# 資訊安全政策

# Information Security Policy

## 目的 ｜ Purpose

建立資訊安全管理體系，遵循相關法規、提升員工資安意識，保障資訊資產之機密性、完整性和可用性。制定資訊安全改善目標和評量目標的達成，降低公司營運風險，確保公司之持續營運。

Establish an information security management system, comply with relevant laws and regulations, and enhance employees' awareness of information security to protect the confidentiality, integrity, and availability of information assets. Formulate information security improvement goals and achieving evaluation goals to reduce the Company's operational risk and ensure the company's sustainable operation.

## 目標 ｜ Objectives

- 機密性 ： 防止本公司機敏性資訊不得被未經授權之個人或程序所取得或揭露，以保護機敏資訊。

  Confidentiality:Safeguard sensitive information by preventing it from being accessed or disclosed by unauthorized individuals or programs.
- 完整性 ： 保護本公司機敏資訊生命週期的一致性和正確性，免於因內外部蓄意或意外之各種
  威脅與破壞，致業務資訊遭受竄改、破壞、遺失等風險。

  Integrity:Protect the consistency and accuracy of the lifecycle of the Company's sensitive
  information from the risk of tampering, destruction, and loss of sensitive business information due to internal and external intentional or accidental threats and damages.
- 可用性 ： 確保本公司之系統、設備及網路，不因各種威脅，破壞或是損壞，而造成服務錯誤
  或中斷無法使用。

  Availability: Ensure that the Company's systems, equipment and networks remain uncompromised from threats, destruction or damage that may cause service errors or interruptions.
- 本政策將於每一年進行定期評估並將內容公告於凌華科技官方網站上。
  The policy will be reviewed annually and published on ADLINK official website.

## 組織｜ Governance

## 管理範疇 | Scope

資訊安全管理政策包含以下管理範疇：

Information Security Policy includes the following areas:

1. 存取控制和帳號安全政策。
   Access control and account security policy.
2. 用戶端電腦安全政策。
   Client computer security policy.
3. 伺服器安全政策。
   Server security policy.
4. 企業網路與網際網路安全政策。
   Enterprise network and Internet security policy.
5. 資料庫安全政策。
   Database security policy.
6. 應用程式與開發安全政策。
   Application and development security policy.
7. 電子訊息儲存與交換管理政策。
   Electronic information storage and exchange management policy.
8. 遠端存取安全政策。
   Remote access security policy.
9. 實體安全政策。
   Physical security policy.
10. 風險分析與定義管理。
    Risk analysis and definition management.
11. 備份與還原政策。
    Backup and restoration policy.
12. 災難復原機制。
    Disaster recovery policy.

## 電腦資安事件應變 ｜ Computer Security Incident Response

- 若遭遇資訊安全事件，將依據「電腦資安事件應變流程」，由應變小組進行統籌對應並執行相關必要措施以降低或終止資安事件所導致的影響。

  All information security incidents will be handled by CSIRT(Computer Security Incident Response Team) based on CSIRT operating process when they are discovered, CSIRT will be responsible and coordinate until resolution is in place to reduce or stop the impact due to the security incidents.