揚智科技
ALi Corporation

主　　題：	資訊安全政策 Security Policy	**文件編號：** O-A-010	**版本：** 4
機密等級：	☐ Public ☑ Internal ☐ Confidential ☐ Strictly Confidential ☐ SL1 ☐ SL2	**生效日期：** 2018/08/31	**總頁數：** 27

修訂原因 / 效益：

1. 將 智權資訊管理規範　整併至 資訊安全政策

2. 增修 新條文

適用範圍：

☑ ALi all
☐ Taipei
☐ Hsinchu
☐ Shanghai
☐ Zhuhai
☐ Shenzhen
☐ Seoul
☐ Others ___

核准：	**審核：**	**制定：**
CEO BU		資訊安全暨文管中心 任繼亮

修訂記錄

版序	生效日	修訂內容提要
1	2013/12/9	新增辦法
2	2017/8/28	增訂 6.5 & 6.6 章節
3	2018/3	修訂 5.2.1 & 5.3.1 及 增訂 9.1 & 9.2
4	2018/8	增訂 4.1.2, 4.2.2, 4.5, 6.7~6.13 章節 修改 6.2.1, 6.2.2, 6.3.3, 6.4.3, 6.4.5
5		
6		
7		
8		

主　　題：	資訊安全政策 Security Policy	文件編號： O-A-010	版本： 4
機密等級：	☐ Public ☑ Internal ☐ Confidential ☐ Strictly Confidential ☐ SL1 ☐ SL2	生效日期： 2018/08/31	總頁數： 27

修訂說明：

1. 修訂目的：

   增訂 4.1.2, 4.2.2, 4.5, 6.7~6.13 章節

   修改 6.2.1, 6.2.2, 6.3.3, 6.4.3, 6.4.5

2. 修訂內容：

原條文	新條文	修訂原因
	4.1.2 訂定相關之管理辦法及標準作業程序	新增
	4.2.2 訂定相關之管理辦法及標準作業程序	新增
	4.5 資安委員會	新增
	6.7 IP 管理規則 6.8 電腦系統管理 6.9 USB 設備管理 6.10 電子資訊媒體管理 6.11 稽核管理 6.12 其他 6.13 罰責	新增
6.2.1　資訊資產對外揭露 B.　向法務單位確認該他人是否已與公司簽妥 NDA。 C.　若他人尚未簽妥 NDA，需向法務單位下載標準 NDA 表單，並與他人完成簽約，簽署完成應傳送附有他人或其機構負責人親筆簽名之 NDA 乙份予法務單位備查。 D.　若與他人有特別協議的內容或條件，在簽署 NDA 前應先諮詢法務單位意見。 E.　僅將資訊揭露給授權知悉之他人。 F.　法務智權處提供資訊揭露人必要的法律諮詢。 G.　法務智權處管理與更新公司 NDA 資料庫。	6.2.1　資訊資產對外揭露 B.　研發相關資料須完成 NDA 或 LSA 簽訂後，依循公司相關作業程序進行交付	將合約相關規定回歸法務智權處頒布: ● 廢止原 B~G 條文 ● 新增 B 條文
6.2.2　接收他人機密資訊	6.2.2　接收他人機密資訊	將合約相關規定

A. 他人主動提供其 NDA 格式時，簽約前應先傳遞法務單位審閱。 B. 接收他人提供之機密資訊後，應將其視同公司內部之機密資訊，並恪遵保密協定。 C. 法務智權處審閱資訊接收人提供之 NDA 格式，並提供必要的修訂意見。 D. 法務智權處管理與更新公司 NDA 資料庫。	A. 他人主動提供其 NDA 格式時，簽約前應先傳遞法務單位審閱。 B. 接收他人提供之機密資訊後，應將其視同公司內部之機密資訊，並恪遵保密協定。	回歸法務智權處頒布: ● 廢止原 C & D 條文
6.3.3 資產銷毀 6.4.5 內部轉送及寄送傳遞 “行政部門”	6.3.3 資產銷毀 6.4.5 內部轉送及寄送傳遞 “人力資源發展處”	組織名稱修訂
6.4.3 FTP 交付 A. 依據公司程序填具「FTP 權限申請單」提出申請。 B. 資訊資產外部交付前，依據 5.3 章節之規定，進行適當的加密作業。 C. 資訊技術處定期備份及刪除 FTP 內的資訊資產 D. 資訊技術處應確保 FTP 傳輸過程的安全性。	6.4.3 FTP 交付 A. 依據公司程序填具「FTP 權限申請單」提出申請。 B. 資訊資產外部交付前，依據 5.3 章節之規定，進行適當的加密作業。 C. 資訊技術處定期備份及刪除 FTP 內的資訊資產 D. 資訊技術處應確保 FTP 傳輸過程的安全性。 E. 申請外部單位之 FTP 帳號以一個為原則，如有特殊需求需開多個帳號，須經由 VP(含)以上之主管核准 F. 資訊技術處須定期刪除 FTP Server 上的資料	增訂 E & F 條文

Revision Description:

1 Revision purpose：
New Added 4.1.2, 4.2.2, 4.5, 6.7~6.13
Amended 6.2.1, 6.2.2, 6.3.3, 6.4.3, 6.4.5

2 Revised Contents：

Current contents	Revised contents	Reasons for revision
N/A	4.1.2 Create and maintain relevant rules and SOP.	New Added
N/A	4.2.2 Create and maintain relevant rules and SOP.	New Added
N/A	4.5 Security Committee	New Added
N/A	6.7 IP Management Rules 6.8 Computer Management 6.9 USB Device Control 6.10 Electronic Information Media Specification 6.11 Auditing 6.12 Others 6.13 Penalties	New Added
6.2.1 Disclose the confidential information B. Check with the legal affairs unit to make sure whether a NDA has been entered into between the company and the persons; C. If the NDA has not yet been concluded, download the standard NDA form from the legal affairs unit and conclude ti with the persons. One copy of the NDA bearing personal signatures of the persons or their responsible persons shall be submitted to the legal affairs for record upon conclusion of the same. D. The special terms and	6.2.1 Disclose the confidential information B. NDA or LSA must be signed, then following the internal relevant operating procedures to deliver R&D materials.	The relevant provisions of the contract, please refer to the regulations that made by the Legal and Intellectual Property Rights Div. ● Abolished the original B~G articles ● New added B article

conditions, if any, shall be conveyed to the legal affairs unit for review prior to conclusion of the NDA; E. The information may be disclosed to the authorized persons on a need-to-know basis. F. The legal affairs unit provide necessary legal advice to the disclosing party; G. The legal affairs unit has to manage and update the company's NDA database.		
6.2.2 Receive the confidential information from others A. Submit the NDA form provided by the persons voluntarily to the legal affairs unit for review prior to concluding the same; B. Treat the confidential information received from the persons as the company's internal confidential information and strictly comply with the NDA; C. The legal affairs unit review the NDA form provided by the receiving party, and advise on amendments to the same; D. The legal affairs unit has to manage and update the company's NDA database.	6.2.2 Receive the confidential information from others A. Submit the NDA form provided by the persons voluntarily to the legal affairs unit for review prior to concluding the same; B. Treat the confidential information received from the persons as the company's internal confidential information and strictly comply with the NDA;	The relevant provisions of the contract, please refer to the regulations that made by the Legal and Intellectual Property Rights Div. ● Abolished the original C&D articles

6.3.3 Destruction of confidential information 6.4.5 Tangible service of confidential information “Administrative Dept.”	6.3.3 Destruction of confidential information 6.4.5 Tangible service of confidential information “Human Resources Development Div.”	Changed Division Name.
6.4.3 FTP transmission A. Follow internal rule, apply FTP account and permission; B. According to section 5.3, data has to be encrypted; C. Information Technology Div. has to backup and delete FTP data regularly; D. Information Technology Div. has to protect security of transmission.	6.4.3 FTP transmission A. Follow internal rule, apply FTP account and permission; B. According to section 5.3, data has to be encrypted; C. Information Technology Div. has to backup and delete FTP data regularly; D. Information Technology Div. has to protect security of transmission. E. Got VP or above approval, external party can create more than one FTP account. F. Information Technology Div. has to delete data of FTP Server regularly.	New added E&F articles

1 目的

為確保本公司相關營運資產的安全，以維持業務之正常維運，提供相關人員在資訊資產處理上應遵守的標準。

2 範圍

本資訊安全政策之適用範圍涵蓋相關資產的處理以及從事管理之人員，所應遵守之要求。

3 名詞定義

3.1 資產(Assets):

為本公司所管理營運的“資訊”的總稱。區分兩種類型

A. 資訊資產(Information Asset): 包含

a. 電子檔案(Electronic documents)
b. 紙本文件(Paper documents)
c. 設計資料(Design data)
d. 軟件(Software)
e. 其他電子資料(Other electronic data)

B. 實體資產(Secure Asset): 包含

a. 資料的載體(Physical data carriers)
b. 設備(Devices)-
c. 光罩(Masks)
d. 配備(Equipment)
e. 其他實體物件(Other Physical Objects)

4 組織與權責

4.1 資訊技術處：

4.1.1 依據資訊安全政策要求，設計及調整相關資訊系統的控管。
4.1.2 訂定相關之管理辦法及標準作業程序

4.2 稽核單位：

4.2.1 依據資訊安全政策要求，設計及執行稽核作業。

4.3 資訊安全及文管中心：

4.3.1 設計及維護資訊安全政策。
4.3.2 定期進行資產盤點作業。

4.4 各處級單位

4.4.1 各單位產出及接收到實体或資訊資產，應依資訊安全等級分類並造冊控管。
4.4.2 各單位配合定期更新清冊及盤點。

4.5 資安委員會：
4.5.1 該組織由總經理，高階主管，資訊技術處處長，稽核單位主管，和資訊安全及文管中心主管共同組成，定期召開會議檢討資安相關議題。
4.5.2 資安委員會決議事項，由各負責單位進行辦理並修訂對應之政策或規範。

5 資訊安全政策內容
5.1 資產的資訊安全等級
5.1.1 資訊資產：

等級	定義
Top Secret	如果該資訊因未經授權的洩漏，可能會造成公司整體營運，面臨到風險
Secret Level2 (SL2)	與ALi產品相關的安全資訊，如果該資訊因未經授權的洩漏，可能會造成所有產品的安全性，面臨到風險
Secret Level1 (SL1)	與ALi產品相關的安全資訊，如果該資訊因未經授權的洩漏，可能會產生出特定產品的安全性漏洞
Strictly Confidential	如果該資訊因未經授權的洩漏，可能會直接造成法務、財務、資安或智財權的問題
Confidential	如果該資訊因未經授權洩漏給非合作的第三方，可能會造成公司的影響
Internal	僅限於內部使用的資訊，如果該資訊因未經授權的洩漏，並不會造成營運負面影響
Public	可以對外公開之資訊，如果該資訊因未經授權的洩漏，並不會造成營運負面影響

5.1.2 實體資產：

等級	定義
Secret Level1 (SL1)	遺失，遭竊或非法使用，會造成營運及客戶的重要影響
Strictly Confidential	遺失，遭竊或非法使用，會造成工作負荷增加
Public	沒有任何影響

5.2. 保護規則

5.2.1 標示規則:

A. 資訊資產標示

	定義
文件 (電子文件 或 紙本文件)	Office (Word/Excel/PowerPoint) & PDF文件需載明: ● 該文件的資安等級 ● 電子文件在對外交付時，需先轉成 PDF 格式，並設置文件安全設定及浮水印 文件安全設定: 1. 禁止列印/複製/變更，2. 依文件重要性決定是否設置“開啟文件密碼” 浮水印格式: 授權使用公司名稱_授權使用人名字_交付日期 (e.g. Kingstereo_Roger_20170825) ● 除“正本合約/政府文件/銀行業務/會計師事務所/業務規定”等有特殊要求之文件，以原始格式交付，但考量是否需增加文件的安全性設定 (e.g. office 文件密碼) 或 加密後傳輸
設計資料，軟件，及其他電子資料	● 以明文格式開發，需於文件表頭增加資安聲明(參考 9.1) ● 歸屬於 SL2/1 等級的資訊資產，其電子檔的附檔名需附有“SL2 or SL1”的縮寫 (e.g. Test_SL2.tar).
電子郵件	確實依據郵件本文及附件內容，選定其資安等級

B. 實體資產標示

該類資產不需要特殊標示，歸屬SL1級別的資產，需有“編號”以進行盤點管控追蹤之使用。

5.3. 資產使用規則

5.3.1 資訊資產使用規則

	授權	使用權限	使用範圍	可否對外交付
Top Secret	VP + NDA	讀	Clean Room	不允許
Secret Level2	BU主管	讀，寫		可，參考 9.2

(SL2)				
Secret Level1 (SL1)				可，參考 9.2
Strictly Confidential	處級主管	讀，寫，列印	公司內部網路	可， ● 透過Email/FTP對外交付 ● 交付前，先完成PGP加密
Confidential				可，
Internal	部門主管	讀，寫，列印，複製		可
Public				可

5.3.2 實體資產使用規則

	授權	儲存地點	跟催及盤點	對外運輸方式	銷毀
Secret Level1 (SL1)	BU 主管	具實體門禁管控之區域	- 集中管控並逐項資產追蹤 - 接收人需簽收每項資產	• 物流公司運輸 (Ref 6.4.5) • 派人親送	歸還至公司內銷毀(Ref 6.3.3)
Strictly Confidential	處級主管	具實體門禁管控之區域	Quantity based tracking		在監督下進行毀損(Ref 6.3.3)
Public		沒限制	不須盤點		在監督下進行毀損(Ref 6.3.3)

6 執行作業

6.1 降級與重分類

6.1.1 當公司營運環境與持有資訊對公司影響程度改變時，決定是否需要降低或將現有資訊之機密分類等級予以變更。

6.1.2 確定機密資訊分類等級有降級或重分類之必要性時，應通知讓資訊使用人知悉。

6.2 對外揭露、接收與遺失

6.2.1 資訊資產對外揭露

A. 確認是否有對他人揭露資訊的必要性，並獲得權責主管許可。

B. 研發相關資料須完成 NDA 或 LSA 簽訂後，依循公司相關作業程序進行交付

6.2.2 接收他人機密資訊

A. 他人主動提供其NDA格式時，簽約前應先傳遞法務單位審閱。

B. 接收他人提供之機密資訊後，應將其視同公司內部之機密資訊，並恪遵保密協定。

6.2.3 資訊資產遺失

A. 當接獲回報機密資訊遺失或不當揭露狀況時，資產保管人應準備摘要報告，並通知處級及BU主管，由BU主管指定調查人員蒐集資料及證據後，召開調查及處理會議。

B. 摘要報告應包含以下事項:

a. 資訊使用人基本資料(姓名、部門、職稱)

b. 事件日期、時間、地點、其他事件關係人、過程摘要

c. 估計對公司可能造成的影響

d. 必須採取的補救措施

e. 其他必要補充資訊

C. 針對狀況發生原因、影響程度進行討論與評估，並擬定具體的補救及預防行動方案，通知相關人員知悉，並監督行動方案執行進度。

6.3 保存、紙本申請與銷毀

6.3.1 資產保存

A. 資產依據5.3章節進行集中儲存，並依資產等級進行權限管控。

B. 收發之所有E-Mail原則上只留存六個月,但若公司對內或對外因有爭議發生或有發生爭議之可能而需用者，不在此限

6.3.2 紙本申請

A. Strictly Confidential(含)以上之資訊資產不可任意進行紙本列印予他人，欲取得額外的紙本複本向資訊資產保管單位提出申請。

B. 紙本列印時應確保複本之機密分類等級標示與備註事項仍然清晰可辨。

C. 副本列印時應全程於印表機、影印機或其他印刷機器旁等候，直至完成方能離開。

D. 非必要時不可將交由外部廠商進行紙本列印，委外前須與外部廠商簽訂NDA。

E. 資訊資產保管單位審閱資訊使用人之申請單是否已由權責主管簽核通過。

F. 資訊資產保管單位簽核完成即紙本複本給該資訊予申請人，並更新申請者資料庫以進行列管。

G. Confidential及Strictly Confidential 級別的紙本複本,應於文件中央以浮水印標示使用者之姓名及交付時間。

6.3.3 資產銷毀

A. 合約簽署單位負責收集銷毀與合約相關之資產，依據合約條文規定進行辦理

B. 紙本資訊資產應使用碎紙機銷毀，或置於公司機密文件銷毀存放處交由人力資源發展處統一處理。
C. 人力資源發展處負責銷毀機密多媒體如錄影帶、錄音帶、磁片、磁帶、光碟片等儲存裝置前，須先刪除儲存之資料且進行格式化，若無法刪除則必須進行消磁或主體分解。
D. 報廢品如PCB、IC晶片等，應交由公司資材管理處統一處理。
E. 人力資源發展處負責不定期公告並回收全公司廢棄之資產。
F. 人力資源發展處負責監督廢棄的資產之運送及銷毀過程。
G. 資訊技術處負責銷毀所有收發超過6個月的E-Mail紀錄。

6.4 資產交付

6.4.1 傳真

A. Confidential(含)以上之資訊資產不可透過傳真機傳遞。
B. 傳真完成後應確認接收方取得之傳真內容及張數正確無誤。
C. 透過傳真傳遞時，應全程於傳真機旁等候，直至確認接收方取得完整之資訊方可離開。
D. 傳真失敗時應確認傳真機記憶體內沒有留存任何暫存檔案，若有即應予以刪除。

6.4.2 電子郵件傳遞

A. Strictly Confidential(含)以上等級的電子郵件在內部傳送時，禁止“回覆/轉寄/複製貼上”等作業
B. 外部傳遞時，依據公司電子郵件外部傳遞規則進行控管。
C. 外部傳遞時，依據5.2 & 5.3章節之規定，進行適當的保護及加密。
D. 外部傳遞時，宜啟動收件人收件後自動回傳功能。
E. 若追蹤回傳之確認函發現有誤傳電子郵件之狀況，應即刻連繫該收件人將信件刪除。
F. 收件人身份若有相互保密之必要性時，應採用副本密送功能進行傳遞。
G. 同仁於公司內限用公司提供之電子郵件信箱傳遞檔案，不得將公司文件寄送至私人信箱。
H. 本公司電子郵件系統為公務使用，同仁應以公務使用為原則，盡量避免用於私人用途。
I. 依公司機密資訊保護政策，對於電子資訊媒體之管理，得依下列規定進行稽核:
   a. 單位依公告之「電子資訊媒體管理規範」檢視同仁使用電子資訊媒體之使用狀況。
   b. 被稽核者主管認為有稽核必要時可提出申請，經副總以上層級許可後，可取得電子資訊媒體相關內容。

6.4.3 FTP交付

A. 依據公司程序填具「FTP權限申請單」提出申請。
B. 資訊資產外部交付前，依據5.3章節之規定，進行適當的加密作業。
C. 資訊技術處定期備份及刪除FTP內的資訊資產
D. 資訊技術處應確保FTP傳輸過程的安全性。
E. 申請外部單位之FTP帳號以一個為原則，如有特殊需求需開多個帳號，須經由VP(含)以上之主管核准
F. 資訊技術處須定期刪除 FTP Server 上的資料

6.4.4 USB管道交付

A. 外部交付前，依據5.3章節之規定，進行適當的加密作業。
B. 交付完畢後，刪除USB內的資訊資產。

6.4.5 內部轉送及寄送傳遞

A. 紙本資訊資產及實體資產，於內部轉送時，由交付人親送，收件人本人親收。若透過內部公文傳遞系統進行跨廠區傳遞時，應將資訊資產完整包裝於密封且不透光之信封或傳遞袋內，送交收發單位統一傳遞。
B. 外部寄送時，應將資產(資訊資產&實體資產)完整包裝於密封且不透光之信封或傳遞袋內，同時外層再以快遞公司提供之專用信封或紙箱進行包裝，送交收發單位統一傳遞。
C. 內部轉送及外部寄送，需向收件人確認已完整取得資訊內容。
D. 人力資源發展處提供託運委託單供資訊傳遞人填寫，並要求收件人簽收重要文件。
E. 人力資源發展處選擇信譽卓著之快遞公司提供傳遞服務。

6.5 IC Design Data控管要求

6.5.1 分類

A. Design Data需進行分類分級作業，依據 5.1 規則

6.5.2 環境設置

A. 專屬系統需置放於獨立網段
B. 需設置專屬系統/目錄(Folder)來儲存Design Data，並依循資產的重要性對目錄(Folder)進行不同的設置、標示及控管機制

6.5.3 使用

A. Design Data 的開發, 使用&交換需在專屬的系統環境下完成
B. Design Data 若有跨部門交互使用或參考時，需設置對應之權限
C. LOG完整的行為紀錄
D. Design Data 只能存放在 Project Folder
E. Design Data 的內容細節，嚴禁使用任何非法方式 (紙本抄寫、列印、錄音、錄影、拍照) 攜出。

6.5.4 流通

A. 若有Design Data 移出專屬系統之需求時，需經過核准後放行

B. 並同步備份移出的Design Data，研發主管需安排查核作業

6.5.5 權限設置

A. 依循開發階段進行人員權限的設置或關閉

6.6 IC 工作站帳號及資料夾管理原則

6.6.1 開發人員的帳號，依據參與的專案進行增設，並設定對應之權限

6.6.2 帳號之權限會依據專案階段進行調整

6.6.3 Home Folder容量要限制到最小範圍

6.6.4 Project Folder的權限控管

A. 已進入MP階段，關閉所有存取權限

B. 進入 Tape Out 階段後 6 個月，關閉所有存取權限

C. 若有特殊需求，經申請後開放

6.7 IP 管理規則

6.7.1 外部取得之 IP (含相關資料) 需集中繳交至 資訊安全及文管中心 控管

6.7.2 特定 IP 使用前，需簽署 “Secured IP 使用規範同意書”

6.7.3 資訊部門針對特殊 IP 使用要求，建置使用之系統環境

6.8 電腦系統管理

6.8.1 未經核准前，禁止同仁攜帶私人電腦進入公司

6.8.2 相關電腦控管機制及網路使用規定，依循資訊技術處須定之辦法執行

6.9 USB 設備管理

6.9.1 禁止使用 USB 設備下載資料，除因工作需求可另行提出申請

6.9.2 USB 下載權限之申請，依循權責單位訂定之作業執行

6.9.3 USB 控管要求，請依循權責單位訂定之程序處理

6.10 電子資訊媒體管理

6.10.1 電子郵件系統、即時通、網路公告的使用規範，請遵循電子資訊媒體管理規範之要求

6.10.2 電子郵件相關控管機制，請參考權責單位訂定之規範

6.11 稽核管理

6.11.1 重要及具敏感性內容的稽核/查核軌跡必須留存

6.12 其他

6.12.1 聘僱與離職，請參照 人力資源發展處 頒布之 新進人員任用管理辦法 及員工離職手續辦理作業要點

6.12.2 門禁要求，請參照 人力資源發展處 頒布之 門禁管理辦法

6.12.3 合約之相關規定，請參考 法務智權處 頒布之相關規定

6.12.4 技術資料持有者應妥善保管所持有之技術資料，並於離職或必要時繳回，一旦遺失將依循 6.13 條文處理。

6.13 罰責

6.13.1 同仁違反本政策之規定，依據人力資源發展處頒定之 員工行為準則 辦理

7 紀錄

無

8 實施與修訂

本規範經總經理核定後實施，修訂時亦同。

9 附件

9.1 資安聲明文件

9.2 SL2-1 outbound delivery SOP

—END—

1 Purpose

The Security Policy (the "Policy") is enacted in order to protect Company's valuable assets and keep business running.

2 Scope

Apply to all of the Company's existing employees.

3 Definitions

3.1 Assets:

Two types

A. Information Asset:
   a. Electronic documents
   b. Paper documents
   c. Design data
   d. Software
   e. Other electronic data

B. Secure Asset:
   a. Physical data carriers
   b. Devices
   c. Masks
   d. Equipment
   e. Other Physical Objects

4 Roles and Responsibilities

4.1 IT Division：

4.1.1 Based on Policy, design and configure systems control.

4.1.2 Create and maintain relevant rules and SOP.

4.2 Audit department：

4.2.1 Based on Policy, design and execution security audit.

4.3 Information Security and Document Center：

4.3.1 Design and update Policy

4.3.2 Execution assets assessment

4.4 Divisions:

4.4.1 Assets are classified

4.4.2 Update and maintain assets list

4.5 Security Committee:

4.5.1 The Security Committee consists of the general manager, high level managers, director of the Information Technology Div., head of the Auditing Unit, and head of the Information Security and Document Center. Regular meetings are held to review issues related to the security.

4.5.2 The resolutions of the Security Committee shall be followed up by the responsible units and the rules or regulations shall be revised.

5 Policy

5.1 Classification Matrix

5.1.1 Information Assets：

Level	Definition
Top Secret	Information that may put the whole business at risk if disclosed.
Secret Level2 (SL2)	Information related to the security of the ALi products that may put the overall security of a product at risk if disclosed.
Secret Level1 (SL1)	Information related to the security of the ALi products that may facilitate a security breach if disclosed.
Strictly Confidential	Information that may have a direct impact on legal, financial, security or intellectual property issues of the ALi if disclosed.
Confidential	Information which may impact the ALi if disclosed without restrictions to third parties..
Internal	Information of internal use with no negative impact on business if disclosed.
Public	Information of public release with no negative impact on business if disclosed.

5.1.2 Secure Assets：

Level	Definition
Secret Level1 (SL1)	Critical impact on the business and/or customer(s) in case of loss, theft or unauthorized

	access.
Strictly Confidential	Important workload would be required in case of loss, theft or unauthorized access.
Public	Does not need specific protection

5.2 Protection Rules

5.2.1 Marking Rules:

A. Information Assets Marking

Level	Definition
Documents (electronic or hard copy)	Office (Word/Excel/PowerPoint) & PDF : ● Marked with classification. ● Before out-bound delivery, documents have to convert to PDF format and configure security setting and embed watermark. Security setting: 1. Forbid print/copy/modify 2. according to data sensitive level, enable "Document open password" function Watermark format: Authorized company name, recipient name and delivery date. (e.g. Kingstereo_Roger_20170825) ● Exception: documents of Contract, Government, banking, accounting firm, and business need.
Design data , software, other electronics data	● If design data are plain text format, the security statement must be embedded. (ref. 9.1) For SL1, SL2 Secret levels, the filename shall be postfixed with the classification level in an abbreviated format with SL1 or SL2 (e.g. Test_SL2.tar).
Email	No marking except in attachments if containing Information Assets.

B. Secure Assets Marking

No marking is wished to have the Secure Assets being

handled as “Incognito”. Solely SL1 assets shall be marked with serial number.

5.3 Handling Rules

5.3.1 Information Assets Handling Rules

	Authorization	Permission	Store	Out-bound delivery
Top Secret	VP + NDA	Read	Clean Room	Never allowed
Secret Level2 (SL2)	BU Head	Read Write		Yes, ref. 9.2
Secret Level1 (SL1)				Yes, ref. 9.2
Strictly Confidential	Director	Read Write Print	Corporate network	Yes (via Email/FTP) with PGP encryption.
Confidential				Yes
Internal	Department Head	Read Write Print Copy		Yes
Public				Yes

5.3.2 Secure Assets Handling Rules

Level	Authorization	Storage	Tracking & inventory	Transport	Destruction
Secret Level1 (SL1)	BU head	The area with physical access control.	-Unit level tracking in a centralized inventory. -Every stock move is confirmed by the signature of the receiver.	• Logistics companies transport • Hand Carry	Returned to ALi for destruction.
Strictly Confidential	Director	The area with physical access control.	Quantity based tracking		Secure Scrapping process with certificates
Public		Free	None.		Secure Scrapping process with certificates

6 Operation

6.1 Degrading and reclassification

6.1.1 Decide whether it is necessary to degrade or reclassify the existing classification, in the case of any change to the impact to be produced by the company's operating environment and information to the company.

6.1.2 After confirming that it is necessary to degrade or reclassify the classification, post such message to users.

6.2 Disclosure, acceptance and loss

6.2.1 Disclose the confidential information

A. Confirm whether such disclosure is required or not and seek the competent supervisor's approval;
B. NDA or LSA must be signed, then following the internal relevant operating procedures to deliver R&D materials.

6.2.2 Receive the confidential information from others

A. Submit the NDA form provided by the persons voluntarily to the legal affairs unit for review prior to concluding the same;
B. Treat the confidential information received from the persons as the company's internal confidential information and strictly comply with the NDA;

6.2.3 Lost the confidential information

A. Prepare the summary report upon receipt of report for loss or inadequate disclosure of confidential information, and inform director and BU head. To call the investigation and response meeting, after gathering data and evidence by investigator that has been assigned by BU head.
B. The summary report shall contain:
   a. User's basic information (name, department, and job title);
   b. Date, time, place, related parties and brief of the matter;
   c. Estimate the potential impact to the company;
   d. Corrective action to be taken;

e. Other necessary information.

C. Discuss and assess the cause and level of impact, and draft the concrete corrective and preventive action plan, inform the relevant staff and supervise the conduct of the action plan.

6.3 Retention, reproduction and destruction

6.3.1 Retention of confidential information

A. According to section 5.3, all of the confidential information shall be storage and access control.

B. All of the emails will be retained for six months only except controversial issues

6.3.2 Paper document of confidential information

A. Security level of Strictly Confidential (or above) cannot be printed to others arbitrarily. Any paper document shall be got approval by the information owner or follow standard of procedure to get it.

B. Ensure that the identification of confidential information grading and remark on the reproduction is readable.

C. Wait beside the printer, copy machine or other printing machines until completion of the reproduction.

D. Forbidden any information data to be printed by external parties. If urgent or special case, external parties have to sign the NDA.

E. Review whether the user's request form has been approved by the applicant supervisor;

F. Paper document delivers to applicant when finished the application process;

G. The applicant's name and delivery date shall be marked in the central area.

6.3.3 Destruction of confidential information

A. Contracts signed units are based on clause of contractual to destroy the confidential information.

B. Paper document of confidential information shall be destroyed by shredder. Human Resources Development Div. announce the recall date to collect assets that should by

destroyed.

C. Human Resources Development Div. responsible for deleting confidential data that stored on multi-media, such as video tape, recording tape, disk, magnetic tape and CD. It must be erased or low level formatted before destroyed. If it is impossible to destroy the data, it has to be demagnetized or take apart the principal parts.
D. The wastes such as PCB and IC chips, shall be handled by Material Management Div.;
E. Human Resources Development Div. responsible for publishing and recalling the destroyed assets or items;
F. Human Resources Development Div. responsible for supervising transportation and destruction of destroyed assets;
G. Information Technology Div. responsible for destroying inbound and outbound emails over than six months.

6.4 Transmission and transportation

6.4.1 Fax

A. The confidential information shall not be transmitted via fax machine;
B. After faxing, call the receiver to confirm the contents and number of pages;
C. Wait beside the fax machine when faxing confidential information, until the receiver has received the information in whole;
D. If faxing failed, please delete the data from fax machine.

6.4.2 Email transmission

A. The internal email identified as Strictly Confidential and Secret Level 1 are prohibited 'reply, forward, and copy and paste.'
B. According to email delivery rules, external transmission has to be monitored and controlled;
C. According to section 5.2 and 5.3, external transmission has to be encrypted;
D. When external transmission, please activate the automatic

feedback function confirming the receipt to make sure whether the recipient receives the information in whole.

E. If the feedback acknowledgement follow-up shows that the email was sent in error, please contact the recipient to delete the email immediately;
F. If it is necessary to keep the recipient's identity confidential, please send the email in the form of blind carbon copy;
G. Prohibit send internal data to private email account;
H. The company's email system is only for official use. The staff shall follow the rules for official use and avoid using it for any personal purposes as practical as possible.
I. To protect the company's confidential information, the company may audit in the following manners:
   a. According to the Electronic Information and Media Management Policy rules;
   b. Got VP's approval, supervisor can get auditing content.

6.4.3 FTP transmission

A. Follow internal rule, apply FTP account and permission;
B. According to section 5.3, data has to be encrypted;
C. Information Technology Div. has to backup and delete FTP data regularly;
D. Information Technology Div. has to protect security of transmission.
E. Got VP or above approval, external party can create more than one FTP account.
F. Information Technology Div. has to delete data of FTP Server regularly.

6.4.4 USB transmission

A. According to section 5.3, encrypt data;
B. After data transmission, delete data from USB device.

6.4.5 Tangible service of confidential information

A. The confidential information to be transmitted internally shall be served personally as practically as possible, and received by the recipient personally. If it is impossible to serve the information personally and it is necessary to transmit it

via the internal transmission system, please put the confidential information into a non-transparent envelop or bag and seal the same. Hand it over to the mailing unit for transmission.

B. To transmit the confidential information, please put it into a non-transparent envelop or bag and seal the same. Then, please use another envelope or carton to wrap and deliver it to Human Resources Development Div.

C. After transmission in such tangible form, please check with the recipient to make sure whether she/he receives the information in whole.

D. Human Resources Development Div. provide the consignment order to the sender, and ask the recipient to sign to acknowledge the receipt of information documents;

E. Human Resources Development Div. selects a creditworthy courier service provider to provide the service.

6.5 Control items of IC Design Data

6.5.1 Classification

A. Design Data must to be classified based on 5.1 rules

6.5.2 Development environment

A. Build up an isolated network for dedicated system.

B. Set up dedicated systems and folders for Design Data and Folders must be configured different security controls (eg. security label marked, permission,) based on assets classification.

6.5.3 Data Usage

A. Any kind of data's behaviors (e.g. Development/exchange/store) must be completed in Development environment.

B. Setting permission for data exchange and access

C. Enable Log function to record all data's behavior.

D. Data cannot be stored in Personal Home Folder.

E. Forbidden capture any content of data through handwritten copy / print / audio record / video record / photo

6.5.4 Exchange

A. Must be got approval, if any data want to move out the Development environment.

B. Execute backup activity when moving out data and backup data must be checked by supervisor regularly.

6.5.5 Permission

A. Permission must be reviewed and configured based on project phase.

6.6 Management rule of IC workstation account and folder

6.6.1 According to Project, every team member has his own dedicated account and configures permission.

6.6.2 Permission will be configured by project phase.

6.6.3 Minimum quota of Home Folder.

6.6.4 Permission control of Project Folder

A. Close any access right when entering MP phase.

B. 6 months after entering the Tape Out phase, close any access right

C. Got approval, to re-open access right

6.7 IP Management Rules

6.7.1 When got external IP and relevant data, receiver have to deliver it to the Information Security and Data Center.

6.7.2 Before using the specific IP, user has to sign the NDA of Secured IP.

6.7.3 According to the requirement of IP's control, Information Technology Div. has to set up suitable development environment.

6.8 Computer Management

6.8.1 It is forbidden to bring a personal computer to the company before approval.

6.8.2 Relevant computer control mechanisms and networking access rules must be implemented by Information Technology Division.

6.9 USB Device Control

6.9.1 It is forbidden to use USB devices for download data, except for work requirements.

6.9.2 Following the procedure that made by authority unit to get the permission of export data to USB device

6.9.3 Relevant USB device control mechanisms must be implemented by authority unit.

6.10 Electronic Information Media Specification

6.10.1 Rules of E-mail system, instant messaging, and network publishing, please follow the key points of the electronic information media specification

6.10.2 Relevant E-mail control mechanism must be implemented by authority unit.

6.11 Auditing

6.11.1 The tracks must be retained when auditing or checking important/sensitive content.

6.12 Others

6.12.1 Hiring and resigning, please refer to the Rules that made by the Human Resources Development Div.

6.12.2 Door access control, please refer to the Rules that made by the Human Resources Development Div.

6.12.3 The relevant provisions of the contract, please refer to the regulations that made by the Legal and Intellectual Property Rights Div.

6.12.4 The holder of technical data shall keep it well and return it when resigned. If it is lost, follow Article 6.13 to handle.

6.13 Penalties

6.13.1 If colleague violates the provisions of this policy, it will follow the employee's code of conduct to handle.

7 Record

None

8 Implementation and Revision

This Code is implemented after approval by the President. The same shall be applicable for any revision.

9 Attachment

9.1 The security statement

9.2 SL2-1 outbound delivery SOP

—END—