第三方网络安全要求

编制：网络安全和技术风险部
版本：2.0
生效日期：2020 年 9 月 24 日

1. 简介

《GE 第三方网络安全要求》文档概述了适用于 GE 第三方（包括供应商和合资企业）的网络安全要求。本文档中概述的安全要求适用于对 GE 敏感信息（内部分类为 GE 机密或 GE 高度机密）、PII 或敏感 PII 进行处理、访问、交互或存储，有权访问 GE 信息系统，或提供某些服务/产品（包括 OT/制造服务）的第三方，如下所述。安全要求因第三方向 GE 呈现的风险级别而异，具体取决于 GE 信息类型、第三方流程、网络连接和第三方提供的产品和服务，以及数据可用性和弹性要求。

GE 保留不时更新本文档的权利。

2. 最低安全要求

适用性：最低安全要求适用于（以逻辑方式）处理、访问或存储 GE 机密信息或个人数据、GE 高度机密信息或敏感个人数据、受控数据的第三方，或与 GE 托管网络建立直接网络连接的第三方。

最低要求的 ISO 27001 管控措施	
2.1	6.2.1 移动设备策略
2.2	7.2.2 信息安全意识、教育和培训
2.3	8.1.1 资产盘点
2.4	8.1.4 资产返还
2.5	9.1.2 访问网络和网络服务
2.6	9.2.1 用户注册和注销
2.7	9.2.2 用户访问设置
2.8	9.2.3 特权访问权限的管理
2.9	9.2.6 访问权限的移除或调整
2.10	9.4.1 信息访问限制
2.11	9.4.2 安全登录程序
2.12	9.4.3 密码管理系统
2.13	10.1 加密控制
2.14	11.1.1 物理安全边界
2.15	11.1.2 物理进入控制
2.16	11.1.3 确保办公室、机房和设施的安全
2.17	11.1.4 防范外部和环境威胁
2.18	11.2.3 线缆布设安全
2.19	12.1.4 开发、测试和运行环境的分离
2.20	12.2.1 恶意软件防控
2.21	12.4.1 事件记录
2.22	12.4.3 管理员和操作员日志
2.23	12.6.1 技术漏洞管理

最低要求的 ISO 27001 管控措施	
2.24	13.1.1 网络控制
2.25	13.1.3 网络区隔
2.26	13.2.3 电子消息传送
2.27	14.1.3 保护应用服务事务
2.28	14.3.1 测试数据的保护
2.29	15.1.1 供应商关系相关信息安全策略
2.30	15.2.1 供应商服务的监控和评审
2.31	15.2.2 管理供应商服务的变更
2.32	16.1.5 信息安全事故响应
2.33	18.2.1 信息安全的独立评审
2.34	18.2.3 软件合规性评审

追加最低安全要求	
2.35	应建立、实施并积极管理所有用于第三方信息系统硬件和软件的安全配置。
2.36	每年至少应进行一次网络和系统漏洞评估。发现危急漏洞后，应在 30 天内对其进行追踪和修复。
2.37	如果不需要或不使用本地帐户，则应禁用本地帐户，且不得将其用于特权访问。
2.38	如果具有 GE 单点登录 (SSO) 凭据的第三方员工被辞退或调离，则第三方应不迟于该事件发生之日通知 GE。
2.39	如果账户闲置不用，则至少应在 90 天之后将其禁用。
2.40	不得在个人帐户上或个人拥有的计算机、设备或媒体上处理或存储 GE 机密信息。
2.41	第三方不得使用或向 GE 提供由卡巴斯基实验室或“实体列表”（《出口管理条例 (EAR)》第 744 部分第 4 号补充文件）中按照“国家/地区”在“中华人民共和国”一栏下所确定的厂商（包括但不限于华为、中兴通讯、海能达通信股份有限公司、杭州海康威视数字技术公司和浙江大华技术股份有限公司，含其关联公司及子公司）生产的任何产品或服务。
2.42	所有连接到 GE 网络的非 GE 端点（笔记本电脑、台式电脑等）都必须至少安装最新的防病毒软件和防火墙。上述端点还应包括 EDR、DLP 和加密等处理。
2.43	如果通过电子邮件发送机密或高度机密的 GE 数据，则应使用 TLS 1.2 或 TLS 1.3（或最新版本的 TLS 加密）对电子邮件进行加密。
2.44	所有非个人帐户（即由 IT 系统而非人员使用的帐户），例如服务帐户或系统帐户，均应由个人或团队管理。
2.45	网络级入侵检测或预防系统应全天候 (24×7×365) 监控“危急”和“严重”级别警报。
2.46	如果适用，应每 12 个月对存储、处理、托管和/或传输 GE 数据的应用程序进行一次 Web 应用程序漏洞评估。

3. 物理安全要求

适用性：物理安全要求适用于（以逻辑方式或物理方式）处理、访问或存储 GE 机密信息或个人数据、GE 高度机密信息或敏感个人数据、受控数据的第三方，或与 GE 托管网络建立直接网络连接的第三方。

物理安全要求	
3.1	对于用于访问、处理、传输和/或存储 GE 数据的所有设施，应在所有入口点使用胸牌读取器，以确保仅限授权人员进行物理访问。注意：如果仅在云环境中存储或处理 GE 数据，请根据您所属组织对云托管服务提供商处适当安全管控措施到位情况的确认来回应此管控措施。
3.2	所有用于存储和/或访问 GE 数据的服务器和网络设备均应置于具有以下管控措施的安全机房中： 1. 入口门上设有附加门禁机制（例如胸牌、生物识别、别针等）； 2. 除非防止粉碎的防护装置已到位，否则机房应位于无窗户的建筑物内部；以及 3. 接收数据或支持服务的电信设备、电缆和中继器以隐蔽方式布置，以遏阻窃听或破坏。 注意：如果仅在云环境中存储或处理 GE 数据，请根据您所属组织对云托管服务提供商处适当安全管控措施到位情况的确认来回应此管控措施。如果上述所有方面均未落实，请回答“否”，并指出在哪些方面未达到要求。
3.3	对于用于访问、处理、传输和/或存储 GE 数据的所有设施，应装设安防摄像头，以监控设施的周边、入口点/出口点和内部。注意：如果仅在云环境中存储或处理 GE 数据，请根据您所属组织对云托管服务提供商处适当安全管控措施到位情况的确认来回应此管控措施。
3.4	安防摄像头记录的影像应保留至少 30 天。
3.5	对于用于访问、处理、传输和/或存储 GE 数据的所有设施，应在人员进入设施时由保安人员、安全门廊或其他方式管控访问。注意：如果仅在云环境中存储或处理 GE 数据，请根据您所属组织对云托管服务提供商处适当安全管控措施到位情况的确认来回应此管控措施。
3.6	应向所有员工、承包商和访客发放识别胸牌，且他们应始终佩戴识别胸牌。注意：如果仅在云环境中存储或处理 GE 数据，请根据您所属组织对云托管服务提供商处适当安全管控措施到位情况的确认来回应此管控措施。
3.7	识别胸牌应将全职员工与承包商和访客区分开来。
3.8	所有包含 GE 数据/信息的物理文档均应置于上锁的办公室、柜子或其他上锁的位置，并且仅限授权人员访问。注意：如果您所属组织不存储包含 GE 数据/信息的物理文档，请选择“不适用”，并添加注释“不存储物理文档”。
3.9	应建立机制来通知、调查和解决潜在的物理安全事故，例如物理入侵或资产被盗。
3.10	如果用于访问、处理、传输和/或存储 GE 数据的所有设施均未配备人员全天候 (24×7×365) 值守，则应安装警报器，以对非工作时间内的访问进行监控。注意：如果用于访问、处理、传输和/或存储 GE 数据的所有设施均未配备人员全天候 (24×7×365) 值守，请选择“不适用”，并添加注释“所有设施均配备人员全天候 (24×7×365) 值守”。
3.11	如果与其他占用者（例如同位数据中心）共享用于访问、处理、传输和/或存储 GE 数据的设施，是否在占用者之间实施了保护机制（例如，上锁机笼、凭胸牌出入等），以防止擅自访问您所属组织的物理设备？注意：如果不与其他占用者共享用于访问、处理、传输和/或存储 GE 数据的设施，请选择“不适用”，并添加注释“不共享设施”。

物理安全要求	
3.12	应每年（至少）审查一次物理访问权限，并根据需要对其进行更新，以确保对用于访问、处理、传输和/或存储 GE 数据的所有设施的物理访问仅限于授权人员。注意：如果仅在云环境中存储或处理 GE 数据，请根据您所属组织对云托管服务提供商处适当安全管控措施到位情况的确认来回应此管控措施。

4. 强化安全要求

适用性：增强安全要求适用于（以逻辑方式或物理方式）处理、访问或存储 GE 高度机密信息或敏感个人数据、受控数据的第三方，或与 GE 托管网络建立直接网络连接的第三方。

强化要求的 ISO 27001 管控措施	
4.1	5.1.1 信息安全政策
4.2	5.1.2 信息安全政策的审查
4.3	6.1.1 信息安全角色和职责
4.4	6.1.2 职责的划分
4.5	7.1.1 筛查
4.6	7.2.1 管理职责
4.7	8.3.1 可移动媒体的管理
4.8	8.3.2 媒体处置
4.9	8.3.3 物理媒体传输
4.10	9.2.4 用户密钥身份验证信息的管理
4.11	9.2.5 用户访问权限的审查
4.12	9.4.5 程序源代码的访问管控
4.13	11.2.7 设备的安全处置或重复使用
4.14	12.1.1 文档化操作程序
4.15	12.1.2 变更管理
4.16	12.4.2 日志信息的保护
4.17	12.5.1 在操作系统上安装软件
4.18	12.6.2 软件安装限制
4.19	12.7.1 信息系统审核控制措施
4.20	14.2.2 系统更改管控程序
4.21	16.1.1 责任和程序
4.22	16.1.2 报告信息安全事件
4.23	16.1.4 信息安全事件评估与决策
4.24	16.1.6 从信息安全事故吸取教训
4.25	18.1.4 个人身份信息的隐私和保护

追加强化安全要求	
4.26	应维护对第三方环境内（永久性或临时性）驻留的所有 GE 高度机密信息、受控数据或敏感个人数据相关数据流的准确记录。
4.27	第三方应实施数据丢失防护 (DLP) 管控措施（例如，禁用 USB 端口、DLP 软件、URL/Web 过滤），以检测并防止擅自从第三方信息系统删除 GE 高度机密信息、受控数据或敏感个人数据。
4.28	除非适用法律法规禁止或另有要求，否则应从事件或日志记录发生之日起将第三方信息系统审计日志集中并保留至少 12 个月。
4.29	应至少每年定期测试事故管理计划一次（例如桌面测试），以验证计划的稳健性。测试应根据第三方环境面临的高风险威胁（例如病毒/蠕虫攻击、数据泄露、实物资产损失）执行，并应与提供给 GE 的服务相关。
4.30	第三方应使流程落实到位，以监控关键安全指标。这些指标至少应包括防病毒代理运行状况、补丁和漏洞管理、安全基线配置管理和信息安全事故管理。
4.31	应通过正式的流程管控密码的分配/重置。应在密码重置之前验证用户身份。应以安全的方式向用户提供临时密码，且临时密码应在首次使用后失效。不得使用基于知识的身份验证重置。不得使用密码提示。
4.32	在授权用户选择其密码之前，应对照已知错误选择的字典检查新密码。
4.33	当用户处于不活动状态 15 分钟之后，第三方应实施机制，以锁定第三方工作站，要求用户重新进行身份验证。当用户处于不活动状态 30 分钟之后，所有其他第三方信息系统（例如应用程序）应实施机制，以锁定该用户。
4.34	第三方应实施机制，以检测并停用未经授权的（例如恶意的）接入点。
4.36	紧急帐户只能在有限的情况下使用，并应有落实到位的机制，以确保对个人的追踪、职责的妥善划分、适当的批准以及对具有高度受控访问权限的凭据的安全存储。
4.37	第三方应至少使用双因素身份验证来远程访问第三方环境。应以与行业标准一致的级别加密此类传输。
4.38	用于访问、处理、传输和/或存储 GE 高度机密信息、受控数据或敏感个人数据的所有设施均应装设安防摄像头，以监控设施的周边、入口点/出口点和内部。记录的影像应保留至少 30 天。所有接收区域均应有人值守或有其他方式来控制物理访问。除非防止粉碎和擅自进入的防护装置已到位，否则服务器机房应位于无窗户的建筑物内部。
4.39	如果使用 Active Directory，则应遵循 Microsoft 最佳安全实践。
4.40	应实施基于网络的 DLP 解决方案，以监视和管控传入和传出的电子邮件、网络和应用程序流量。
4.41	应在所有台式电脑、笔记本电脑和服务器上安装基于主机的入侵防护系统 (HIPS)。

5. 软件开发

适用性：软件开发要求适用于开发特定于 GE 需求的软件，或处理 GE 高度机密信息、机密信息、受控数据或敏感个人信息的主机应用程序的第三方。

软件开发要求的 ISO 27001 控制措施	
5.1	14.2.1 安全开发策略
5.2	14.2.8 系统安全测试
5.3	14.2.9 系统验收测试

追加软件开发要求	
5.4	第三方应向所有开发人员提供应用程序安全培训。应向开发人员提供有关已发现常见漏洞数量以及预防和修复措施的反馈。
5.5	应将信息安全检查要点纳入软件开发生命周期，包括但不限于： a. 风险评估流程 b. 文档化安全要求 c. 安全编码指导原则和检查表 d. 安全设计/架构审查 e. 源代码审查 f. 安全测试
5.6	如果在测试期间发现危急/严重漏洞（中等和轻微漏洞取决于影响），应在识别后 30 天之内且在将代码投入生产之前修复并重新所有已确认的危急/严重漏洞。 应根据要求向 GE 提供一份包含安全测试范围和结果（包括任何问题/异常情况）的正式报告。
5.7	除非 GE 批准，否则为 GE 开发的任何软件均不得包含由签约第三方以外实体开发或销售的任何软件（无论是专有还是开源软件）。
5.8	交付给 GE 的所有软件均不得含有被认定为“危急”或“严重”风险的缺陷/漏洞。如果要交付具有危急或严重风险漏洞的软件，则应获取 GE 业务应用程序所有者的批准。申请批准时，应将业务应用程序安全负责人姓名抄写在通讯上，通讯应采用电子邮件方式。
5.9	如果第三方托管应用程序经历重大更改或增强，GE 可以选择在向生产中实施更改之前（以手动和/或自动方式）执行技术渗透测试。在 GE 认为可接受的情况下，如果报告符合 GE 的质量标准且于过去 12 个月之内编制，则应利用第三方的渗透测试结果。
5.10	应每两年重新评估一次所有的第三方托管应用程序。重新评估包括但不限于（以手动和/或自动方式执行的）技术渗透测试。

6. 强化软件开发

适用性：强化软件开发安全要求适用于开发特定于 GE 需求的软件，或通过与 GE 的受信任第三方网络连接处理高度机密信息、机密信息、受控数据或敏感个人数据的主机应用程序的第三方。

要求的 ISO 27001 管控措施	
6.1	7.2.2 信息安全意识、教育和培训
6.2	14.2.6 安全开发环境
6.3	14.2.7 外包开发

追加强化软件开发要求	
6.4	第三方应指定一名应用程序安全代表担任第三方与 GE 在安全应用程序开发相关事宜上的主要联络人，从而确保第三方开发团队满足 GE 对安全应用程序开发的所有要求，并根据要求向 GE 提供符合本节所列要求的证据。
6.5	在启动任何项目之前，第三方应向 GE 应用程序所有者申请获取应用程序的风险分类（危急还是非危急）和网络暴露标志（面向外部还是内部）。应在启动代码开发之前确定这些风险因素。
6.6	应为应用程序的所有新开发（包括涉及对 GE 标记为“危急”和/或“面向外部”的现有应用程序进行重大更改的项目）正式定义文档化安全要求。应在必要时与 GE 应用程序所有者和其他主要利益相关者合作制定这些要求。应将所有安全设计要求与更广泛的一系列应用程序要求一起记录和维护。
6.7	软件开发团队应使用 GE 提供的版本控制流程和工具。
6.8	应用程序开发应在安全的开发环境中进行。开发环境应包含以下管控措施：访问管控、异地备份、不同开发环境（例如开发、暂存、测试等）之间的逻辑分离、对支持开发环境的关联系统的更改管控、生产发布前应用程序代码更改的批准流程、特定权限以及与将代码和测试数据移入和移出环境相关的审批记录。
6.9	以 GE 解决方案支持的编程语言所编码的所有应用程序均必须进行静态应用程序安全测试 (SAST)。《GE 网络安全和技术风险要求》中提供了编程语言列表。如果 GE 提供的解决方案不支持应用程序源代码，则不需要进行 SAST，而只需要进行手动代码审查。
6.10	如果在手动和自动 (SAST) 代码审查期间发现严重/危急漏洞，则应在向 GE 发布（包括部署到生产中）之前纠正所有已确认的严重/危急漏洞。应使用 GE 提供的解决方案执行 SAST。如果暂停或停止编码，则在继续编码之前不需要执行 SAST。
6.11	所有具有浏览器界面的应用程序均必须进行动态应用程序安全测试 (DAST)。应至少在项目完成前进行一次该测试。如果在 DAST 测试期间发现危急和严重漏洞，则应在发布回 GE（包括部署到生产中）之前修复并验证所有已确认的危急和严重漏洞。应使用 GE 提供的解决方案执行 DAST。
6.12	应纳入安全设计审查，以验证要求的安全特性和功能。
6.13	为 GE 开发的所有应用程序均需要防威胁模型。

7. 系统和数据可用性

适用性：系统和数据可用性要求适用于处理、访问或存储具有高可用性要求的高度机密信息、机密信息、受控数据或敏感个人数据，或具有 GE 所定义之高可用性要求的第三方服务/应用程序的第三方。

要求的 ISO 27001 管控措施	
7.1	12.1.1 文档化操作程序
7.2	12.1.3 容量管理
7.3	12.3.1 信息备份
7.4	17.1.1 规划信息安全连续性
7.5	17.1.2 实施信息安全连续性
7.6	17.1.3 验证、审查和评估信息安全连续性

	追加系统和数据可用性要求
7.7	第三方应为用于向 GE 提供服务的所有位置和应用程序维持灾难恢复计划 (DRP)。DRP 应当包括下列要素： a. 以文档记录的关键业务功能、应用程序和配套技术。 b. 记录引发灾难的因素、有权宣布灾难的人员以及沟通计划，包括通知 GE。 c. 确定具有满足恢复需求的必要基础设施的备用位置。 d. 记录灾难响应和恢复团队的管理和成员资格。 e. 记录服务级别、RTO 和 RPO。 f. 记录所需的恢复措施，确定并确保所需资源的可用性，并将此信息汇编为恢复计划。 g. 确定关键技术服务提供商依赖项和恢复支持能力。
7.8	如果第三方提供 SaaS 服务，则第三方应向 GE 提供地域弹性托管选项。对于存在服务交付依赖项的每项服务，第三方应具有多个提供商。
7.9	必须每 12 个月审查并签核灾难恢复计划一次。应将吸取的经验教训体现为灾难恢复演习的一部分。
7.10	所有数据保留要求都应通过文档记录并由 GE 批准。

8. 云安全

适用性：云安全要求适用于（在 SAAS、PAAS、IAAS 或 DRAAS 环境中）托管处理 GE 高度机密信息、机密信息、受控数据或敏感个人数据的云计算应用程序的第三方，或提供使 GE 能够开发、运行和管理应用程序的云计算平台的第三方，或负责管理虚拟机映像和/或虚拟机监控程序的第三方。

云安全要求	
8.1	对管理控制台的根目录/管理员访问应需要多因素身份验证。
8.2	专用安全网络应与客户生产基础设施分离，用于提供对云基础设施的管理访问权限。
8.3	第三方供应商应有能力提供特定于用于 GE/GE 参与的实例的日志。
8.4	第三方供应商应在云基础设施中跨区域启用控制台和资源级日志记录。
8.5	云环境中的所有日志都应馈入中央日志聚合工具。
8.6	第三方供应商应定期备份应用程序配置、应用程序内的数据、数据库和云基础设施内系统的配置，以确保在需要时可以恢复数据。
8.7	第三方供应商应保留云应用程序中所驻留数据的原始结构和格式，从而使这些数据可以轻松地转移到另一个云解决方案/云服务提供商。
8.8	第三方供应商应支持联合身份验证（例如：SAML）或用于通过 SaaS 和 API 传播并强制执行身份管控的基于标准的身份协议（例如：OpenID Connect、OAuth2 等）。
8.9	第三方供应商应实施加密管控措施（例如：AES-256:），以确保云基础设施中的 GE 静态数据始终处于加密状态。
8.10	第三方供应商应使机制落实到位，以管控加密密钥的生成、分发、存储、访问和销毁。
8.11	第三方供应商应有权访问通过基于角色的访问管控且根据最小特权原则所限制的管理控制台和云应用程序。
8.12	如果密钥（例如：访问密钥、云帐户的密钥或用于管理云实例的 SSH 密钥）用于管理云基础设施，则第三方厂商应将密钥存放在具备访问管控措施的受保护保管库中。
8.13	第三方供应商应将网络事故管理计划落实到位，据其对网络事故进行评估、遏制、补救和响应。
8.14	第三方供应商应具有补丁管理流程，以便在厂商发布补丁后 30 天内（为托管、存储、处理或传输 GE 数据的云基础设施）识别并应用所有相关的厂商补丁和安全更新。
8.15	第三方供应商应使用保管库存放根/管理员帐户凭据。
8.16	应对过去 12 个月内托管、存储、处理和/或传输 GE 数据的云应用程序进行 Web 应用程序漏洞评估或渗透测试。
8.17	应对过去 12 个月内存储、处理、托管或传输 GE 数据的云实例和系统（服务器、数据库、联网组件/设备）进行网络漏洞评估。
8.18	第三方供应商应具有适用于单租户型以及多租户型部署的应用程序支持。
8.19	第三方供应商应支持至少符合应对 OWASP 前 10 大风险要求的 Web 应用程序防火墙 (WAF) 实施。
8.20	第三方供应商应使管控措施（包括但不限于 S3 存储桶和 Elasticsearch）落实到位，以确保数据的非公开披露。
8.21	第三方应具有监控配置漂移的审核措施。
8.22	第三方应具有自动关闭公开披露的管控措施。

9. 数据中心安全

适用性：数据中心安全要求适用于提供数据中心设施服务的第三方。

数据中心安全要求的 ISO 27001 管控措施	
9.1	11.1.4 防范外部和环境威胁
9.2	11.1.6 交付和加载区域
9.3	11.2.1 设备选址和保护
9.4	11.2.2 配套实用工具
9.5	11.2.4 设备维护
9.6	17.2.1 信息处理设施的可用性

追加数据中心安全要求	
9.7	数据中心墙壁应防火或防爆。
9.8	除非防碎耐冲击屏障设置到位，否则不允许使用带有玻璃窗的数据中心。
9.9	应至少每季度使用文档化流程对物理数据中心访问权限进行一次审查。
9.10	所有数据中心均应由签约的安全监控服务机构或建筑物内的本地安全团队成员来监控专业安装的入侵警报系统。应对所有入口点设置警报器并进行监控。警报系统应能在断电的情况下持续运行。
9.11	应急门应具有音响警报器并显示适当的标牌。
9.12	一旦人员进入数据中心，则访问应仅限于该人员需要访问的区域。应对入口点以及出口点进行全天候 (24×7×365) 管控和监视，以尽量减少尾随并提供详细的位置日志记录。除非适用法律法规禁止或另有要求，否则应从事件或日志记录发生之日起将日志保留至少一年。应按照 GE 的指示，保存与未决或可预见诉讼、调查或审计相关的日志（即使是不受正式文件保留通知的约束时也是如此）。应始终陪同或注意访客。
9.13	应在外部和所有数据中心楼层入口点将闭路电视 (CCTV) 系统和适当的标牌安装到位。应在工作时间内监控摄像头，并应将其保留至少 30 天。
9.14	安全警报器、入口管控措施、环境管控措施和 CCTV 系统应在物理和逻辑上仅限于由负责这些功能的人员来管理。
9.15	包含数据中心的建筑物的所有入口均应设计为阻止人员在未经人工识别检查之前进入建筑物内部或登上电梯。应安排专人全天候 (24/7) 值守可供公众使用的主入口。公共区域与数据中心楼层区域之间应存在多个安全入口。
9.16	应对包含 GE 机密信息的资产设置护笼，以在物理上将其与数据中心的其余部分隔开。护笼应使用具有多因素身份验证或受控密钥流程的主安全卡门禁系统。护笼的范围应为真实地板到真实天花板，以防止人员擅自进入。护笼应设计为防止人员从护笼外侵入或闯入。最后，护笼应具有视界覆盖入口的摄像头，并应通过线缆连接到内部全天候 (24×7×365) 闭路电视系统。
9.17	任何需要使用胸牌访问任何机房的人员均应遵循第三方批准的规定程序，其中包括胸牌持有者的姓名、胸牌号码、机房位置、需要访问的原因以及固定期限的终止日期。第三方安保办公室不得就未经第三方或指定团队成员授权的机房访问配置任何胸牌。

追加数据中心安全要求	
9.18	应通过预先安排的安全走查对建筑物外部进行定期检查。应调查可疑的包裹、活动、车辆和/或人员。
9.19	数据中心停车区应将物理屏障设置到位，以降低车辆或汽车炸弹穿透外墙的风险。
9.20	所有的数据中心工作人员均应接受有关管控和储存易燃材料（包括纸张和纸板）以及探测到火灾时应遵循的正确流程的培训。
9.21	服务器机房不得用于存储，并应清除所有未使用的非必要设备和材料。
9.22	应实施检测性监测和管控，以降低架空水源影响 IT 设备的风险。应将水检测设备布置在机房最低层的空调以及任何其他水源附近。
9.23	应实施并全天候 (24×7×365) 监控多种早期火灾探测方法，包括烟雾和温度检测。
9.24	所有数据中心均应配备灭火系统。
9.25	装载台和月台应配备提供车辆清晰正面视图的 CCTV。该视图应经过妥善定位，以便识别驾驶员、车辆品牌和注册车号牌。从等候区进入数据中心的门应符合数据中心入口的内部安全要求。应记录进出设施的任何材料或设备的移动、交付或移除。
9.26	所有允许重要系统紧急关闭的开关和/或控件均应配备物理保护装置、音响警报器和标牌，以避免意外激活。
9.27	第三方应确保将所有计算机设备都连接到电涌保护器，以保护它们免受电源中尖峰和电涌的影响。
9.28	第三方应确保以本地发电机的形式提供备用电源。
9.29	第三方应确保按照制造商规范维护所有电气和机械基础设施。
9.30	应根据当地消防和健康与安全法规，在整个数据中心内实施由除主电源以外电源供电的应急照明。当火灾警报响起时或电源劣化阻碍标准灯具工作时，应激活应急照明。
9.31	数据中心应配备到位的系统以控制和监测温度和湿度，且应配备空调系统以控制空气质量并尽量减少污染。应将服务器机房温度控制在 18-27° C 的范围内。应将服务器机房湿度控制在 40-60% 的相对湿度范围内。
9.32	数据中心应配备具有用于标准工作区域以及服务器机房等包含设备区域的独立分区的空调系统。
9.33	为服务器机房提供支持的空调系统具有安装到位的灰尘过滤系统，并应定期接受检查，以确保空气质量不会劣化/污染不会加剧。
9.34	服务器机房应具有正压，以尽量减少进入这些区域的污染物。
9.35	应将流程落实到位，以对所有关键的数据中心基础设施（包括安全、电力和环境系统）进行预先安排的测试和维护。应记录对设施安全组件（例如门、锁、墙壁、硬件）进行的维修或修改。
9.36	应将包括电力和环境系统在内的关键数据中心基础设施设计为可在运行中断期间发挥作用。该设计应至少为 N+1 方案。具有多个电源的 IT 设备应利用冗余电源基础设施。
9.37	应将数据中心的门禁系统和门设计为可在如下场景下保持运行：门禁应用程序或硬件平台发生故障以及公用电源停电。
9.38	应将所有 GE 设备正确地安装在按照当地抗震指导原则安装于地面和/或天花板上且大小合适的机架中。应在机架上粘贴标签。机架中的设备以及延伸到机架中的电缆也应贴有标签。

追加数据中心安全要求	
9.39	应将新设备存储在受保护区域。第三方人员应在打开机箱之前检查机箱是否被篡改。应在第三方人员的监督下，通过批准的安全流程移动包含 GE 数据的旧设备。
9.40	第三方应具有文档化设备或媒体交付或处理流程。
9.41	数据中心应具有适用于设施和环境的灾难恢复计划，该计划可确定并减轻灾难发生时 GE 服务所面临的风险。该计划应规定在发生灾难时用于恢复设施服务的应急措施，例如确定的备用数据中心站点。应与 GE 共享该计划，以确保 GE 能够与自己的 DRP 进行协调。
9.42	数据中心应至少每年进行一次断电测试，以通过运行中断验证继续功能。此外，数据中心应参与并支持 GE DRP 和相关测试。
9.43	应将所有 GE 设备与数据中心的非 GE 部件完全网络隔离。

10. 直接网络连接安全

适用性： 直接网络连接安全要求适用于与 GE 建立了受信任第三方网络连接的第三方。

直接网络连接安全要求	
10.1	第三方应仅使用 GE 托管网络设备连接到受信任第三方连接。GE 要求与远程设备建立带外连接以进行管理。
10.2	第三方应在第三方上级网络和受信任第三方网络之间实施防火墙。防火墙应由 GE 进行管理，并应配置为仅允许经 GE 授权的连接。
10.3	GE 对所有 GE IP 地址进行定期扫描。如果 GE 将发现的任何已确认的严重或危急漏洞通知第三方，则第三方应在 30 天内修复已确认的漏洞。受信任第三方应确保，线路中将不会放置任何东西来限制 GE 对受信任第三方网络执行漏洞扫描的能力。
10.4	应将所有互联网流量定向到 GE 托管外部代理服务器。
10.5	对受信任第三方网络的远程访问仅允许通过具有双因素身份验证功能的 GE 虚拟专用网络 (VPN) 集线器基础设施来进行。
10.6	GE 托管网络设备应布置在笼式环境中，并/或应通过物理方式与第三方设备分离。第三方应确保，网络设备处于锁定状态，并仅限经 GE 批准的第三方工作者以及经批准的 GE 员工具有权访问。第三方还应维护列明所有具备设备访问权限的个人名单。
10.7	受信任第三方应确保，其员工不会将受信任第三方网络与非受信任第三方上级网络桥接。不得与除 GE 网络以外的任何网络建立物理或逻辑连接。第三方的业务网络不得与 GE 共享除终结防火墙以外的任何二层交换机或网络设备。
10.8	第三方应确保，受信任第三方网络上的所有无线部署均遵循 GE 第三方网络更改请求流程并由 GE 配置/管理。
10.9	应在网络设备上禁用所有未使用的交换机端口。此外，应向 GE 提交所有新连接请求。

11. 产品安全

适用性：产品安全要求适用于根据合同文档提供包含可执行二进制代码的任何产品（如下文所定义）的第三方。如果第三方提供包括或支持下列各项的产品、组件或服务，则产品安全要求同样适用：软件、固件和/或复杂硬件（即逻辑承载设备）；设计为在联网环境中运行（即提供通信接口）；USB/便携式媒体访问（例如 CD/DVD/扩展磁盘）；远程访问（例如远程桌面协议）；包括软件或联网组件的服务。

产品安全要求	
11.1	供应商应确保，已按照与软件开发行业最佳实践（包括安全设计审查、安全编码实践、基于风险的测试以及修复要求）一致的安全软件开发原则开发所有产品。供应商用于开发产品的软件开发环境必须具有安全控制措施，这些安全管控措施能够通过以基于风险的方式使用网络层防火墙和入侵检测/防护系统 (IDS/IPS) 来检测和防止攻击。
11.2	供应商应实施流程，以确保为产品开发环境和相关资产实施恶意软件防护措施。
11.3	供应商应设有妥善的流程，以确保产品开发环境中使用的系统得到正确且及时的修补。
11.4	供应商应将网络安全指南纳入提供给 GE 的产品文档中。该文档应包括有关如何配置产品和/或周围环境以最令人满意地确保安全性的指南。该文档还应包括有关需要使用哪些逻辑或物理端口才能使产品发挥功能的指南。如果将身份验证用于保护对产品任何服务或功能的访问，那么无论该服务/功能的预期用户如何，供应商均应确保： (i) 产品不得使用默认帐户/密码提供对该服务或功能的访问； (ii) 产品应就所有用户帐户、文件系统和应用程序间通信配置最小特权，根据特权实施文件保护的典型文件系统为 *nix 和 NTFS； (iii) 产品不得使用“后门”帐户或密码提供对该服务或功能的访问； (iv) 产品的关联身份验证和密码更改流程应以适当的安全加密级别实施；且 (v) GE 应能够更改产品支持的任何密码。
11.5	实现产品功能时不需要的服务或功能应默认禁用，或应要求进行身份验证，以保护对该服务或功能的访问。

产品安全要求	
11.6	如果任何产品中包含任何无线技术，则供应商应证明，该无线技术符合适用无线标准或规范（例如 802.11 等适用的 IEEE 标准）中规定的标准运行及安全要求。
11.7	如果产品中包含任何加密系统，则供应商应仅使用达到或超过美国国家标准与技术研究院 (NIST) 特别出版物 800-131A 最新版本的加密算法和密钥长度，且应提供一种保护加密密钥机密性和完整性的自动化远程密钥建立（更新）方法。
11.8	厂商应维持列明了产品开发过程中使用的所有高风险技术（例如来自华为、中兴和卡巴斯基的技术）的清单。除非事先获得 GE 的批准，否则不得在为 GE 开发的产品中使用高风险技术。
11.9	供应商必须制定和维护最新的网络安全漏洞管理计划，该计划旨在及时识别、预防、调查和缓解任何网络安全漏洞，并执行任何必要的恢复措施以补救造成的影响。
11.10	如果发现任何潜在的安全网络漏洞，则供应商应在合理期限（在任何情况下均不得超过发现该漏洞后的五 (5) 个工作日）内或在更短时间内（如果适用法律或法规要求如此）通知 GE。供应商应使用修复程序，通过 security@ge.com 向 GE 报告所有会对 GE 造成重大不利影响的危急网络安全漏洞以及任何网络安全漏洞，并在主题行或不时传达给供应商的此类联系信息中注明“PSIRT”。在此后的一段合理时间内，供应商应免费向 GE 提供修复任何网络安全漏洞所需的任何升级、更新、发布、维护发布以及错误或缺陷修复程序。供应商应合理配合 GE 调查不论是由供应商、GE 还是第三方发现的网络安全漏洞，这种配合应包括向 GE 提供网络安全漏洞的详细描述、修复计划，以及一旦可以收集或以其他方式获得，GE 便可能就网络安全漏洞而合理要求获取的任何其他信息。GE 或 GE 的代理商应有权对适用的产品和产品开发生命周期进行网络安全评估，其中包括旨在识别潜在网络安全漏洞的测试。供应商应指定一名负责管理网络安全漏洞的人员，且应及时向 GE 确定该人员。
11.11	供应商应设立一项流程，以确保适当的物理和数字安全机制到位，包括但不限于 (i) 只允许供应商和 GE 批准的人员访问 GE 的组件环境； (ii) 在媒体和容器上使用防篡改封条（例如防篡改标签或封条，一旦被揭下，它们会自毁并留下残留贴纸），以检测对受保护产品的擅自访问；以及 (iii) 防篡改生产（例如软件和相应硬件机制的数字签名）。
11.12	开源软件和第三方材料保证。供应商声明、保证并承诺：(i) 其已披露与产品一起使用的所有开源软件和第三方材料，且除非事先获得 GE 的书面授权，否则任何开源软件或第三方材料均未曾或不会提供给 GE 或用作根据协议提供的任何产品的组件或与该产品相关的组件；同时 (ii) 产品中包含的所有开源软件均已且应在实质上符合管控其使用的适用许可证之条款和条件，且产品或 GE 对产品的使用不得致使 GE 或 GE 的知识产权受非盈利版权许可证之条款或条件的约束，或要求 GE 为产品中包含的任何开源软件履行任何开源许可义务。
11.13	代码完整性保证。供应商声明、保证并承诺产品：(a) 不包含可能会限制，或以其他方式损害产品或体现或包含该产品的任何材料的任何限制性设备（例如，任何密钥、节点锁、超时装置、定时炸弹或无论是通过电子、机械还是其他方式实现的其他功能）；且 (b) 应无任何可能对产品使用造成干扰的病毒、恶意软件和其他有害代码（包括但不限于超时功能），而不论供应商或其人员是否已有意将此类代码置于该产品中。

产品安全要求	
	除了根据本协议或其他法律或衡平法行使 GE 的任何其他权利和修复措施外，供应商应免费向 GE 提供产品的一切新版本、升级、更新、发布、维护发布以及错误或缺陷修复程序（统称为“修订代码”），该修订代码将防止违反根据本协议提供的任何保证的行为，或纠正违反此类保证的行为。产品中包含的修订代码构成就本协议而言的产品。
11.14	供应商应购买技术错误和遗漏责任保险（每次索赔的最低合计金额下限为 5,000,000 美元），以备足额抵偿所有产品因 IT 安全措施失效、数据隐私违反以及软件版权侵犯等遭受的损失。如果承保范围基于期内索赔式保单，则该保单必须包含一个处于本协议生效日期之前的追溯日期，并且连续性必须在本协议终止或到期后保持 1 年。
11.15	应指定产品安全负责人和企业安全架构师，为执行产品安全计划和解决网络威胁提供支持。
11.16	所有软件和固件组件均应经过静态应用程序安全测试 (SAST)，且应使所有危急和严重漏洞在 GE 将购买的产品版本中得到修复。注意：可以在源代码或二进制文件上完成此操作。
11.17	应在所有外部接口上执行动态应用程序安全测试 (DAST)。
11.18	应在 GE 将要采购的组件上进行渗透测试。
11.19	应对组件的远程访问进行配置，以限制并发远程会话数量。
11.20	应对组件的远程访问进行配置，以在预定义的不活动时间段结束后自动终止用户会话。
11.21	组件应具有审计日志记录功能，涵盖登录成功及失败记录、时间、用户登录持续时间等指标。
11.22	组件应具有内置机制，以防止除管理员之外的普通用户访问日志。
11.23	组件应能够将审核日志存储至少 180 天。
11.24	组件应能够将审核日志传输到诸如 Syslog 服务器之类的外部系统。
11.25	组件应使用内部系统时钟为审核记录生成时间戳。
11.26	您所属的组织应制定产品安全事故响应策略，该策略处理目的、适用范围、角色、管理承诺以及组织实体间的协调，且已将合规性记录在案并向在产品开发、计划、项目或管理人员岗位上工作的所有员工宣传合规性。
11.27	应至少每年使用桌面演练、自动模拟和事故测试计划，对产品安全事故响应能力进行一次测试，以确定事故响应的有效性并记录结果。
11.28	您所属的组织应持续接收网络厂商和 US-CERT 发出的安全警报、公告和指令，并在必要时生成内部安全警报、公告和指令。
11.29	您所属的组织应制定特定于角色的网络安全意识和培训计划，该计划将确定培养和维护产品安全完整性文化所需的培训，以及有效且一致地执行产品安全活动以设计安全产品所需的专业知识。
11.30	您所属的组织应每年审查当前的安全意识和培训策略一次，并应至少每三年将其更新一次。

产品安全要求	
11.31	您所属的组织应在向员工授予产品开发所用系统的访问权限之前，为员工提供基于角色的安全培训，并在此之后每年提供一次该培训。
11.32	您所属的组织应记录和监控个人信息系统安全培训活动（包括基本安全意识培训和基于角色的安全培训），并将个人培训记录保留至少两年。
11.33	您所属的组织应要求您的供应商遵守与本要求文档一致的产品网络安全要求。
11.34	您所属的组织应定期对供应商进行安全审查和/或现场审核/评估，以确保所有第三方供应商的安全管控措施与您所属组织的安全策略一致，且按照您所属组织与供应商签订的合同实施。
11.35	您所属的组织应制定文档化安全开发生命周期标准，其中就 GE 将要采购的产品提出以下要求：1. 产品固有风险评估；2. 安全计划；3. 定义安全要求；4. 架构安全解决方案；5. 实施安全解决方案；6. 执行剩余风险评估；7. 维护产品库存；8. 产品生命周期考虑事项；9. 持续部署合规性。
11.36	对于 GE 将要采购的组件中所用编程语言和框架中存在的已知漏洞，应建立解决它们的编码标准。
11.37	应制定一份确定适用软件开发生命周期目标和客户/监管网络安全要求的计划。
11.38	GE 将要采购的组件应经过威胁建模演习，以评估和记录组件的固有安全风险。
11.39	应记录安全要求和假设，以提供必要的措施来减轻威胁建模演习期间识别的每个威胁。
11.40	根据最佳实践和吸取的经验教训，定义一组适用于将向所有项目实施的技术和用例的基本安全要求。
11.41	应为 GE 将要采购的组件开发并记录安全架构。
11.42	应为数字组件和涵盖的产品制定并执行实现以下目标的数字淘汰和生命周期结束策略：1. 向相关的利益干系人（包括客户）告知 PLC；2. 通过如下适当的风险补救措施解决 PLC 带来的风险：缓解、接受、转移或“生命周期结束”流程。
11.43	应制定持续部署合规性计划，其中包括经常性验证的时间表和范围。

12. 弹性安全要求

适用性：如果供应商对 GE 而言是产品、组件或材料的单一来源制造商的唯一供应来源，且供应商在产品、组件或材料方面对关键产品的经营/生产具有关键或重要影响，则弹性安全要求适用于（以逻辑方式或物理方式）处理、访问或存储 GE 高度机密信息或敏感个人数据、受控数据的第三方。

弹性安全要求	
12.1	应审查并更新信息安全事故管理计划。
12.2	您所属的组织应确定利益干系人，并为员工分配角色和职责，以执行安全事故管理计划中描述的活动。
12.3	您所属组织的安全事故管理流程应体现以下方面： 1. 安全事件的分类 2. 对安全事件的分析，旨在确定它们是否与其他事件有关 3. 划分安全事件优先级的方法 4. 记录并追踪所有安全事件的状态 5. “您所属组织的安全事故管理流程是否体现了以下方面？” 1. 安全事件的分类 2. 对安全事件的分析，旨在确定它们是否与其他事件有关 3. 划分安全事件优先级的方法 4. 记录并追踪所有安全事件的状态 5. 审查为安全事件执行的补救活动，以确保追踪它们，直到妥善解决安全事件。
12.4	应设立适当的流程，以确保按照法律或其他义务（规则、法律、法规、政策等）的要求识别、收集和处理安全事件证据。
12.5	应设立适当的流程，以便通过其向利益干系人上报安全事故来获取建议并解决事故。
12.6	应将事故状态和回应告知受影响的各方（包括公共关系人员和外部媒体渠道）。
12.7	事故管理流程与其他相关流程（问题管理、风险管理、变更管理等）之间应存在联系。
12.8	应将从事故管理中吸取的经验教训用于改进资产保护和服务连续性战略。
12.9	应识别、分析、处置、监测并管控与事故管理活动执行相关的风险。
12.10	应对事故管理活动的执行进行管理监督。
12.11	服务连续性计划应以受控方式存储，且可供所有需要了解它的人员访问。
12.12	应实施多种机制（例如故障保护、负载平衡、热插拔功能），以达到正常和不利情况下的弹性要求。
12.13	应确定服务连续性活动的利益干系人，并使其明白他们所承担的角色。
12.14	应对服务连续性活动的执行进行管理监督。
12.15	您所属的组织应为外部依赖项/关系（服务提供商、供应商、厂商、合作伙伴、顾问、外包合作伙伴等）管理制定文档化计划，包括但不限于： 1. 识别对提供给 GE 的服务而言至关重要的所有外部依赖项/关系 2. 维护列出了与提供给 GE 的服务相关的所有外部依赖项的有效清单

弹性安全要求	
	3. 优先考虑外部依赖项列表 4. 确定与外部依赖项管理活动相关的利益干系人 5. 为与外部依赖项管理活动相关的利益干系人建立角色和责任 6. 实施与外部依赖关系管理活动相关的指导原则和流程
12.16	应存在业已建立的流程来识别、分析并管理外部依赖项/关系管理引起的风险。
12.17	对于对提供给 GE 的服务至关重要的所有外部依赖项/关系，您所属的组织应制定文档化弹性要求计划，包括但不限于： 1. 确定每个外部依赖项/关系的弹性要求 2. 定期审查弹性要求 3. 外部依赖项/关系满足弹性要求的能力 4. 将弹性要求纳入与外部依赖项/关系签署的正式协议中
12.18	根据弹性要求监控外部依赖项/关系的表现。
12.19	应采取纠正措施，以处理外部依赖项/关系引起的性能问题（与弹性要求相关），并进行追踪，直至问题解决。
12.20	应确定关键服务（电信和电话服务、能源等）所依赖的基础设施提供商。
12.21	应定期审查和衡量外部依赖项/关系管理活动，以确保这些活动有效，正在产生预期的效果，且遵循计划。
12.22	应对外部依赖项管理活动的执行进行管理监督。
12.23	应分配监控威胁信息来源的职责。
12.24	应实施威胁监控程序。
12.25	应分配并训练多项资源，以执行威胁监控。
12.26	应确定必须向其告知威胁信息的内部利益干系人（例如关键服务所有者和事故管理人员）。
12.27	应确定必须向其告知威胁信息的外部利益干系人（例如紧急事件管理人员、监管机构和信息共享组织）。
12.28	应将威胁信息告知利益干系人。
12.29	应向资源赋予与告知威胁信息相关的权力和责任。
12.30	资源应就其在告知威胁信息方面发挥的具体作用接受训练。

13. 运营技术 (OT)/制造安全要求

适用性： OT/制造安全要求适用于为 GE 制造产品、组件或材料的第三方；不包括商业现货 (COTS) 物品、低成本大批量物品以及可以从市场上购得的原材料。

运营技术安全要求	
13.1	应在资产库存系统中记录并跟踪您所在制造环境中的所有硬件和软件资产。
13.2	应将您所在制造环境中的所有资产收纳于上锁设施或使用胸牌管控进出的设施中。
13.3	您所在制造环境中的所有系统驱动器和媒体均应在使用之前接受扫描，以防恶意软件侵入。
13.4	应使用最新的安全补丁/更新维护您所在制造环境中的所有资产操作系统、软件和固件。
13.5	应至少每两年对您所在制造环境中的所有资产进行一次扫描，以防恶意软件侵入。
13.6	应使用专用的集中管理式受监控防火墙，对您所在制造环境中可（直接地或经由另一个连接的系统）通过网络访问的所有资产进行保护。
13.7	如果在您所处制造环境中使用可移动媒体（例如 USB 设备、外部硬盘器、软盘或光盘），则应对这些媒体加以保护。
13.8	应为每个可移动媒体分配一个所有者。
13.9	在您所处制造环境中使用的所有可移动媒体设备均应由您所在的公司拥有和发放。
13.10	所有可移动媒体设备均应在您所处制造环境中使用之前接受扫描，以防恶意软件侵入。
13.11	您所在制造环境中所有具有远程控制功能的软件都应通过软件请求和许可流程进行注册以供使用，并应在投入使用前取得使用批准。
13.12	所有远程访问您所在制造环境中资产的个人均应使用唯一的 ID 和密码。
13.13	所有远程访问您所在制造环境中资产的个人均必须至少使用用户名和密码进行身份验证。
13.14	所有远程访问您所在制造环境中资产的高特权用户（例如系统管理员）均必须至少使用双因素身份验证。
13.15	应使用 AES 128、192 或 256 对所有与您所在制造环境中装置/设备建立的远程网络连接进行加密。
13.16	应将防火墙限制实施到位，以限制远程连接仅限于授权端点。
13.17	应在所有具有数据存储媒体的资产离开您所属公司的保管库或重新部署到其他站点之前，安全地清理或销毁这些资产。
13.18	应监控您所在制造环境中的所有资产是否存在异常/恶意活动。
13.19	您所属的组织应为您的制造运营和资产制定文档化信息安全事故管理计划，该计划包括以下方面：1.报告（提出潜在事故的内部和外部机制）；2.准备（程序、检查表、适用时包括法律/政府机构和监管机构的沟通计划用）；3.识别（报告事故的到位方法、严重性评估）；4.遏制（日志记录步骤、证据收集）；5.根除（根本原因分析）；6.恢复（系统恢复步骤）；7.吸取的经验教训（事故报告）；以及 8.追踪（事故清单、工作流、状态、结果）。
13.20	您所属的组织应至少每年对事故管理计划进行一次定期测试，以验证用户是否接受过适当的培训，以及必要时该计划是否可以有效地执行。注意：桌面测试是适当事故管理计划测试的典型组成部分之一。

运营技术安全要求	
	此外，必须根据您所属组织的环境所面临的高风险威胁（例如病毒/蠕虫攻击、数据泄露、实物资产损失）执行测试。
13.21	如果您的制造运营因网络事故而受到不利影响，则您的组织应有能力在发现违规行为或擅自访问 GE 数据之后 72 小时内通知 GE。
13.22	应制定并记录您所在制造环境的业务连续性和灾难恢复计划。
13.23	您所属的组织应至少具有一个可以在主要制造场所因网络事故而受到不利影响时使用的制造场所。
13.24	您所属的组织应尽可能获取并保留制造系统软件和固件资产的备份。
13.25	您所属的组织应对制造硬件、软件和固件资产实施更改管控和更改通知流程。
13.26	应在中央系统中对更改管控和通知流程进行管理。
13.27	您所属的组织应在您所在的制造环境中使用第三方软件、固件或硬件。
13.28	应记录列出了第三方以及所用软件、硬件或固件的清单。
13.29	应管理并定期审查有权远程访问您所在制造环境中任何资产的第三方，以确保准确性。

15. 安全管控适用性矩阵

适用性	最低安全	物理安全	强化安全	软件开发	系统可用性	云	数据中心安全	直接网络连接	产品安全	运营技术安全	弹性
处理 GE 机密信息或个人数据	X	X									
处理 GE 高度机密受控数据或支持一项或多项关键业务	X	X	X							X	X
与 GE 的受信任直接网络连接	X	X	X					X			
存储物理文档		X									
提供数据中心服务							X				
需要 GE 所定义高可用性的服务或数据					X						
开发特定于 GE 需求的软件或处理 GE 数据的主机应用程序				X							
利用云技术（SAAS、PAAS、IAAS）						X					
提供将在 GE 产品中使用的数字组件									X		
唯一来源或单一来源制造供应商										X	X

适用性	最低安全	物理安全	强化安全	软件开发	系统可用性	云	数据中心安全	直接网络连接	产品安全	运营技术安全	弹性
供应商对关键产品的运营/生产的影响 = 深刻或严重影响										X	X
供应商为 GE 制造产品、组件或材料的第三方；不包括商业现货 (COTS) 物品、低成本大批量物品以及可以从市场上购得的原材料										X	

17. 定义

*受控数据*是具有法律所禁止的分发和/或处理要求的技术或政府信息，包括但不限于受控非机密信息和许可证所需出口受控数据，该数据由 GE 提供给与履行合同文件有关的第三方。

*非盈利版权许可证*是指 GNU 通用公共许可证 2.0 版 (GPLv2) 或 3.0 版 (GPLv3)、Affero 通用公共许可证第 3 版 (AGPLv3)，或（作为使用、修改和/或分发或通过网络提供的条件）要求根据此类许可证获得许可的任何材料满足以下条件的任何其他许可证：(a) 根据其原始许可证获得许可；(b) 以源代码形式披露或分发；(c) 免费分发；(d) 受许可人或分发人的专利主张的相关限制约束。

*网络安全漏洞*是指任何错误、软件缺陷、设计瑕疵或与某一产品相关的软件的其他问题，它们可能会对与该产品相关的信息或流程的机密性、完整性或可用性产生不利影响。

*GE 机密信息*是由 GE 创建、收集或修改，披露或使用不当时可能会对 GE 造成损害，且根据合同文件向供应商提供且如此注明的信息。GE 机密信息包括高度机密、个人、受控或敏感数据。
*GE 数据*包括高度机密、机密、个人、受控或敏感个人数据。

*GE 高度机密信息*即 GE 在合同文件中标识为“高度机密”，或 GE 在披露时标识为“受限”、“高度机密”或类似字样的 GE 机密信息。

*GE 信息系统*是指由 GE 管理的任何系统和/或计算机，其中包括笔记本电脑和网络设备。

*GE 受信任第三方网络*是指可供受信任第三方安全地连接到 GE 网络 的 GE 网络隔离部分。

高特权帐户（用户），简称 HPA，是对设备、应用程序或数据库具有系统级管理或超级用户访问权限，可以管理系统上的帐户和密码，或能够替代系统或应用程序控件的帐户。

*移动设备*是指运行移动操作系统的平板电脑、智能手机或类似设备。笔记本电脑不视为移动设备。

*开源软件*是指作为“开源软件”或“免费软件”分发，或以其他方式公开分发，或根据允许在以下一项或多项条件下修改和重新分发材料的条款以源代码形式普遍提供的任何材料：(a) 如果重新分发该材料（无论是否经过修改），它应：(i) 以源代码形式披露或分发；(ii) 为制作衍生作品而获得许可；且/或 (iii) 免费分发；(b) 重新分发必须根据任何非盈利版权许可证或以下任何许可协议或分发模式获得许可或分发：(1) GNU 的通用公共许可证 (GPL)、较宽松/库 GPL (LGPL) 或 Affero 通用公共许可证 (AGPL)；(2) 艺术许可证（例如 PERL）；(3) Mozilla 公共许可证；(4) 通用公共许可证；(5) Sun 社团源代码许可证 (SCSL)；(6) BSD 许可证；(7) Apache 许可证；和/或 (8) 其他开源软件许可证；和/或 (c) 材料受任何专利主张相关限制的约束。

*个人数据*是指与适用法律所定义之已识别或可识别的自然人（数据主体）相关的任何信息，该信息结合合同文件进行处理。在法律要求的情况下，法人是数据主体。个人数据是 GE 机密信息。

*产品*是指根据合同文件供应的任何货物、产品、软件和可交付成果。

*处理*是指对 GE 数据执行任何操作或一组操作（无论是否通过自动方式），包括但不限于收集、记录、组织、存储、改编或改变、检索、访问、咨询、使用、通过传输、传播或以其他方式提供来披露、对齐或组合、封锁、擦除或销毁。

*敏感个人数据*是一类被认为特别敏感的个人数据，包含医疗记录和其他个人健康信息，其中包括：如《1996 年美国健康保险便携性法案》所定义，并受该法案约束的受保护健康信息 (PHI)；个人银行帐户和支付卡信息以及其他财务帐户信息；客户银行帐户和支付卡信息；国别标识；根据适用法律规定的特殊类别数据（例如种族或民族、政治观点、宗教或哲学信仰、工会会员资格、基因和生物特征数据、家庭生活和性取向）。

*（对软件的）重大更改或增强*是指：

- 影响应用程序接口（修改数据流输入/输出）的任何代码更改。
- 对外部组件（数据库、文件、DLL 等）的访问或使用进行修改的应用程序所发生的任何代码更改。
- 影响访问管控的任何代码更改。
- 将应用程序完全或部分重写为另一种语言（例如从 C++ 转变为 Java）或另一种框架（例如Struts 和 Spring）。
- 引起之前在互联网上未发生过的曝光的应用程序更改。
- 导致风险级别升高的应用程序更改（例如从第 4 级重新分类到第 3 级）。
- 开发责任从一个第三方转移到另一个第三方，从第三方转移到 GE，或从 GE 转移到第三方。对任何现有危急或严重漏洞的纠正必须在转移之前进行或包含在工作订单中，以便新的第三方在适用的补救时间范围内纠正漏洞。

*第三方或供应商*是按照合同文件向 GE 提供货物或服务的实体。它也指通用 GE 合资企业。

*第三方信息系统*是指按照合同文件用于处理、存储、传输和/或访问 GE 机密信息的任何第三方系统和/或计算机，包括笔记本电脑和网络设备。

*第三方材料*是指供应商在提供给 GE 的任何产品中包含的材料，其所有权归属一个或多个第三方个人或实体。

*第三方工作者*是指按照合同文件提供服务和/或可交付成果的所有个人或实体，包括供应商的员工、允许的关联公司、供应商、承包商、分包商和代理商，以及他们任何一者直接或间接雇用或聘请的任何人员。

*受信任第三方网络连接*是以与标准 GE 办公室相同的方式连接到 GE 内部网络的第三方网络的物理和/或逻辑隔离段。