生物保全計畫指引

訂定日期：111.5.1

1. 前言

處理或保存病原體或毒素會對工作人員、社區和環境構成風險。要管理這些風險，就必須使實驗室和其他從事病原體、毒素、感染性物質或受感染動物工作阻隔區域內的工作人員了解並應用生物安全和生物保全規範。

生物保全計畫的目的是防止生物資產（即病原體、毒素和其他受管制的感染性材料）和相關設施資產（例如無感染性生物材料、設備、動物、敏感資訊）的遺失、遭竊、濫用、移轉或蓄意釋出。本指引述明全面性生物保全計畫的訂定，該計畫是基於對設施所持有的資產和展開相關活動的生物保全風險評鑑。儘管所有設施都必須有一個生物保全計畫，但其複雜性(例如詳細程度、保全措施）與生物保全風險評鑑期間確定設施所持有的資產損害所帶來的風險成正比。

本指引就處理或保存病原體和毒素之設施的生物保全計畫所需要件提供詳細指導。本指引旨在協助設施符合疾病管制署(以下簡稱疾管署)「實驗室生物安全規範」(以下簡稱生安規範)及「感染性生物材料管理辦法」(以下簡稱管理辦法)規定之最低生物保全要求。包括指導訂定全面性生物保全計畫和實施與生物保全風險評鑑所鑑別的風險相當的有效生物保全管制和程序。

2. 開始作業

2.1. 角色和責任

設施內的高階管理階層具最高權力，負責將生物保全的適當權力授權。被授權者可以是生物安全主管（簡稱生安主管）或其他生物安全代表，也可以是保全人員或其他適當的人員；然而，生物保全計畫的成功訂定和實施往往需要一個由具有廣泛知識、技能和專業的主題專家組成的多學科團隊的貢獻。團隊成員可以包括管理階層、財務主管、建築師、工程公司、生安主管或生物安全代表、保安人員、科學家、實驗室工作人員、維修人員和當地執法部門，具體取決於實際狀況。

該被授權人員的職責包括籌組團隊（根據需要），訂定、實施和改進生物保全計畫，並可能包括作為任何生物保全相關事故的聯絡人，維持一份可以取得病原體、毒素和其他受管制感染性材料的人員名單，維持訓練紀錄，並確保採取措施充分保護敏感資訊。依管理辦法規定，由生安主管擔任

與對外聯繫之窗口。

此外，其他人員在維持生物保全方面扮演關鍵角色。在生物保全計畫鑑別這些人員以及其聯繫資訊，對於計畫的訂定和實施至關重要。這些關鍵人員可能包括：

- 負責管理和監督科學研究計畫或專案的人員（例如計畫主持人、實驗室/設施管理人或主管）。
- 現場保全人員（如果適用）。生物保全計畫應說明保全人員在生物保全方面的具體責任（例如監看入侵偵測系統、對警報作出反應、維持訪客進出紀錄、發放識別證）。
- 當地執法部門。當地執法部門的任何額外角色可在約定備忘錄概述（如果適用）。
- 所有能取得高風險病原體和毒素的人員（即管制性病原及毒素、RG3 和 RG4 病原體）。
- 負責進行人員適任性篩選和評估結果的人員。
- 人力資源部門可參與管理行為問題，並能促進與聘僱人員協助計畫和員工工會的溝通（如果適用）。
- 負責資訊技術（IT）和網路保全的人員；以及
- 所有可能有能力從設施內部或外部（例如經由建築自動化系統、電腦或安全控制台）遠端控制門禁系統的人員（維修人員、動物飼養員、保全人員等）。

2.2. 生物保全風險評鑑

生安規範規定，應根據對設施所持有的資產（即病原體、毒素和相關資產）以及在設施內進行的活動所涉及的生物保全風險的特定地點評鑑，訂定生物保全計畫。風險是依據事件發生的機率，以及事件發生後果的嚴重程度。生物保全風險評鑑是對蓄意事件的機率進行評估，例如資產（例如病原體、毒素、感染性材料、設備、動物、資訊）遭竊，以及該事件的後果（例如蓄意釋出病原體造成的公共衛生影響，或專有資訊遭竊）。將鑑別並優先考慮經由生物保全計畫描述的建議策略和最佳規範減低風險。

生物保全風險評鑑不同於生物安全風險評鑑(即總體、病原體及毒素、局部風險評鑑)，在評估事件發生的機率時，還需要考慮可能對資產有惡意的個人或團體（即威脅）。威脅可以分為兩類：未經授權取得資產的個人或團體被認為是外部威脅，而經授權取得資產的個人或團體被認為是內部威

脅。

此外，生物保全風險評鑑需要考慮具有雙重用途潛力之資產的更高保全要求。亦即，這些資產可以用於合法的科學應用，但由於其固有的開發和使用為生化武器的潛力，構成更大的生物保全風險。具有雙重用途潛力的資產包括管制性病原體和毒素，但也可以包括與處理和保存有關的資產（例如設備、資訊）。

經由生物保全風險評鑑鑑別的風險聲明和等級，可以透過各種方式（例如風險登記表）進行記錄，是訂定任何生物保全計畫的起點。

2.3. 訂定生物保全計畫

生物保全計畫詳細說明與生物資產相關已鑑別的生物保全風險減害策略。生物保全計畫描述為防止未經授權取得資產而實施的實體和操作管制，以及偵測和應對企圖未經授權取得的事故。生物保全計畫應補充生物安全手冊、緊急應變計畫、單位保全計畫和員工協助計畫的現有減害措施。在這些計畫或文件中，進入管制可能在某種程度已存在（例如可能有一些生物保全風險已經藉由解決生物安全風險而實施的措施獲得管理）。例如人員身家調查和實體保全措施可用以減輕生物安全和生物保全風險(生安規範第 4.1 節)。將生物保全計畫的各項內容整合到整個生物安全計畫中，可以更有效管理生物安全，並儘量減少資訊的重複。

2.3.1. 生物保全計畫的要素

每個生物保全計畫都必須提到 6 個要素，下面列出這些要素，以及其績效目標：

- 實體保全：經由建立適當的實體保全管制，減少未經授權取得已鑑別的資產和其他敏感材料的風險。
- 人員的適任性和可靠性：經由評鑑個人當前和持續的職位適任性，減少被授權的個人損害資產的風險。
- 病原體和毒素的責任：建立病原體和毒素的"所有權"，以及個人的責任和授權。
- 庫存清單管制：經由追蹤病原體、毒素、感染性物質和其他相關資產，並允許快速鑑別遺丟的項目，阻止內部威脅。
- 事故和緊急應變：促進人員安全以及病原體和毒素的保全；為持續改進生物保全措施提供證據基礎。

- 資訊管理和保全：保護敏感資訊免受未經授權的取得或遭竊，並確保必要的保密性。

2.3.2. 訂定風險減害措施

訂定生物保全風險減害措施應採用系統的方法，建立在有據可查的操作流程之上，以鑑別、評鑑、理解、決定和溝通風險議題，努力確定最佳行動方案。確保某一特定資產保全的所有措施應達到相同的水準。例如主要入口、窗戶和緊急出口的保全應達到相同的水準，所有能進入阻隔區域的個人（人員和訪客）應符合相同的進入要求。

每個單位都有獨特的風險文化（即在一個單位內發現有關風險管理的態度和行為）和風險容忍度（即一個組織接受或拒絕特定水準之剩餘風險的意願）。風險文化和容忍度可以根據單位的優先事項、利害相關者和資源的可用性而改變。進行生物保全風險評鑑的多學科團隊必須清楚瞭解，並隨後訂定減害措施，並在生物保全計畫詳細說明。

2.3.2.1. 與生物保全風險相稱的減害措施

由於生物保全計畫是以生物保全風險評鑑為基礎，將根據每個設施或阻隔區域的情況進行調整，其詳細程度和複雜程度將根據設施的性質（即規模、結構、複雜程度）和每個阻隔區域內進行的活動而有所不同（例如進行體外工作的 BSL-2 實驗室需要減害的生物保全風險可能比進行管制性病原及毒素體內工作的 BSL-3 實驗室少）。

雖然所有受監管的設施都必須訂定生物保全計畫，以解決第 2.3.1 節所述的 6 個要件，但本文件所述的許多減害措施超出許多 BSL-2 實驗室減害風險的需要。在為特定設施訂定生物保全計畫時，應結合生物保全風險評鑑鑑別的風險考慮生物保全計畫各組成部分的績效目標。在此之後，將仔細考慮適合於解決所鑑別風險的管制措施。

以下各章節將進一步闡述生物保全每個組成部分的理論，並提供可用於減輕生物保全風險的實體和操作管制範例。

2.3.3. 在需要了解的基礎上取得生物保全計畫

完整、詳細的生物保全計畫包含敏感資訊，例如漏洞、風險、具體減害措施、平面圖、保全系統和門禁管制細節。對詳細的生物保全風險評鑑（包括風險登記表）和完整的生物保全計畫的取得，應限於需要瞭

解以履行其職務的被授權人員（例如生安主管、保全人員、高階管理階層等）。該計畫包含的詳細資訊並非針對所有設施人員。關於資訊分類和保全的進一步說明，詳見第 7 章。

生物保全計畫的描述必須出現在生物安全手冊（生安規範第 4.1 節）。該說明可以是一個概述，也可以是適用於所有人員的生物保全風險減害措施的簡略版本，同時省略敏感細節。該版本可用於人員訓練，並包括針對生物保全的標準作業程序（SOP）。在認為適當的情況下，訓練可以針對具有類似職能的個人群體（例如只處理 RG2 病原體的實驗室工作人員與處理管制性病原及毒素的工作人員）。

3. 實體保全

實體保全是指為從實體上防止未經授權進入設施、設施的一部分或取得資產，並保護其免遭損壞、盜竊或濫用而設置的屏障或措施。應實施充分的實體保全，以儘量減少個人未經授權進入阻隔區域和其他區（例如儲存區）的機會，以及未經授權從設施中移出病原體、毒素、其他受管制的感染性材料或其他資產的機會。

實體保全系統的複雜性應與生物保全風險評鑑所確定與資產相關的風險等級相稱。可參照生安規範，了解每種生物安全等級實驗室的實體阻隔要求和特定操作規範要求。

生物保全計畫中的實體保全部分應鑑別並描述現有的保全系統，以限制或約束進入存在病原體、毒素和其他資產區。現有的各種實體保全系統都發揮一種或多種功能，以管制或阻止對資產的取得，偵測未經授權的進入企圖（例如防篡改裝置、警報、閉路電視系統(CCTV)、照明），並對事故進行處置。

以下章節有助於確定適當的實體保全等級。表 3-2 提供減輕與實體保全有關的生物保全風險而可能實施措施的範例。

3.1. 實體屏障和分級保護

阻止未經授權人員的措施通常從場地周邊開始，並在設施內越需保全的區域周邊設置額外的屏障。阻止未經授權人員措施的一些範例，包括周邊圍欄、電子式門禁管制系統、鑰匙鎖、高保全性門窗。

確定最合適的實體保全屏障的第一步是鑑別通往或進入阻隔區域的

所有入口（即門、窗和其他通道）。存在管制性病原及毒素的設施中，要考慮管制依法核准之被授權人員進入處理和保存管制性病原及毒素設施的機制。

實體保全措施可以分級的方式實施，為高風險的生物資產（例如管制性病原及毒素）提供更高等級的保護。這可經由創建多個巢狀區(nested area)實現，要求個人通過每個區的進入管制屏障，以到達設施內更高保全區（圖3-1）。

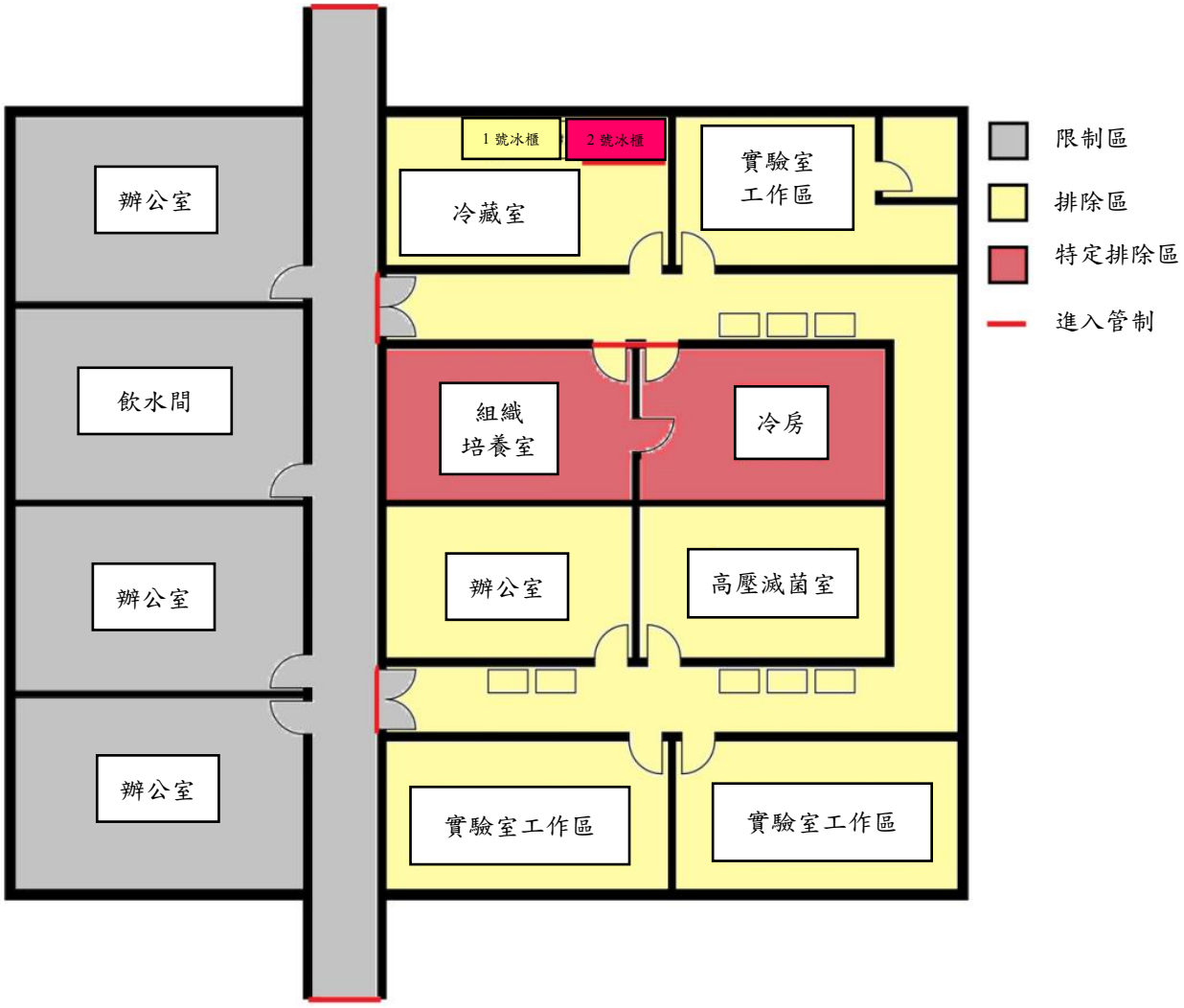

圖 3-1：設施內分級保護區範例。

灰色陰影表示設施的辦公室和公共區（飲水間），只限被授權人員進入設施。額外的進入管制，在入口處用紅線表示，限制被授權的實驗室人員進入實驗室側邊（黃色陰影）。另一等級的進入管制，限制被授權人員進入實驗室側邊內的特定區域（紅色陰影）。冷藏室的 2 號冰櫃的存取管制，可以採用冰櫃上鎖的方式。

3.1.1. 額外保全屏障

多重屏障也可能迫使未經授權的人員使用不同的策略突破每個屏障，從而拖延為反應人員提供應變時間。額外的保全屏障包括鎖或固定，以確保設備的保全，以及為儲存在公共或共用空間的材料提供可保險箱或可上鎖的冰櫃。例如如果管制性病原及毒素儲存在 BSL-2 或 BSL-3 實驗室阻隔區域之外，則有必要使用固定在原地的上鎖儲存設備，例如櫃子、冰櫃或冰箱，這些設備固定在牆壁或地板上，無法移動。

保全的儲存地點或容器應：

- 配備堅固的鎖定機制或採取其他措施，以防止未經授權的取得或移出。
- 在無人看管的情況下，能使內容物得到保護；以及
- 配備一個系統或機制來偵測未經授權的進入或取得。

3.1.2. 鑑別管制性病原及毒素區

“設施中授權進行管制性病原及毒素列管活動的部分"是由設施決定，要考慮到什麼是最適合其特殊情況。這可以是一個具有管制性病原及毒素所要求的獨特保全特徵的單一房間，並管制少數人員進入，也可以是一個更大的區域，包括許多房間或整棟建築，符合相同的生物保全要求，許多人員都可以進入。

例如，在圖 3-1 中，設施的管制性病原及毒素部分可以定義為：

- 所示的整個區域。
- 包括冷藏室和組織培養室在內的實驗室側邊；或者
- 組織培養室、冷房和 2 號冰櫃。

每種情況都有優點和缺點，如需要額外的實體保全和操作生物保全程序；例如，需要符合法規核准的人員數量，以及為適應非法規核准的人員進入而需要訂定的操作程序。

3.2. 進入管制

實體和操作上的進入管制限制被授權人員進入設施中處理或儲存病原體或毒素的部分，或其他敏感資產。最適合的門禁系統類型（例如無法複製鑰匙鎖系統、電子門禁讀卡器系統、鑰匙密碼系統、生物識別讀卡器等）將取決於特定情況。

以下措施是管制取得資產的方法範例：

- 建立 "管制 "的進入點。
- 在 "管制"入口處實施手動啟動的鎖定裝置、掛鎖、讀卡機，或生物識別裝置/系統。
- 在保全區附近實施局部警報，提醒附近人員注意入侵或其他問題。

表 3-1 中總結進入管制措施範例。第 3.4 節討論操作進入管制。

表 3-1：進入管制措施概述以及選擇和實施的注意事項

進入管制	保全規範及注意事項
機械鑰匙	・使用不可複製的鑰匙 ・追蹤所有發放給授權人員的鑰匙，並將其記錄在案，保持更新 ・在鑰匙丟失或損壞的情況下，更換或重新配製鎖具 ・當人員不再需要進入時，或在離職或解雇時，立即歸還鑰匙 ・保全存放未發放的鑰匙（例如存放在鑰匙箱中）
密碼鑰匙/密碼鎖	・保存一份持有進入密碼或鑰匙的人員名單 ・如果密碼或鑰匙遭到破壞，則更改進入密碼或鎖 ・記錄所有對進入密碼或鎖具的變更，並將此文件視為敏感資訊 ・將鑰匙紀錄歸檔並保持更新 ・將可以更改密碼的人員名單保存檔
電子鑰匙卡	・在鑰匙卡日誌或資料庫可追溯所有發給被授權人員的鑰匙卡 ・將鑰匙卡的紀錄歸檔並維持更新 ・在電子鑰匙卡上包括有照片的身份證明、姓名和到期日期 ・在人員離職或解雇時立即歸還鑰匙卡 ・對鑰匙卡進行程式設計，只允許在需要時進入限制區域。(即當人員不再需要進入該區域時，就取消對該區域的進入權限）
生物識別	・生物識別系統與生物安全要求的潛在衝突（例如在要求人員戴手套的地方，不合適指紋掃描） ・生物識別資料的資訊保全要求
遠端開啟（例如人員進入時發出聲響）	・在檔案中保留一份有被授權進入的人員名單 ・訂定並遵守流程或 SOP ・該系統的資訊保全要求

保全警衛的視覺識別	・在入口處安排一名保全警衛，以目視方式確認進入證件。
同一門上有多種類型的門禁管制	・使用互補的保全做法（例如電子鑰匙卡加上保全警衛的視覺識別）以提高保全性

3.2.1. 窗戶

窗戶和其他可以進入保全圍欄的開口，例如通風管道，可以安裝欄杆、金屬格柵或金屬網，以加強保全。安全膜和玻璃嵌裝也可以幫助將玻璃碎片固定在一起，防止窗戶被打破後從窗框中脫落。在某些情況下，防窺膜也可能具有保全價值（例如動物阻隔區域的窗戶），但這種膜只在某些照明條件下提供隱私。窗戶的保全硬體應從內部貼上，以防止被破壞，如果從外部貼上，則應安裝防破壞錨。位於底層的窗戶更容易接近，因此應採取額外的措施（例如較小的開口）來防止進入。就玻璃的強度而言，大多數類型的玻璃都可以用堅固的物體（例如石頭）輕易擊碎。然而，鋼化玻璃和夾層玻璃比片狀玻璃更厚、更堅固。一些類型的玻璃（例如夾層玻璃）在被打破時也能抵抗破碎。

3.2.2. 門

為處理或儲存資產的區域提供通道的門，在這些區域不使用時應上鎖。金屬包層或實心木結構的門，如果安裝在同等材料包層的加固框架內，將提供相當程度的保護。在鉸鏈安裝在非保全一側的情況下，使用不可拆卸的銷釘鉸鏈將有助於防止門被拆除。如果門上有窗戶或通風口，在窗戶上安裝安全玻璃，或在任何大的通風口（格柵）上安裝柵欄、金屬格柵或類似物，將防止其被打破或拆除。柵欄應該用防破壞的錨固定。生安規範規定，阻隔區域的門要有生物危害標誌，有助於避免未經授權的人員無意進入。同樣，其他門上的標誌，例如緊急逃生門，也有助於避免無意間進入（例如，"出口僅限緊急逃生"）。

3.2.3. 柵欄和大門

含有高風險資產的設施可以考慮在建築物的週邊安裝圍欄。高度低於 2.13 公尺的柵欄一般認為無阻止效果。柵欄上的出入口應保持在最少數量。可以藉由在不使用時將大門上鎖，或在每個大門設置一個持續配備保全人員的入口管制站進行管制。額外的阻止效果包括在圍欄頂部設置有

刺鐵絲網或有剃刀鐵絲卷。

3.2.4. 鎖具硬體

機械鎖的有效性取決於製造品質(例如插銷排列)、安裝、鎖的設計(例如插銷數量，使用材質)和維修的狀態。有許多類型的鑰匙操作的鎖，可以經由機制區分（例如盤式翻轉器，針式翻轉器，杠杆翻轉器）。無鑰匙鎖，如密碼鎖，使用轉輪機制。帶有密碼的鎖或基於密碼的無鑰匙鎖可能不適合用來保護需要高度保全的資產。帶有字母或數位鍵盤的密碼鎖可能容易被那些能夠從鑰匙的外觀推論出密碼的個人或團體破解。沒有任何一種鎖能提供有保障的保護，但用武力或技巧成功破解高保全性的鎖所需的專業知識和時間可能足以阻止未經授權的個人。當使用傳統的鎖和鑰匙時，應該使用高品質，或是高保全性的鎖設計，例如帶有高保全性鎖芯的鑰匙模型，其中包含第二組插銷、防撬性或不易複製的鑰匙（即不允許鎖匠、五金店或家用切割機複製）。在掛鎖方面，可以使用高保全性的鋼罩型掛鎖。

可攜式鎖（例如使用鑰匙的掛鎖）可以用來將多個物體固定在一起，一般使用鎖扣。鎖應該以堅硬的材料製成，以抵抗使用暴力攻擊，並有遮罩的鎖扣，以防止鎖被切割。當需要合理的保全等級時，不建議使用彈簧掛鎖，因為使用墊片可能會使鎖具脫離，如果掛鎖的主體被強行損壞或鑽洞，鎖可能會彈開。

主鑰匙和萬用鑰匙有時被用於設施中，允許需要進入許多房間的人用一把鑰匙打開多個門。在一個萬用鑰匙系列的鎖，一把萬用鑰匙可以打開該系列的所有鎖，而主鑰匙可以打開該系列中的一個子集的鎖。不鼓勵使用有一把主鑰匙和一把萬用鑰匙的鎖系統，主要是因為一把鑰匙的遺失或遭盜可能會危及整個區域的保全，同時也因為這些鎖通常更容易被撬開（鎖室內有多個剪切點）。

門上有兩種類型的鎖體：閂鎖和死鎖。閂鎖有一個斜面，並有彈簧載入，所以當門關閉時，會自動插銷（或鎖住）。閂鎖的缺點是其保全性不如死鎖；除非閂鎖配備墊片裝置，否則用單個閂鎖鎖住的門可以用一個薄的墊片（如信用卡）相對容易打開。死鎖只能用鑰匙（或從裡面的旋轉按鈕）移動到鎖定或打開的位置。伸入門框至少 2.4 公分的死鎖可以提供良好的保護。

3.2.5. 電子門禁系統

電子門禁系統，例如生物識別和鑰匙卡/讀卡器系統，可用於為經授權的人員提供管制性進入。在入口處向門禁系統出示進入憑證。與讀卡器相連的資料庫識別有關個人的資訊，包括該人員是否有權從某一入口點進入。鑰匙卡上可能有被讀卡器讀取的磁條，或者包含一個圖案，讀卡器會對其進行掃描。鑰匙卡/讀卡器系統是目前最常見的電子門禁形式，鑰匙卡也經常被用作身分卡。在使用電子系統的地方，應該有一個備用的或輔助的電源，以便在停電的情況下使用。另外，如果進入管制之保全失效，可以實施一個備用的管制進入系統（例如使用鑰匙鎖和不易複製的鑰匙）。

鑰匙卡/讀卡器系統的優點是如果就業狀況發生變化，或者鑰匙卡遺失或遭竊，可以從資料庫變更與卡相關的權限。

電子門禁系統的一些特點包括：

- 能夠鑑別和記錄進入的地點和使用的門禁憑證。
- 能夠根據一天中的不同時間允許或拒絕進入。
- 能夠在不改變任何硬體的情況下改變進入許可。
- 能夠監視門的狀態，以顯示開關或是上鎖。
- 連接個人資訊的能力（例如照片、職員身份、進入到期日期）；以及
- 與其他電子保全裝置（例如攝影機）連線能力。

應該考量電子門禁系統的一個限制是遠端干擾的可能性（例如蓋台），無論是經由建築自動化系統或場所內的保全控制台，還是來自場所外的電腦或設備。另一個限制是尾隨，也就是允許別人和本人一起進入管制區。這在工作場所很常見，因為替同事開門被認為是一種禮貌。一個可能的解決方案是讓開門的人員確認同事的身份證件。在保全意識訓練期間，應明確描述單位政策和對人員的期望。保全訓練在第 7.2 節進一步說明。

有許多類型的生物識別裝置可用來限制進入設施或設施的某些區域。這類系統可以基於對個人的眼睛、手、手指、臉、聲音或血管進行識別。掃描器用於捕捉個人的資訊，並將這些資訊與包含授權個人的掃描模式的資料庫進行比對。如果確定符合，該人員就被授予進入權限。生物識別系統的錯誤率可能會有所不同，取決於該特徵每天的變化程度。例如語音辨識系統可能會錯誤拒絕喉嚨痛的個人授權。

表 3-2：為減輕 BSL-2、BSL-3 實驗室和管制性病原及毒素區域內與實體保全有關的生物保全風險而實施的措施

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
實體保全	未經授權的人員進入阻隔區域。	・進入阻隔區域的門有鑰匙鎖。 ・禁止人員複製鑰匙的程序。	選項 1 ・在進入阻隔區域的門使用不可複製的鑰匙鎖。 ・取消進入授權的程序。 選項 2 ・電子鑰匙卡進入阻隔區域。 ・使用帶有不可複製鑰匙的鑰匙鎖的後備限制進入系統。 ・在緊急情況下，進入管制將轉成無保全狀態。	選項 1 ・在進入阻隔區域的門使用不可複製的鑰匙鎖。 ・當人員未經依法核准之門禁程序。 ・取消進入授權的程序。 選項 2 ・以電子鑰匙卡進入阻隔區域。 ・使用帶有不可複製鑰匙的鑰匙鎖的後備限制進入系統。 ・在緊急情況下，進入管制將轉成無保全狀態。
	未經授權的個人取得儲存在阻隔區域外的病原體或毒素。	位於阻隔區域外的儲存設備要用鑰匙鎖系統上鎖住（例如冰櫃要上鎖）。	位於阻隔區域外的儲存設備用不可複製的鑰匙鎖系統上鎖，並位於一個限制的進入區域內。	位於阻隔區域外的儲存設備要固定在原地（例如用螺栓固定在牆上），並用不可複製的鑰匙鎖系統上鎖。

3.3. 偵測未經授權進入和企圖進入

設施中的偵測系統通常用於監測和保護一個區域（例如，場地周邊、限制進入區域），而不是一個物體。對於一些 BSL-2 實驗室，執行操作程序確認未被識別的個人可能足夠。在保全性較高的區域，可能需要採用實體偵測手段監控（例如透過保全攝影機、閉路電視或警報器）和紀錄（例如進入的電子紀錄）進入或離開該區域的個人。

以下措施可以及時發現企圖或成功未經授權的進入：

- 視覺觀察。

- 通過視頻進行報警評鑑。
- 入侵偵測裝置。
- 庫存清單紀錄（如果經常查證）；以及。
- 封條或其他防篡改的裝置。

未被實際使用的區域（例如在非工作時間）可以藉由入侵偵測系統和警報器進行保護。表 3-3 描述各種類型的入侵偵測系統。入侵偵測系統的感測器通常放置在入侵者進入的潛在點（例如窗戶）。如果入侵偵測系統被觸發，最好能及早向應變小組（例如保全人員、執法人員）發出警報，以便及時進行應變。如果使用鍵盤對入侵偵測系統進行佈防和撤防，該設備及其電氣接線盒應安裝在保全區，以減少被篡改的風險。

3.3.1. 入侵警報系統

為偵測未經授權的進入、企圖進入或篡改，警報系統應：

- 在偵測到入侵或篡改事件時立即啟動。
- 保持警報狀態，直到被授權人員確認。
- 使用一個以上的感測器或感測器類型，提供備援。
- 包括重疊的感測器偵測區域。
- 使用受監督的專用通訊連結，並持續進行監測。
- 具備用的或輔助的電源，或相當的電源，以便在主電源失效的情況，保持偵測能力；以及
- 具有較低的干擾和誤報率，並具有較高的偵測機率。

此外，在使用室內警報系統時，應考慮以下一般建議：

- 警報監測裝置和備用電池電源應受到保護，以防止未經授權的個人篡改（例如電子面板或接線盒）。
- 專門的警報區域可以設在儲存區（即與其他警報區域，例如實驗工作區分開）。
- 應保持稽核追蹤，以記錄任何警報的原因；以及
- 警報監測站應持續配備人員。

3.3.2. 閉路電視監測

閉路電視系統為保全人員提供從一個中心位置看到許多保全區的能力。許多系統還可以包括音訊。最基本的系統包括一個攝影機，一個將視

訊訊號從攝影機傳輸到觀看地點的方法，一個觀看螢幕，以及一個監控即時視訊訊號或錄製視頻的人員。更複雜的系統可能有多台攝影機、視頻運動偵測器、在攝影機之間切換的切換器或同時查看多個視訊訊號的多工器、記錄視頻時間和日期的註釋器以及執行影像處理功能的電腦(例如物體識別、搜索和重播功能)。攝影機可以放置在設施內和設施周邊的策略位置（例如入口和出口點，與警報器相連的感測器處)。從閉路電視系統拍攝的視頻可提供事故的重要紀錄，在事故調查中可以作為證據使用。

隨著類比成像技術朝向數位成像技術發展，各種計算功能可整合到保全系統。例如可以對視頻進行篩選，以尋找不經常出現的影像序列，例如可能具有重要意義的人、物或車輛的存在。攝影機也可進行遠端控制。技術的改進也導致具有更高解析度的彩色攝影機的使用，使物體更容易被識別。

閉路電視系統也可以在緊急應變中發揮作用。允許保全人員從遠端查看地點並評鑑情況。如果閉路電視系統與入侵偵測系統整合，可用來確定入侵警報的原因（例如如果是人為觸發)。電子檔案可以複製到其他媒體（如 DVD、USB 快閃記憶體驅動器)，以便在需要時作為證據長期保存。

表 3-3：入侵偵測系統摘要

偵測系統	說明	可能用途	限制	依賴性
紅外線移動偵測器	檢測環境溫度的變化	・在管制進入區內 ・沿著通向管制進入區的走廊 ・經過通往管制進入區的關閉門 ・含有病原體或毒素的保存設備附近	・含有產生熱的物品/設備區 ・極大型區 ・安置動物的房間	需要放置在整個設施的策略區。
接觸開關	偵測電路是否中斷（例如門窗被打開）	・通往管制進入區的門窗	・有玻璃窗或門的區域，可直接進入管制進入區	可能需要玻璃破碎感測器
破碎玻璃感測器	偵測玻璃破碎產生的聲音頻率和振動	・有玻璃窗的實驗室，可以進入管制進入區	・頻繁發生暴風雨地區的設施 ・非玻璃窗的設施	所有門窗都需要配備感測器

偵測系統	說明	可能用途	限制	依賴性
聲學移動感測器	經由發射和偵測物體反射的聲波偵測移動	・在管制進入區內 ・沿著通往管制進入區的走廊 ・通往管制進入區的門附近 ・含有病原體或毒素的保存設備附近	・動物房 ・含有噪音設備的房間（例如振動器、培養箱） ・極大型區	系統需要放置在特定的關鍵區
聲學感測器	監測聲音以確定何時發生入侵或確定入侵的性質	・在管制進入區內 ・沿著通往管制區的走廊	・動物房 ・有背景雜音的房間(例如會有噪音設備的房間)。 ・沒有外在聲音阻隔的設施	需要充分阻隔外在聲音(例如來自隔壁實驗室的聲音)
視覺監測	視頻影像由攝影機拍攝，並由保全人員監視（例如閉路電視）	・攝影機可以放置在設施周邊的入口處	・視頻品質受到能見度條件的影響（例如光照度、大雨）	影像需要持續配備人員，或記錄視頻資料並與入侵警報系統整合

3.3.3. 防偽技術

防偽膠帶、標籤和封條可用於目視偵測對受保護資產的未經授權取得，例如冰箱、小瓶、盒子或其他裝有病原體或毒素的容器。市面上的裝置包括翻蓋小瓶和旋蓋容器，可用塑膠裝置固定，在打開時分離。

3.3.4. 照明

設施的室外照明可用於加強被授權人員進出建築物的安全。還可以藉由提高室外攝影機的影像品質阻止或偵測入侵。幾種類型的照明，包括白熾燈、高強度充電燈、螢光燈和發光二極體(LED)。照明應根據其預期的應用選擇。例如移動啟動照明需要迅速達到最大輸出，而視頻監測區的照明可能需要特定的顏色輸出，以捕捉影像細節。

一些專家認為，昏暗的照明條件比完全不提供照明更糟糕。考慮到明亮的光線可以使入侵者容易被目視發現，雖然完全的黑暗可以提供掩護，

但也使入侵者難以克服屏障。然而，昏暗的光線可能足以讓入侵者操縱鎖，但可能不足以讓攝影機偵測到。

3.4. 進入管制的操作注意事項

操作進入管制措施可以單獨使用，也可以與實體措施結合使用，以管制進入設施或設施的部分。訂定政策和程序（例如鑰匙管制、進入碼和訪客）並對人員進行訓練，使其瞭解並遵守規定程序，是維護設施保全的基礎。這些政策和程序還應該概述設施內能夠核准人員授權程序的負責部門，並確定那些被允許授權人員進入特定區域的個人。授權過程可能涉及一系列的審核（例如來自人力資源、設施保全和主管），個人必須在獲准進入之前符合所有的進入要求（例如適當專業資格，完成生物安全和生物保全訓練，如果需要的話，還要符合法規核定要求）。

3.4.1. 鑑別被授權人員

應訂定程序或政策，以便在人員（例如阻隔區域人員、受訓人員、訪客、管理人員、學生、維修人員、緊急應變人員）需要臨時進入、不再需要進入、離職或被解雇時，授予、改變或取消進入授權。該過程可以包括停用電子鑰匙卡，交出鑰匙、鑰匙卡和識別證，或變更鑰匙密碼。該政策應規定在允許進入前必須符合的標準，其中可能包括健康檢查、訓練要求、或陪同和監督人員。還要符合法規核定要求。

應定期審查被授權人的名單。在以下情況的設施中，審查可能更為頻繁

- 有處理或儲存管制性病原及毒素的設施；
- 有大量的人員進入（例如大型設施）；
- 有頻繁更換的人員進入（例如學術設施）；
- 有頻繁更換的專案（例如動物研究）。

還應考慮對保全管理系統和軟體的管制登入，以防止未經授權的干擾。

3.4.2. 訂定進入管制程序

應訂定標準作業程序或書面流程，以協助工作人員確定某人是否被授權進入設施，包括鑑別、質疑、移除和報告未經授權和可疑人員的步驟。還應訂定清潔、維護和維修人員進入設施的政策和程序（例如有陪同人員，保全病原體或毒素，無法取得）。關於佩戴有照片的識別證政策（例如在

設施內佩戴，而不是在外面佩戴）將有助於鑑別被授權人員。

在電子門禁系統使用鑰匙密碼或卡片時，應訂定政策，禁止人員分享門禁憑證（例如分享自己的卡片或密碼，或尾隨）。與鑰匙密碼一起使用的鑰匙卡可以提高保全級別。

最後，應訂定標準作業程序，用於報告遺失、遭竊或受損的門禁鑰匙、卡片或密碼，以便及時採取矯正措施。

3.4.2.1. 鑰匙

鑰匙和相關系統（例如鑰匙卡、密碼和密碼鎖）應維持紀錄，這些系統限制或管制進入阻隔區域、取得感染性材料或毒素。這些紀錄應包括：

- 鑰匙、密碼或密碼鎖發給的個人姓名；
- 發放或撤銷日期。

單位應訂定程序，以便在不再需要進入時收回鑰匙或由人員歸還，並保全儲存未發放的鑰匙（例如，安全的鑰匙櫃或保險箱）。

優良鑰匙管制規範是：

- 將持有鑰匙的人數限制在需要進入的人數。
- 將萬用鑰匙的數量限制在管理階層和可能需要進入所有區域的個人（例如生安主管）。
- 根據工作人員的更替情況，定期（例如每月、每半年、每年）對鑰匙庫存和鑰匙持有者進行審查，以瞭解所有已發放和未發放的鑰匙，以及已報告遺失或遭竊的鑰匙情況。
- 在鑰匙發放者和人力資源部門之間建立溝通管道，以便及時通知個人在職狀況的改變。
- 禁止人員複製鑰匙。
- 使用已獲專利的不可複製的鑰匙或專用鑰匙槽，以防止未經授權的複製行為。
- 確保發放給保全人員的鑰匙，如萬用鑰匙，在值班之間交接，並且永遠不離開設施；以及
- 在安裝鎖的時候，如果適用的話，將門禁密碼從出廠時的預設值進行變更。

應將緊急進入鑰匙保存在一個保全地方（例如保全鑰匙箱），以便在緊急情況下使用。如果使用緊急進入鑰匙，應在使用鑰匙紀錄中進行記錄，並通知負責人員（例如生安主管）。

3.4.2.2. 識別證

識別證是由單位核發帶有照片的身份證明，不與電子門禁系統相聯繫；然而，如果被授權人的姓名和照片出現在卡上，電子鑰匙卡也可以作為識別證。

識別證應包含被授權人的照片，供保全和其他人員對照，並註明個人姓名和有效日期。識別證可以用顏色編碼，以表示授權進入設施的特定管制部分。該系統使管制區域內的人員能夠監測和發現未經授權的個人。例如保全人員可以根據對職員證書的目視查證（例如帶有照片的有效識別證、照片識別和個人姓名出現在被授權人員名單），允許個人通過有人駐守的保全檢查站。根據所需的保全等級，對於擁有眾多員工（例如每班超過 30 人）的單位來說，由保全人員進行目視鑑別可能不是一個合適的管制進入方案。

為使識別證系統發揮作用，所有被授權的人員在設施內需要一直佩戴證件，除非生物安全要求不允許（例如 BSL-3、BSL-4 實驗室）。工作人員應定期查證在一天中偶然遇到的其他人員身份，如果發現任何沒有識別證的人員，應將其驅離管制區域或通報適當的內部負責部門。

核發給需要進入設施或設施部分人員的識別證，應以類似於上述鑰匙的方式進行記錄。當不再需要進入時（例如職務異動、退休、離職），也應及時將識別證歸還負責發放的人員。與電子鑰匙卡相關的進入權限，可以很容易在電子門禁系統變更。

用來減少與識別證篡改有關風險的操作管制涉及到交換系統。職員會獲得兩張帶有相同照片的識別證。一張只是作為職員的身份證明，而另一張則是編碼（例如有不同的邊框或背景顏色），以清楚表明個人被授權進入的設施部分。職員在開始工作時，將非編碼的身份證換成編碼。在下班時，雇員將編碼的識別證歸還，以換取非編碼的識別證。

3.4.2.3. 電子鑰匙卡

電子鑰匙卡，無論是通用的還是作為識別證，都可以用來提供進入阻隔區域的電子入口（例如刷卡、感應或晶片讀卡器）。在保全性較低區，僅憑卡片就可以。要進入保全等級較高區，使用與卡相連的鑰匙密碼可以防止發現或偷竊卡的人未經授權進入。

3.4.2.4. 陪同和監督

受訓人員、訪客、學生、維修人員、緊急應變人員和其他需要臨時進入人員的進入流程，是評估門禁管制時的重要考量。可能包括記錄個人的姓名和進入的日期，發放臨時識別證，明確鑑別該人的目的（例如訪客、維修技術人員），以及該人員的陪同人員姓名（如果適用）。

經授權的人員進入設施的管制進入部分，應符合疾管署生安規範及相關法規的所有要求。由局部風險評鑑決定的其他單位要求也可能適用。

在生物保全計畫應包括允許訪客進入設施中限制或管制僅限被授權人員進入區的程序。根據阻隔區域的情況，可能包括不同程度的監督。例如對於參觀 BSL-2 實驗室的大學生而言，一名監督人員可能就足夠。

對於處理或以其他方式取得管制性病原及毒素的設施，被授權的人員必須經主管機關核定。只有在管制性病原及毒素已被保全並且無法取得的情況下，或者在有經核定的被授權人員陪同和監督下，才允許未被核定人員（包括訪客）進入。被授權的陪同人員每次只能陪同和監督一個人，在陪同和監督被陪同人員時，要隨時監控其活動。被授權的陪同人員應保持警覺，注意被陪同人員的可疑行為。

以前被拒絕或被暫停或撤銷核定的人員，即使是在監督下，亦不允許進入該區域，除非已取消拒絕、暫停或撤銷而重新核定。

3.4.2.5. 撤銷進入授權

當人員不再需要進入某區，或者其進入某區的授權被撤銷時，設施的負責部門應採取措施，取消該人員對不再需要進入該區的進入授權。在處理或儲存管制性病原及毒素區，必須立即取消進入授權。適當的措施可能包括收回鑰匙和識別證，更換鎖，以及更新電子進入紀錄。

在管制性病原及毒素區，負責部門應立即通知受影響的人員，是其不再被授權進入設施的該部分，或整個設施。

3.4.3. 保全和共用空間

共用實驗室空間是一種正在變得越來越普遍的實驗室模式。這種模式創造的實驗室環境既能符合當前的需要，又能適應未來的需求。位於設施內部的共用空間，其管制性病原及毒素的列管活動是經核准，可能會給所有需要進入的人員帶來挑戰。設施管理部門、主管將需要確定如何應對這些挑戰。

一個選擇是，所有在共用空間工作的人員都要依法被核定，這樣就可

以在任何時候自由進入有管制性病原及毒素的設施部分。另外，未被核定的人員（例如那些實際上不需要取得管制性病原及毒素的人員）對共用設施的進入，可以管限制在沒有管制性病原及毒素的時候，管制性病原及毒素被上鎖且無法取得的時候，或者由經核定可進入該部分設施的人員陪同和監督。這種替代方案可以經由使用排程表和保全的管制性病原及毒素儲存區實現。

共用實驗室空間的使用注意事項：

- 在共用空間內進行的活動類型。
- 需要進入的人員。
- 按時間區分活動的可能性（在需要加強保全措施的活動進行的具體時間）。
- 管制性病原及毒素廢棄物管理程序；以及
- 對特定設備的上鎖和警報器的需求，例如內含資產的冰箱和培養箱，以及資訊或資產儲存區。

4. 人員適任性和可靠性

應訂定人員適任性和可靠性政策和程序，以界定和記錄可取得病原體、毒素或其他感染性材料人員的訓練、經驗、能力和適任性要求。應訂定職員聘用前的篩選流程，以評估可取得病原體、毒素或其他列管感染性材料的個人忠誠度，可包括背景調查；此時也應評估行為指標。持續可靠性計畫，旨在尋求促進可接受行為也有利於減少與人員相關的風險。例如提供員工協助方案（例如諮詢服務），為減少員工因遭遇個人困難而成為內部威脅風險的一種方法。表 4-1 提供為減輕與人員適任性和可靠性有關的生物保全風險而可能實施措施的範例。

4.1. 人員適任性和可靠性的篩選

應訂定收集和查證應徵人員資訊的人員適任性和可靠性政策和程序，以因應來自潛在內部威脅的風險。這些政策和程序應包括描述如何評估和使用這些資訊確定應徵人員的適任性。對取得病原體或毒素人員的訓練、經驗、能力和其他適任性要求，應明確界定並記錄備查。在生物保全計畫概述評估人員適任性的程序也是謹慎的做法。預先篩選程序的嚴格程度（例如審查人員經歷、推薦人人數、審查評選主題數）應與資產的相關風險等級

相對應。

通過招聘過程，在錄取並獲准取得病原體、毒素或其他資產之前，對應徵人員進行篩選，確認具有從事病原體或毒素工作的適當資歷、技能和個人特質，並確認最適合該職務。學術和專業證書、先前的經驗和發表論文（例如簡歷包含的資訊）以確定其科學能力和可信度，而個人和專業推薦人可以提供該人員是否適合處理或取得病原體和毒素的指標。

除上述幾點外，招聘前的篩選流程還可能包括查證以下事項：

- 移民和簽證狀況。
- 犯罪紀錄；以及
- 單位認為合適的其他標準（例如信用紀錄檢查、職業健康評估、藥物測試）。

如果招聘單位無法獲得這些篩選過程所需的工具，可請當地執法機關提供協助。

表 4-1：為減輕 BSL-2、BSL-3 實驗室和管制性病原及毒素區域內與人員適任性和可靠性有關的生物保全風險而實施的措施

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
人員適任性和可靠性	不符合最低適任性和可靠性要求的人員被允許取得病原體和毒素	・招聘政策包括查證應徵人員的簡歷、推薦人和學歷證明。 ・推薦人鑑別應徵人員的技術和行為能力。	・招聘政策包括查證應徵人員的簡歷、推薦信、學歷證明和其他適當標準（例如信用調查）。 ・推薦信評估應徵人員的技術和行為能力。	・招聘政策包括查證實應徵人員的簡歷、推薦人、學歷證明及有效主管機關的核定。 ・推薦信評估應徵人員的技術和行為能力。
	不再符合可靠性最低要求的個人繼續取得病原體和毒素	持續的可靠性評鑑： ・程序包括自我和同儕的報告程序。 ・對不遵守既定生物保全規範的人	持續的可靠性評鑑： ・程序包括自我和同儕的報告程序。 ・對不遵守既定生物保全規範的人	持續的可靠性評鑑： ・程序包括自我和同儕的報告程序。 ・對不遵守既定生物保全規範的人員訂定分級懲處措施。

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
		員訂定分級懲處措施。 ・取消或暫停人員取得病原體和毒素或進入阻隔區域的程序。	員訂定分級懲處措施。 ・取消或暫停人員取得病原體和毒素或進入阻隔區域的程序。 ・要求對休假回來上班的人員進行評鑑的政策(例如壓力)。	・取消或暫停人員取得病原體和毒素或進入阻隔區域的程序。 ・要求對休假回來上班的人員進行評鑑的政策(例如壓力)。 ・報告有關可能影響經法規核定個人資訊的程序。

4.2. 持續的可靠性評鑑計畫

一個持續的可靠性計畫旨在查證被授權取得病原體、毒素或其他資產的人員是否繼續符合既定的人員適任性標準，並尋求加強可接受的行為。這種類型的計畫可以經由鑑別和向遭遇問題的人員提供幫助，有利於減少與人員相關的風險（即內部威脅）。對於一個單位來說，重要的是保持參與，並定期查證當前資訊，以確保人員持續適任取得病原體和毒素。

應鼓勵人員向內部負責部門或設施保全人員報告任何可能影響個人、設施資產或整個社區的安全或保全的資訊。這些資訊可能包括：

- 可能影響人員依法核定的情況。
- 可能影響人員以安全可靠的方式執行職責的情況（例如注意力分散或錯誤明顯增加；承擔風險行為增加）。
- 行為、態度、舉止或行動發生重大變化，如：
  - 越來越退縮。
  - 顯著和長時間的外觀惡化。
  - 毫無理由的憤怒或攻擊行為。
  - 酗酒/吸毒的跡象。
  - 犯罪活動。
  - 無法解釋的曠職。
- 對同事、單位、資產保全、實驗動物的福祉或公眾進行明示或暗示的威脅。

- 故意不遵守單位政策和 SOP，以及適用的法規和生安規範。
- 導致個人對其自身安全和可靠完成工作的能力產生擔憂的資訊。
- 看起來很可疑的情況，例如：
  - 與正式專案工作或目標不相符的實驗工作。
  - 對保全或實驗室資訊的無理要求。
  - 破壞行為或財產損失。
  - 企圖讓朋友或同事未經授權進入設施的某些部分；以及
- 在非上班時間內進行未經授權的工作。

單位應考慮拒絕或取消對那些表現出沒有能力安全處理或保護設施內的病原體、毒素或其他資產的人員授權。單位應訂定有關自我報告和同儕報告的政策，以及取消個人取得設施部分或資產的授權流程，或立即清除被認為構成不可接受的安全或保全風險的人員。所有人員都應得到關於所有政策和流程的明確指示。在某些情況下，匿名檢舉的方法可以鼓勵舉報，在訂定舉報政策和程序時應考慮到這一點。這些過程和程序應與單位的人力資源部門協商訂定。

4.3. 法規保全審查

由於與管制性病原及毒素相關的生物保全風險增加，有必要採取額外的生物保全措施，例如對取得管制性病原及毒素的人員進行保全審查，以減少潛在的內部威脅的風險。因此，保全檢查程序包括對在處理管制性病原及毒素或以其他方式取得管制性病原及毒素的設施中工作人員的額外要求。詳見疾管署「管制性病原及毒素管理作業規定」。

5. 病原體和毒素責任制和庫存清單管制

訂定病原體和毒素的責任制和庫存清單管制程序，是為追蹤和記錄單位內長期保存的所有病原體、毒素和其他受列管的感染性材料，以保護和保全這些資產免於遺失、遭竊、濫用、移轉和釋出。材料管制還包括對設施內的病原體或毒素進行盤點和安全移動，或將其運送到單位內的不同建築物或不同單位的程序。責任制和管制措施的等級由生物保全風險評鑑鑑別。

5.1. 病原體和毒素責任制

責任制是確立病原體和毒素所有權的一種方法，並確定每個被授權人員

對設施內病原體和毒素的監督責任。根據相關法規規定，所有被授權人員都要對其涉及病原體、毒素和其他被列管的感染性材料的行為和決定負責。該等人員也要對其主管、阻隔區或設施管理人員負責。

對於風險較高的病原體和毒素（即管制性病原及毒素、RG3 和 RG4 病原體），責任措施應包括定期進行庫存清單稽核，以查證庫存清單的準確性，並在適用情況下查證庫存清單材料或庫存清單未被篡改。可以經由以下方式實現：對庫存清單所列材料進行實物查證，在現場移動或移轉過程進行查證，經由閉路電視進行遠端觀察，或查證保存容器和設備上的封條或其他防篡改裝置。強有力的庫存清單管制程序可能包括進行定期分析，以確認容器內容物。保存所有人員的進出紀錄，以確認在任何時間點在阻隔區域內之人員名單。此一資訊可用於調查庫存清單遺失的病原體或毒素。

表 5-1：為減輕 BSL-2、BSL-3 實驗室和管制性病原及毒素區域內與責任有關的生物保全風險而實施的措施

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
病原體及毒素責任制	病原體或毒素在運輸途中遺失	・要求在運輸過程中對包裹進行追蹤的程序。 ・概述運輸過程中遺失病原體和毒素的報告架構和時限的程序。 ・通知衛生局、疾管署遺失病原體或毒素的程序。	・要求在運輸過程中追蹤包裹的程序。 ・概述運輸過程中遺失的病原體和毒素的報告架構和時限的程序。 ・通知衛生局、疾管署遺失病原體或毒素的程序。 ・要求托運人員確認接收人員收到材料的程序。	・要求在運輸過程中對包裹進行追蹤的程序。 ・對於在預期 24 小時內沒有收到管制性病原及毒素的報告架構的程序，包括強制通報疾管署。 ・要求托運人員確認接收人員收到材料的程序。

5.2. 庫存清單和庫存清單管制

根據生安規範第 4.10 節規定，需要對阻隔區域內長期保存（即超過 30 天）的病原體、毒素和其他列管感染性材料進行盤點，這也是生物保全

計畫的重要組成部分。此要求不適用於使用時間少於 30 天的材料（例如正在進行的感染性材料培養、長期動物感染研究）。庫存清單的要求和庫存清單資訊的詳細程度將與保存的材料相關風險和阻隔區域或設施的其他需求成正比（例如符合品質管理標準，例如國際標準組織 ISO 9001）。庫存清單可以採用任何形式（例如書面帳簿、電子資料庫或試算表），只要能準確反映設施內長期保存的病原體和毒素的存在。

對於長期保存的 RG2 病原體和毒素，只需記錄其位置和危險群等級即可。對於長期保存的 RG3、RG4 病原體和管制性病原及毒素，庫存清單必須包括病原體和毒素的具體標識，以及及時發現遺失或遭竊樣品的方法（例如建築物、房間和在冰櫃內的確切位置、小瓶數量的紀錄）。

雖然不要求維持保存時間少於 30 天的病原體和毒素的清單，例如最近收到的材料或正在使用的材料（例如培養物），但維持所有進入或離開阻隔區域的材料紀錄是最佳做法。

如果病原體或毒素遺失，即使是實驗室筆記或診斷活動紀錄（例如培養物）也是有其價值。

建議各單位對其庫存清單和進入紀錄進行審查，以查證在任何可疑活動或事故中可能被取得庫存清單的準確性。

對長期保存的病原體和毒素採取有效的庫存管理措施，可以成為阻止和偵測內部威脅的合適方式。實施強有力的病原體和毒素庫存管理和問責制度的注意事項包括：

- 指定具資格的人員負責維持庫存清單。
- 隨著材料的增加和移除，更新庫存清單。
- 記錄所有材料的移轉、去活性和處理情況。
- 掌握庫存清單所有病原體、毒素和其他列管感染性材料，包括保存在阻隔區域外的材料。
- 界定並記錄所有可以取得材料以及處理或保存材料區域的人員；
- 參考相關文件（例如病原體移轉授權、輸入許可證）。
- 對長期儲存的所有病原體、毒素和其他列管感染性材料進行適當的標識；以及
- 依順序給物品貼標籤（例如未依排序的小瓶很容易被偵測）。

與庫存清單相關的資訊保全等級應與所使用的病原體或毒素的危險群等級相關（例如 RG2 病原體與管制性病原體），並且至少要符合生安規範列出的要求。表 5-2 提供減輕與庫存清單管制有關的生物保全風險而可

能實施的措施範例。

表 5-2：為減輕 BSL-2、BSL-3 實驗室和管制性病原及毒素區域內與庫存清單管制有關的生物保全風險而實施的措施

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
庫存清單管制	沒有偵測到遺失的病原體或毒素。	·要求實驗室管理人員進行半年一次的庫存稽核和生安主管進行無預警稽核的程序。	·要求由生安主管進行半年一次的稽核和實驗室管理人員進行每季稽核的程序。	·要求由管制性病原及毒素主管進行半年一次的稽核和實驗室管理人員進行每季稽核的程序，及增加樣本量時的措施。

5.3. 移動和運輸期間的保全

生物保全計畫應包含政策和程序，說明在材料從一個地方移動或運輸到另一個地方時，保護病原體和毒素免受內部和外部威脅的責任措施。包括將病原體和毒素運送到另一設施，以及在同一建築物內將其從一個地點移動到另一個地點。

還可以建立程序管制，以減少與接收包裹相關的生物保全風險。包括人員訓練和訂定針對病原體或毒素的意外運輸的流程。所有包裹和物品在被移入或移出獲准進行列管活動的設施部分之前，都應進行查核。

有些設施可能有一個集中的接收區，由設施人員將所有包裹未開封送到收貨人員（接收人員）處。其他設施可能指定一個 "檢體接收區"，在該處打開含有病原體、毒素和其他感染性材料的包裹，記錄包裹的接收情況，並對檢體進行分類，以便移動（或運輸）到適當的人員或區域進行進一步處理或保存。如果在檢體接收區接收管制性病原及毒素（即打開管制性病原及毒素包裹），則接收區須是處理或保存管制性病原及毒素設施的一部分，當管制性病原及毒素存在現並可取得時，必須管制經核定的被授權人員進入該區。

病原體及毒素的所有移轉，無論是內部還是外部，即使在不需要向疾管署報告的情況下，都需要在移轉之前通知生安主管。

5.3.1. 內部移轉

在單位內部移轉病原體或毒素的設施應在生物保全計畫中描述如何進行移轉的政策和程序，包括保護病原體和毒素免於遭竊、遺失或釋出的規定（例如禁止將病原體和毒素留在公共區而無人看管的政策）。

如果是移轉 RG2 病原體和一般生物毒素，免經疾管署核准，但必須經生安主管審查及生安會核准；移轉 RG3 以上病原體，除經生安主管審查及生安會核准，須經疾管署核准後，始得為之。

材料移轉協定或類似的紀錄可用來記錄材料的所有權者，並在移動或移轉的每個環節負責。對於像管制性病原及毒素的高風險材料，簽名或監管鏈表(chain-of-custody sheet)將提供在移轉過程中所有持有人員的紀錄，並確認依法獲得許可。

5.3.2. 外部移轉及輸出

有關外部移轉 RG2 病原體和一般生物毒素，免經疾管署核准，但必須經生安主管審查及生安會核准；移轉 RG3 以上病原體，除經生安主管審查及生安會核准，須經疾管署核准後，始得為之。對於輸出感染性生物材料，應遵循疾管署「感染性生物材料暨傳染病檢體輸出入管理規定」（疾管署全球資訊網首頁>應用專區>申請>感染性生物材料輸出入>申請相關規定）

根據規定，在安排輸入或接收人類病原體或毒素之前，必須通知生安主管。如此，若在預期的合理時間內沒有收到包裹，就應進行了解。根據不同的快遞服務，托運人和收件人也可以使用快遞公司的線上工具追蹤包裹。此外，在訂定任何運送計畫之前，都要告知提供及接收單位的生安主管或管制性病原及毒素主管有關移轉事宜。例如接收單位如果未於預定送達時間收到、遺失，或是接收包裹發現有損毀、 品項短少等異常情形時，應於 48 小時內依規定方式通報疾管署。

6. 事故和緊急應變

事故是指有可能對人員、社區或環境造成傷害的事件。緊急應變計畫應包括及時有效應變可能影響阻隔區域生物保全情況的程序，這些情況可能包括無意或有意釋出病原體或毒素、天然災害、職場暴力、炸彈威脅、保全漏洞（例如未經授權進入、未經授權取得敏感資訊）和緊急情況（例如火災、

醫療緊急情況）等事件。表 6-2 提供減輕與事故和緊急應變有關的生物保全風險而可能採取的措施實例。

6.1. 事故報告

為報告事故而訂定的程序應符合適用的法規，以及單位內部事故報告和調查程序。事故報告和調查的 SOP 是設施緊急應變計畫的一個組成部分，在訂定時應補充或配合現有的設施範圍內的計畫（例如職業健康安全）。

生安規範規定，涉及病原體、毒素、其他列管感染性物質、受感染動物或阻隔系統或控制系統失效的事故，應立即報告給適當的內部負責部門，在某些情況下，應報告給所在地衛生局及疾管署。例如，如果有理由相信病原體或毒素已遭竊或遺失，應通報所在地衛生局及疾管署。

特別是以下生物保全事故應立即報告給單位內的負責人員或部門：

- 鑰匙、密碼、密碼組合、遠端存取設備（例如筆記型電腦、個人電腦和平板電腦）或其他關鍵保全資訊的任何損失或損壞。
- 未經授權進入或試圖進入管制進入區，例如保存管制性病原及毒素區，或 BSL-3 或 BSL-4 實驗室，或有敏感資訊區。
- 任何可疑的人員或活動。
- 任何遺失的具有雙重用途潛力的設備；以及
- 庫存清單中的任何差異，或有跡象顯示庫存清單被篡改或受到損壞。

設施應鑑別並記錄可能需要單位保全部門或當地執法機關及早介入的情況。

6.2. 事故應變規劃

及時、協調和有效應變嚴重和意外的特定情況，可能需要立即採取有計畫的應變措施，以減少對人員、社區和環境的傷害影響。因此，專門針對單位、設施和阻隔區域的生物保全相關事故應變計畫可以納入緊急應變計畫。表 6-1 列出一個成功的事故應變計畫的 5 個關鍵項目。

表 6-1：成功的事故應變計畫的 5 個關鍵項目

1. 重點是先保護人命，再保護財產。
2. 人員接受訓練，以便對事故作出快速有效的應變。
3. 設施人員和最先應變人員之間合作的結果。
4. 最先應變人員參與事故準備訓練。
5. 解決眼前的危險，以及對在該設施工作的人員的次要影響。

根據事故的性質，應變措施可能包括疏散或封鎖受影響區，通知最先應變人員，例如執法機關或緊急服務部門，評鑑事故的嚴重性（例如阻隔失效、暴露或釋出的可能性），防止再次事故，以及鑑別和保存證據鏈。每個事故都應該記錄，包括假警報。雖然”生物安全手冊”包含緊急應變計畫，但生物保全方面的內容需要在生物保全計畫的事故和緊急應變部分進行描述，或在計畫中提及緊急應變計畫。

表 6-2：為減輕 BSL-2、BSL-3 實驗室和管制性病原及毒素區域內與事故和緊急應變有關的生物保全風險而實施的措施

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
事故和緊急應變	未報告遭竊的病原體	・要求工作人員調查任何遺失病原體或毒素的程序。 ・如果在合理時間內沒有找到病原體或毒素，則通知生安主管。 ・生安主管將遺失的病原體或毒素通報所在地衛生局及疾管署。	・要求立即通知生安主管的程序。 ・生安主管將遺失的病原體或毒素立即通知所在地衛生局及疾管署。 ・生安主管調查任何遺失的病原體或毒素，並保存證據。	・要求立即通知管制性病原及毒素主管的程序。 ・管制性病原及毒素主管將遺失的病原體或毒素立即通知所在地衛生局及疾管署。 ・管制性病原及毒素主管調查任何遺失的病原體或毒素，並保存證據。 ・管制性病原及毒素主管對可疑的偷竊案件通知執法機關。
	未報告進入阻隔區域的鑰匙或鑰匙卡遺失或遭竊	・要求在合理時間內將遺失或遭竊鑰匙報告實驗室主管之程序。 ・在合理的時間範圍內更換或重配	・規定遺失或遭竊鑰匙應立即報告主管和保全之程序。 ・立即更換或重配鎖具。	・規定遺失或遭竊的鑰匙應立即報告給主管、管制性病原及毒素主管和保全之程序。 ・立即更換或重配鑰

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
		鎖具。	・遺失或遭竊的鑰匙卡在報告後立即停用。	匙。 ・在更換/重配鑰匙之前，採取替代性的臨時保全措施（例如將管制性病原及毒素轉移到另一個保全地點，或者放置在上鎖的保存設備內）。 ・遺失或遭竊的鑰匙卡在報告後立即停用。

6.3. 事故調查

生物保全事故可能顯示生物保全系統出現失效，也可能是人為錯誤的結果。調查和報告是必要的，以使設施能夠準確界定情況，確定事故發生的原因（即鑑別根本原因），是故意或是意外，是否為獨立事件，並採取矯正措施以防止日後發生類似事故。

事故發生後，可能不知道或不清楚是否為一起生物保全事故，如果事故是故意的，這可能是有目的的隱瞞。因此，在事故調查的所有危害方法中應考慮生物保全因素，以便不忽視重要證據。對任何事故的調查都應考慮故意行為的證據可能被故意隱瞞。在證據顯示情況並非如此之前，不應排除生物保全因素。如果事故有可能是犯罪行為的結果，那麼在早期階段須尋求執法機關的協助。

事故調查過程須系統化，一般包括以下幾個階段：

- 初始反應；
- 收集證據和資訊；
- 分析和鑑別根本原因；
- 訂定矯正和預防行動計畫；以及
- 評估和持續改進。

與生物保全有關事故的調查可能已經包含在與生物安全有關事故調查的 SOP 中，這些 SOP 包含在”生物安全手冊”中，或者可以作為專門針對

生物保全的特定 SOP 訂定。與其他 SOP 一樣，應定期審查和更新，以確保是最新和正確，並應指派專人負責。

根據事故性質和嚴重程度，可以指定專人進行調查，也可以為更複雜的情況組成調查小組。調查人員或小組應以開放的心態進行調查，不要對事故有任何先入為主的想法或意見。事故調查的範圍和深度可能有所不同，這取決於事故的嚴重程度。

7. 資訊管理和保全

生物保全計畫的一個組成部分是解決如何保護和保障與病原體和毒素有關的資訊資產。一個設施擁有許多不同類型的資訊可被認為是需要保護的資產，以防止遺失、遭竊、損壞或釋出。資訊保全的目標是保護資訊--對敏感資訊進行保密（例如關於設施中管制性病原體和毒素的資訊），保持所有資訊的完整性，並使其只被需要的人取得。

資訊保全的目的是保護所有形式的資訊資產，無論是紙本(hard-copy)、電子，還是人員保留的知識，同時只允許需要的人授權取得。資訊保全評鑑要考慮何人需要取得什麼資訊，以及用來保護與生物保全風險相當的資訊方法。表 7-1 提供減輕與資訊保全有關的生物保全風險而可能實施措施的範例。

7.1. 資訊資產

資訊資產可提供與人類和動物病原體、毒素和其他需要保護的列管感染性材料有關的資訊。與其他資產一樣，需要經由生物保全風險評鑑過程，根據資訊的價值（包括關鍵性及其被破壞或被釋出的敏感性）以鑑別和分類這些資訊。

了解哪些資訊需要保護以及保護到什麼程度，有助於維持工作人員有責任保護資訊的意識。在生物保全方面，資訊資產可能包括以下內容：

- 庫存清單；
- 生物安全和生物保全風險評鑑；
- 實驗流程和結果；
- 專有科學資訊（例如過程、技術、基因序列等）；
- 取得授權和日誌；
- 建築計畫；

- 人事紀錄和財務紀錄；以及
- 生物材料庫存清單和保存地點。

雖然生安規範要求生物保全計畫描述出現在”生物安全手冊”中，但完整詳細的生物保全計畫和生物保全風險評鑑可能需要保密，因為可能包含機密資訊（例如，關於保全系統、人員、病原體、程序）。

7.2. 資訊分類

對資訊進行分類將有助於確定所需的保全等級。以下類別僅作為範例參考，單位可能已經有分類系統，或選擇修改建議的類別。還要注意的是，某些資訊可能受到相關法規管制（例如個人資訊）：

- 公用--經適當核准後提供給一般公眾的資訊；
- 內部--不針對一般的資訊。例如資料分析和分發給其他人員審查的文件草案；。
- 限制或管制的取得--只針對被授權人員的資訊。資訊的發佈可能對單位產生負面影響。範例包括 SOP 和研究資料；以及
- 機密--資訊只提供給少數需要了解的被授權人員。資訊的發佈可能會損害設施保全或關鍵的阻隔系統。範例包括功能研究的雙重用途之獲得、關鍵的專有資訊和保全系統的細節。

資訊的分類在不同的單位中可能有所不同。如何做到這一點是由單位決定，這將取決於所持有資訊的類型。單位認為受管制的資料可能另一單位認為是機密。需要更高的保全性的資訊可能會導致巨大的成本（例如硬體、軟體、取得便利性）。應將資訊洩露造成的損失與實施減害策略的成本進行衡量。

7.3. 資訊保全

有效的資訊保全措施應從電子和非電子形式的資訊資產產生到其轉移、銷毀、刪除或處置，包括在資訊保存或轉移的過程中對其進行保護。有些設施可能傾向將資訊保全作為一個單獨的計畫維護，但在生物保全計畫中應包括對現有資訊保全措施的描述。資訊保全計畫的成功很大程度上依賴於管理階層的支持。訂定、實施和維護資訊安保全需要資源（人員、資金）以及所有人員的投入。

在任何一種情況下，都應該有專人或團隊負責資訊保全，這樣就可以定期（例如每月、每半年、每年）審查潛在的威脅和保全選項。包括隨時瞭

解最新的威脅（例如社會工程、惡意軟體、垃圾郵件、網路釣魚、駭客攻擊），並實施最新的因應措施（例如安裝防毒軟體和防火牆，通知人員網路釣魚的企圖，如果最近有保全漏洞或過去有多個保全漏洞，要求經常更改密碼）。

表 7-1：為減輕 BSL-2、BSL-3 實驗室和管制性病原及毒素區域內與資訊保全有關的生物保全風險而實施的措施

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
資訊保全	儲存在共用網路磁碟上的實驗室資料遭到破壞	・儲存在共用網路磁碟上的實驗室資訊被保存在存取控制資料夾中，只有實驗室人員可以取得(例如經由設施的通用用戶帳戶)。	・只有經由個人的帳號和密碼才能進入共用網路。 ・儲存在共用網路磁碟上的實驗室資訊被保存在管制取得的資料夾中，只有被授權的人員才能取得。	・取得共用網路需要雙因素認證(例如個人帳號和密碼與密碼鑰匙、網格卡、指紋相結合)。 ・高度敏感的管制檔案被加密或儲存在共用網路之外。 ・儲存在共用網路磁碟上的實驗室資訊保存在管制取得的資料夾中，只有經法規核准的被授權人員才能取得。 ・阻止對包含管制性病原及毒素紀錄的共用網路資料夾的遠端存取。 ・經由電子稽核日誌記錄對管制資料夾的取得和更改。
	遺失存有實驗室資料的 USB 快閃記	・限制使用 USB 快閃記憶體驅動器的政策和程序。	・限制使用 USB 快閃記憶體驅動器的政策和程序，並	・限制使用 USB 快閃記憶體驅動器的政策和程序，並要求每

保全計畫要件	風險	可能減害措施		
		BSL-2 實驗室	BSL-3 實驗室	管制性病原及毒素區
	憶體驅動器	·	要求使用密碼來保護文件。 ·遺失必須報告生安主管。	次使用都要得到核准。 ·使用加密的 USB 快閃記憶體驅動器。 ·遺失必須報告管制性病原及毒素主管和保全。

7.3.1. 政策和標準

訂定政策管理敏感資訊的鑑別、分類（例如專有、機密、管制）和處理，並解決如何收集、文件化、傳輸、保存、取得和銷毀資訊。關於網路使用和卸除式存放裝置介質（如 UBS 快閃記憶體驅動器）使用的政策可以為人員提供明確的資訊，說明對其使用的規定。良好的政策要簡單明瞭。例如遠端登入（例如從住家）到設施網路，只能使用安裝最新防毒軟體的設施筆記型電腦，必須使用強度大的密碼，並且不能將密碼寫在容易獲取的地方。可以使用保密協議禁止人員討論或發佈專有或保全敏感資訊。

7.3.2. 紙本資訊

實施 "清理辦公桌"政策，要求工作人員將敏感文件歸檔或妥善保管（即根據情況放在上鎖的辦公桌抽屜、辦公室檔案櫃、保全櫃、保險箱或其他保全傢俱內），這些文件可能包括實驗室筆記本、密碼資訊、資料和 SOP，這將防止未經授權的人員取得。另外，針對人員需要運輸敏感文件的情況以及複製技術（例如影印機、掃描器、照相機、行動電話和裝置）的使用訂定政策或程序，也有助於保護紙本中存在的資訊。敏感資訊應在工作站列印，並在列印後立即從印表機中取出，如果使用的是集中式印表機，則應使用鎖定列印選項進行列印。

7.3.3. 管制性病原及毒素資訊

要求限制授權人員取得與 RG3 和 RG4 病原體、管制性病原及毒素列管活動有關的紀錄和文件（生安規範第 4.10 節）。這也延伸到任何可能接觸到電子資訊的人員。雖然取得或管制管制性病原及毒素資訊的人員，例

如資訊技術管理人員，不需要經法規許可，但設施應考慮實施一項政策，以便只有被授權的人員才能取得該資訊。在科學出版刊物介紹與管制性病原及毒素相關的研究時，應考慮到雙重用途應用和資訊的敏感性（例如重建已絕跡病毒的複製程序）；然而，這些議題已超出本指引範圍。

7.3.4. 電子資訊保全

資訊技術保全是指對電子資訊的保護，如儲存在個人電腦、伺服器或可移動媒體上的資訊，或以電子方式傳輸的資訊。這包括雲端計算，可能需要額外的保全預防措施。

根據資訊的保全要求，將資訊儲存在保全網路上是可以接受的；但是，如果將敏感資訊加密儲存在可移動媒質（例如光碟或 USB 快閃記憶體驅動器）或僅以紙本形式儲存，並保存在只有被授權人員才能取得的安全地點，則更為安全。在沒有適當保護的情況下，這類資訊絕不應儲存在開放或共用的網路中。所選擇的儲存文件的地點應該只允許由單位確定需要取得（即"需要知道"）的被授權人員取得（例如生安主管、部門主管、實驗室主管）。儲存區應該有足夠的保全性，以防止資訊的損壞或遺失。含有過時或不再相關的敏感資訊的文件應根據指定銷毀材料的保全等級進行粉碎或銷毀。

除了資訊本身之外，還需要考慮資訊保全的其他方面。諸如 USB 快閃記憶體驅動器等可移動媒體很容易放錯地方，而筆記型電腦也很容易成為竊賊的目標。雖然所包含的資訊可能很難被未經授權的個人取得，但若遺失會對單位產生不良影響（例如庫存清單、被授權進入阻隔區域的人員名單）。

常用的裝置容易被隱藏起來，或者被認為是無害的（例如智慧型行動電話、個人數位助理(PDA)、USB 快閃記憶體驅動器、SD 記憶卡），對資訊保全構成一項弱點。這些裝置的問題在於能夠在微小的可移動媒體上儲存大量的資訊，可以很容易被攜帶進入設施而不被發現。此外，將檔案從家用電腦轉移到工作電腦有可能引入惡意軟體。設施應考慮將這些類型的裝置納入其資訊保全政策，認識其可能被濫用，並著眼於以適當的妥協減少這種風險。

以下關於電子資訊使用的注意事項可用於訂定政策或標準。

7.3.4.1. 一般的電子資訊保全

- 實施螢幕保護政策，在電腦或終端顯示器無人看管時，鎖定螢幕或退出，以防止未經授權的人員登入電腦。
- 對電腦或終端顯示器使用隱私螢幕，以防止同事或外人經由窗戶觀看。
- 鎖定敏感的電子檔案，使其成為 "唯讀"，以防止編輯。
- 瞭解可以共用的資訊類型，以防止無意間將此類資訊傳遞給未經授權的人員。執行關於可接受使用的電腦、網際網路和軟體安裝的政策，以防止無意間安裝惡意軟體、病毒和間諜軟體。
- 管制筆記型電腦的使用和遠端工作，例如避免使用不安全的 Wi-Fi 網路，只使用有防毒保護的裝置進行遠端存取，以協助保護電腦和區域網路（LAN）。
- 使用保全的資訊傳輸方法，例如經由電子郵件使用受密碼保護的檔案或加密，或使用傳真，以防止檔案發送到錯誤的位址。
- 將電腦和伺服器放置在保全區域，例如上鎖的區域網路壁櫥、上鎖的電腦或伺服器房間。在授予取得權之前對用戶進行驗證。根據保全要求，可以是需要用戶名和強式密碼的單因子驗證，或雙因子驗證，也需要使用使用者持有的實物（例如鑰匙、網路卡、USB 金鑰），或使用者的物理特徵（如指紋、聲音、眼睛）。
  使用保全網路，包括信譽良好的第三方供應商。
- 如果可行時，使用虛擬私人網絡（VPN）在辦公室或類似的地方進行通訊。

7.3.4.2. 區域網路保全

- 實施關於密碼政策（即創建一個高強度密碼，保護密碼，並定義更換密碼頻率）。
- 安裝網路防火牆以防止垃圾郵件和惡意軟體。
- 定期更新防毒軟體，以防止病毒入侵。
- 管制對網路磁碟和資料夾的取得，只有需要的人員才能取得，以增加敏感檔案的保全性。

7.3.4.3. 網際網路

- 只連結合法、可信的網站。雖然特定的網站可被防火牆遮罩，但管理員需要不斷地將新的網站添加到列表中，以使其有效。
- 訂定線上儲存（例如雲端儲存）和應用程式的使用政策。

- 查證網頁位址，或將連結複製並黏貼到流覽器搜尋引擎中，而非單純點擊。
- 使用網際網路保全套裝軟體。
- 不要修改或關閉防毒軟體等保全保障措施。
- 只向可信的保全來源提供個人或敏感資訊（例如只在保全供應商的網頁完成信用卡購買）。
- 依要求更新軟體，以便所有保全修復和防毒碼都是最新。
- 安裝防火牆。
- 使用管理選項，納入篩檢程式，以管制對外部網站的登入（過濾與未過濾的登入，僅授予授權人員登入）。

7.3.4.4. 電子郵件

- 訂定電子郵件管理政策。
- 安裝垃圾郵件篩檢程式。
- 勿點擊電子郵件中的連結。
- 對所有電子郵件帳戶實施嚴格的密碼設定標準。
- 勿將可能有害的電子郵件轉寄給其他人員。
- 保持人員被授權通過電子郵件發送哪些資訊之意識。
- 如果要經由電子郵件發送敏感檔案，須使用加密技術

7.3.4.5. 數據

- 將資料備份到一個保全的外部驅動器或遠端伺服器，以避免潛在的損失。這也可以防止意外的中斷（例如，硬體故障）。備份的頻率將取決於文件被修改的頻率。
- 將自動備份功能納入軟體。

7.3.4.6. 遠端存取

- 理想情況下，從遠端位置取得設施網路的人員應使用與路由器的直接連接（即乙太網路電纜）。如果要使用無線登入，只能使用保全的 Wi-Fi，並打開加密功能。
- 對用於遠端存取的電腦的登入應受到限制（例如不允許兒童和訪客使用該電腦）。

7.3.4.7. 行動電話和裝置

- 對待移動裝置和電話的保全預防措施與桌上型電腦或筆記型電腦相同。
- 使用系統登入密碼選項，並在不使用時將裝置鎖定。
- 使用裝置上的保全功能，如果有反惡意軟體，則安裝該軟體。
- 定期備份儲存在裝置上的資訊。

7.3.4.8. 數據儲存裝置

- 執行關於使用和運輸可移動電子儲存裝置的政策，如 USB 快閃記憶體驅動器、SD 記憶卡和可移動硬碟。

7.3.4.9. 相機和錄影裝置

- 對相機和錄影裝置（包括智慧行動電話）的使用以及此類資訊的傳播和公佈實施明確的政策

8. 生物保全計畫的實施、評估和改進

要訂定、實施、審查和改進必要的生物保全計畫，並維持更新。實施將涉及實體保全組件的安裝和測試，還包括對人員進行保全政策和程序的初步訓練，以及持續的生物保全意識。

在日常工作中，當發生可能影響生物保全的變化時，以及在應變生物保全事故時，對生物保全計畫的有效性進行評估，將有助於發現任何弱點環節和需要改進的地方。

8.1. 訓練

訓練是生物安全和生物保全的一個核心要素，對生物安全計畫的成功至關重要。工作人員需要了解與工作環境中存在的病原體和毒素有關的危害，包括任何相關的生物保全威脅，了解可以防止意外暴露或釋出病原體和毒素的規範和工具，並維護資產的保全。訓練可以解決個人的特殊需要，將從事的具體工作，以及設施中處理或保存的病原體和毒素所帶來的風險。

在人員獲准取得病原體和毒素之前，重要的是要了解並遵守設施訂定的所有生物保全流程（包括資訊保全）。生物保全要素應被納入現有的訓練計畫，並提供給所有被授權進入阻隔區域的人員。建議生物保全訓練包括

具體的保全流程和程序模組，以管制取得並防止病原體、毒素和其他資產的遺失、遭竊或破壞。應按照訓練需求評鑑確定的頻率或在實施過程和程序的變化時提供在職訓練。

8.1.1. 生物保全意識

人員的生物保全意識訓練使人員對角色和責任有清楚的認識，並對如何保護設施內的資產建立明確的期望。這種訓練是正在進行的可靠性評鑑計畫的一個重要組成部分，有助於發現和阻止其他內部和外部威脅。生物保全意識應該：

- 為人員提供鑑別、了解潛在影響和報告可疑活動的訓練，例如：
  - 使用造假身份證明；
  - 可疑的行為；
  - 遺失或遭竊的鑰匙、鑰匙卡或材料；
  - 不安全的行為。
- 概述組織的政策和程序，以保護敏感資訊；
- 包括關於鑑別可疑活動和人員或訪客行為變化的技術和指標的訓練；
- 告知員工不適當行為的後果；以及
- 提供關於保全規範和程序以及報告可疑事件和保全事故的說明。

生物保全意識在職訓練的建議主題包括：

- 鑑別可疑人員和應變措施（即報告、驅離）；
- 識別內部威脅；
- 陪同和監督程序；
- 關於緊急應變程序的在職訓練（生安規範第 4.3 節）；以及
- 審查單位內的事故報告或媒體公佈的事故，以總結經驗教訓。

持續的生物保全意識活動可以使人員了解最近的威脅，如企圖未經授權的取得，或關於新電腦病毒，同時提醒其責任。

8.1.1.1. 社交工程

社交工程往往只是一個複雜的欺詐行為的許多步驟之一。犯罪分子利用社交工程獲取資訊（例如個人資訊、密碼），這些資訊可用於取得資產或機密資訊。社交工程被使用是因為很有效。應訓練告知人員：

- 對詢問有關人員、其家人或敏感資訊的個人保持懷疑態度；

- 要求對任何進行不尋常詢問的人員身份進行查證；以及
- 向管理階層報告任何可疑的活動。

8.1.1.2. 資訊保全意識

保全意識計畫將使人員瞭解設施的保全規範、政策和標準。資訊保全應包括在訓練中，但資訊保全意識需要的不僅僅是訓練。雖然在最初的保全意識訓練可以在基本水準上介紹資訊保全的主題，但隨著時間的推移，應該擴大到包括更深入的訓練。人員應定期接受更新和提醒，以保持意識，並在必要時提高意識。

8.2. 保全系統的維護和測試

必須定期檢查與維護實體保全屏障有關的任何設備和程序，包括實體屏障本身，以查證其是否有效發揮功能。所有門禁系統、入侵偵測系統和鎖具的安裝、操作和維護都應符合製造商的規範。應在風險評鑑的基礎，定期（例如每月、每半年、每年）查證入侵偵測裝置的性能，以確認其持續有效運行，並將這些性能測試的紀錄存檔。電子系統的查證也應在停電期間進行，或審查這種情況的緊急流程。

8.3. 生物保全計畫的評估和持續改進

擁有生物保全授權的人員應定期審查並不斷改進生物保全計畫，以查證該計畫是否仍然相關、適用和有效。審查周期將取決於生物保全風險。例如對於低阻隔性（即 BSL-2 實驗室），審查可能只是確認生物保全風險保持不變（例如處理或保存的病原體和毒素沒有改變），並且在審查期間沒有發生與生物保全有關的事故，在這種情況下，每次審查生物保全風險評鑑時都需要進行深入的生物保全計畫審查。此外，在發生任何事故後，都應審查生物保全計畫，並根據鑑別的根本原因進行更新。

高階管理階層也可定期審查生物保全計畫，以確認現有計畫符合單位的需要，並繼續反映長期目標和目的。

審查將有助於解決與生物保全有關的廣泛問題，例如：

- 目前的計畫是否符合單位的需要?
- 所有 6 項生物保全要素是否都得到適當的處理?
- 所有適當的生物保全程序和過程是否已經就位?
- 工作人員是否接受充分的生物保全訓練?

・計畫是否需要更新（例如為因應變化或事件）?

・是否有足夠的資源維持生物保全?

審查期間發現的任何生物保全問題，可能需要經由更新計畫或實施新程序解決。