瑞昱供應鏈資訊安全管理政策

Realtek Supply Chain Information Security Management Policy

一、 目的 Purpose

為確保瑞昱半導體於委外或採購活動中，供應商能妥善保護瑞昱半導體之資訊資產及機密資訊，降低因供應鏈風險所造成之資訊安全及隱私保護衝擊，特訂定瑞昱供應鏈資訊安全管理政策（以下簡稱本政策），作為供應商遵循之基本原則與要求。

To ensure that suppliers of Realtek Semiconductor Corp. (hereinafter referred to as “Realtek”) can properly protect Realtek's information assets and confidential information during outsourcing or procurement activities, and to mitigate the impact on information security and privacy protection caused by supply chain risks, Realtek Supply Chain Information Security Management Policy (hereinafter referred to as "this Policy") is established to serve as the fundamental principles and requirements for supplier compliance.

二、 基本管理原則 Basic Management Principles

供應商應建立與其業務規模及風險相符之資訊安全管理機制，至少涵蓋下列原則：

Suppliers shall establish an information security management mechanism commensurate with their business scale and risks, covering at least the following principles:

- 制度建立：具備書面化之資訊安全與隱私保護相關政策、程序或作業規範。
  System Establishment: Possess documented policies, procedures, or operational standards related to information security and privacy protection.
- 責任明確：指派適當之人員或單位負責資訊安全管理與聯繫窗口。
  Clear Responsibility: Assign appropriate personnel or units to be responsible for information security management and serve as contact points.
- 持續改善：定期檢視與調整資訊安全措施，以因應威脅、法規或業務變化。
  Continual Improvement: Regularly review and adjust information security measures to respond to threats, regulations, or business changes.

三、 資訊安全管理要求 Information Security Management Requirements

1. 資安規範與控制 Security Norms and Controls

   供應商應參考國際標準 ISO 27001、TISAX，制定合理之管理、技術及實體控制措施，以保護其處理或保存之瑞昱半導體資訊，包含但不限於：

   Suppliers shall reference international standards such as ISO 27001 and TISAX to formulate reasonable managerial, technical, and physical control measures to protect Realtek's information processed or stored by them. This includes, but is not limited to:

   - 存取權限控管與身分驗證機制

Access control and identity verification mechanisms.

- 系統與設備之安全設定與更新管理
  Security configuration and update management for systems and equipment.
- 資料之保存、傳輸與銷毀保護措施
  Protection measures for data storage, transmission, and destruction.

2. 檢核與稽核機制 Self-Assessment and Audit Mechanism
   供應商應具備資訊安全自我檢核或內部查核機制，並於瑞昱半導體合理要求下：
   Suppliers shall possess information security self-assessment or internal audit mechanisms and, upon Realtek's reasonable request, shall:
   - 提供相關佐證文件（如政策摘要、檢核結果或第三方驗證）
     Provide relevant supporting documents (e.g., policy summaries, assessment results, or third-party certifications).
   - 配合瑞昱半導體進行必要之書面或訪談式審查
     Cooperate with Realtek to conduct necessary document reviews or interview-based audits.
3. 資訊安全風險管理 Information Security Risk Management
   供應商應識別與評估其業務活動中可能影響瑞昱半導體之資訊安全風險，並採取適當之風險降低措施，包括：
   Suppliers shall identify and evaluate information security risks in their business activities that may affect Realtek and take appropriate risk mitigation measures, including:
   - 重要系統或服務中斷風險
     Risks of interruption to critical systems or services.
   - 外包或次級供應商所衍生之風險
     Risks derived from outsourcing or sub-suppliers.
   - 人員異動、資安事件或環境變動所帶來之影響
     Impacts caused by personnel changes, security incidents, or environmental changes.

四、 資安事件通報與應變 Incident Notification and Response
供應商應建立資安事件通報與處理流程，並至少符合以下要求：
Suppliers shall establish a process for reporting and handling information security incidents and must meet at least the following requirements:

1. 當發生或疑似發生可能影響瑞昱半導體資訊、系統或營運之資安事件時，應於 24 小時內主動通知瑞昱半導體。
   Immediate Notification: Upon the occurrence or suspected occurrence of an information security incident that may affect the information, systems, or operations of Realtek, the supplier must actively notify Realtek within 24 hours.

2. 提供事件影響範圍、初步原因及已採取之應變措施。
   Incident Details: Provide the scope of impact, preliminary causes, and response measures already taken.
3. 配合瑞昱半導體進行後續調查、改善與預防措施之執行。
   Cooperation: Cooperate with Realtek in subsequent investigations and the implementation of improvement and preventive measures.

五、 遵循與違反處理 Compliance and Violation Handling

供應商應配合本政策之要求，並將其落實於相關作業中。若供應商未能遵循本政策，產生資訊安全風險或導致事件的發生，瑞昱半導體得視情節：

Suppliers shall comply with the requirements of this Policy and implement them in relevant operations. If a supplier fails to follow this Policy, resulting in information security risks or incidents, Realtek may take the following actions depending on the severity of the situation:

1. 要求限期改善 Require improvement within a specified deadline.
2. 調整合作範圍或條件 Adjust the scope or conditions of cooperation.
3. 依契約約定採取相應處置措施 Take corresponding measures as stipulated in the contract.

六、 政策檢討 Policy Review

瑞昱半導體得視法令、產業趨勢及實務需求，定期或不定期檢討與修訂本政策，並通知相關供應商配合執行。

Realtek may review and revise this Policy periodically or irregularly in response to laws, regulations, industry trends, and practical needs, and will notify relevant suppliers to comply with the execution thereof.