| **C級第二類學校資訊安全管理及防護具體作法** |
| --- |
| 資訊系統分類分級 | ISMS推動作業 | 資安專責人力 | 稽核方式 | 業務持續運作演練 | 防護縱深 | 監控管理 | 安全性檢測 | 資安教育訓練(一般主管、資訊人員/資安人員、一般使用者  | 專業證照 |
| 核心業務如有建置資訊系統，可參考行政院國家資通安全會報頒訂之資訊系統分類分級與鑑別機制參考手冊，視資源能力，建置必要之防護基準。 | 對核心業務之應用資訊系統進行資訊資產清查，檢視可能之風險，並視資源能力實施適當之管控作為。 | 應指派一員兼任人員，執行資訊安全管理相關業務 | 結合機關內部管理機制，每年辦理一次資訊安全自我檢查作業。 | 對核心業務應用資訊系統依實務需要訂定業務持續運作計畫，並每年至少一次定期檢視計畫適用性。 | 由各直轄巿及縣(巿)教育網路中心於網路收容節點，設置防毒及防火牆設備，集中實施資安防護。 | 結合臺灣學術網路資安監控系統(北區SOC、南區SOC、Mini-SOC、TACERT)或本部資安監控系統機制，進行資安預警情資、事件通報及應變處置。 | 核心業務如有運用資訊系統(或網站)，於系統建置或更新時，或每年至少辦理一次資安弱點檢測作業，並對弱點進行修復作業。 | (1)擔任資安業務人員應接受六小時資安專業課程訓練(包括行政院、教育部、各級教學機構、各區網中心及各直轄巿及縣(巿)教育網路中心等辦理之資安課程、訓練、講習等)，並獲得研習證明，以增進資安專業知識與能力。(2)一般使用者及主管至少應接受三小時資安宣導課程(包括機關自辦資安宣導講習、上級機關辦理之資安宣導課程)，以提升資安防護認知。 | 擔任資安業務人員每年至少參加一項資安專業訓練，並取得上課證明。 |