供应商信息安全管理指引

版本生效日期：2025 年 01 月 07 日

大联大控股股份有限公司（以下简称「本公司」）为确保本公司及其所属关系企业（以下合称「大联大」）与客户的信息安全，我们致力于建立和维护高标准的信息安全管理，本公司特订定供应商资安管理指引（以下简称「本指引」），旨在期望供应商之资安管理符合法律法规、行业标准及本公司相关信息安全要求，适用于与本公司进行合作的所有庶务性供应商[备注]，包括但不限于产品供应商、服务供应商、外包伙伴及其他第三方。

备注：大联大控股为半导体零件通路商，供应商分别为「原厂/ IC 设计供应商」及「庶务性供应商」两大类型（请详官网：通路整合与创新：：大联大控股）。 本指引所称供应商，不包括「原厂/IC 设计供应商」类型之供应商。

1. [信息安全]供应商应确保其信息系统的安全，包括但不限于设置有效的防火墙、权限设定、稽核轨迹保存等保护措施。 防止未经授权的进入、使用、披露、破坏、修改、检视、记录及销毁等行为。
2. [访问]供应商应建立适当的访问相关政策、程序、流程和技术控制措施，确保访问大联大数据仅授权之人员具访问权限。
3. [加密]供应商仅能在合作期间内，基于合作需求搜集、处理、利用、传输、保管或阅览相关资料，需经授权和核准不得超出合理使用范围，并采取必要的技术和管理措施，确保资料的安全性，包含但不限于资料静态加密、资料传输加密、装置及储存媒体控制。
4. [保密]除经大联大书面同意外，供应商不得将机密信息（包括但不限于合约约定、因合作关系获悉大联大未公开信息）揭露给其他任何第三人知悉，且如知悉本合作之机密信息有外泄情形，应即通知本公司，并负防止机密信息继续外泄之义务。 在合作结束后，供应商应依照本公司的要求，将所有相关资料返还或彻底销毁/删除，并提供相应的证明文件。
5. [安全计划]供应商应根据大联大的信息安全性和数据隐私权要求，建立并维护有效的安全计划，包括技术和组织措施，以防止滥用、破坏、遗失、更动或未经授权的揭露、获取或存取机密的专有信息或受保护的信息。
6. [个资保护]供应商应建立适当的流程和措施来保护个人资料。 供应商应遵守本公司及其自身适用的隐私权或资料保护安全法律，确保个人资料在搜集、处理、利用、传输和保管的过程中，符合隐私和数据安全的法律及监管要求。
7. [培训]供应商应定期为其员工提供信息安全意识和培训课程，涵盖如何实施及遵守其信息安全计划的要求。
8. [法令遵循]供应商应遵守所有适用的法律法规、契约、行业标准、及国际标准，必要时，本公司得要求供应商提供相关的合规证明文件。

9. [事件回应]供应商如有违反信息安全相关法令、疑似或已知发生信息安全事件（例如个人资料外泄、非法入侵或病毒攻击等），即将或已经使大联大受到影响，应立即通知大联大指定窗口并配合进行相关处理措施。
10. [应变计划]供应商应建立事件应变计划或相关程序，包含但不限于资料备份计划和灾难恢复计划。
11. [稽核]为确保供应商落实执行上述资安管理措施，大联大得不定期对供应商进行信息安全稽核，供应商应配合大联大资安稽核之实施。
12. [违反效果]供应商应承诺遵守本指引或本公司要求的信息安全标准，供应商如未遵守本规范或无法达成大联大要求的信息安全标准，且无法于期限内配合改善者，大联大将依合约终止合作关系，并自第三方名单中除名。

如有任何有关本规范的问题或需要进一步的信息，请不吝联络本公司，联络人：资安推行单位 ，联络方式：WPGISPG@WPGHOLDINGS.COM。