致和證券股份有限公司

Concord International Secunrities Co., Ltd.

資訊安全政策

文件編號：ISMS-1-01
機密等級：一般
版　　次：1.0

目錄

1. 目的.....1

2. 目標.....1

2.1 機密性.....1

2.2 完整性.....1

2.3 可用性.....1

2.4 適法性.....1

3. 範圍.....1

3.1 管理制度適用範圍.....1

3.2 人員適用範圍.....1

3.3 資訊安全定義.....2

4. 政策.....2

4.1 作業原則.....2

4.2 審查與實施.....2

1. 目的

致和證券股份有限公司（以下簡稱本公司）為保護本公司資訊資產，免於遭受破壞，不論這些破壞是來自於公司內部或外部以及來自人為、蓄意或意外，爰制定本資訊安全政策，以作為實施各項資訊安全措施之標準。透過本資訊安全政策之制定，明確宣示高階主管支持資訊安全之決心，並使相關人員有所依循。

2. 目標

配合營運策略制定資訊安全目標，於落實資訊安全目標基礎上協助達成營運策略，設定以下目標：

2.1 機密性

確保資訊業務資訊與服務安全存取與保護機密資訊。

2.2 完整性

確保資訊業務資訊內容正確與完整。

2.3 可用性

確保資訊業務服務持續可用與降低事故衝擊。

2.4 適法性

確保資訊業務符合法令法規要求。

3. 範圍

3.1 管理制度適用範圍

資訊安全管理制度實施範圍為各項資訊作業。

3.2 人員適用範圍

資訊安全管理政策適用於致和證券股份有限公司全體同仁與廠商人員。

3.3 資訊安全定義

確保資訊服務符合機密性、完整性、可用性及適法性之要求。

4. 政策

4.1 作業原則

4.1.1 日常作業中應確實遵守資訊安全管理制度規範相關法令規定，審慎處理維運資訊機房業務。

4.1.2 定期考量相關法律規章及營運要求，進行資產風險評估，確認資訊作業安全需求，建立標準作業程序，並採取適當資訊安全控制措施。

4.1.3 定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實度。

4.1.4 建立資訊安全事故管理程序，以確保事故妥善回應、控制與處理。

4.1.5 應訂定營運持續計畫並定期演練，以確保重要業務於災害發生時能於預定時間內恢復作業。

4.1.6 員工依規定接受資訊安全教育訓練與宣導，以加強資訊安全認知。

4.1.7 若違反本政策與資訊安全相關規範，應依據本公司獎懲規定辦理懲處；若涉及違反法令法規時，依相關法律規定追究民事、刑事責任。

4.2 審查與實施

4.2.1 資訊安全管理審查委員會每年審查政策與資訊安全目標，以符合相關法令、技術、利害關係者（Interested Parties）期待，以及與營運策略連結，依業務變動、技術發展及風險評鑑的結果修訂之。

4.2.2 本政策經董事會通過後實施，修訂時亦同。