估工作形式
		6-1-4 风险评估相关工具
2	6-2 工业互联网安全监测预警	6-2-1 安全监测
		6-2-2 风险预警
3	6-3 工业互联网安全应急响应	6-3-1 应急响应处置流程
		6-3-2 常见安全事件的处置
4	6-4 工业互联网安全威胁信息共享	6-4-1 威胁信息内容
		6-4-2 威胁信息共享模型
		6-4-3 威胁信息共享流程
5	6-5 工业互联网安全审计	6-5-1 审计流程
		6-5-2 审计形式
		6-5-3 常见产品与工具

2023年全国行业职业技能竞赛——第二届全国工业和信息化技术技能大赛网络与信息安全管理员（工业互联网安全方向）赛项广东省选拔赛理论知识竞赛样题

考试时间：60分钟　　考试形式：上机考试

一、单项选择题（共40题，每题1分，共40分）

1．中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施（）和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

A　网络安全法　　B　数据安全相关标准

C　国家数据安全战略　　D　数据安全法

2．《中华人民共和国网络安全法》规定，网络运营者应当制定（），及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

A　网络安全应急演练方案　　B　网络安全事件应急预案

C　网络安全规章制度　　D　网络安全事件补救措施

3．根据《工业互联网标识管理办法》要求，标识服务机构应当建立网络安全防护技术手段，依法记录并留存标识注册日志、标识解析日志、维护日志和变更记录，各日志留存时长不少于（）个月，保障标识服务的质量和标识服务系统安全。

A　3　　B　6　　C　9　　D　12

4．（）的正式印发，成为我国工业互联网发展的纲领性文件。

A　《中华人民共和国网络安全法》

B　《关于深化“互联网+先进制造业” 发展工业互联网的指导意见》

C　《工业互联网发展行动计划（2021-2023年）》

D　《推动工业互联网加快发展的通知》

5．在下列标准中，属于强制性标准的是（）。

A　GB 40050-2021 网络关键设备安全通用要求

B　GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

C　GB/Z 41288-2022 信息安全技术 重要工业控制系统网络安全防护导则

D　YC/T 580-2019 烟草行业工业控制系统网络安全基线技术规范

6．以下属于 GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》所规定的信息安全事件类型的是（）。

①有害程序事件　②设备设施故障　③信息破坏事件　④信息内容安全事件

A　①②　　B　①③④

C　①②④　　D　①②③④

7．“工业互联网”的概念首次是由（）提出。

A　微软公司　　B　华为公司　　C　英特尔公司　　D　通用电气公司

8．P2DR 模型建立在基于时间的安全理论基础之上，将网络安全的实施分为防护、检测和（）三个阶段。

A　评估　　B　响应　　C　应急　　D　溯源

9．IATF（信息技术保障框架）提出保障信息系统安全应具备的三个核心要素包括人、技术和（）。

A　环境　　B　设备　　C　规范　　D　操作

10．工业互联网安全框架中（）视角涵盖设备、控制、网络、应用和数据五大安全重点。

A　防护对象视角　　B　防护措施视角　　C　防护管理视角　　D　防护流程视角

11．DES 是一种数据分组的加密算法，它将数据分成长度为（）位的数据块，其中一部分用作奇偶校验，剩余部分作为密码的长度。

A　56 位　　B　64 位　　C　112 位　　D　128 位

12．关于防火墙的部署位置，正确的是（）。

A　只需要在与 Internet 相连接的出入口设置

B　在需要保护局域网络的所有出入口设置

C　需要在出入口和网段之间进行部署

D　只需在 DMZ 区部署

13．以下哪项不属于确保工业互联网物理安全应采取的措施（）。

A　加装门禁卡　　B　加装温湿度计

C　部署态势感知系统　　D　安装视频监控系统

14．以下属于对智能设备固件进行安全加固的措施的是（）。

A　漏洞扫描　　B　加装安全芯片　　C　出厂前检测　　D　数据传输链路加密

15．关于控制协议 Modbus 的安全缺陷，哪一项是错误的（）。

A 没有认证机制 B 没有终端加密 C 没有数据加密 D 没有消息检验

16. 以下哪项措施无法提升 SCADA 系统中监控软件的安全防护水平（）。

A 为运行监控软件的主机的操作系统安装防病毒软件

B 及时备份监控软件数据库中存储的数据

C 为所有使用监控软件的用户分配账户并启用监控软件的操作记录功能

D 为运行监控软件的主机所在的房间加装视频安防系统

17. 防火墙按照其工作原理可划分为（）。

A 独立式防火墙和集成式防火墙 B 网络防火墙和主机防火墙

C 包过滤防火墙、代理防火墙和状态检测防火墙 D 软件防火墙和硬件防火墙

18. Zigbee 具有三级安全模式，其数据加密标准是（）。

A DES B 3DES C AES64 D AES128

19. 以下不属于工业互联网平台基础设施层安全防护范围的是（）。

A 操作系统安全 B 网络通信设备安全

C 磁盘阵列设备安全 D 数据建模服务安全

20. 以下哪项是无法通过移动应用加固可以解决的安全问题（）。

A 二次打包 B 恶意篡改 C 权限滥用 D 代码破解

21. 境内数据与跨境数据应根据（）进行保护。

A 国家要求 B 省份要求 C 行业要求 D 企业要求

22. 下列不属于数据脱敏操作必须满足的要求的是（）。

A 单向性 B 无残留 C 易于实现 D 双向性

23. 以下属于工业互联网安全策略需阐述的内容的是（）。

A 管理办法 B 防护范围 C 操作规范 D 处罚条例

24. 对于工业互联网安全防护，其保密性、完整性、可用性按照重要程度由高到低依次为（）。

A 保密性、完整性、可用性 B 可用性、完整性、保密性

C 完整性、可用性、保密性 D 可用性、保密性、完整性

25. 企业内部建设的工业互联网安全态势感知平台在运行过程中应配备系统管理员、（）和安全管理员。

A 运维管理员 B 测试管理员 C 数据管理员 D 审计管理员

26. 关于工业互联网平台运行过程中安全相关岗位人员管理的要求，不正确的是（）。

A 平台安全管理员和系统管理员不能由一人兼任

B　平台开发人员不能兼任安全管理员、系统管理员

C　平台系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作

D　平台数据库管理员在对平台数据库中的数据进行全量备份时，应保证至少两人同时在场

27．工业互联网安全防护措施应与业务建设过程同步规划、同步建设、（）。

A　同步设计　　B　同步开发　　C　同步测试　　D　同步使用

28．工业互联网网络安全设计的原理不包括以下哪项（）。

A　纵深防御　　B　网络分区　　C　弹性设计　　D　绝对安全

29．以下属于漏洞扫描工具的是（）。

A　Nmap　　B　OpenVAS　　C　Snort　　D　WireShark

30．商用密码服务使用网络关键设备和网络安全专用产品的，应当经（）对该商用密码服务认证合格。

A　商用密码认证机构　　B　专用密码认证机构

C　普通密码认证机构　　D　核心密码认证机构

31．工业互联网数据生命周期风险中，数据处理阶段面临的风险主要是（）。

A　处理过程中的恶意操作，缺少命令自动审批机制，治理流程脱管，隐私泄密风险

B　数据保护措施与敏感级别不匹配，统一访问控制机制存在短板，运营/运维人员拖库撞库风险

C　明文传输、内容嗅探、内容截取、内容篡改等风险

D　未授权访问、数据窃取、数据破坏及篡改、明文存储等风险

32．开展工业互联网安全评估评测工作，组建评估团队人数建议为（）。

A　1-2 人　　B　2-3 人　　C　3-5 人　　D　7-10 人

33．工业互联网安全风险预警主要包含哪些内容（）。

A　安全漏洞预警　　B　威胁情报预警　　C　用户行为基线　　D　以上都是

34．在工业互联网安全监测服务体系建设方面我国采取的是“部—省—（）”三级联动的体系。

A　市　　B　行业　　C　协会　　D　企业

35．网络安全事件应急响应的“黄金时间窗口”是（）。

A　24 小时　　B　48 小时　　C　72 小时　　D　96 小时

36．下列哪项不属于工业互联网安全应急响应流程抑制阶段应采取的措施（）。

A 控制事件蔓延　　B 日常运维监控　　C 抑制响应　　D 抑制监测

37．目前威胁信息的用途日趋广泛，以下不属于其用途的是（）。

A 安全体系建设与完善　　B 攻击检测与防御

C 安全部门汇报　　D 安全事件分析及响应

38．威胁信息是一种基于证据的知识，它就网络资产可能存在或出现的风险、威胁，给出了相关联的场景、机制、指标、内涵及可行的建议等，可为企业响应相关威胁或风险提供决策信息，但在威胁信息共享的过程中也需考虑对信息的敏感性保护，以下属于 Web 攻击威胁信息中不可提供的是（）。

A IP　　B URL　　C 域名　　D 口令

39．工业互联网安全审计的作用不包括（）。

A 为网络故障提供准确的故障定位和责任定位

B 实现充分隔离，防止蠕虫病毒等安全威胁通过网络向不同用户扩散

C 通过改进降低或杜绝同类事故的发生率

D 为故障定位提供有效的事件链数据

40．关于对工业互联网平台进行安全审计，下列说法不正确的是（）。

A 应对平台中与安全有关的活动的相关信息进行识别、记录、存储和分析

B 应对平台的安全状况做到持续、动态、实时的有依据的安全审计

C 应对平台的源代码进行逐条检查和分析，发现是否存在程序错误，安全漏洞和违反程序规范

D 应向用户提供安全审计的标准和结果

二、多项选择题（共 30 题，每题 1.5 分，共 45 分）

1．《中华人民共和国密码法》中规定了（）的相关要求。

A 核心密码　　B 重要密码　　C 普通密码　　D 商用密码

2．《网络产品安全漏洞管理规定》鼓励发现网络产品安全漏洞的组织或者个人向以下哪些机构报送网络产品安全漏洞信息（）。

A 工业和信息化部网络安全威胁和漏洞信息共享平台

B 国家网络与信息安全信息通报中心漏洞平台

C 国家计算机网络应急技术处理协调中心漏洞平台

D 中国信息安全测评中心漏洞库

3．下列哪些是《加强工业互联网安全工作的指导意见》的联合印发部门（）。

A　工业和信息化部　　B　国家市场监督管理总局　C　公安部　　D　应急管理部

4．在《工业互联网安全标准体系》（2021 年）中，包含以下哪三类标准（）。

A　分类分级防护　　B　安全运维　　C　安全管理　　D　安全应用服务

5．工业互联网作为全新工业生态、关键基础设施和新型应用模式，通过人、机、物的全面互联，实现（）的全面连接。

A　全要素　　B　全流程　　C　全产业链　　D　全价值链

6．工业互联网平台 PaaS 层提供以下哪些功能（）。

A　IT 资源管理　　B　工业数据与模型管理

C　工业建模分析　　D　工业应用创新

7．德国 RAMI4.0 从哪三个视角构建了工业 4.0 参考架构（）。

A　CPS 功能视角　　B　CPS 安全视角

C　全生命周期价值链视角　　D　全层级工业系统视角

8．无线网络所面临的安全威胁包含以下哪些（）。

A　偶然连接　　B　身份盗窃　　C　中间人攻击　　D　拒绝服务

9．针对机房中放置的服务器等设备可能存在的电磁泄露问题，可采取以下方法进行防护（）。

A　抑源防护　　B　屏蔽防护　　C　滤波防护　　D　干扰防护

10．以下属于 HMI 设备自身安全防护措施的是（）。

A　对 HMI 固件版本进行升级　　B　在不传输运行日志时关闭 FTP 服务

C　为 HMI 提供双网冗余　　D　为 HMI 设置操作口令

11．软件防篡改是保障控制软件安全的重要环节，具体措施包括下列的（）。

A　控制软件在投入使用前进行代码测试

B　采用完整性校验措施对控制软件进行校验

C　对控制软件中的代码进行加密

D　做好控制软件和组态程序的备份工作

12．为了保障商用密码安全，国家商用密码管理办公室制定了一系列密码标准，下列属于对称算法的是（）。

A　SM1　　B　SM2　　C　SM3　　D　SM4

13．网络分区与隔离在一定程度上保证了内部网络的安全性，以下哪些设备或系统不能用于网络分区与隔离（）。

A　防火墙　　B　入侵检测系统　　C　日志审计系统　　D　网闸

14．根据工业互联网安全框架，工业互联网应用安全包含以下哪些内容（）。

A　工业互联网设备安全　　B　工业互联网网络安全

C　工业互联网平台安全　　D　工业应用程序安全

15．以下哪些措施可用于工业互联网平台 PaaS 层安全防护（）。

A　设备接入认证　　B　网络隔离　　C　文件加密　　D　数据脱敏

16．在进行工业互联网业务数据备份过程中常用的备份方式有（）。

A　完全备份　　B　按需备份　　C　差分备份　　D　增量备份

17．下列哪些选项属于网络安全管理制度应该包括的主要内容（）。

A　网络安全配置　　B　安全策略　　C　授权访问制度　　D　补丁升级制度

18．下列哪些事项应列入需建立工业互联网业务安全审批程序的事项（）。

A　新增控制系统　　B　MES 系统运维人员培训

C　设备机房空调维修　　D　工业互联网平台功能升级

19．企业应与工业控制系统运行相关关键岗位的所有人员签署保密协议，保密协议内容应包括（）。

A　保密范围　　B　保密责任　　C　免责条款　　D　保密期限

20．以下属于工业互联网安全建设管理的内容是（）。

A　安全方案设计　　B　产品采购和使用　　C　设备维护管理　　D　供应商选择

21．对于工业互联网业务系统的数据备份，应明确其（）。

A　备份方式　　B　备份频度　　C　存储介质　　D　保存期限

22．一般情况下对于工业互联网业务的运维不得采用远程在线方式，如确需远程在线方式则需采取的安全防护措施包括（）。

A　补丁升级　　B　访问控制　　C　流量监测　　D　行为审计

23．工业互联网安全评估评测项目主要包括以下哪几个阶段（）。

A　准备阶段　　B　编制工作方案　　C　开展现场评测　　D　编制报告

24．BurpSuite 是渗透测试中经常用到的工具，下列属于其主要功能的是（）。

A　数据包抓取与篡改　　B　端口扫描　　C　口令破解　　D　流量重放

25．态势感知在网络安全方面具有检测、分析、预测、防御的能力，以下属于网络安全态势预测方法的是（）。

A　神经网络　　B　时间序列预测　　C　无规则预测　　D　支持向量机

26．根据演练深度的不同，灾难恢复演练可分为（）。

A 数据级演练　　B 应用级演练　　C 业务级演练　　D 计划外演练

27．下列不属于工业互联网安全应急响应在根除阶段应采取的动作的是（）。

A 查找病毒木马、非法授权、系统漏洞并及时处理

B 根据发生的安全事件修订安全策略，启用安全审计

C 阻断正在发起的攻击行为，降低影响范围

D 确认安全事件造成的损害程度，上报安全事件

28．威胁信息的共享流程包括（）。

A 需求分析　　B 信息收集　　C 信息分析　　D 信息反馈

29．网络安全审计的内容包括（）。

A 监控网络内部的用户活动　　B 对数字证书的签发、撤销

C 对日常运行状况的统计和分析　　D 对安全事件的事后分析

30．网络安全审计系统一般包括（）。

A 网络探测引擎　　B 数据管理中心　　C 审计中心　　D 声光报警系统

三、判断题（共 30 题，每题 0.5 分，共 15 分）

1．根据《工业和信息化领域数据安全管理办法（试行）》，工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。（）

2．《工业互联网创新发展行动计划（2021-2023 年）》着力解决工业互联网发展中的深层次难点、痛点问题，推动产业数字化，带动数字产业化。（）

3．《加强工业互联网安全工作的指导意见》中提出地方工业和信息化主管部门监管本行政区域内标识解析系统、公共工业互联网平台等的安全工作。（）

4．YD/T 3865-2021《工业互联网数据安全保护要求》规定了工业互联网数据安全保护的范围及数据类型、工业互联网数据重要性分级与安全保护等级划分方法。（）

5．IEC 62443-2-2 中提出了对工业自动化控制系统制造商信息安全政策与实践的认证。（）

6．工业互联网是跨界融合的系统性工程，是与工业生产紧密相关的新型网络基础设施。（）

7．工业互联网总体业务视图包括产业层、商业层、应用层、能力层四个层次。（）

8．P2DR 模型是一种基于闭环控制的动态安全模型，适用于需要短期安全防护的网络系统。（）

9．HTTPS 是指用 HTTP 和 SSH 结合的技术来实现网络浏览器和服务器之间的安全通信。（）

10. 网络中的安全域是一个逻辑区域，同一安全域中的设备资产具有相同或相近的安全属性。（）

11. 智能设备自身安全防护手段薄弱以及攻击者利用智能设备作为跳板攻击工业互联网平台或其他网络，成为工业互联网设备目前面临的两大安全问题（）。

12．从网络安全角度考虑，DCS 控制站不能进行开放性互联设计，各 DCS 厂家应采用自行研发的通信标准。（）

13．在“5G+工业互联网”应用场景中，可通过网络切片实现不同生产区域网络之间的物理隔离。（）

14．对于标识解析系统首先应保障其解析结果的保密性。（）

15．虚拟化安全是工业互联网平台基础设施层安全防护的主要需求之一。（）

16．由于工业 APP 需通过编译器将源代码编译成二进制可执行文件，因而在工业 APP 开发过程中可将默认账户口令以明文形式写在源代码中以减少用户在登录过程中的等待时间。（）

17．工业数据在不同平台间持续流动，加剧了工业数据的安全风险。（）

18．工业互联网安全管理制度体系在执行过程中，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。（）

19．为减小工业互联网业务遭到网络攻击的可能性，工业互联网业务安全管理机构应尽量避免与外部专家及组织开展合作与交流。（）

20．负责污水处理控制系统的系统管理员离岗后，应立即注销其所使用的账户或更换操作密码。（）

21．委托第三方开发的工业 APP 在上线前应对其安全性进行测试。（）

22．鉴于目前针对 Linux 系统的恶意代码较少，因而在制定针对工业互联网平台所使用的 Linux 服务器安全管理制度时无需要求在服务器上安装恶意代码防范程序。（）

23．多人使用统一账号对工业防火墙进行管理有利于提升工业互联网安全防护效果。（）

24．在开展工业互联网安全评估评测工作时，完成编制工业互联网安全评估评测工作方案后即可开展现场评估评测工作。（）

25. 网络安全预警级别根据网络安全保护对象的重要程度和网络安全保护对象可能受到损害的程度分为四个级别：红色预警、橙色预警、黄色预警和蓝色预警。（）

26．工业互联网应急响应实施过程包括准备、检测、抑制、根除、恢复、跟踪 6 个步骤。（）

27．last | more 命令在数据泄露事件检测过程中可用于查看最近启动的进程信息。（）

28．威胁信息共享的出现将工业互联网安全防护从传统的静态被动防护转向主动式、覆盖全生命周期的防护，而时效性是威胁信息共享机制构建过程中应考虑的主要因素之一。（）

29．安全审计产品按照其采用的关键技术可划分为系统审计、网络审计、综合审计等。（）

30．网络安全审计的作用在于建立事后安全保障机制。（）