ERICSSON

供应商信息安全要求

ISRS

Security Requirements

介绍

Ericsson 供应商信息安全要求（以下简称"要求"）是供应商在其所有供应商关系中必须遵守的最低水平的信息安全要求，具体包括以下方面：

1. 处理、存储和/或访问爱立信信息。
2. 可以访问爱立信网络/基础设施。
3. 为爱立信开发或定制软件。
4. 提供 IT 硬件或软件产品以及支持和维护服务。

这些要求并非信息安全要求的详尽列表。除要求外，每项服务可能还需要满足特定的要求，而这些特定要求必须借助相关协议中进一步明确的适当信息安全控制措施来予以落实。

本文档会定期审查并随时更新。

内容

1 信息安全要求

供应商必须通过遵循最新版国际标准 ISO/IEC 27001 或根据书面协议规定的同等标准，来证明其采用了系统化的方法进行信息安全管理。

1.1 信息安全管理

a. 供应商的高层管理人员必须明确信息安全的方向，并作出相应承诺。至少必须有一个适用于整个企业的高级信息安全政策和支持计划。

b. 上文 a. 小节提及的信息安全政策，必须经由供应商管理层批准，于供应商组织内部公布，并传达给相关的供应商工作人员。

c. 供应商的信息安全政策必须由供应商按计划的间隔时间对其进行审查，但不得少于每二十四 (24) 个月审查一次，或在发生重大变化时进行审查，以确保其持续的适用性、充分性与

有效性。

d. 必须指定一名或多名合格人员负责维护信息安全计划。

e. 供应商定期开展信息安全意识活动，教育员工了解自己在创建和维护安全工作场所方面的责任。

f. 在相关情况下，供应商必须保持适当的职责分离。

1.2 风险管理

供应商必须建立风险管理框架/流程，以识别和解决信息安全风险。

1.3 人力资源安全

a. 供应商必须根据适用法律对所有供应商人员进行就业前背景调查。必须保留此类背景调查的证据并提供给爱立信（根据爱立信的要求）。

b. 在获取 Ericsson 信息之前，供应商人员必须遵守与供应商签订的书面协议（如雇佣协议或 NDA）中规定的保密限制。该协议应禁止供应商人员向第三方披露 Ericsson 信息，且其限制性不得低于供应商根据本协议对 Ericsson 做出的保密承诺。

c. 有权访问爱立信网络基础设施和/或爱立信信息的供应商人员必须签署爱立信的保密和访问指示文件 (NDI)。

d. 供应商必须制定纪律流程来处理信息安全违规行为。

1.4 资产管理

a. 供应商必须将 Ericsson 信息作为机密信息来处理，并通过遵守本文件中列出的要求来保护这些信息。

b. 供应商必须登记和维护作为服务组成部分的信息技术资产清单。

c. 供应商不得为履行本协议项下义务以外的其他目的存储、打印、复制、披露或处理爱立信信息。

d. 供应商必须制定流程，以确保在供应商人员终止或变更雇佣关系时归还 Ericsson 资产。

e. 供应商必须依据行业最佳实践，建立并维护针对 Ericsson 信息的安全删除程序（包括将电子介质重用前的安全删除）。

f. 在协议结束或终止时，供应商必须依照行业最佳实践，归还或安全销毁其所持有的 Ericsson 信息的所有副本，包括所有备份和存档副本，无论其为电子或非电子形式。根据要求，供应商必须向爱立信提供书面确认或销毁证明（如适用）。

1.5 访问控制

a. 仅当借助经批准的 Ericsson 远程访问解决方案时，才允许非 Ericsson 成员的个人或机构从 Ericsson 控制范围之外的网络访问 Ericsson 的资产。

b. 对爱立信信息的访问必须仅限于特定个人，并基于按需知悉的原则。

c. 严禁共享帐户。每个访问爱立信信息的个人都必须拥有自己专属的帐户。

d. 所有访问包含爱立信信息的系统和网络都必须按照行业最佳实践实施多因素身份验证 (MFA)。

e. 供应商在访问爱立信信息时必须按照行业最佳实践实施密码选择和管理控制，例如但不限于密码复杂性、允许的最大错误登录尝试次数以及所有密码的有效期限。

f. 供应商必须制定一套流程，确保在其处理、传输或存储 Ericsson 信息的网络及系统中，均需事先获得批准方可添加、更改或删除用户。

g. 供应商务必制定相关流程，以便在终止或变更雇佣关系的情况下，能够及时撤销/更新访问权限。

h. 供应商需对处理 Ericsson 信息的系统及网络的访问权限展开审查，包括管理员访问权限。定期审查应至少每十二 (12) 个月进行一次，而对于特权用户的审查应至少每三 (3) 个月进行一次。

i. 供应商必须制定管理特权账户的流程。

j. 必须以可审核的形式留存记录，用以表明哪些 Ericsson 信息已被访问、修改、披露或处置。

1.6 加密

a. 加密控制的实施必须符合所有相关协议、法律和法规。

b. 供应商必须能够使用符合行业最佳实践的加密技术，通过加密电子邮件与 Ericsson 安全地通信。

c. 无论是在传输过程中还是存储时，都必须依据行业最佳实践采用加密技术来保护 Ericsson 信息。

d. 加密密钥必须按照行业最佳实践进行集中管理，并制定密钥生成、更新、访问、分发、存储、存档、撤销和销毁的流程。

e. 不得在操作环境中使用根证书。

1.7 物理和环境安全

a. 供应商须将处理或存储 Ericsson 信息的设施及数据中心的实际访问权限，限定于特定个人，且这些个人仅能基于按需知悉原则进行访问。

b. 处理爱立信信息的信息处理设施必须始终受到监控并控制访问（24x7）。

c. 供应商务必保护用于处理 Ericsson 信息的信息处理设施，使其免受外部以及环境方面的威胁与危害。

d. 为切实保护 Ericsson 信息与资产，必须推行清台清屏政策。

e. 必须使用个人刷卡/感应卡或其他等效系统来限制对爱立信提供服务的地点的物理访问。

f. 对为爱立信提供服务的地点的物理访问必须持续记录物理访问相关事件，例如日期、时间、刷卡/感应卡 ID、门 ID、拒绝访问或授予访问。

1.8 操作安全

a. 供应商的系统必须配备足够的容量，以确保在发生安全事故或需求增加时能够持续可用。

b. 供应商务必确保在自身系统中部署恶意软件防护措施，且依据行业最佳实践持续进行更新。

c. 所有特权用户的操作均须予以记录。系统、特权用户或最终用户对这些日志所做的任何更改都应具备可检测性。日志记录还必须定期进行独立审查。

d. 必须在日志中记录与安全相关的重要事件，包括登录失败、系统崩溃、访问权限变更等事件

类型以及日期、时间、用户 ID、文件名、用户活动类别和 IP 地址等事件属性。

e. 日志记录必须以加密形式保存至少六 (6) 个月，并应 Ericsson 的要求随时提供。

f. 必须执行和维护备份以确保协议下的连续性和交付预期。

g. 必须建立漏洞管理流程，根据漏洞的性质/严重程度确定漏洞的优先级并进行修复。

h. 必须建立补丁管理流程来确保及时应用补丁。

i. 供应商应运用行业最佳实践，针对用以支持 Ericsson 业务参与的系统及基础设施，至少每年开展一次渗透测试。

j. 供应商必须将所有相关信息处理系统的时钟同步到单一参考时间源。

k. 必须对所有系统采用当前行业最佳实践进行加固，以减少攻击面。

l. 供应商应实施相关政策，防止在未经 Ericsson 事先书面授权的情况下在便携式设备上存储 Ericsson 信息。

m. 供应商务必通过恰当的物理、技术和/或逻辑方式，确保 Ericsson 信息与应用程序/系统与供应商自身或其他客户的系统和数据实现隔离。

n. 包含爱立信信息的开发、测试和生产环境必须在逻辑上和物理上彼此分离。

o. 除非本协议中另有明确约定，否则供应商不得将 Ericsson 信息用于任何人工智能。

1.9 通信安全

a. 包含 Ericsson 信息的系统必须按照行业最佳实践进行加固，包括但不限于删除或禁用不使用的软件和功能。

b. 供应商必须采用分层安全方法，利用安全加固防火墙、入侵检测/防御系统、网络分隔以及符合行业最佳实践的其他相关措施来保护 Ericsson 信息。

c. 供应商必须根据行业最佳实践实施电子邮件安全解决方案，以防止恶意软件、电子邮件欺骗、网络钓鱼攻击和垃圾邮件等恶意攻击。

1.10 分包商关系

a. 向分包商披露爱立信信息必须事先获得爱立信的书面同意，并且只能用于履行供应商在本协议项下的义务。

b. 分包商对Ericsson信息的访问、使用、保留和披露仅限于履行合同义务所必需的范围。

c. 供应商有责任通过书面协议的方式将此处规定的相同义务转授给其分包商。

d. 供应商必须在引入新的分包商之前评估相关风险，并且必须制定第三方风险管理流程。

e. 供应商必须定期监控、审查和审核分包商对要求的遵守情况。

1.11 事件管理

a. 供应商必须有成文的安全事故管理流程来检测和处理事件。

b. 供应商在发现影响爱立信信息的事件后必须立即通知爱立信。在任何情况下，该等通知都必须在获知任何已发生或疑似事件后二十四 (24) 小时内或另行商定的时间内通知以下人员：

   i. 协议中规定的 Ericsson 联系人；以及

   ii. gs.sim.dispatch@ericsson.com

c. 所有安全相关事件的报告都应视为机密信息，并使用行业最佳实践加密方法进行加密。

d. 供应商在处理这些报告时必须与Ericsson充分合作。合作可能包括提供对基于计算机证据数据的访问，以进行司法鉴定评估。

e. 供应商应与 Ericsson 合作，确保实施经双方同意的、适当的安全措施和程序，作为对影响服务或涉及 Ericsson 信息的安全事件或薄弱环节的补救措施的一部分。

1.12 业务连续性管理

a. 供应商必须实施业务连续性和灾难恢复计划，并至少每年记录和测试一次，且能够应 Ericsson 的要求提供副本。

b. 供应商必须确保将信息安全和 ICT 就绪要求纳入业务连续性和灾难恢复计划。

c. 供应商必须应 Ericsson 的要求，参与 Ericsson 指定的业务连续性和灾难恢复活动。

1.13 系统获取、开发和维护

以下信息安全要求适用于为软件或硬件提供开发或定制服务（包括处理 Ericsson 信息）的供应商

a. 供应商必须有成文的软件开发生命周期 (SDLC) 方法。

b. 必须保护系统源/目标代码以防止未经授权的访问。必须定期审查源代码存储库的访问权限，并仅限于授权员工。

c. 源自生产系统的 Ericsson 信息不得用于测试和开发系统。

d. 供应商必须确保处理 Ericsson 信息的软件和/或其他产品不存在所有已知的安全漏洞或其他安全缺陷。

e. 供应商必须应 Ericsson 的要求，披露在开发支持处理 Ericsson 信息的软件时使用的任何第三方软件/插件（专有或开源）。

f. 供应商必须遵循文档化的变更管理程序来请求、测试和批准应用程序和基础设施相关的变更。

1.14 软件供应链安全

供应商必须明确并记录所使用的第三方软件组件及其各自的版本号（包括开源组件和专有组件），并向 Ericsson 提供符合 SPDX 规范 V2.2.1/ISO 5962:2021 和供应商 SBOM 规范的软件物料清单 (SBOM)（请参阅*条件和指南 - 供应商和合作伙伴 - Ericsson*）。该要求适用于交付给 Ericsson 或提供给 Ericsson 的所有软件（独立提供或嵌入硬件）。

2 合规性

a. 供应商有关信息安全的内部审计和/或评估必须由经过培训的供应商人员或供应商指定的第三方定期执行，并且必须及时纠正任何发现的问题。

b. 根据爱立信的要求，供应商必须在十（10）天内证明其符合本要求以及与爱立信约定的任何其他信息安全要求。任何已查明的不合规行为必须立即纠正，Ericsson 不承担任何额外费用。

c. 供应商应根据 Ericsson 的要求，向 Ericsson 提供分包商遵守这些要求的证据。

d. 供应商必须应 Ericsson 的要求向其提供渗透和/或漏洞测试的任何及所有结果，或允许 Ericsson 对供应商管理或托管的处理或存储 Ericsson 信息的系统或环境进行渗透和/或漏洞测试。

e. 供应商必须保留并保护所有必要的记录，以证明其符合要求。

3 定义

就本文件而言，除非上下文明显另有要求，下列词语和表述应具有下文赋予它们的含义。

协议	供应商与 Ericsson 之间的协议，根据该协议，Ericsson 将从供应商处购买、获得许可或租赁产品（包括软件和其他受 IPRs 保护的产品）、服务或其他交付物，本要求适用于该协议。
背景核实检查	背景调查的含义与 ISO/IEC 27001/27002 中规定的含义相同。
爱立信信息	Ericsson、Ericsson 客户、与 Ericsson 有业务关系的其他第三方的专有信息以及作为服务一部分的其他信息。爱立信信息包括个人信息。
行业最佳实践	指在相同或类似情况下，从事与接收方或任何承包商（如适用）同类工作的熟练和称职的服务供应商在合理和通常情况下应具备的技能、谨慎、预见性和操作惯例。
信息处理设施	任何容纳处理或存储 Ericsson 信息的系统的物理位置。
个人信息	个人信息必须是指与已识别或可识别的自然人（"数据主体"）相关的任何信息，或法律、法规或合同协议另有定义的信息。可识别的个人是指可以直接或间接识别其身份的人员，特别是通过姓名、身份号码、位置数据、在线标识符等标识信息或与其身体、生理、心理、经济、文化或社会身份有关的一个或多个特定因素。
服务	供应商根据本协议向爱立信提供的任何服务、产品或其他可交付成果。

单一参考时间源	时间服务器源直接链接到可靠的 UTC（协调世界时）源，UTC 是全球用于调节时钟和时间的主要时间标准，即 Stratum1。
供应商	与爱立信签订协议并提供服务的公司。当"供应商"一词根据本文件对供应商提出义务或要求时，该词也包括供应商的关联公司、分包商和员工。