# 我國大專以上院校及高等學術研究機構防止敏感或管制技術移轉指引手冊

主辦單位：經濟部國際貿易局

受委託單位：國立陽明交通大學企業法律中心

中華民國 110 年 6 月

# 免責聲明

本指引手冊係本局委外研究之成果，旨在提供我國學術與研究機構管理建議及幫助，降低法律風險。各單位仍應檢視各相關之法令規定，確認行為符合法令規範，不得援引本指引手冊內容作為違法抗辯事由。

經濟部國際貿易局　啟

# 目錄

# 壹、本指引之目的和用途

敏感技術為國家重要資產，無論軍商兩用技術，或任何發展中的新興技術，皆屬於敏感技術的範疇。若未妥適管制敏感技術的出口，則可能足以動搖國家安全之根本。因此，在數位化的浪潮之下，如何有效控管敏感技術出口成為國家安全考量的重要議題。

學術與研究機構為國家敏感技術發展之核心，是以，一旦學術與研究機構欠缺對於敏感技術的保護意識，其研究量可能因此受到重大衝擊，進而導致機構的財務、聲譽受損，亦可能使機構喪失未來的資助機會。

為協助學術與研究機構能自我提升敏感技術之管控意識，爰參照美國、英國、日本及紐西蘭之因應方式，制定本指引手冊，盼能協助學術與研究機構了解敏感技術之範圍，及其種類、態樣，又若未保護學術及研究機構之敏感技術則可能面臨何種風險。最後，本指引亦整理了英國敏感技術移轉之案例，並輔以美國之作法，再進一步給予建議與提出具體之應對計畫，盼能於敏感或管制技術保護之議題上為我國學術與研究機構提供建議及幫助。

# 貳、名詞解釋[1]

本章節主要分為敏感技術之範圍、技術移轉之範圍，及應受到高度管制情形三部分，從而以敏感技術之範圍切入，並列出風險較大，需要給予特別注意的情形，提出相關建議，供我國學術與研究機構參考。

## 一、敏感技術之範圍

### 1. 敏感技術之一般認定原則

為善盡國際責任，維護國際安全，我國貿易法第 13 條規定，加強管理戰略性高科技貨品之輸出入及流向。若違法將戰略性高科技貨品出口，將面臨貿易法第 27 條、27 條之 1、27 條之 2 的有期徒刑及罰鍰。為因應戰略性高科技貨品輸出入管理之需要，戰略性高科技貨品輸出入管理辦法定有詳細的進出口管制規定；我國經濟部國際貿易局（下稱貿易局）對於涉及軍事用途的高科技貨品出口，亦訂有管制清單。其主要目的係防止將可能被使用於武器或軍事用途的貨物轉讓給特定國家或恐怖分子，滋長恐怖主義活動或區域戰爭。

同理，為維護國際社會之和平及我國國家安全，我國國家安全法，及國家機密保護法亦規定，將國家機密、敏感技術移轉予恐怖分子或敵對勢力者，將處以刑事處罰。 因此，可能用於武器之技術也應該受到學術與研究機構的關注。本指引所稱之敏感技術，係指可用於設計、製造、使用或研發常規武器或大規模毀滅性武器之技術。與這些技術領域相關的研究人員需要認識到，這些研究成果與國際社會的安全密切相關。以下僅列出常見的敏感技術：

A. 核子技術

B. 精密機器/加工/測量技術，

C. 自動化和機器人技術

D. 化學和生物化學（特別是對人體有害的化學品或解毒劑）

E. 生物學，包括生物技術和醫學（特別是傳染病和疫苗）

---

[1] 此章節參考自 Ministry of Economy, Trade and Industry Trade Control Department (METI), *Guidance for the Control of Sensitive Technologies for Security Export for Academic and Research Institutions,* 3rd Edition (2017).

F. 高性能/功能材料技術（耐熱、耐腐蝕材料等）

G. 航空技術和高性能發動機技術

H. 導航技術

I. 海洋技術

J. 通訊、電子和光學技術

K. 用於設計、製造和使用受管制貨物的電腦程式開發技術

L. 模擬程式設計技術

學術與研究機構於移轉敏感技術前，除檢視該技術是否符合上述所列之技術領域外，也可透過檢視下列問題來輔助判斷，若問題中任一答案為是，則該技術即屬於敏感技術，而應受到管制：

A. 根據所獲得的資訊和網站上的公開資訊，欲移轉的技術是否有被用於開發、製造、使用或儲存大規模毀滅性武器（Ex：核武器、化學武器、生化武器、火箭、無人駕駛飛行器）或常規武器的疑慮？抑或是可能用於開發上述武器的先進技術材料、部件、產品？還是可能用於研究核聚變、開發核燃料材料或核反應爐等？

B. 根據所獲得的資訊和網站上的公開資訊，移轉的技術是否有被外國軍隊或員警使用的疑慮？例如用於開發化學物質、微生物、毒素或空間研究等？

## 2. 敏感技術認定之例外

然而，雖技術可用於設計、製造、使用或研發武器，但若符合下列情況者，例外不屬於敏感技術，於移轉至國外時，可豁免管制：

A. 移轉公眾所已知的敏感技術

若欲移轉之敏感技術已透過報紙、書籍、學術期刊、專利公報或電子檔向公眾公開發表過，蓋此係公眾所已知的公開技術，並無限制之實益。

惟為了防止以移轉此類技術為由，藉此與高風險或不受信賴的移轉對象進行可疑的技術移轉，學術與研究機構在參與相關的交流前，仍應進行內部審查。

B. 基礎科學領域之技術移轉

所稱基礎科學領域中的技術移轉交易，主要是指能幫助驗證科學理論或進行科學實驗，而不以開發或生產產品為目的進行之研究活動。基於促進科學知識傳播之目的，此類技術之移轉可豁免管制。

C. 出口貨物伴隨的最低限度技術

貨物出口時，賣方可能需要一併提供一些最低限度之技術知識，否則買方可能無法使用、安裝或維修該貨物。在這種情形下，若限制此類技術的移轉，買方將無法達成交易目的，因此這類技術之移轉得以豁免管制（惟操作軟體仍可能需進行管制）。惟必須注意的是，所出口的貨物必須為未違反我國貿易法，並在貿易局對於涉及軍事用途的高科技貨品出口管理制度下，依法取得許可證者。

D. 設計或製造民用電腦或相關產品的技術

須為專為設計或製造民用電腦或相關產品的技術，若為軍民兩用之電腦或相關產品之技術，仍須受到管制。

# 二、技術移轉之範圍

敏感技術之移轉，係透過將與敏感技術相關之特定技術資料，移轉給外國政府、機構、法人或自然人之方式完成。以透過對技術資料、技術援助及自然人分類之說明，幫助學術與研究機構釐清技術移轉可能發生之方式與特殊情形。

## 1. 技術資料

技術資料係指任何能夠清楚說明該技術運作原理、操作方式或實驗數值的文字或圖表。以下列出常見的技術資料種類：

A. 技術報告

B. 研究紀錄

C. 設計圖紙、原理圖

D. 製造配方

E. 測試紀錄

F. 圖表、模型、公式

G. 實驗數據

H. 實驗、製作設備的規格

I. 手冊、說明書

J. 程式代碼

技術資料的紀錄、儲存方式可能為紙質文件；亦可能為數位檔案，儲存於磁片、磁帶、光碟、電腦硬碟、手機的唯獨記憶體（Read-Only Memory，ROM）、隨身碟等媒介，抑或是存於雲端資料庫中。因此，技術之移轉有可能透過移轉儲存媒介完成，例如將儲存有敏感技術的隨身碟轉交予外國人，如此即係涉及實體物品交換之移轉方式。然而近年來，由於網際網路的發達，資料的傳輸方式更加多元化，技術資料之移轉也能以不依靠實體物品交換的方式完成，例如電子郵件、傳真或共用雲端資料庫，都能夠將技術移轉出去，不僅使移轉方式更加快速、方便，也大幅增加管制的難度。

## 2. 技術援助

除了直接將技術移轉予他人，敏感技術也可能透過技術援助方式流向外國。技術援助係旨透過知識、技能的培訓或諮詢等方式，將敏感技術直接或間接傳授予外國實體。常見的技術援助包含技術指導、技能培訓、知識傳授或諮詢服務等形式。

A. 技術指導

技術指導係指由學術或研究機構派遣人員，透過線上或實體的方式，指導外國實體了解該技術之原理、操作方式或配方製備等，使該外國實體有能力進行設計、製造、使用或研發活動。這種方式偏重於與敏感技術內容的傳授。

B. 技能培訓

不同於技術指導較為注重技術本身，技能培訓聚焦在培訓技術人才。學術或研究機構派遣人員，透過線上或實體的方式，訓練外國技術人員，使其具備將敏感技術付諸實行的能力。許多敏感技術都需要以精密儀器輔助，例如生物技術在分析檢體時，需要使用精密的檢測儀器。這種情況下，一批能夠有效地操作使用和維修保養精密儀器的技術人員為研究敏感技術之要件。因此，替外國機構從事技能培訓工作，也是常見的技術援助。

C. 知識傳授

知識傳授是指學術或研究機構的學者或研究人員，透過線上或實體的方式，舉辦講座或開設課程，將與敏感技術相關之知識傳授給外國學生。不論這樣的課堂或講座是在外國或本國學術或研究機構開設開設，抑或是聯合開設，都有可能讓特定國家或機構，透過派遣學生上課的方式，獲得敏感技術相關的知識。

# 三、應受到高度管制之情形

## 1. 不受信賴的機構

敏感技術可能用於開發大規模殺傷性武器或其他武器之技術，若提供給特定實體，可能被其用於開發武器，威脅國際社會安全，因此為善盡國際責任，學術與研究機構應避免敏感技術流向這些組織。我國貿易局公告之「我國戰略性高科技貨品出口實體管理名單」列出之特定國家或組織，即為有高度風險且可能將敏感技術用於開發武器之名單，而不應被信賴。

依照貿易法與戰略性高科技貨品輸出入管理辦法，在出口貨物時，需要審查交易對象是否為「我國戰略性高科技貨品出口實體管理名單[2]」。若是，則應於出口前取得戰略性高科技貨品輸出許可證。若未經許可而出口，將違反貿易法。因此，若移轉敏感技術之對象，係「我國戰略性高科技貨品出口實體管理名單」上之不受信賴的移轉對象，學術與研究機構亦事先申請許可。

若學術或研究機構欲移轉敏感技術，應針對下列問題一一檢視，當任一答案為「是」，則該移轉技術之對象為不受信賴的對象：

D. 移轉敏感技術之對象是否被列入「我國戰略性高科技貨品出口實體管理名單」？

[2] 貿易局經貿資訊網，https://www.trade.gov.tw（最後造訪日：2021 年 5 月 30 日）。

E. 移轉之技術是否會流向較有疑慮的國家（如伊朗、伊拉克或北韓）？抑或是聯合國安理會實施武器禁運的國家、地區[3]（如阿富汗、中非共和國、剛果、伊拉克、黎巴嫩、北韓、索馬里亞、利比亞、南蘇丹或蘇丹）？

F. 根據獲得的資訊和貿易局網站上之公開資訊，移轉對象是否已經被懷疑，將敏感技術用於開發、製造、使用或儲存大規模毀滅性武器或常規武器？抑或是可能用於開發上述武器的先進技術材料、零件、產品？

## 2. 留學生及外國研究員

學術與研究機構經常接受留學生來台學習，或聘請外國人擔任研究員、講師、教授等。在接受留學生或聘任外國工作人員時，應審查其所隸屬的機構或組織，是否在「我國戰略性高科技貨品出口實體管理名單」中或存有疑慮。除此之外，下列問題亦可輔助學術與研究機構判斷接受該人員的風險：

A. 該人員之國籍是否為有疑慮的國家（如伊朗、伊拉克或北韓）？抑或是聯合國安理會實施武器禁運的國家（如阿富汗、中非共和國、剛果、伊拉克、黎巴嫩、利比亞、北韓、索馬里、南蘇丹或蘇丹）？

B. 根據獲得的資訊和網站上的公開資訊，該人員的原所隸屬的機構或組織（包括國際留學生的大學、學院、研究室）是否被懷疑參與開發大規模殺傷性武器（核武器、化學武器、生化武器、火箭、無人駕駛飛行器）或常規武器，以及用於這些武器的先進技術材料、零件、產品？

C. 若其為國際學生，是否曾經、正在或即將接受由原國籍政府、機構或組織（包括私人機構）支付其學習費用？

D. 若其為國際學生，從過往與該學生的交流中，其是否即將或有意願在與軍事有關的部門或軍火公司工作？

E. 該人員過去的研究的目的是否被懷疑是為了開發大規模殺傷性武器或常規武器？

另一值得特別留意的狀況是，該人員是否由外國政府或組織資助，因接受資助者有可能承擔著該政府或組織賦予之責任或使命，而於將來返回本國時，一同將敏感技術移轉至本國。再者，外國留學生或研究人員亦有可能於進入我國學術或研究機構後，其原本所屬的機構或組織才被列入「我國戰略性高科技貨品出口實體管理名單」，因此學術與研究機構應定期重新審查所接受或雇用的外國人員的身分。

[3] 聯合國安理會官網，https://www.un.org/securitycouncil（最後造訪日：2021年5月30日）。

### 3. 聯合研究案專案及跨國學術交流

近年來在國際化浪潮下，我國學術與研究機構與外國的學術或研究機構進行聯合研究專案，及舉辦跨國學術交流活動之情形屢見不鮮。然於活動籌備與進行時，若將接受來自海外人員的訪問，且可能通過設施參觀，或在實驗、交流中解釋敏感技術，亦應審慎對待，以防敏感技術外流。再者，舉行此類活動前，學術與研究機構亦應檢視：

A. 敏感技術是否不包括在要移轉、交流的技術中？活動涉及的技術，是否可能被用於開發大規模殺傷性武器或常規武器？

B. 參與的學術機構是否為不受信賴的機構？

## 小結

本指引之目的係鼓勵學術與研究機構建立有效的制度，以加強對敏感技術之資訊控制。任何移轉可能用於設計、製造、使用或研發武器之技術都應受到學術與研究機構的重視，並在進行相關領域聯合研究開發時審慎應對。除此之外，凡涉及與相關領域之國際人員交流或涉及外籍人士、非長住本國國民之活動，也應受到學術與研究機構的密切關注，並建議參照本指引之建議，利用附錄一之預先審查清單進行預先審查及監督。

# 參、敏感技術不當移轉之風險[4]

本章節旨在使學術與研究機構了解一旦研究成果遭不當移轉，研究主體可能面臨之風險來源、成為目標之原因以及風險之態樣。無論是敏感性研究資料，或是研究者及研究贊助者持有之商業性的機密資訊，皆對學術與研究機構和其合作夥伴至關重要，故應保護研究成果不為外國份子（foreign state actor）濫用或利用。蓋源自於外國份子的惡意行動不僅將破壞我國的國際研究合作體系，亦將損及我國的研究成果，甚至是減緩全球科學的進步。

## 一、 誰可能造成威脅

外國份子竊取敏感性研究之目的：藉由竊取敏感性研究，尋求機會發展研究和創新之基礎，以強化自身的經濟、軍事及科技能力；以政權的穩定為優先，並致力於壓制內部異議份子、政治反對派或媒體自由度；透過科技及社會控制優勢來對付自己的人民，以維持政權的穩定。

## 二、 如何成為鎖定目標

國際合作為外國份子提供了自研究過程中獲益的機會，例如獲取研究人員資料、IT 網路等相關敏感研究之應用或成果，而無須再仰賴傳統的間諜活動或網路攻擊行動。

又傳統的學術活動亦為外國情報機構提供了一條便捷的途徑，使其能夠在國際會議、研究實習等活動中獲得與研究者接觸的機會。此外，研究者也可能因遭受網路攻擊而成為目標。以網路釣魚郵件為例，它可能試圖誘使使用者透露敏感性資訊、點擊惡意網站連結或受感染的附件。這些皆為研究者所應注意的風險。

## 三、研究成果可能面臨的風險

[4] 此章節參考自 New Zealand Government, *Trusted Research Guidance for Institutions and Researchers*, Dec. 1, 2020.

競爭與剽竊是學術與研究機構時常面臨的隱憂。此時，無論外國份子是否透過合法手段獲取研究成果，研究者和其研究成果仍可能受到以下四種不利的影響：

## 1. 減損信任關係

研究與研發機構的長期發展，需要獲得公私部門對其研究的信任。又該信任關係實為研究資料和資金來源的基石。此時，為維持此種信任關係，研究者需證明他們有能力保護相關研究資料免於被竊取。若研究成果因缺乏適當的保護而遭濫用，研究者與公私部門間的信任關係便可能產生動搖。未來，研究者可能無法再使用相關資料來進行研究。

## 2. 破壞學術誠信與合法性

學術倫理及學術誠信誠為研究成果值得社會信賴的基石，此時若研究成果遭不當移轉，則研究者可能因違反學術倫理及學術誠信而遭到懲處。除此之外，研究者必須遵守相關法律規定，以避免遭受相應的懲處。例如，我國為防範外國或中國大陸竊取科技相關產業技術及人才挖角，訂有若干法規[5]。按《國家安全法》第 2 條之 1 之規定，人民不得為外國或大陸地區、港澳、境外敵對勢力及其派遣之人為刺探、蒐集、交付或傳遞公務上應秘密之之文書、圖畫、影像、消息、物品或電磁紀錄，違反者將依同法第 5 條之 1 處以刑罰。又《國家機密保護法》第 32 條亦規定，若洩漏或交付依本法核定之國家機密，則最高可能被處以 10 年有期徒刑。又為發展對外貿易，健全貿易秩序，以增進國家之經濟利益，我國《貿易法》規範國家出口管制措施，並涵蓋了戰略性高科技貨品的出口管制。又《貿易法》第 27 條、第 27 條之 1、第 27 條之 2 及第 28 條訂有罰則，若研究者不遵守相關規範，將面臨刑事或行政處罰的風險。

## 3. 喪失資助機會和面臨財務損失

若研究機構曾被外國份子竊取敏感性文件，則其未來很難再吸引到其他資助者。當資料遭到竊取後，外國政府不一定會按照我國的法規來保護資料隱私，或者試圖將研究濫用於和倫理規範相悖之目的。此時，研究機構將面臨潛在的經濟損失。

---

[5] 趙晞華，「我國敏感科技技術外流之防制及處罰機制」，軍法專論，67:1 期，頁 19-27（2021）。

### 4. 損及聲譽

研究者及研究機構的聲譽在成功的研究上扮演了重要的角色。若他國明顯地將研究成果用於軍事或獨裁主義相關的目的，研究者及其機構的聲譽必定會受影響。不僅如此，國家的聲譽也可能一併蒙受損害。

## 小結

本指引之目的係為了避免學術與研究機構忽視敏感技術移轉的風險，而導致其研究量能受到損害，亦影響機構的長遠發展。故學術與研究機構應更加重視風險實現可能造成的後果，進而提升對敏感技術的保護意識，以免損及其利益，動搖國家安全之根本。

# 肆、案例研析[6]

本章節係以敏感技術移轉之案例為借鏡，進一步提出相關建議，以供我國學術與研究機構參考。案例主要分兩部分，其一係涉及學術機構之案例，其二則係涉及研究人員之案例。

## 一、涉及學術機構之案例

### 1. 案例介紹

| 案例 01　英國大學涉嫌間接支援伊朗導彈計畫 |
| --- |
| 英國《金融時報》於 2015 年報導了 A 理工學院和 B 大學與 C 航空製造工程研究所(隸屬於 D 國航空工業集團)簽署了研究協議，C 航空製造商是 D 國國有獨資企業，曾於 2014 年因向伊朗的彈道導彈計畫提供資源而被美國商務部產業與安全局列入出口管制名單。<br><br>A 理工學院和 B 大學帝國雖然都表示他們對 C 研究所的研究參與係符合該國出口管制組織的標準，且其等之研究計畫是落入基本研究的範圍，並符合基本科學研究的管制。然而，根據該研究的資訊，許多項目雖然符合基本研究豁免的標準，但是同時也可能有機會使用於進階飛機的應用技術。因此，這些研究勢必會引起軍用及民用飛機研發人員的關注。 |

本案說明了與外國國有企業簽訂研究協議所涉及的複雜性及困難度。進一步言之，在與外國企業達成研究協議之前，應先檢查管制實體清單。在簽署協議後亦不得鬆懈，仍須保持定期的審查制度，使大學和研究機構自身能夠確實了解合作的風險。此外，從本案中該 D 國公司與伊朗的關聯性，亦進一步證實了學術機構可能間接將知識移轉到受管制國家的風險。

[6] 此章節參考自 Emma Scott, Ross Peel, Felix Ruechardt & Nick Mitchell, *Catalogue of Case Studies on Intangible Technology Transfers from Universities and Research Institutes: Revised edition*, King's College London (2020).

| 案例 02　CSSTEAP 遭聯合國專家小組調查 |
| --- |
| 1995 年，亞太地區太空科學和技術教育中心（The Centre for Space Science and Technology Education in Asia Pacific，CSSTEAP）（下稱 CSSTEAP）根據亞太地區 10 個國家的協議成立，其為亞太地區提供有關太空科學和技術教育、培訓和研究課程。根據 CSSTEAP 網站的資訊，該中心提供了六門與太空科學技術相關領域的課程，目的是為增強各成員國在該領域的能力。<br><br>由於北韓和伊朗都是 CSSTEAP 理事會的成員，且兩國都有積極的太空計畫，專家們擔憂這些研究課程可能被用於軍事目的，故聯合國專家小組提請注意該中心的教育活動所引起的核武擴散風險，同時並發現在 1996 年至 2016 年期間錄取 CSSTEAP 課程的 30 名北韓學生與聯合國專家小組提出制裁的項目有關。在專家小組提供報告後，CSSTEAP 取消了四名北韓學生參加的課程，其中包括隸屬於朝鮮國家宇宙開發局（National Aerospace Development Administration，NADA）的學生。 |

本案說明了敏感技術對於核武擴散計畫有重大的風險。在聯合國專家小組對該 CSSTEAP 進行審查前，CSSTEAP 並未採取任何行動阻止北韓學生加入敏感計畫，其中最根本的原因在於 CSSTEAP 對敏感技術將如何促進擴散計畫缺乏了解，因此並未在入學前對參與者進行實體名單查核。

此外，從本案可知，一方面北韓打著使用和平技術計畫的名號，例如尋求進入國際組織的太空計畫，實際上則係積極地為其非法核武器和彈道導彈計畫獲取技術。另一方面，北韓及伊朗亦藉由派遣學生至 CSSTEAP 修課之機會，將敏感技術的知識間接移轉回自己的國家。

| 案例 03　歐洲大學禁止北韓學生修習進階物理課程 |
| --- |
| 根據聯合國安理會決議，禁止北韓人民參與有助於北韓計畫的「專業教學或培訓」。例如：高級物理學、地理空間導航、航空工程及機械工程等。聯合國朝鮮問題專家小組調查發現有兩個北韓學生於意大利的里雅斯特國際理論物理中心（Abdus Salam International Centre for Theoretical Physics，ICTP）和國際高級研究學院（Scuola Internazionale Superiore di Studi Avanzati，SISSA）學習。得知這項消息後，這些大學將這兩個北韓的學生轉到其他學科學習。 |

本案說明了學術與研究機構在與外國大學合作以及招收與擴散相關國家的學生時面臨的困境：除了需要區分基本研究與應用研究外，尚須確保該研究不受出口管制的限制，以及該子學科是否落入相關制裁的學科。由於制裁決議中提及的學科相對較廣，例如高級物理學，因此，即使高級物理學的某些子學科可能與核武擴散無關，學術與研究機構也可能因為招收來自受管制地區的學生而違反該決議。

| 案例 04　美國大學向巴基斯坦國家太空機構出口受管制的技術 |
| --- |
| 本案涉及馬薩諸塞州洛厄爾大學(University of Massachusetts Lowell，UML)向巴基斯坦受制裁實體，即巴基斯坦國家航天局空間科學委員會出口管制技術。這些技術包含用於大氣控制設備的天線和電纜、大氣測試設備。美國商務部工業和安全局認為馬薩諸塞州洛厄爾大學違反了《出口管理條例》(Export Administration Regulations)第 764.2 (a)條。2013 年 3 月，馬薩諸塞州洛厄爾大學與美國商務部工業和安全局達成和解協議，遭處 10 萬美元的民事罰款，緩刑兩年。 |

本案強調了大學在何種情況下可能受到出口管制法規的約束。其中，半自治研究機構或非核心大學課程同樣可能違反出口管制法規。相較於產業，學術界的權力下放結構意味著學者們可能在沒有出口管制風險意識情況下進行教學工作。

| 案例 05　美國喬治亞理工學院機密課程外流 |
| --- |
| 喬治亞理工學院 (Georgia Institute of Technology，Georgia Tech)是美國一所著名的工程學校，其為美國聯邦僱員和國防技術和其他領域的承包商提供 69 項培訓課程，其中有 8 項被列為機密，15 項受到美國國務院的規範。只有美國公民、政府僱員或具有適當安全許可的人員才能參與這些課程，且學生於教室中不得使用任何電子設備。<br><br>為了培訓新任的講師，即將退休的講師錄製了課程影片，並將錄影和投影片提供給該學院的影片製作團隊，要求他們製作成 DVD。由於影片製作團隊在製作 DVD 上遇到技術問題，因此，他們改將影片及投影片上傳至學院的服務器並提供連結使學生得以下載，且限制該影片只能在學院內部使用。<br><br>然而在這樣嚴密的控管下，該學院被列為機密的紅外線技術和應用課程仍意外地外流。通過 IP 位址追踪後發現，該影片在美國境內遭瀏覽 16 次，投影片則受到包括中國、巴基斯坦、伊朗等管制國家在內的全球用戶瀏覽 660 次。 |

本案資訊的外流明顯是由於退休教師與影片製作團隊之間關於課程內容機密性質的認知出入所致。該名教師未於課程資訊註記其「課程之敏感度和特殊處理的必要性」，導致影片製作團隊未能辨識該課程的機密性。透過本案可得知研究人員於處理敏感資訊時，應進行充分的「溝通」以避免資訊外流的風險。

| 案例 06　英國與印度簽署的核能合作協議遭到英國出口管制局的審查 |
| --- |
| 英國與印度於 2010 年在新德里簽署了英印民用核能研究合作協議。主要參與的機構是英國的工程和物理科學研究理事會（The Engineering and Physical Sciences Research Council，EPSRC）和印度的原子能部門（Department of Atomic Energy，DAE）。由於身為研究協議一方的印度部門參與了印度民用和非民用領域核能計畫，英國的研究可能將為印度核子武器的發展提供貢獻，因此使該合作具有敏感技術移轉的潛在風險。英國出口管制部門意識到這種風險，因此對合作的項目進行了嚴格的審查。然而，審查結果發現沒有任何項目屬於受管制項目，且該合作的最終用途也未能助於於產生大規模殺傷性武器。 |

本案由於研究的性質而引起了出口管制主管機關的關注，雖然在受到出口管制當局的審查後，該研究得以繼續進行。然而由於研究的結果通常是不可預測的，因此很難對研究項目提前進行是否受到管控的評估。舉例而言，許多項目因為涉及核能開發，研究結果可能包含一些潛在的管制項目。因此，主管機關須持續地評估當前及未來的研究是否會導致管制技術的出口，以確保應用於民用核能發展的技術不會對貢獻於他國的軍事應用。

| 案例 07　挪威能源技術研究所提供管制技術援助(assistants)巴西海軍計畫 |
| --- |
| 挪威能源技術研究所（下稱 IFE）是一家研究能源技術的單位， 其主要運作哈爾登核反應堆，並定期以商業形式向其他國家提供技術援助。IFE 於 2010 年與巴西海軍計畫的運營商聖保羅中央海洋技術中心（CTMSP）簽訂契約，內容是為巴西海軍核潛艇推進項目的燃料顆粒的開發提供資源。巴西海軍計畫目標係尋求開發和部署常規武裝潛艇，這些潛艇需仰賴核反應堆推進提供熱量、電力和動力。此案引起了公眾的關注，因為根據相關出口管制規定，其等之合作未得到挪威政府的授權，於是警政單位開始調查該合作是否違反法律。在隨後的調查中，發現 IFE 還參加了俄羅斯，阿根廷，法國和美國的其他核能開發項目，然而也未申請出口許可證。<br><br>本案 IFE 傳輸的數據主要由電子資訊組成，而電子資訊的出口受到挪威的控制。根據哈爾登反應堆的道德準則規定：未得挪威外交部的出口許可，它們不應出口可用於增強另一個國家的軍事能力的技術。最終，IFE 的管理層承認其未申請出口許可並表示他們已審查並改善了其出口管制程序。 |

本案中，IFE 儘管沒有轉移任何物理核能原料，但敏感技術的轉移仍然受到出口管制，鑑於巴西正在尋求資源以發展核技術的軍事能力，即使這並非出於生產大規模毀滅性武器的行為，仍違反了 IFE 的倫理政策。本案說明即使在受到嚴格管制的區域內的研究機構也可能無法妥善地遵守出口管制法規。

## 2. 建議

綜合以上案例，本文試提供下列建議供我國學術與研究機構參考：

A. 招收來自有不當移轉風險的國家的學生時，應確實審查敏感技術領域的研究人員及學生的背景，以確保學術與研究機構自身未違反國際法或國內法。

B. 與我國出口管制主管機關(經濟部國際貿易局)合作，尋求合規的方案，以確保合法的學術及科學交流。

C. 對簽署研究協議的外國企業進行管制實體清單審查。學術機構除可依據「我國戰略性高科技貨品出口實體管理名單」作查核，亦可參考以下與我國貿易往來頻繁國家之管制實體清單，以識別出受管制的對象。

| 國家 | 管制實體清單 |
|---|---|
| 美國 | 1. Specially Designated Nationals List<br>2. Denied Persons List<br>3. Unverified List<br>4. The Entity List |
| 日本 | End User List |
| 歐盟 | EU Consolidated List |
| 澳洲 | Consolidated List |

D. 建立內部規範和出口管制單位，由獨立專家對出口管制的遵守情況進行定期審查，並設立嚴格的的內部控制，該程序要能識別出違規行為，方能確保該機構完全遵守法規。

E. 提供出口管制法律方面的教育培訓，在課程中宣導敏感技術之管制，特別是當這些培訓和教育課程可能被用於核武擴散活動時。

F. 對研究計畫將使用的基礎設施（例如實驗室設備）進行全面評估及檢驗，以審查其研究的敏感度及該技術的所有適用性，須注意的是，不能僅關注於該技術「合法」的適用性，還須考量其遭「非法」使用的結果。

G. 當機構內的研究涉及雙重用途（尤其是軍事用途）時，注意內部的擴散風險。

H. 密切關注出口管制法規，如果研究具有軍事用途，則須申請必要的許可證。

I. 鼓勵機構內部人員舉報可疑行為，並與主管機關就涉嫌違反出口管制的行為進行合作，以及時發現和應對內部威脅。

J. 對該技術的最終用途進行評估，檢驗其轉變成與軍事大規模殺傷性武器相關之運用的風險。

K. 要求外國研究夥伴遵守出口管制程序，並確保其遵守有關防止核武器擴散的國際標準。

L. 大學及學術機構內部應提高處理機密技術之安全層級，對於受管制課程須有清楚註記，並確保內部人員間已清楚地溝通，以確保該技術之機密性。

# 二、涉及研究人員之案例

## 1. 案例介紹

| 案例 01　美國教授因非法出口等離子執行器數據而被判入獄 |
| --- |
| 美國教授羅斯與他的前學生謝爾曼共同創立了一家名為 AGT 的私人公司。美國空軍於 2005 年與 AGT 簽署契約，該契約涉及研究離子執行器在控制空氣運動和方向方面的應用。隨後，AGT 將此契約分包給羅斯及田納西大學，以開發用於軍用無人機飛行控制等的離子執行器。<br><br>羅斯與 AGT 和美國空軍的分包契約中明確約定該項目要遵守美國的出口管制法規。然而，羅斯仍讓擁有中國國籍的博士生協助他完成美國空軍的項目。自 2002 年起，該名博士生在羅斯的指導下在田納西大學擔任研究助理。謝爾曼擔心敏感資訊可能因此洩露給中國，因此僅允許該名博士生從事基礎研究，而美國國籍的研究生則進行敏感資訊的應用研究。然而，謝爾曼並未防止兩國的學生們交流研究成果。田納西大學曾多次警告羅斯，不要將敏感數據帶到中國，也不要討論他正在從事的項目。<br><br>2006 年時，美國聯邦海關探員發現羅斯在中國時曾就離子執行器項目進行了演講。之後，聯邦調查局在羅斯家發現了該名中國博士生透過中國教授發給羅斯關於離子體空氣動力學的論文草稿，這一系列的事情意味著美國政府認為高度敏感的文件已發送給中國科學家。最後，羅斯因未遵守《武器出口管制法》被判處四年徒刑。謝爾曼則被判處 14 個月監禁，並被禁止日後從事聯邦契約工作。田納西大學未遭起訴，因為他們聲稱對羅斯的行為一無所知，並在得知後立即向政府揭露了羅斯的違規行為。 |

本案彰顯了學術活動和出口管制間之緊張關係，大部分衝突係源自於對專業術語的不同解釋。儘管羅斯未曾將敏感的資料從美國運走，但他轉移專業知識和數據方面的行為仍然違反了出口管制的規定。

羅斯訪華的行動包含三種被視為出口的移轉方式，包括：攜帶存有美國空軍項目相關的敏感文件的筆記本電腦、向中國聽眾進行該項目的演講，以及將文件通過電子郵件發送給中國國民的行為均構成了技術移轉。換言之，本案說明了移轉敏感技術，不一定要採用物理形式，例如在該項目中僱用一名中國人，即能分享敏感資料的研究，故即使沒有商品離開美國，這仍然是技術的出口。

案例 02　伊朗籍研究人員涉嫌移轉技術至伊朗

本案涉及一名在法國從事研究之伊朗籍研究人員賈拉勒羅霍拉尼賈德（Jalal Rohollahnejad），他在美國遭通緝，罪名是企圖向伊朗出口大功率工業微波系統和美國的無人駕駛飛機系統。高功率工業微波系統可使用於一種遠程但非致命的定向武器，能使受害者失去行動能力。據稱這些系統經過修改後將在伊朗用於軍事目的。然而， 羅霍拉內賈德堅稱他只是一名工程師和研究員，未從事犯罪行為。

羅霍拉尼賈德也是一位光纖專家，他被指控使用中文筆名掩護其對伊朗聯合酋長國的出口，據報導，這與伊朗伊斯蘭革命衛隊（下稱 IRGC）有聯繫。伊朗聯合酋長國是美國外國資產與控制局隸屬的實體，根據美國外國資產與控制 的新聞稿，該公司生產了 IRGC 無人機計畫的技術組件，並試圖維修 IRGC 軍事裝備。

在羅霍拉尼賈德的科學文章中，有一篇題為「使用紅外線探測導彈」的軍事導彈技術的文章，曾在德黑蘭舉行的電子防禦研討會上發表。在該篇論文中，他的隸屬單位據既是伊朗海軍防禦導彈集團（SAIG）的子公司，且為伊朗航空工業組織（AIO）的子公司。值得注意的是，這些都是受制裁的實體。 AIO 本身是伊朗國防部和武裝部隊後勤部（MODAFL）的子公司，負責監督伊朗的導彈生產。與 AIO 相關的許多個人和實體都因為它們支持伊朗的彈道導彈計畫而受到聯合國安理會和美國的制裁。

本案說明，研究人員若與涉及武器擴散之國家或實體有密切關連者，確實有可能作為敏感技術移轉到這些國家的渠道。

案例 03　美國及加拿大籍教授向中國出口半導體晶片技術

2019 年 6 月，擁有美國和臺灣雙重國籍的 Shih 被指控犯有 18 項聯邦刑事罪名， 他與其他兩人被列為共同被告。此三名被告被指控非法獲取半導體晶片並將其出口到被美國商務部列於實體清單的一家中國公司。這些半導體晶片因具有多種軍事用途而被列為出口管制，即必須獲得美國政府的許可證才能出口。這些晶片製造公司的客戶包括美國空軍、美國海軍和國防高級研究計畫局（DARPA）。

Shih 是成都一間製造該半導體晶片公司（下稱 CGTC）的總裁兼技術顧問；2014 年，美國商務部將 CGTC 列入實體清單，因為它涉及了替中國非法採購未經授權的軍事最終用途的技術。被列入實體清單意味著該公司須取得美國政府許可才能出口或在國內轉運任何技術。換言之，實際上 CGTC 被推定將被拒絕以任何方式從美國獲得所有出口管制設備或技術的許可證。

被告三人利用了幾家在美國和加拿大註冊的公司從中國獲得資金，並將其用於幫助他們獲取半導體及其技術。最後，其中兩名被告均被判罪名成立（其中大多是與稅收詐欺等相關罪名）。

本案顯示，研究具有軍事應用技術的研究人員熟稔出口管制法的必要性。同時，研究人員必須持續核對國際間和國內的管制實體清單，以確保他們不與被制裁的外國企業合作。

| 案例 04　美國國防部承包商的員工因向中國出口軍用鈦技術而被判入獄 |
| --- |
| 本案涉及一名中國公民 A 從美國國防部的承包商竊取軍事商業機密。A 曾擔任聯合技術研究中心（下稱 UTRC）的高級工程師科學家， UTRC 係美國國防部主要的承包商。<br>2013 年，A 雖仍在 UTRC 任職，但他積極尋求在中國國立大學工作的機會，並成功獲得瀋陽自動化研究所（下稱 SIA）的職位。SIA 指示其提供其在美國的工作資料，以證明其與其提供的履歷相符。於是，A 提供其擁有某些專利的資訊以電子郵件寄給 SIA 主任，而其中一份正是被美國管制出口的文件。<br>2014 年，A 帶著存有商業機密及其他高度敏感的資訊硬碟至中國。三個月後，A 在機場被捕，政府當局對其行李進行了搜索，發現其中包含機密，專有和出口管制文件的電子副本。機密的專有文件包含詳細的方程式和測試結果，這些方程式和測試結果係應用於開發美軍飛機。A 在 UTRC 工作時曾藉職務之便影印這些文件。最終，他因違反《美國武器出口管制法》和《國際武器貿易條例》，被判刑入獄兩年半。 |

本案說明了，在出口管制沒有嚴格執行的情況下，違反出口管制要求的嚴重後果。A 所獲得及攜帶至中國的技術屬高敏感資訊，並且受出口管制。它涉及美國軍用飛機發動機部件的製造，此類資訊通常受到美國國防部非常嚴格的保護。雖然 A 已接受所有與出口管制有關的教育培訓，並簽署了保密協議，但內部程序仍欠缺諸如隨機檢查的後續機制來加強管控，這反映了美國工業界以及政府當局所採用的保護體系存有漏洞。

## 2. 建議

綜合以上案例，本文試提供下列建議供我國學術與研究機構之研究人員參考：

A. 研究人員在準備從事研究合作時，應先審查該技術或貨品是否可能因任何原因受到出口管制。

B. 研究人員倘有疑義者，應向我國主管機關(經濟部國際貿易局)尋求協助。

C. 研究人員應與學術或研究機構內部的出口管制單位或法務部門合作，以核對國內外出口管制實體清單並申請任何必要的許可證。

# 小結

藉由本章節引介之學術與研究機構案例可知，學術與研究機構應提前制定對於風險管控的嚴密程序，並且應由專責人員來監督這些程序。CSSTEAP 機構的案例可以充分地說明風險管理的重要性，在該案中，由於機構內部的教育人員對於敏感技術移轉的風險毫無意識，而機構本身又欠缺一套偵測風險之程序，因此其等未能及時審查修習這些課程的學生背景，進而產生敏感技術移轉之風險。另一方面，學術與研究機構在簽署可能與管制相關之研究協議時，也應積極與國家出口管制單位合作，例如本章節所舉之 A 理工學院與 D 國國有獨資企業研究協議一案，這些大學即是與該國出口管制單位合作，以管控敏感技術移轉之風險。

另外，藉由本章節所引介之研究人員案例可知，各國政府近來逐漸增加學術研究的管制項目，因此，學術與研究機構應設立獨立審查單位，對於研究項目是否落入管制範圍加以評估，以避免觸法並面臨不利聲譽之後果。

望本章節所提供之建議能供我國學術研究機構對於風險管控作進一步的研析，相信透過與政府出口管制單位的對話，能使研究機構避免違反出口管制法規，並確保研究人員能持續地進行合法的學術交流，同時亦能維護國際間對於防止核武擴散的共識。

# 伍、給學術與研究機構的建議-制定應對計畫[7]

臺灣的學術與研究機構在一個高度全球化的環境中運作，擁有廣泛的自主權，使其得發揮許多優勢，卻也因此面臨著沒有能力處理的風險。本指引已舉例說明這些風險帶來的影響並以案例分析之形式給予建議，本章節參考美國學術機構所提出之「全球參與之風險評估應對計畫（Global Engagement Risk Assessment & Management Program，GERAMP）」（下稱 GERAMP），欲進一步提出一套具體的風險應對方式。首先，以 GERAMP 的概念，為學術與研究機構如何評估和管理外國參與風險提供了一個組織和操作框架。再者，成立「全球參與之審查辦公室（Global Engagement Review Office，GERO）」（下稱 GERO），負責全球參與計畫的行政領導、監督和協調，並與相關政府機關進行聯絡。第三，建議學術與研究機構採用「風險處理流程（Operational Security，OPSEC）」（下稱 OPSEC）作為對外交往風險的處理模式。

## 一、全球參與之風險評估應對計畫（GERAMP）

### 1. 基礎任務 - 盡職調查

盡職調查是任何風險評估和管理計畫的根本。在對外合作的背景下，機構和研究人員必須確保對潛在合作的所有參與者進行明確的記錄，無論合作是正式還是非正式的。他們還必須核實合作的性質、範圍和目的是否明確和透明，是否符合相關的法律和法規，是否在完全知情和同意的情況下進行，以及是否避免損害核心價值和國家利益。具體應做到的事項包括：

A. 瞭解你的合作夥伴

機構和研究人員必須先瞭解他們的潛在夥伴有哪些，而非等這些夥伴主動出現。調查背景時，應多加利用各種不同的來源，必要時亦可與政府機構合作。而對於機構的調查，一般包括分析其過去的活動、經營的部門或與之相關的部門、其受益人，以及機構的商業和道德地位。

---

[7] 此章節參考自 Jeffrey Stoff, Glenn Tiffert & Kevin Gamache, *Global Engagement : Rethinking Risk In the Research Enterprise*, Hoover Institution Press (2020).

對個人的審查則應確認其是否來自有信譽的組織，以及是否擁有相關的合作資格，再加上其背景是否有任何無法解釋的差距或令人擔憂的事項。蓋高風險的合作者有時會提供經過包裝的簡歷，刻意省略重要的出版物、附屬機構和獎項，或將其錯誤地翻譯成中文。因此，應充分的進行背景調查，包括以其母語搜尋該合作者之出版記錄，藉以獲得有價值的資訊，從而使該合作者的簡歷更完整。而這種背景調查的深度將取決於合作的性質，但至少應包含所有的關鍵參與者，而不僅僅是主要研究人員，因為過去的經驗揭示，研究生和博士後學者也可能帶來高度威脅性。

B. 瞭解你的資助者

贊助研究和慈善捐贈也會為學術與研究機構帶來風險，且若未仔細應對，容易於過程中承受極大的聲譽損害。蓋贊助研究和慈善捐贈為外國個體進入和影響學術與研究事務開闢了渠道，進而動搖機構的自主權，而 COVID-19 疫情爆發造成的金融沖擊，更使這些弱點更加突出。因此，應建立更多的保障措施和更嚴格的監督，並借助相關專家的力量，以協助了解外國資助者的背景。

C. 嚴肅看待契約

學術與研究機構可能因缺乏法律背景，而在簽署契約時無法充分理解條文，且外國合作者也可能主張由其草擬契約。因此，學術機構應建立共用之契約模板和注意事項列表，且正式簽署前，亦應交由專業人員審核。

D. 訓練

應訓練學術與研究機構人員對於潛在風險的敏銳度，相關領域包含適用法律、政策和計畫進行方面的培訓。舉例而言，外國合作者可能有某些重要關係未揭露、或其來自不同價值觀和道德觀的國家、抑或是不了解我國的法律。另外，外國合作者，亦有可能將獲得的資訊、數據，用於意料之外的地方，或在未獲授權的情況下移轉技術。因此，研究人員必須受有足夠的訓練，以應對這些狀況。

E. 反覆驗證與適應

法律和政府政策不斷進化，同時，學術合作的範圍、參與者、他們的行為和其他情況也可能發生變化，進而改變原始的風險評估結果。因此，有效的盡職調查必須定期審查正在進行的合作和正式協議，重新評估風險，並根據需要調整保障措施。另外，也必須確保正在進行的合作和正式協議符合最新的指導和法律要

求，如果不符合，則使其符合規定。

## 2. 具體步驟

一個成功的GERAMP會做到以下幾點：首先，對學術與研究機構的所有國際活動進行全面監督，且相關政策和程序應促進一個有誠信又安全的環境，以保護構成學術和研究生態系統支柱的人員、資訊和資產；再者，定期進行實務培訓，以減少非正式和正式研究活動中的外國參與風險、維護機構的核心價值、保護附屬機構和智慧財產，並能更好的遵守政策與法律規範；第三，公開透明的報告對有效的風險管理至關重要，另外，應及時向決策者提供報告的資訊，並將這些資訊整理歸檔，以便未來參考；第四，當管理者進行風險評估時，他們應該詳細記錄他們所評估的資訊，以便指導未來的決策，同時也是對過去決策的重新審查；第五，機構必須在其風險評估報告中納入正在進行中的，對內部安全策略、政策和程序的審查，特別是與國際交流有關的面向。

另外，為了讓GERAMP有效，參與人員必須瞭解現有的威脅，並能夠在適當的時候採取對策。只有當機構的所有成員都認識到機構面臨的各種威脅，並積極支持風險評估和管理計畫時，才能有效的防堵各類風險。

GERAMP包含的面相有：人力資源、研究與教學、設施安全、資訊技術、國際旅行、研發和商業管理。其實，許多學術與研究機構已經在不同程度上具備了這些要素，但往往缺乏一個整合的核心。GERAMP為這些項目提供了概念和操作上的一致性，並使它們保持一致，同時還建立了一個方法論，以即時發現任何落差與持續優化。

首先，建立流程是達成目的很好的途徑。舉例而言，GERAMP可以建立一套流程，以確定與外國合作的研究是否會被他國不當的應用。詳言之，系統化對外國實體的審查，並以網絡系統監視以防止未經授權而洩漏的研究數據，並訂定數據洩漏之預防措施。為此，學術與研究機構可以聯合建立和管理一個區域審查中心，並使部分人員被授權利用從敏感或機密資訊中獲得的資訊來加強公開來源的審查。這樣的區域審查中心將有助於平衡整個機構中資訊、資源和能力。這個區域審查中心更將成為一個平臺，成員機構可以通過這個平臺獲得關鍵語言和各領域的專業知識、收集數據、獲得諮詢和援助。此外，區域審查中心將提供共同的聯絡點，以便在必要時就敏感技術、新出現的威脅以及監管和執法的新重點與政府進行聯絡。這將加深政府和機構之間的相互理解和信任關系，打破資訊共用的障礙，並使各個機構有能力根據自己的條件做出更好的風險評估和管理決策。

最後，強化科技設備也能有效降低與外國交流的風險。第一步即加強設備的註冊流程以強制機構內部的網路用戶達到最基本的安全標準。第二，為硬體加密，並擁有高性能VPN，為個人擁有的電腦設備提供安全認證和數據保護。這可以確保工作人員

使用安全、可管理的電腦平臺。第三，將商業合規管理資料庫（commercial compliance management databases）和私營部門的威脅管理解決方案納入研究機構的盡職調查計畫。這些資料庫包括用於管理出口管制程序的產品，用於背景調查的商業資源，有助於研究關係和資金來源分析的資料庫。

# 二、建立一個全球參與之審查辦公室（GERO）

在一個典型的學術或研究機構的環境中，應建立一個「全球參與之審查辦公室（Global Engagement Review Office，GERO）」，直接向校長或機構之首長報告並提出建議，同時作為該機構的協調中心，協調和監督所有與對外交往有關的事項。GERO將定期召集並主持一個類似於機構審查委員會的組織，其中包括：該機構的研究安全負責人、負責處理國際事務的代表人、主要研究人員的代表人、顧問代表、相關的外國領域和主題的專家，以及負責學術機構發展、贊助研究、和政府聯絡的代表。具體言之，GERO 將負責以下事項：

## 1. 與外國交流之風險評估管理

建立一個全球參與之成熟度模型（Global Engagement Maturity Model，GEMM）（詳下述），以正式實施和優化GERAMP。同時，與其他利益相關者（如資訊技術和人力資源辦公室）協調，監督GERAMP的實施、監測和改進。再根據已建立的政策和流程，向學術機構負責人與其他利益相關者，提供有關外國參與風險的建議。

## 2. 與國外簽訂契約

編制最新的、實用的指南與清單，介紹與外國研究合作、簽約的政策和流程。另外，系統地審查與國外的所有正式和非正式的約定，這種審查的範圍將取決於外國個體的身份和業務性質。另外，對每項審查的投入及其結果進行整理歸檔，供今後參考。還有，提供有關外國參與風險的內部咨詢服務，使機構人員能主動維護學術價值、研究完整性和安全性、法律合規性和機構利益。最後，將數據收集、衡量標準、揭露和報告系統化，以滿足GERAMP的監測和合規要求。

## 3. 人員

在機構內安置具國際合作之誠信與安全方面受訓經驗的人員，以作為聯絡窗口。另需一批人員負責系統地審查外國個體，如訪問者、學生、學者、研究合作者和研究贊助者，審查程度與他們可能構成的風險相當。還需人員負責分析內部威脅並採取保障措施，任何能夠接觸到技術和資訊的人都可能在沒有適當授權的情況下將其移轉。因此，明確的流程和培訓可以減少這種危險並及時發現問題。最後，應制定一套核實外國的揭露與承諾的流程，以及另一套在任何人離開時迅速取消附屬機構的系統和資源使用權的流程。

## 4. 網路

應定期實施網路安全教育訓練，蓋終端用戶是網路攻擊的重要媒介，透過實施教育訓練可有效防止相關資安問題；然而對相關知識的了解並無法保證該等用戶正確理解研究事業所重視的網路安全威脅問題的複雜、嚴重程度。因此，需引進網路安全區（Secure Computing Enclaves），此種分享環境所需之費用合理，且係在不影響搜尋的前提下最易被接受的網路安全方案

## 5. 國外旅行

建立一套政策以保護學術與研究機構的海外人員。首先，在出口控制、運輸、軟體使用限制和其他安全問題方面，建立國外旅行的審查流程。再者，對於位於海外的附屬機構或於前往海外的機構人員進行培訓，使其瞭解特定環境下的風險管理和緩解做法。最後，提供政治風險咨詢和技術支持服務，如加強手機、平板、筆電和其他電子設備的防火牆，以防止網路攻擊，並在前往已知有威脅的國家後對其進行清理、重置，或直接另外提供借用設備。

## 6. 事件回報和回覆

首先，建立機構內的一套流程，以回報、調查、記錄外國的干預、利用。並根據已建立的調查流程，監督涉及外國個體的研究誠信和安全事件的反應。再者，對作為和不作為的不合規行為提出紀律處分建議。

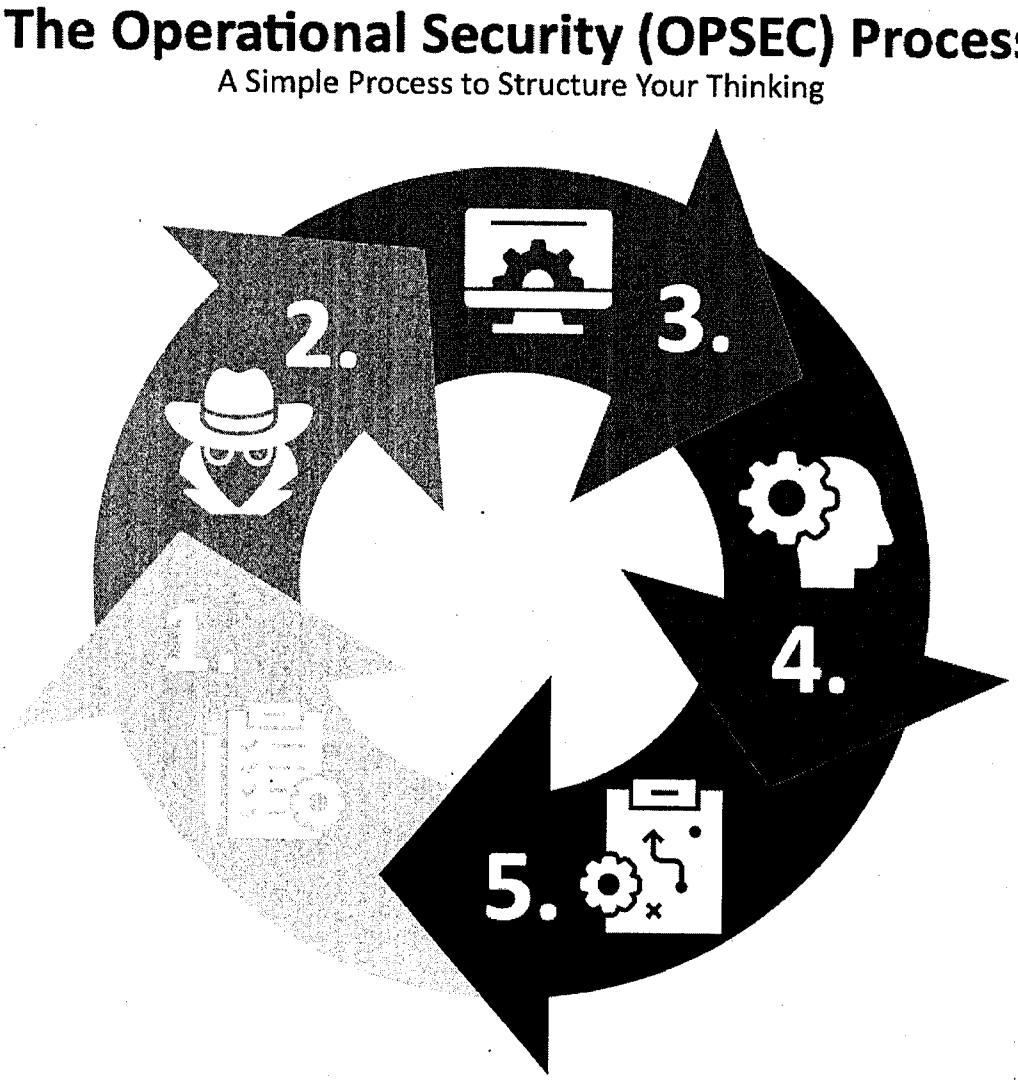
## 7. 與政府的關係

學術與研究機構和政府之間應建立相互信任的關係，進而促進明智和精準的資訊共享，對政府資助的研究進行適當的監督，並及早識別和保護敏感技術。建立一個特

定部門負責就與外國的交流事項與政府聯繫，可促進這樣的關係，並使研究研究機構跟上趨勢和不斷變化的指導方針，為新的要求做好準備，並避免出現意外。

## 8. 建立主動的風險處理流程（OPSEC）

GERO 可成為管理我國學術與研究機構所面臨、且日益嚴峻的外國參與風險的基石。然而，若無自「單純遵循法令」到「積極訂立 OPSEC」的典範轉移與之相應，GERO 將無法實現其應有之效果。OPSEC 是一套兼顧審視風險和創新的處理流程，起源於美國軍方，包含五個反覆循環進行的步驟（見下圖）。



① 辨識資產 – 包括敏感資訊，如研究數據、智慧財產權、遭出口控制之數據和人事記錄。

② 辨識威脅 – 評估每一類敏感資訊對第三方和研究機構內部人員的潛在價值以及他們可能構成的威脅。

③ 分析差距 – 評估當前的保障措施、安全漏洞和其他脆弱處，以確定存在哪些（如果有的話）漏洞或弱點，可以被利用來獲取敏感資訊。

④ 分析風險 – 比較威脅和脆弱處，評估非傳統資訊收集行為帶來的潛在風險及其發生的可能性。非傳統的資訊收集行為可能發生於電子郵件、實驗室、會議期間和其他學術交流的非正式個人接觸中。

⑤ 實施應對措施 – 制定和執行一項計畫，以減少威脅和減輕風險。這可能包括更新硬體，創建有關敏感資訊的新政策，或對附屬機構進行健全的安全政策和實踐培訓。成本/效益分析可用於評估潛在的反擊措施。反擊措施必須直接、最小的侵入性，並且對附屬機構來說容易實施。

# 陸、結論

數位化的時代帶給學術研究者更多研究合作的可能性，與此同時，也使研究者面臨難以預測的風險。藉由本指引所引介之案例可知，當研究領域涉及出口管制技術時，學術與研究機構唯有擬定詳盡的計畫和設立獨立審查單位方能有效降低敏感技術遭不當移轉的風險。

首先，學術與研究機構應保持開放的態度與國家出口管制機構合作，例如當機構與外國實體簽署合作協議時，可以透過與國家出口管制機構合作來管理風險。唯有通過與主管當局的密切交流，方能確保研究人員從合法的學術交流中受益，並避免損害國際間對於防止核武擴散所做的努力。其次，本文發現許多違反出口管制法規的研究人員皆認為自身的學術自由權可以凌駕於國家安全風險之上，抑或是認為自身的研究能落入基本研究豁免的範圍而與管制技術無關，因此，最根本的防治端賴學術與研究機構透過內部的教育訓練提升研究人員對於出口管制法規的認識。最後，研究機構須建立有效偵測內部威脅並能快速回應的防禦體系，尤其應針對涉及研究敏感技術或來自不被信任的國家的研究人員，以作為防止擴散的最後一道防線。一旦研究人員故意地違反出口管制的規定，這些內部威脅將可能導致知識產權或技術遭竊取，並可能對機構帶來不利的聲譽及法律風險。

臺灣尊重學術獨立性與機構自主性，才能造就如今卓越的研究事業，然而這些良好的特質也產生了對國家和經濟安全日益不利的脆弱性。因此，本指引提出一套綜合的應對計畫，旨在協調我國學術交流的發展與維護國家安全的必要性。首先，學術界與政府應改變風險管理的方式，使雙方得以各自最擅長的事物，在中間相遇。具體而言，第一，研究機構應制 GERAMP，以嚴格評估風險，並通過相應的管理來減少風險。第二，研究機構應設立 GERO 將該框架付諸實施，並為整個機構提供統一的行政指揮、監督和協調。第三，採用 OPSEC 使各研究機構從遵守規定的形式主義轉變為積極主動的適應姿態，重新獲得主動權。第四，通過 GEMM 提供一種結構化的持續改進方法。

望本指引提供的方法能使學術與研究機構及學者在進行國際學術交流時，得以識別出自身研究和國家利益間潛在的緊張關係，進而提升決策的細緻度。誠然，所有改變都需要投資時間和成本，惟相信只要學術與研究機構和政府之間能維持緊密的合作關係，必能更有效地調整和利用現有資源，並在學術發展與國家安全間取得良好的平衡。

# 附錄

# 學術與研究機構自我審查清單[8]

## 1. 了解合作關係

| | |
|---|---|
| 進行國際合作前是否針對合作夥伴進行盡職調查，包含合作對象母國之法律及政治情形、合作對象與國家之間的關係、過去的研究內容、資金來源、附屬機構等？ | 是 / 否 |
| 進行國際合作前是否檢視雙方有無存在利益衝突？ | 是 / 否 |
| 進行國際合作時是否將研究與控制存取權分開，以保護智慧財產權、研究成果或個人資料？ | 是 / 否 |
| 進行國際合作時是否將資訊安全視為合作的首要考量之一，並進行降低資安風險的安全措施？ | 是 / 否 |
| 進行國際合作時是否在研究人員間制定一致的行為準則，以形成良好的研究文化？ | 是 / 否 |
| 進行國際合作時是否已確保資助者與研究者間之間的資訊共享為公開且透明，並已建立暢通的溝通管道？ | 是 / 否 |

## 2. 技術移轉對象若為機構

| | |
|---|---|
| 移轉技術之對象是否被列於「我國戰略性高科技貨品出口實體管理名單」？ | 是 / 否 |
| 移轉之技術是否會流向較有疑慮的國家（如伊朗、伊拉克或北韓）或聯合國安理會實施武器禁運的國家、地區（如阿富汗、中非共和國、剛果、伊拉克、黎巴嫩、北韓、索馬里亞、利比亞、南蘇丹或蘇丹）之一？ | 是 / 否 |
| 根據獲得的資訊和貿易局網站上之公開資訊，移轉對象是否已經被懷疑，將敏感技術用於（開發、製造、使用或儲存）大規模毀滅性武器或常規武器的開發？或者是否有可能用於開發上述武器的先進技術材料、零件、產品？ | 是 / 否 |

[8] 此清單僅以列表方式舉例說明研究人員對風險意識的評估與宣導事項，但不應以此表為限。

## 3. 技術移轉對象若為外籍自然人

| | |
|---|---|
| 該人員本國是否為有疑慮的國家（如伊朗、伊拉克或北韓）或聯合國安理會實施武器禁運的國家、地區（如阿富汗、中非共和國、剛果、伊拉克、黎巴嫩、利比亞、北韓、索馬里、南蘇丹或蘇丹）之一？ | 是 / 否 |
| 該人員在本國之原組織（包括國際留學生的大學、學院、研究室）是否被懷疑參與開發大規模殺傷性武器（核武器、化學武器、生化武器、火箭、無人駕駛飛行器）或常規武器，以及用於這些武器的先進技術材料、零件、產品？ | 是 / 否 |
| 若為國際學生，是否曾、正在或將接受由原籍國的政府或機構、組織（包括私人機構）協助支付其學習費用？ | 是 / 否 |
| 若為國際學生，是否即將或有意願在與軍事有關的部門或軍火公司工作？ | 是 / 否 |
| 若為國際學生或研究員，過去的研究目的是否被懷疑是為了開發大規模殺傷性武器或常規武器？ | 是 / 否 |

## 4. 移轉之技術類別

| | |
|---|---|
| 是否為敏感技術領域？ | □ 核子技術<br>□ 精密機器/加工/測量技術<br>□ 自動化和機器人技術<br>□ 對人體有害的化學品或解毒劑相關技術<br>□ 生物技術和醫學（特別是傳染病和疫苗）<br>□ 高性能/功能材料技術（耐熱、耐腐蝕材料等）<br>□ 航空技術和高性能發動機技術<br>□ 導航技術<br>□ 海洋技術<br>□ 通訊、電子和光學技術<br>□ 電腦程式開發技術<br>□ 模擬程式設計技術 |
| 雖為上述領域<br>但是否可豁免管制？ | □ 移轉公眾所已知的技術<br>□ 移轉基礎科學領域之技術<br>□ 出口貨物所伴隨的最低技術<br>□ 專為設計或製造民用電腦或相關產品的技術 |

## 5. 了解相應法律風險

| | |
|---|---|
| 是否了解簽訂的合作契約內容，並留意可能產生的未來爭議，與面臨訴訟時對研究本身將產生的深遠影響？ | 是 / 否 |
| 是否留意研究有無受限於我國或合作對象母國之出口管制措施？ | 是 / 否 |
| 是否留意各國不同立法框架下可能對於協議以及合作關係產生的影響？ | 是 / 否 |
| 是否留意海外投資之相關規範？ | 是 / 否 |
| 是否留意個人資料保護相關法律？ | 是 / 否 |

## 6. 了解網路安全性問題

| | |
|---|---|
| 是否建立保護性強的獨立密碼來保護電子郵件？ | 是 / 否 |
| 是否安裝最新的軟體和定期更新應用程式？ | 是 / 否 |
| 是否避免許多應用程式要求不合理的許可權來存取裝置上的資料和活動？<br>註：應考慮限制得下載到工作設備上的應用程式的數量，並多與 IT 部門協商以便了解下載任何應用程式可能面臨的風險。 | 是 / 否 |
| 是否在電子郵件和協作平臺上啟用雙重認證？ | 是 / 否 |
| 是否使用密碼管理器來協助建立和記憶密碼？ | 是 / 否 |
| 是否使用螢幕鎖定來保護智慧手機和平板電腦？ | 是 / 否 |
| 是否在 USB 插入任何裝置前確認 USB 驅動器來源值得信任？ | 是 / 否 |
| 存取 USB 內的資料前是否確保防毒軟體已進行自動掃描？ | 是 / 否 |
| 是否對網路惡意行為有基本的認識？<br>Ex：釣魚郵件為獲取個人和其他資料的最常見方式之一 | 是 / 否 |

## 7. 了解員工赴海外工作之安全性問題

| | |
|---|---|
| 是否知道若員工在海外工作時發生意外，該員工應該向誰回報？ | 是 / 否 |
| 是否定期了解員工於海外工作可能面臨的困境？ | 是 / 否 |
| 是否確認機構與海外接待機構之間有何種協議？ | 是 / 否 |
| 是否使員工了解其應遵守哪些海外的法律？ | 是 / 否 |
| 是否確認該國的法律與所達成的任何協議間並無衝突？ | 是 / 否 |
| 是否了解員工在海外所做的工作是否會受到我國出口管制影響？ | 是 / 否 |
| 是否使員工了解當地出口管制法、國家安全法和其他相關之重要法規範？ | 是 / 否 |