資料處理協議

本資料處理協議 (以下稱「協議」) 的簽約雙方分別為 Siemens Product Lifecycle Management Software Inc.，亦稱為 Siemens Industry Software (以下稱「SISW」) 和表示接受本協議條款與條件的客戶 (以下稱「客戶」)。 SISW 保留透過其關聯公司行使其在本協議項下的任何權利並履行其在本協議項下任何義務的權利。 因此，本文所用的「SISW」一詞也可能是指 Siemens Product Lifecycle Management Software Inc. 母公司直接或間接擁有或控制的，以及經 Siemens Product Lifecycle Management Software Inc. 授權可散發 SISW 雲端服務 (以下稱「雲端服務」) 的關聯公司。

客戶應對資料類型的判斷和受資料處理所影響的個人負全責，且應確保此類運用雲端服務方法處理資料的合法性。 客戶也應對任何利用雲端服務所提供之功能，將個人資料更正、刪除或封鎖的行為負責。 客戶可以利用雲端服務所提供之功能匯出和刪除其資料 (包括個人資料)。 在本資料處理協議終止後，客戶可於 30 天內將允許客戶下載客戶資料的書面申請寄給 SISW。 SISW 為回應此類申請而說明的任何期限屆滿後，客戶的其餘資料將隨時刪除，不再供客戶使用。 SISW 和客戶皆同意，在雲端服務的範圍內，客戶可利用雲端服務所提供的功能，行使發佈指示的客戶專有權利。 有關客戶資料的其他指示則需 SISW 和客戶另外簽訂書面協議，包括實行此類指示時客戶將支付任何其他費用的協議。 客戶得立約承諾不會在雲端服務中上傳或儲存任何受保護的健康資訊 (PHI)，除非 SISW 和客戶雙方另外簽訂書面協議，明確允許在雲端服務中儲存 PHI。

在提供雲端服務時，關於生產系統相關事宜，SISW 應遵守本資料處理協議證物 A 附錄 2 中所述之技術與組織上的各項措施。 與雲端服務無關的生產系統可不必遵守證物 A 附錄 2 中所述之各項措施。且 SISW 還可不時變更適用於生產系統的技術與組織措施，前提是此類變更不會對該類措施可達到的保護層級產生任何材料方面的不利影響。 SISW 會限制其人員不得未經授權收集、處理或使用個人資料，並將雇用專門人員處理經特別指示須遵循資料隱私權保護需求的客戶個人資料。

SISW 在雲端服務效能方面有權委託轉包處理者。 在無法排除轉包處理者存取客戶個人資料的範圍內，SISW 將應客戶要求向其提供一份此類轉包處理者及其各自位置的清單，並將在任何新的轉包處理者獲准存取客戶的個人資料前更新此清單。 若客戶有合理原因反對委託任何新的轉包處理者，客戶應告知 SISW 此類異議說明，且如果 SISW 堅持採用新的轉包處理者，則客戶有正當理由終止本資料處理協議。 在委託任何此類轉包處理者時涉及跨國轉移個人資料的範圍內，SISW 須盡力使該轉包處理者保持與此類個人資料相關的足夠資料保護層級。

SISW 須定期確認遵循適用的技術與組織措施，且於客戶提出合理要求時，須向客戶確認是否已遵循各項適用的技術與組織措施。 若客戶有理由相信 SISW 的確認有誤，客戶有權在合理提前通知的情況下，排定對 SISW 進行稽核的時間，從而確認是否遵循技術與組織的各項措施。 實行此類稽核的成本與支出應由客戶負擔。

SISW 和客戶皆同意，歐盟認為不具有足夠個人資料保護層級的任何客戶個人資料傳送 (從歐盟國家至歐盟以外的國家)，將根據歐盟標準合約條款之規定 (在證物 A 中載明且完全合併於本文) 執行。 若本資料處理協議與該標準合約條款衝突，則以該標準合約條款之規定為準。 而該標準合約條款將由建立資料輸出者 (於證物 A 中定義) 之歐盟成員國的法律規定。

證物 A
歐盟標準合約條款

出於 95/46/EC 指令第 26(2) 條將個人資料傳送給創立於第三個國家/地區的、無法確保提供足夠資料保護層級的處理者之目的

雙方分別為

客戶及/或駐歐盟之客戶的關係企業

(以下稱「**資料輸出者**」)

與

Siemens Product Lifecycle Management Software Inc. (亦稱為 Siemens Industry Software)，包括 Siemens Product Lifecycle Management Software Inc. 母公司直接或間接擁有或控制的，並經 Siemens Product Lifecycle Management Software Inc. 授權代表其處理資料的任何關聯公司

(以下稱「**資料輸入者**」)

每個都為「一方」；一同則為「雙方」，

皆同意遵守合約條款 (以下稱「條款」)，以針對附錄 1 中指定之資料輸出者傳送個人資料至資料輸入者的傳送行為，為個人基本權利與自由和隱私權保護等相關層面提供足夠的防護。

第 1 節： 定義

出於本條款之目的：

(a) 「個人資料」、「資料特殊分類」、「處理/處理過程」、「控制者」、「處理者」、「資料主體」和「監督機關」在 1995 年 10 月 24 日歐盟議會與理事會制定關於個人資料處理之個人保護，以及自由移動此類資料的 95/46/EC 指令中，應均具有相同的意思；

(b) 「資料輸出者」表示傳送個人資料的控制者；

(c) 「資料輸入者」表示同意從資料輸出者接收並按照其指示和本條款傳送的個人資料，用以代為處理的處理者，且處理者不受第三國家/地區系統確保依據 95/46/EC 指令第 25(1) 條中之意思提供足夠保護的規範。

(d) 「轉包處理者」表示資料輸入者委託的任何處理者，或資料輸入者其他轉包處理者所委託的處理者，他們同意從資料輸入者或從資料輸入者其他轉包處理者接收並按照其指示、條款規定和書面轉包合約條款傳送的個人資料，專門用以代表資料輸出者處理即將實行的活動；

(e) 「適用的資料保護法」表示保護個人基本權利與自由的法律規定，尤其是其個人資料 (適用於資料輸出者創立時所在成員國的資料控制者) 處理相關的隱私權；

(f) 「技術與組織上的安全措施」表示為保護個人資料免於意外或非法毀損，或意外遺失、更改、未授權揭露或存取的措施，尤其是涉及在網路上傳輸資料的處理，以及免於所有其他形式的非法處理。

第 2 節： 傳送的詳細資料

傳送的詳細資料，尤其是特殊分類的個人資料 (如適用) 會在構成本條款不可或缺之部分的附錄 1 中予以指定。

第 3 節： 第三方受益人條款

1. 資料主體可作為第三方受益人，對資料輸出者強制實施本條款、第 4(b) 至 (i) 款、第 5(a) 至 (e) 款和第 (g) 至 (j) 款、第 6(1) 和 (2) 款、第 7 款、第 8(2) 款，以及第 9 至 12 款。

2. 若資料輸出者確實已消失或在法律上已不復存在，資料主體可對資料輸入者強制實施本條款、第 5(a) 至 (e) 和 (g) 款、第 6 款、第 7 款、第 8(2) 款，以及第 9 至 12 款，除非任何接替實體已經依合約或法律規定承擔資料輸出者的全部法律義務，因而取得了資料輸出者的權利與義務，在此情況下，資料主體可向此類實體強制實施以上責任。

3. 若資料輸出者和資料輸入者確實已消失或在法律上已不復存在或無力償債，資料主體可對轉包處理者強制實施本條款、第 5(a) 至 (e) 和 (g) 款、第 6 款、第 7 款、第 8(2) 款，以及第 9 至 12 款，除非任何接替實體已經依合約或法律規定承擔資料輸出者的全部法律義務，因而取得了資料輸出者的權利與義務，於此情況下，在此情況下，資料主體可向此類實體強制實施以上責任。 根據本條款，轉包處理者的此類第三方責任應限於其自己的處理作業。

4. 如果資料主體表明願意履行且得到國家法律准許時，雙方均不得對代表協會或其他單位的資料主體提出異議。

第 4 節： 資料輸出者的義務

資料輸出者同意並保證：

(a) 個人資料的處理過程 (包括傳送本身) 已經且將會按照適用之資料保護法的相關規定 (且如果適用，已通知資料輸出者創立時所在之成員國的相關機構) 繼續實行，且不違反該國的相關規定；

(b) 已指示，並且將會在整個個人資料處理服務期間指示資料輸入者僅代表資料輸出者並依照適用之資料保護法和條款處理所傳送的個人資料；

(c) 資料輸入者將充分保證本合約附錄 2 中所指定之技術與組織上的安全措施。

(d) 在評估適用的資料保護法律需求後，安全措施均適合保護個人資料免於意外或非法毀損，或意外遺失、更改、未授權披露或存取 (尤其是處理涉及在網路上傳輸資料時)，以及免於所有其他形式的非法處理，且基於最新實作技術與成本的考量，這些措施可確保對處理資料時產生的風險和資料本身帶有的風險提供適當層級的安全保護；

(e) 將確保遵循安全措施；

(f) 如果傳送涉及特殊分類的資料，資料主體已得知，或將事先得知或將於事後盡快得知資料可能傳輸至未提供 95/46/EC 指令意指之足夠保護的第三國家/地區；

(g) 如果資料輸出者決定繼續傳送或解除暫停，則會將第 5(b) 和 8(3) 款相關的資料輸入者或任何轉包處理者接收的任何通知轉寄給資料保護監督機關；

(h) 可依請求讓資料主體使用本條款副本，但附錄 2 和安全措施的摘要說明，以及須遵守本條款之轉包處理服務的任何合約副本不在此限，除非本條款或合約含有商業資訊，此情況下可移除此類商業資訊；

(i) 在進行轉包處理時，轉包處理者須依照第 11 款實行處理活動，並針對資料主體的個人資料與權利，至少須提供如同資料輸入者根據本條款所享有之相同層級的保護；且

(j) 將確保遵循第 4(a) 至 (i) 款。

第 5 節： 資料輸入者的義務

資料輸入者同意並保證：

(a) 僅代表資料輸出者並依照其指示和本條款處理個人資料；若因故無法遵循，則同意立即告知資料輸出者無法遵循，於此情況下，資料輸出者有權暫停傳送資料及/或終止合約；

(b) 無理由相信適用於其自身的法律規定會妨礙其履行從資料輸出者處收到的指示和本合約中規定的義務，且若此法律規定經變更後，可能對本條款提供之保證與義務產生較大的不利影響，應於察覺後盡快立即通知資料輸出者變更的消息，此情況下，資料輸出者有權暫停傳送資料及/或終止合約；

(c) 在處理已傳送的個人資料前，已實施附錄 2 中所指定的技術與組織安全措施；

(d) 將立即通知資料輸出者以下相關事宜：

(i) 執法機關要求披露個人資料的任何具法律約束力之要求，除非遭到禁止，例如依刑法禁止保存執法調查的機密資訊；
(ii) 任何意外或未經授權的存取；以及
(iii) 任何直接從資料主體收到而又未作出回應的要求，除非經授權可以如此；

(e) 立即且適當地處理資料輸出者提出的所有個人資料傳送處理的相關詢問，並遵循監督機關對已傳送資料處理的相關建議；

(f) 依資料輸出者的請求，提交資料處理設施，以便稽核本條款所涵蓋的應由資料輸出者或檢查單位 (由獨立成員組成) 實行的處理活動，並且因規定持有受職務機密之約束、由資料輸出者選擇的專業資格，於適用情況下同意監督機關的建議；

(g) 可依請求讓資料主體使用本條款副本，或任何現有的轉包處理合約，除非本條款或合約含有商業資訊，此情況下則可移除此類商業資訊，但應替換為安全措施摘要說明的附錄 2 不在此限，在這些情況下，資料主體無法從資料輸出者取得副本；

(h) 在進行轉包處理時，已先告知資料輸出者並已提前取得書面同意；

(i) 轉包處理者提供的處理服務將依照第 11 款實行；

(j) 立即將根據本條款訂立之任何轉包處理者協議副本寄給資料輸出者。

第 6 節： 責任

1. 雙方皆同意任何資料主體，若已受有損害以致任何一方或轉包處理者違反第 3 款或第 11 款中的義務，則有權受領資料輸出者因所受損害而給付的賠償。

2. 如果資料主體依第 1 項對資料輸出者的規定 (因資料輸出者確實已消失或在法律上已不復存在或無力償債，以致資料輸入者或其轉包處理者違反在第 3 款或第 11 款中的任何義務) 不能提出賠償要求，則資料輸入者同意資料主體可向資料輸入者 (視為資料輸出者) 提出索賠，除非任何接替實體已經依合約或法律規定承擔了資料輸出者的全部法律義務，此情況下，資料主體可向此類實體強制行使其權利。

   資料輸入者不得仰賴轉包處理者違反其義務來規避自身責任。

3. 如果資料主體依第 1 項和第 2 項規定 (因資料輸出者和資料輸入者確實均已消失或在法律上已不復存在或無力償債，以致轉包處理者違反該雙方在第 3 款或第 11 款中的任何義務) 不能向資料輸出者或資料輸入者提出索賠，則轉包處理者同意資料主體可向資料轉包處理者 (與本條款中其本身處理作業相關；且視為資料輸出者或資料輸入者) 提出索賠，除非任何接替實體已經依合約或法律規定承擔了資料輸出者或資料輸入者的全部法律義務，此情況下，資料主體可向此類實體強制行使其權利。 根據本條款，轉包處理者的責任應限於其自己的處理作業。

第 7 節： 調解與管轄權

1. 資料輸入者同意如果資料主體依本條款訴諸其第三方受益人權利及/或要求損害賠償，資料輸入者將接受資料主體的決定：

   (a) 由獨立之個人或 (如果適用) 由監督機關提出糾紛調解；

   (b) 向資料輸出者創立時所在之成員國內的法院提出糾紛調解。

2. 雙方皆同意，依照國內或國際法的其他規定，資料主體所做的選擇將不會影響其實質或程序上尋求補救之權利。

第 8 節： 與監督機關合作

1. 資料輸出者應同意監督機關寄存本合約副本，若監督機關要求或若適用之資料保護法要求寄存。

2. 雙方皆同意，監督機關有權對資料輸入者和轉包處理者進行稽核，其範圍和依據條件與適用的資料保護法中資料輸出者稽核所適用的相同。

3. 根據第 2 項規定，資料輸入者應立即向資料輸出者告知，存在會妨礙對資料輸入者或任何轉包處理者執行稽核，且適用於資料輸入者或任何轉包處理者的法律規定。 在此類情況下，資料輸出者有權採取第 5(b) 款中預見的措施。

第 9 節： 準據法

本條款應受資料輸出者創立時所在之成員國的法律管轄。

第 10 節： 合約變動

雙方不得變更或修改本條款。 只要不與本條款抵觸，這不會妨礙雙方應要求增補業務相關問題的條款。

第 11 節： 轉包處理

1. 根據本條款，若未提前經過資料輸出者的書面同意，資料輸入者不得代表資料輸出者轉包任何處理作業。 若資料輸入者經過資料輸出者同意，轉包其於本條款中的義務，則須僅透過與轉包處理者簽訂書面協議的方式進行轉包，但會根據本條款對轉包處理者施加與資料輸入者相同的義務。 若轉包處理者無法根據此類書面協議履行其資料保護的義務，資料輸入者應根據此類協議，為轉包處理者的義務表現對資料輸出者負全責。

2. 若資料主體不能依第 6 款第 1 項對資料輸出者或資料輸入者提出賠償要求，因為他們確實已消失或在法律上不復存在或無力償債，且無接替實體依合約或法律規定承擔資料輸出者或資料輸入者的全部法律義務，資料輸入者與轉包處理者提前簽訂的書面合約也應同第 3 款中所訂定之規定提供第三方受益人條款。 根據本條款，轉包處理者的此類第三方責任應限於其自己的處理作業。

3. 依第 1 項轉包處理合約資料保護之相關規定，應受資料輸出者創立時所在之成員國的法律管轄。

4. 資料輸出者應保留根據本條款訂立之轉包處理協議的清單，並隨時接獲第 5(j) 款相關之資料輸入者的通知，應至少每年一次接獲更新消息。 該清單應可供資料輸出者的資料保護監督機關使用。

第 12 節： 個人資料處理服務終止後的義務

1. 雙方皆同意，在資料處理服務之規定終止時，資料輸入者和轉包處理者應按照資料輸出者的選擇，將所有已傳送的個人資料和副本歸還給資料輸出者，或應將個人資料全數銷毀並向資料輸出者證明已銷毀，除非加諸於資料輸入者之法律規定會妨礙其全數或部分歸還或銷毀已傳送的個人資料。 該情況下，資料輸入者保證將保障已傳送之個人資料的機密性，並且不會再主動處理已傳送的個人資料。

2. 資料輸入者和轉包處理者保證，在資料輸出者及/或監督機關提出要求時，將會提交資料處理設施，以便依第 1 項規定稽核各項措施。

標準合約條款附錄 1

資料輸出者
資料輸出者係指 (請指明與資料傳送相關的活動)：

客戶為訂閱 SISW (准許經客戶授權之終端使用者輸入、修改、使用、移除、下載，以及處理客戶資料，其中可能包括本協議與雲端相關文件中所述之個人資料) 所提供之雲端服務的訂閱者。

資料輸入者
資料輸入者係指 (請指明與資料傳送相關的活動)：

Siemens Product Lifecycle Management Software Inc. 本身及/或透過其轉包處理者提供雲端服務，其中包括維護在美國和歐盟運作雲端服務的運算基礎架構；將客戶上傳至雲端服務的客戶資料儲存於基礎架構上；監控雲端服務和基礎架構的可用性與持續進行的作業；以及維護本協議和雲端相關文件規定之基礎架構的安全性。

資料主體
已傳送的個人資料與以下的資料主體分類有關 (請指定)：

除非資料輸出者以書面形式載明，否則資料主體可能包括經客戶授權使用雲端之終端使用者，以及其他將個人資料儲存於雲端服務的客戶人員。

資料分類
已傳送的個人資料與以下的資料分類有關 (請指定)：

儲存於雲端服務的特定資料分類，由客戶透過可能儲存於雲端服務的一些常見資料分類來進行重要組態，這些分類為 (但不限於以下範例)：姓名、電子郵件地址、公司名稱、電話號碼、工作地點、國籍或公民身分，以及存取與使用雲端服務的相關資訊。 視客戶的雲端服務組態，客戶資料中可能存在多種其他資料分類。

特殊分類的資料 (若適當)
已傳送的個人資料與以下的特殊資料分類有關 (請指定)：

任何要儲存於雲端服務的特殊資料分類都會經過協議或訂單雙方同意，或是在向客戶提供的做為雲端服務部署一部分的專業服務工作說明中載明。

處理作業
傳送的個人資料將以下列基本處理活動為準 (請指定)：

個人資料可能由以下方式處理：根據客戶的設定，作為雲端服務正常作業的一部分；在單一租用戶或多租用戶的環境中，儲存及/或封存於資料輸出者所維護的運算基礎架構；根據由客戶授權可使用雲端服務之終端使用者發給雲端服務的指示，以進行存取或傳輸；以及作為資料輸出者執行雲端服務維護作業的一部分。

標準合約條款附錄 2

部分的雲端服務供應項目係根據不同規定提供，若其規定適用，則將於訂單中載明。 否則，資料輸入者將依照本條款中的第 4(d) 款和第 5(c) 款規定，採用以下所述與個人資料儲存於系統相關的技術與組織措施。

依照第 4(d) 款和第 5(c) 款規定，說明技術與組織安全措施由資料輸入者實施：

1. 實體存取控制。 未經授權的人員將禁止實際出入資料處理系統所在的處理及/或使用個人資料之場所、建築物或房間。

   措施： 所有的資料中心均嚴格遵循由安全人員、監視設備、動作偵測器、存取控制機制和其他防止設備與資料中心設施破壞之措施強制執行的安全程序。 只有經授權的代表才可存取資料中心設施中的系統和基礎架構。 為了確保實體安全設備 (例如動作感應器、錄影機等) 功能正常，會定期進行維護。 詳細來說，以下實體安全措施皆會在所有的資料中心實施：

   a. 一般而言，建築物都會透過門禁系統 (智慧卡門禁系統) 進行防護。
   b. 授權憑證 (包括員工、廠商或承包商專用的電子門禁徽章) 和 PIN 皆會提供給經授權的人員，以便實際進出資料中心設施。
   c. 由讀卡機和 PIN 輸入裝置組成 (PIN 輸入裝置用於進入建築物和房間，讀卡機則僅用於從建築物和房間出去) 的電子門禁系統，可強制執行在系統邊界內實際出入資料中心。
   d. 視安全分類，建築物、個人區域和周圍的場所都會受到其他措施的進一步保護。 這些包括特定的存取設定檔、視訊監視、入侵警報系統和生物辨識門禁系統。
   e. 根據以下規定的系統與資料存取控制措施，存取權將以個人為單位授與給經授權的人員。 這也適用於訪客存取。 SISW 的來賓和訪客必須在接待處登記其姓名且必須由經授權的 SISW 人員陪同。 SISW 和所有的第三方資料中心供應商將會記錄在資料中心內進入 SISW 私人區域的人員姓名和次數。
   f. SISW 員工和外部人員必須在 SISW 的所有地點都佩戴 ID 卡。

2. 系統存取控制。 用於提供雲端服務的資料處理系統必須防止未經授權的使用。

   措施：

   a. SISW 或其轉包處理者會進行環境管理，以遵守 NIST SP 800-53 修訂版 4 存取控制 (AC) 和身分驗證 (IA) 的需求。
   b. 有多種授權層級可用來授與敏感系統存取權，包括那些正在儲存和處理中的個人資料。 程序處理到位可確保只有經授權之使用者擁有適當的授權以增加、刪除或修改使用者。
   c. 所有使用者須使用必須符合特定最低複雜性條件的專用使用者名稱和密碼來存取 SISW 的系統。
   d. SISW 和其轉包處理者將程序處理到位，可確保已申請之授權變更僅依照規範 (例如未經授權則不可授與任何權利) 執行。 如果 SISW 使用者的職位已變更或離職，程序會執行撤銷進入環境的存取權。
   e. SISW 和轉包處理者已建立了密碼原則，禁止共享密碼、規範公開洩露後的因應事項、要求定期變更所有使用者的密碼，以及要求變更預設密碼。 指派個人化使用者 ID 進行驗證。 所有密碼都必須符合最低的複雜性需求並以加密的形式儲存。 若是網域密碼，系統會強制每 60 天變更密碼，以符合最低的複雜性需求。 每台 SISW 電腦皆有受密碼保護的螢幕保護程式。
   f. SISW 或其轉包處理者會自動稽核以下帳號事件：建立、修改、啟用、停用和移除。 系統管理員會定期檢閱這些記錄。
   g. 防火牆會保護 SISW 和其轉包處理者的網路免於公用網際網路侵害。
   h. SISW 和其轉包處理者會在公司網路的存取點和所有的檔案伺服器與工作站，針對電子郵件帳號使用最新的防毒軟體。
   i. SISW 和其轉包處理者執行安全性修補程式管理，以確保部署相關的安全性更新。
   j. SISW 公司網路和重要基礎架構的完整遠端存取是由強式的多重要素驗證保護。

3. 資料存取控制。 有權使用資料處理系統的人員將僅能存取他們有權存取的個人資料，且在處理、使用和儲存的過程中，若未經授權則不得讀取、複製、修改或移除個人資料。

措施：

a. 個人、機密或敏感資訊的存取，須秉承相關原則。 換言之，員工或外部第三方可存取其完成工作所需的資訊。 SISW 使用授權概念記錄如何指派授權，以及該指派那些授權。 所有個人、機密或敏感資料均依照 SISW 的安全原則和標準而受到保護。
b. 任何 SISW 雲端服務的所有生產伺服器都在相關的資料中心運作。 保護應用程式處理個人、機密或其他敏感資訊的安全措施都會接受定期檢查。 為此目的，SISW 也納入外部的定期稽核，以確認這些措施皆以適當的方式套用。
c. SISW 不會允許將未經 SISW 核准的個人軟體或其他軟體安裝至任何雲端服務所使用的系統。
d. 若因下方的資料儲存媒體故障而需要傳送資料時，完成此類傳送後，故障的儲存媒體將遭消磁 (針對磁性儲存裝置) 或絞碎 (針對固態或光學儲存裝置)。

4. 資料傳輸控制。 不得讀取、複製、修改或移除傳送期間未經授權的個人資料。

措施：

a. SISW 或其轉包處理者會進行基礎架構和設定管理，以遵守 NIST SP 800-53 修訂版 4 系統與通訊保護 (SC) 的需求。 這也包括在系統邊界上的網路入侵預防系統 (NIPS) 和防火牆，以免基礎架構在外部邊界上遭受惡意通訊的侵害。 NIPS 和防火牆是依據美國國防資訊系統局《安全技術實作指南》(Defense Information Systems Agency Security Technical Implementation Guide, DISA STIG) 的標準來設定。 資料在傳輸時會使用符合聯邦資訊處理標準 140-2 (Federal Information Processing Standards 140-2, FIPS 140-2) 的密碼編譯模組加密。
b. 在資料載體實際傳輸的位置上，適當的措施會在 SISW 實施，以確保遵守議定的服務層級 (例如加密和襯鉛容器)。
c. 根據 SISW 的安全原則，個人資料在 SISW 內部網路上的傳輸過程，將以等同任何其他機密資料的方式受到保護。
d. 資料在 SISW 和客戶之間傳送時，針對已傳送個人資料的保護措施會在本協議或雲端服務的相關文件中載明。 這適用於實體與網路型的資料傳送。 客戶須承擔從 SISW 的劃分點 (例如託管雲端服務之資料中心的連出防火牆) 傳送任何資料的責任。

5. 資料輸入控制。 雲端服務將准許追溯決定，不論是否及由誰輸入、修改或從用於提供雲端服務的基礎架構中移除個人資料。

措施：

a. SISW 僅允許經授權的人員存取其工作過程中所需的個人資料。 SISW 已執行用於輸入、修改和刪除，或由 SISW 或其轉包處理者封鎖個人資料的記錄系統，以充分發揮雲端服務所支援的限度。
b. 發生或懷疑未授權的事件或故障時，稽核記錄可提供協助重建事件所需的充分詳細資料。 每個作業系統的事件記錄檔包括事件類型、時間戳記、事件來源、事件位置、事件結果，以及與事件相關的使用者。

6. 工作控制。 根據本協議規定和客戶所提供的任何相關指示，個人資料將單獨處理。

措施：

a. SISW 會透過控制項和各項程序，確保遵循 SISW 與其客戶、轉包處理者或其他服務供應商之間的合約。
b. 根據 SISW 資訊分類的標準，客戶資料將受到至少等同於機密資訊的保護層級所規範。
c. 所有 SISW 的員工與具有契約關係之合作夥伴均受到合約的約束，以尊重所有包括 SISW 客戶與合作夥伴之交易秘密等敏感資訊的機密性。

7. 可用性控制。 個人資料將受到保護，免遭意外或未授權毀損或遺失。

措施：

a. SISW 會運用備份程序和其他措施，於需要時可確保迅速還原業務重要系統。
b. SISW 仰賴全球的雲端服務供應商，以確保資料中心的電源可用性。
c. SISW 已定義應變計劃，以及雲端服務適用的業務與災難復原策略。

8. 資料分離控制。 因不同目的而收集的個人資料可分開處理。

   措施：

   a. 在可適用的情況下，SISW 會使用已部署軟體的技術功能 (例如多租用或分離的系統環境)，以達到客戶與任何其他客戶之個人資料的資料分離。
   b. SISW 會利用邏輯或實體分離，維護每位客戶的專屬執行個體。
   c. 客戶 (包括其關係企業) 僅可存取自己客戶的執行個體。

9. 資料完整性控制。 可確保個人資料在處理活動中，將能保持完整無缺並處於最新狀態。

   措施： SISW 已實施多層防禦策略，以免遭未授權的修改。 這指的是上述控制與措施區段中說明的控制項。 防火牆組態會帶來多個可分隔公用與私人存取的網路區段。 每個防火牆規則集都包含特定的存取控制項，用以指定這些區段間允許的通訊方式。

   a. 安全監控中心： 自動化入侵偵測軟體將用於結合其他的安全預防與鑑識軟體和程序，以提出警訊、調查，並在必要時通知和協助修復任何安全事件。
   b. 防毒軟體：所有系統將具有最新的防毒定義，以設定用來防禦病毒、蠕蟲、特洛伊木馬病毒，以及其他形式的惡意程式。
   c. 備份與復原：所有系統將具有基本層級的資料與組態備份快照。 若適用，SISW 和其轉包處理者也將會藉由高可用性的組態來執行客戶的執行個體，以確保將資料儲存於距離相隔夠遠的兩個資料中心。
   d. 定期進行外部稽核以檢驗各項安全措施。 SISW 和其轉包處理者將會定期進行外部稽核，以測試上文列出的安全措施。