文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

□ 其他_
事件區分: ■制定 □修訂 □廢止 □外來文件 □ 客戶往來文件__
內容說明:

核准	審查	單位主管	制定者
總經理 劉o金Terry	研發兼營運副總 謝o遠 Eric	數位副總經理 張oo Fu	ISO-27001 專案主管: 季o錦 Bill
發行章			
愛生育科技股份有限公司 2025.10.11 資料中心發文章			

修訂紀錄				
.版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
V1.0	2025年10月1日	P1-P15	季O錦	初版文件發行

文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

目　　錄

1、 目的 4

2、 範圍 7

3、 權責 8

4、 名詞定義 8

5、 作業說明 9

6、 相關文件及表單 14

文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

1、目的

為說明愛生育科技股份有限公司(以下簡稱為本公司)資訊安全管理制度(以下簡稱本制度)實施之管理機制與相關規範程序，以確保本公司資通資產之機密性、完整性與可用性，達成資通安全目標並符合資通安全管理法及其子法之要求，特訂定「資通安全政策」（以下簡稱本政策)。

資安政策

資訊安全政策願景:

1. 強化人員認知。
2. 避免資料外洩。
3. 落實日常維運。
4. 確保服務可用。
5. 資料備份&系統還原。

資訊安全目標

確保公司營業秘密與依據政府個人資料保護法，持續對資訊安全精進治理與強化防護能力，所有資訊作業遵行國際資安標準外，更要符合國、內外資訊安全法令規範。

風險管理與利害關係人

風險管理組織架構與執掌

一、董事會：本公司董事會為公司風險管理之最高單位，以遵循法令，推動並落實公司整體風險管理為目標，明確瞭解營運所面臨之風險，確保風險管理之有效性，並負風險管理最終責任。

二、營管會議：為董事長或總經理主持之主管會議或營運會議，負責審核控管層級起動的各種計劃及專案的風險評估。

三、財務部門：為獨立於各業務部門之資金調度單位，負責處理每一業務單位之財務作業情況，及投資評估之報告。

四、稽核單位：為隸屬董事會之獨立部門，職司內部控制及內部稽核，以強化內部控制功能，促進公司之健全經營，並適時提供改進建議，以確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據。

五、各級業務單位：各級業務單位主管負有第一線風險管理之責任，分析及監控所屬單位內之相關風險，強調全員全面風險控管，平時落實層層防範，確保風險控管機制與程序能有效執行。

本公司從事各項業務所涉及之風險包括

市場風險、投資風險、信用風險、策略風險、危害風險、作業風險、法律風險、資訊安全風險、其他風險等等。

利害關係人之鑑別及溝通

本公司之利害關係人包含員工、客戶、公益團體、媒體、供應商及投資人等，本公司秉持與利害關係人保持良好關係，推行各項對內、對外的溝通事務，依據各利害關係人所關注項目，分別列入相關單位的職責，對於環境趨勢演變、法令修訂等亦能透過各單位合作進而因應處理。為滿足利害關係人的期待，本公司透過各種溝通方式，一方面確保相關工作達成，一方面維持溝通管道的暢通無誤，並將相關資訊回饋與經營團隊，作為日後改進或規劃之參考。

2、範圍

一、適用於資通作業流程與相關資訊及資通系統資產。

文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

二、本公司同仁(含正式、約聘僱人員、技工、工友等人員)及提供服務之委外廠商人員。

三、資訊安全管理涵蓋 14 項管理事項:

3.1 資訊安全政策訂定與評估。

3.2 資訊安全組織。

3.3 人力資源安全管理。

3.4 資訊資產管理。

3.5 存取控制安全管理。

3.6 資訊加密管理。

3.7 實體與環境安全管理。

3.8 系統作業管理。

3.9 通訊安全管理。

3.10 資訊系統獲取、開發與維護之安全管理。

3.11 支援關係管理。

3.12 資訊安全事件之通報與應變管理。

3.13 營運持續運作管理。

3.14 相關法規與施行單位政策之符合性。

3、權責

一、本公司資安長核定本政策。

二、 資通安全推動小組審查及推動本政策，並負責宣導達成資通安全目標之要求。

4、名詞定義

文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

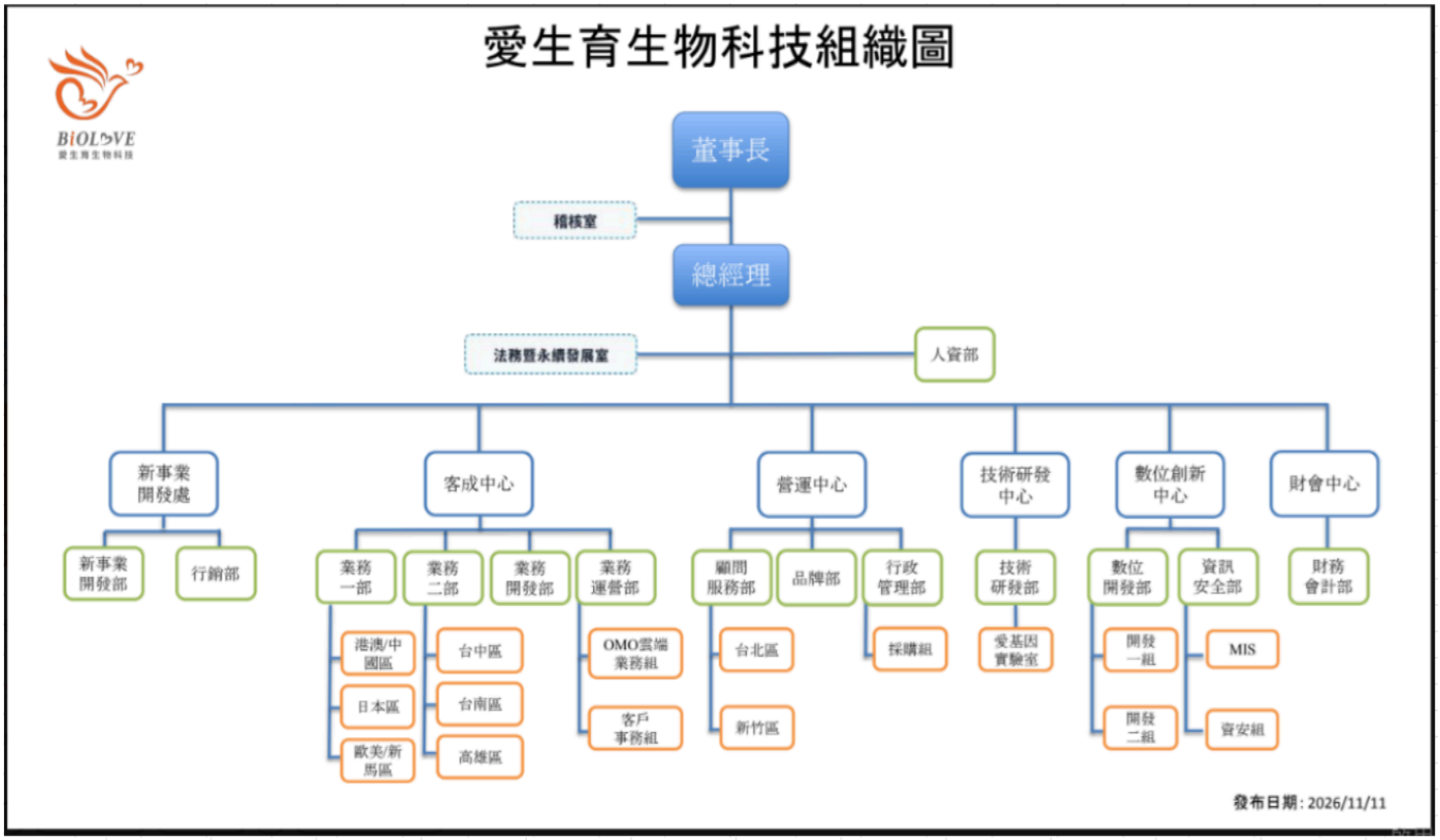
4.1 資訊資產分類:

係指為維持本公司資訊業務正常運作之硬體、軟體、通訊、資料、服務、文件及人員。

4.2 營運持續運作之環境:

係指為維持本公司各項資訊業務正常運作所需之作業環境。

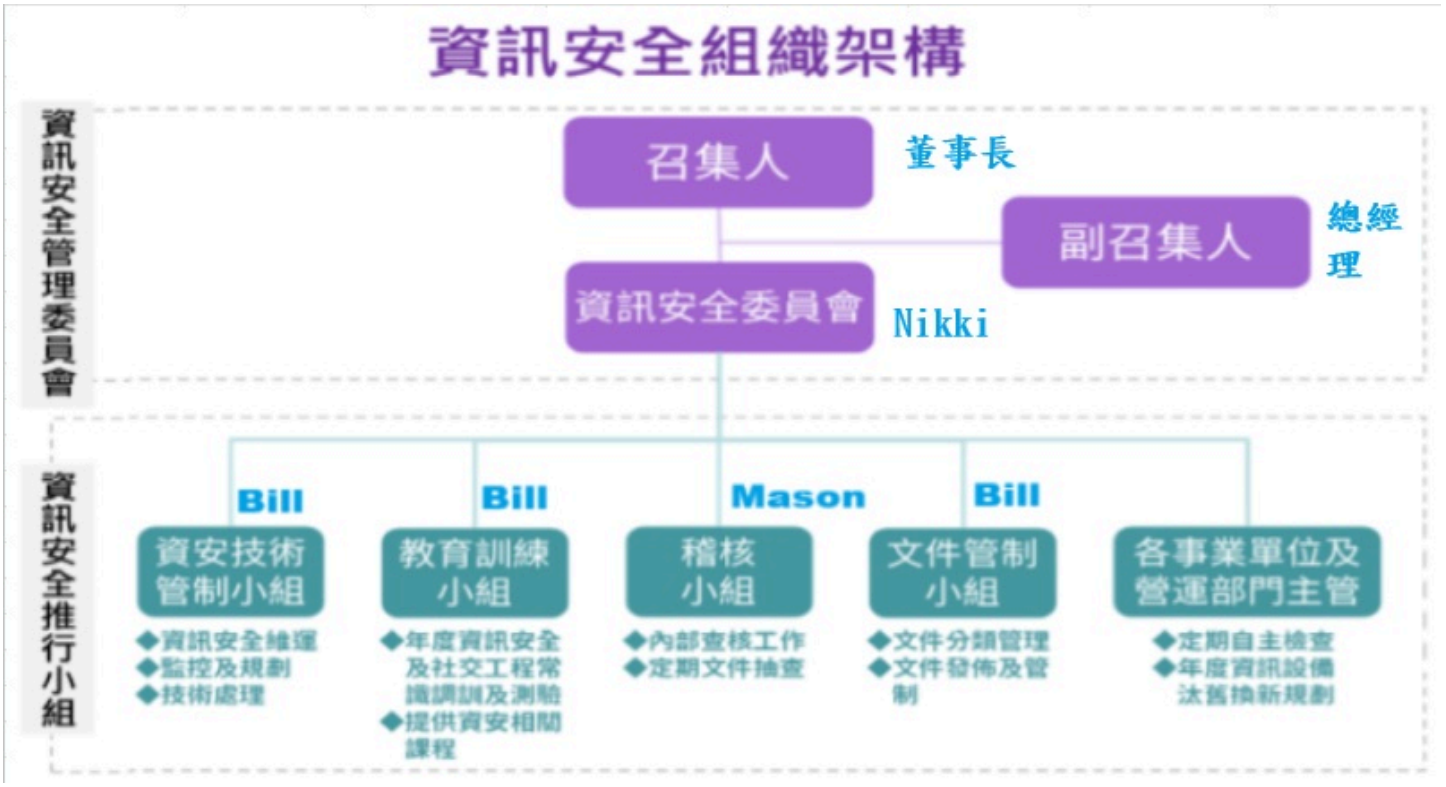
5、作業說明



文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========



5.1 資訊安全政策

5.1.1 為使本公司業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

5.1.2 應因應資通安全威脅情勢變化，本公司同仁應參與資通安全教育訓練，以提高資通安全意識。

5.1.3 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

5.1.4 確保所有人員在僱傭關係終止或合約結束時，將資產歸還公司進

行管理。並修改記錄於ISMS-4-018四階:　資訊資產清冊、ISMS-4-019四階:帳號權限申請表。

5.2 責任

5.2.1　本公司員工及與本公司往來之外部單位、廠商及第三方人員等，皆需遵守本公司資訊安全相關制度及規範，如有違反者，必須自行承擔所有引發的風險及責任。

5.2.2 所有人員於知悉任何危及資訊安全之事件或風險時，皆需依程序進行通報。

5.2.3 因故意或過失之行為，危害本公司資訊安全者，將視情節輕重追究其民事、刑事及行政責任。

5.3 審查

5.3.1 定期:

本政策應每年審查 1 次，以反映法規、技術及業務等最新發展現況。

5.3.2 不定期:

當本公司面臨下列狀況時，應針對資訊安全政策進行檢討與審查。

5.3.2.1 本公司營運策略發生重大變更。

5.3.2.2 資訊安全管理委員會召集人異動。

5.3.2.3 發生重大資訊安全事件。

5.3.2.4 組織應定期監控、審查、評估及管理供應者資訊安全實務作法及服務交付之變更。

5.4 實施

本政策發行、修訂與廢止需經資訊安全管理委員會召集人進行審核後以適

當方式公告實施。本政策應每年定期審查，遇組織、業務、法令或環境等因素之更迭，予以適當修訂，經資通安全推動小組核定後公告施行，以確保資訊安全運作之有效性，修正時亦同。

6、相關文件及表單

6.1、ISMS-2-001 全景與範圍程序書

6.2、ISMS-2-002 資訊安全組織程序書

6.3、ISMS-2-003 文件管理程序書

6.4、ISMS-2-004 人員安全與教育訓練程序書
(人力資源安全管理)

6.5、ISMS-2-005 溝通管理程序書

6.6、ISMS-2-006 風險管理程序書

6.7、ISMS-2-007 資訊資產管理程序書

6.8、ISMS-2-008 存取控制管理程序

6.9、ISMS-2-009　密碼管理程序書

6.10、ISMS-2-010 實體安全管理程序書

6.11、ISMS-2-011 作業管理程序書

6.12、ISMS-2-012 通信管理程序書

6.13、ISMS-2-013 系統開發與維護程序書

6.14、ISMS-2-014　委外管理程序書

6.15、ISMS-2-015　資訊安全事件管理程序書

文件名稱	ISMS-1-001_資通安全政策	文件編號	ISMS-1-001
		版　　次	1
		頁數/總頁數	15

機密等級:■一般 □敏感 □機密　　編號:ISMS-1-001
版本:V1.0

==========

6.16、ISMS-2-016　營運持續運作管理程序書

6.17、ISMS-2-017 資訊安全稽核作業程序書

6.18、ISMS-2-018 矯正管理程序書