总结

一. 介绍

本合作伙伴信息安全政策的主要目标是指导有效的信息资产保护计划，以确保信息的机密性、完整性和可用性，这是在 WEG 集团内建立信息安全标准和程序的基础。

二. 范围

所有合作伙伴（与 WEG 集团有法律关系的任何人如产品、许可或服务的供应商）必须遵守此处定义的信息安全要求。

遵守既定的指导方针对于签署有效的合作伙伴关系和实现足够的信息保护水平至关重要。

此处建立的指南和要求适用于所有有权访问 WEG 集团数据、信息和系统的合作伙伴。合作伙伴将对自己及其员工、供应商和服务提供商负责。

三. 定义

- **DPIA：**是数据保护影响评估的首字母缩写词，代表巴西通用数据保护法 （LGPD） 中的个人数据保护影响报告 （RIPD）。
  此过程在实施数据项目之前识别、评估和缓解数据项目中的隐私风险。当数据处理可能使数据主体的权利和自由面临风险时，这是一项法律和强制性责任。
- **选择加入：**这是一个英文术语，表示用户授权从公司接收信息。
- **选择退出：**这是一个术语，意思是“选择离开”，这是一个运动，在这个运动中，个人可以自主地停止成为插入的事物的一部分。
- **职责分离 （SOD）：**SOD 是职责分离的首字母缩写词，它是一种内部控制原则，旨在避免组织中的风险，例如欺诈、错误和网络攻击。职责分离基于在不同人员或组之间委派任务，以防止同一个人完全控制系统、流程或机密活动。
- **最低权限策略：**这是一个网络安全概念，包括仅向用户提供履行其职责所需的最低权限。
- **运行手册：**概述组织程序和流程的详细指南，目的是确保活动一致、安全、高效地执行。
- **强化：**旨在加强系统、网络、软件、硬件、固件和 IT 基础设施安全性的流程，使它们更能抵御网络攻击。
- **安全补丁：**旨在修复软件和平台中的漏洞、缺陷和错误的纠正性更新。
- **OWASP：**Open Worldwide Application Security Project （OWASP） 是一个国际非营利组织，致力于提高 Web 和移动应用程序的安全性。OWASP 是打击网络犯罪的领先举措之一。
- **隐私和安全设计：**从项目或服务的概念中主动提及数据保护和系统安全的概念。
- **网络钓鱼：**一种旨在窃取个人信息或访问在线帐户的网络攻击。诈骗者使用看似合法的欺诈性消息来诱骗受害者泄露敏感数据。
- **道德黑客：**道德黑客是一种数字安全实践，包括模拟网络攻击以识别和纠正系统、网络或应用程序中的漏洞。

- **渗透测试：**渗透测试是组织对自己的计算机系统或网络进行的授权模拟攻击，用于评估其安全性。目标是使用与黑客相同的工具、技术和流程来发现漏洞。通过暴露网络安全弱点，渗透测试有助于降低恶意网络攻击的风险。

四. 责任

4.1. 供应商服务合同区域

- 在雇用需要访问 WEG 集团内部网络、系统、信息或数据的合作伙伴（包括与合作伙伴相关的员工、供应商和服务提供商）的过程中，签约区域必须确保所有相关人员都了解此信息安全政策。
- 签约区域必须确保与合作伙伴签订的合同包含有关信息安全和数据保护的具体条款，包括明确引用本信息安全政策。

4.2. 合作伙伴

- 合作伙伴有责任遵守本信息安全政策中规定的准则;和
- 所进行的活动必须符合现行法律以及适用于合同标的的与信息安全相关的监管机构和实体的标准化。

五. 指引

5.1. 常规

合作伙伴，无论他们是产品、许可证还是服务的供应商，都必须承诺完全遵守以下规定：

- 保护信息免遭未经授权的访问、修改、销毁或披露，同时保持其机密性;
- 确保提供给他们的资源仅用于 WEG 集团批准的目的;
- 确保其负责的系统和信息根据 WEG 集团的标准得到充分保护;
- 确保关键业务信息的处理连续性;
- 遵守规范知识产权方面的法律和标准;
- 根据最佳市场惯例和适用法规实施和维护信息安全控制措施;
- 立即向 WEG 集团报告任何不遵守合作伙伴信息安全政策的行为，无论是他们自己还是其他人，无论他们是否与合作伙伴有关联。
- 遵守 WEG 集团采购商品、材料和/或服务的一般条件（“GCC”）——网址为： https://www.weg.net/ > 这是 WEG>供应商的一般采购条件——以及 WEG 集团的供应商道德准则（“道德准则”）——网址为：https://www.weg.net/ -> 这是 WEG -> 供应商道德准则。合作伙伴必须严格遵守任何适用法律中规定的数据保护和隐私参数，并遵循有关该主题的最佳市场惯例。
- 代表 WEG 集团开展关键活动的合作伙伴必须经过信息安全（“IS”）评估流程。在 IS 评估过程中，将在供应商资格认证和合同谈判阶段进行 IS 自我评估。根据自我评估的结果，WEG 集团可能会要求额外的程序，以验证合作伙伴是否符合本合作伙伴信息安全政策中建立的 IS 参数。

六. 信息安全要求

6.1. 合作伙伴在 WEG GROUP 环境中的行为

6.1.1. 逻辑访问和可接受使用

- 对于需要远程访问 WEG 集团环境的合作伙伴，负责合同的 WEG 经理必须通过单个用户提供访问权限，在该用户中，他们只能访问履行其职能所需的工作资源和环境;
- 未经负责信息安全的区域事先批准，合作伙伴的计算机不能连接到 WEG Group 的内部网络，合作伙伴设备的软件必须获得正式许可;
- 禁止访问、下载或分发任何侵犯 WEG 集团版权或财产的内容。同样，不允许访问或分发任何性质的非法色情内容或违反《儿童和青少年法规》的内容;
- 提供给合作伙伴的访问凭证仅供独家使用，不得与他人披露或共享;
- 合作伙伴必须确保其访问凭证的安全，并且对于使用其访问凭证进行的任何使用（包括任何误用）负有唯一和独有责任;
- 合作伙伴有责任传达其员工、供应商或服务提供商的任何解雇情况。

6.1.2. 信息安全事件通知

当合作伙伴发现事件或合理怀疑事件正在发生或已经发生时，合作伙伴应：

- 立即启动事件处理，以调查、及时遏制和保护任何有风险的 IT 系统和公司数据，最大限度地减少和减轻事件对 IT 系统的影响;
- 立即通过电子邮件通知 WEG 集团 soc@weg.net。

合作伙伴必须通知事件，包括以下信息：

- 事件的性质和可疑范围;
- 事件开始的可疑日期;
- 发现事件的日期和时间;
- 合作伙伴采取措施确保持续提供范围，并在相关情况下保护和恢复公司数据;
- 合作伙伴代表的联系方式，以回应 WEG 集团对此类信息的请求。

合作伙伴必须尽快向 WEG 集团提供以下信息：

- 事件的可疑原因及涉案行为者;
- 事件的估计影响;
- 建议的纠正措施和从事件影响中完全恢复的预计时间;
- 建议的纠正措施，包括确保继续提供范围以及在相关情况下保护和检索公司数据。

合作伙伴应向 WEG 集团提供根据前款提供的信息的定期更新，以及 WEG 集团可能合理要求的与事件相关的任何其他信息（包括与事件有关的相关 IT 系统的所有访问记录以及证明有效保护和恢复公司数据的证据）。

合作伙伴应立即向 WEG 集团提供 WEG 集团可能需要的所有协助，使其能够调查、响应、减轻影响和纠正事件（包括保护和恢复公司数据），并与个人或公共机构（包括相关监管机构）进行沟通和回应。

合作伙伴应尽快向 WEG 集团提供事件的最终报告，包括根本原因分析。

即使合同中有任何相反的规定，如果事件是由于违反本附件或合作伙伴成员的疏忽造成的，则不应被视为不可抗力事件。

6.1.3. 设备安全

- 每个合作伙伴都有责任保护其保管的包含 WEG 集团信息的物理设备;
- 合作伙伴须知，访问任何 WEG 集团环境或使用 WEG 集团环境中的任何 IT 资源，即使在合作伙伴使用个人拥有的设备的情况下，也会受到监控和检查，除非适用的当地法律明确禁止此类行为。

6.1.4. 违反行为

以下情况被视为违反本合作伙伴信息安全政策，但不限于：

- 任何可能使 WEG 集团直接或间接、潜在或实际地遭受财务或形象损失的行为、疏忽或其他情况，从而损害其信息资产;
- 未经 WEG 集团明确许可，滥用或披露任何信息，例如：公司数据、商业秘密或其他信息;
- 纵容或不遵守本合作伙伴信息安全政策中确立的任何指导方针、规则、参数或义务;
- 将数据、信息、设备、软件、系统或其他技术资源用于非法目的，其中可能包括违反法律、内部和外部法规、道德或 WEG 集团运营领域监管机构的要求;
- 未能立即将任何信息安全事件或不遵守本合作伙伴信息安全政策的情况传达给 WEG 集团。

6.2. 合作伙伴环境中的安全和隐私控制

应 WEG 集团业务领域的要求，信息安全治理团队将在工具中注册相关合作伙伴，以验证其网络健康状况。该平台提供评分分数。

合作伙伴的总分必须至少达到 80% 或工具本身提供的细分市场平均分，以较高者为准。

未达到预期分数的合作伙伴将收到 WEG 集团的充分性和合规性报告，以便合作伙伴可以在 180 天内采取措施达到预期分数。

除了上述注册程序外，合作伙伴还必须遵循以下信息安全准则，这些信息安全准则也在信息安全部门发送和维护的自我评估文件中提供。

6.2.1. 隐私

- 通过文档展示合作伙伴环境中的 WEG 数据流，包括其整个生命周期（收集、处理、存储、共享和删除）。
- 告知 WEG 集团收集了哪些信息，出于什么目的，处理数据的法律依据是什么，数据存储在哪里以及存储多长时间，始终寻求最小化存储期限和收集的信息量。
- 进行与持有人个人数据 （DPIA） 相关的影响评估，并制定允许 WEG 集团在合同范围内不受限制地访问其处理和存储信息的流程。

- 有一个*选择加入*和*选择退出流程* ，以便 WEG 集团和个人数据的持有者通过合作伙伴关系事先自由表达有关共享的信息。还值得注意的是，默认值应为不分享。只有在相关方*选择加入*后，合作伙伴才能与合作伙伴共享数据。

6.2.2. 访问控制

- 拥有正确记录的访问管理流程;
- 根据定义的特定服务，使 WEG 集团能够不受限制地访问已存储或待处理的数据和信息，并重视这些数据和信息的机密性、完整性、可用性和可恢复性;
- 使 WEG 集团了解用于遵守合同的程序和控制措施，如上文所述，特别是通过物理或逻辑控制来识别和隔离 WEG 集团的客户数据;
- 不允许将共享帐户或通用用户用于关键系统，以及维护与登录相关的控制，例如（但不限于）：在首次访问时强制更改，在多次某些无效尝试后阻止用户，要求复杂的密码模式和符合最佳市场标准的其他信息安全实践;
- 有一个正式的、记录在案的流程来授予、更改和撤销访问权限，尤其是那些具有特权共享的人;
- 有一个控制功能分离 （SOD） 缺失的过程;
- 采用最低权限策略;
- 拥有对访客进行物理和逻辑访问控制的方法;
- 在远程办公*期间* 为员工/服务提供商提供远程访问控制。

6.2.3. 服务和信息安全运营管理的监控

- 确保其在提供信息和充足的管理资源方面具有最高水平的能力，以监督将提供的服务，并确保遵守现行法律和法规;
- 应要求，通知并授予 WEG 集团适当的管理资源，以监控合同服务;
- 拥有用于监控资产容量和可用性、关联警报和以自动方式生成事件票证的资源和工具;
- 制定结构化的事件响应流程，包括事件分类以及用于 *处理和解决已知事件的*运行手册。
- 预防、检测和减少与网络环境相关的事件，证明程序和控制措施至少包括身份验证、加密、入侵预防和检测、数据泄漏预防、定期测试和扫描以检测漏洞、安全*补丁*的应用、*强化*的应用在其服务器和工作站上，防止恶意软件和阻止未经批准的软件，建立计算机网络的可追溯性和分段机制，维护和信息安全副本;
- 如果 WEG 环境中发生涉及合作伙伴的安全事件或异常/不当行为，WEG 保留立即单方面撤销任何访问权限的权利，无论是已确认、可疑还是正在调查;
- 应要求提供与过去 24 个月内发生的事件数量相关的信息，并按其相关性对其进行分类。合作伙伴必须将有关“中”、“高”或“非常高”严重性事件的所有数据存储至少 5 年;
- 将可能影响提供服务或遵守现行法律法规的任何限制永久告知 WEG 集团。

6.2.4. 威胁管理

合作伙伴应确保及时修补或更新 IT 系统中的漏洞。在任何情况下，合作伙伴应：

一) 在承包小组的相关 IT 系统中发现任何非第三方提供的严重漏洞（CVSS 或 CVE 9.0 或更高版本）后的 24 小时内：

- 开始开发和部署更新或补丁以修复漏洞的过程;
- 通过 soc@weg.net 通知 WEG 集团，并提供有关漏洞和相关威胁的详细信息，以及合作伙伴为减轻威胁或漏洞而采取的措施。
- 确保所有相关的合作伙伴 IT 系统都已安装和部署了最新的第三方提供的补丁;
- 在更新或补丁发布后的 24 小时内，安装并部署美国网络与基础设施安全局已知被利用漏洞目录中包含的漏洞的更新或补丁。如果任何更新或补丁因任何原因无法在 24 小时内应用，合作伙伴必须立即通过 soc@weg.net 通知 WEG 集团。

二) 合作伙伴应：

- 确保持续监控相关 IT 系统，以确保其安全性、真实性、机密性、完整性和可用性;
- 持续生成必要的相关 IT 系统日志，以便：（A） 启用事件响应;（B） 确定事件的来源;以及 （C） 重现导致事件的事件顺序。合作伙伴必须自生成之日起将这些记录安全地保留至少 180 天，以便只有授权用户才能访问这些记录。

6.2.5. 系统开发的安全性

- 在软件开发流程中 *采用* Privacy and Security by Design 实践;
- 描述应用程序访问的安全功能和数据，这些特征和数据必须在审批阶段由信息安全部门进行评估（例如：技术规范和/或功能图）;
- 使用完整性验证例程来防止在非生产环境中使用虚构数据或匿名化的错误，无论是非自愿的还是有意的;
- 在源代码中采用安全分析实践;
- 在其应用程序中采用安全分析实践（道德黑客测试和渗透测试）;
- 在代码质量和验证过程中提供安全验证。至少应考虑出现在 OWASP TOP 10 中的那些。

6.2.6. 业务连续性、数据管理、保留和存储。

- 制定业务连续性计划，以确保可能发生的事件不会影响向 WEG 集团提供的服务，特别是考虑灾难恢复计划，定期测试保障控制措施，以验证公司对真实情况的准备程度;
- 应要求，使用安全排除程序（数字和/或物理）通知并授予 WEG 集团有关数据和信息传输和存储及其处置的安全措施;
- 定期对存储 WEG 集团信息的资产执行备份执行流程，以避免或最大限度地减少事件发生时的数据丢失。

6.2.7. 培训和意识

- 确保为其所有员工、供应商和服务提供商提供信息安全和数据隐私方面的培训和意识计划，至少每年一次，并且必须考虑对新聘用的员工、供应商和服务提供商强制适用合作伙伴行为准则。
- 包括在其信息安全和数据隐私培训和宣传计划活动，以防止 *网络钓鱼* 和社会工程指导，以及讲座、发行 IS 和数据隐私时事通讯等。

- 有权访问或处理个人数据和/或敏感信息的合作伙伴员工、供应商或服务提供商必须了解本政策及其涉及的信息安全培训内容。

6.2.8. 服务和认证

合作伙伴应：

- 提前正式通知与 WEG 集团签订合同对象相关的服务分包;
- 获得信息安全或业务连续性认可，并得到独立外部审计报告的证明;
- 应要求，通知并授 WE 集团有关提供服务所需的认证，以及与提供合同服务时使用的控制措施相关的报告，这些报告由专业的独立审计公司准备;
- 拥有将异常或安全事件传达给 WEG 集团、相关个人和国家数据保护机构的机制。

七. 定期评估

WEG 集团可以在其认为必要时进行评估，以证明实施本文件中所介绍的控制措施的有效性，为此，WEG 集团必须提前 30 天通知合作伙伴。如果发生安全事件或适用于合作伙伴或 WEG 集团细分市场的市场条件发生变化，也可能进行评估。

八. 制裁

违反控制或不遵守合作伙伴信息安全政策及其定义被视为严重错误或违规行为，可根据 WEG 集团的内部政策和/或合同规定实施相应的处罚或制裁。

如果合作伙伴、其员工、供应商、服务提供商和/或与合作伙伴相关的任何人违反本政策的任何义务或规定，合作伙伴承诺赔偿、保护并使 WEG 集团免受任何和所有损失或损害，而不影响合同或法律规定的其他处罚、制裁和/或处罚。

合作伙伴承认并同意，单纯的赔偿可能不是补救任何违反本政策行为的适当方式，WEG 集团可以使用任何形式和/或方式来具体执行义务，这些义务可能在受到威胁或有效违反本合作伙伴关系的情况下适用。