發佈通用技術規範　明確網安義務要求

第 13/2019 號法律《網絡安全法》已於 2019 年 12 月 22 日正式生效，為構建本澳網絡安全防範性管理體系奠定了法律基礎。法律明確規定關鍵基礎設施營運者須履行指定網絡安全負責人、制定管理制度和操作程序、採取措施預防、檢視和應對網絡安全事故等一系列維護其自身網絡安全狀況的義務和責任。但鑑於資訊科技發展日新月異，營運者須因應不同情勢，適時更新調整所需採取的防護機制及技術措施。為此，特區政府遵照適度立法原則，在《網絡安全法》這部基礎框架性法律中並沒有直接規範營運者就履行網安義務具體運作和技術要求，而是透過向營運者發出具約束力的技術規範來明確有關規定。

一、基於本澳實際環境，集思廣益制定技術規範

為明確關鍵基礎設施營運者就履行法定義務所需採取的具體技術措施及開展的網絡安全活動，並為各監管實體制定專屬的行業性技術規範提供基礎，由司法警察局、行政公職局及郵電局聯合組成的網絡安全事故預警及應急中心，自 2018 年中開始根據《網絡安全法》第三條，制定《網絡安全—管理基準規範》及《網絡安全—事故預警、應對及通報規範》等兩份適用於各領域行業營運者的通用性網絡安全技術規範。根據本澳實際環境，顧及中資及外資企業的背景差異，經參考國家等級保護制度、國際 ISO/IEC27001 網絡安全管理認證、以及周邊國家及地區的同類型制度，並經過先後兩次向監管實體及營運者徵詢意見並修訂完善後，上述兩份技術規範已於本年 5 月 13 日刊登於《澳門特別行政區公報》，並自 5 月 14 日起正式生效。

二、《網絡安全—管理基準規範》主要內容

《網絡安全—管理基準規範》旨在訂定關鍵基礎設施營運者在日常網絡安全管理和運作中，包括管理制度、操作程序、安全

措施、等級評定、風險評估等各方面的基本要求。其核心內容要求營運者根據各個資訊網絡和電腦系統對維持社會正常運作、保障市民合法權益的重要程度，評定系統的網絡安全保護等級並實施分級保護。營運者需要根據系統的保護等級，在“安全建設管理”、“安全運維管理”、“物理和環境安全”、“網絡和通訊安全”、“伺服器安全”、“應用和電腦數據資料安全”等六大面向範疇中，實施不同程度的安全保護規格。例如，評為“一般級”的系統需要滿足總共 46 項措施要求，而評為“高級”的系統則需要滿足總共 130 項措施要求，從而引導營運者將各類資源合理分配到所需之處，達致按需分級保護、妥善管控風險之目的。

三、《網絡安全—事故預警、應對及通報規範》主要內容

《網絡安全—事故預警、應對及通報規範》旨在訂定預警及應急中心、監管實體和營運者之間發出預警信息和接收事故通報的雙向溝通協調機制，並向營運者提供預防及應對網絡安全事故的一般性指引。其中，預警及應急中心負責從不同渠道收集與分析各類網安風險及威脅資訊，及時向營運者發出預警信息和處置建議，協助營運者防範事故發生。而當營運者不幸發生網安事故時，須根據事故的性質、對社會和市民造成的影響等因素進行評級，根據其嚴重性在規定時限內向預警及應急中心和監管實體作出通報，並定期匯報事故的應急處置工作進展情況，以便特區政府及時掌握相關最新資訊、協調事故處理、並於必要時提供適當的支援及協助，以盡量減輕事故對社會及市民所造成的損害。此外，營運者於完成事故的應急處置工作後，需向其監管實體提交事故的總結報告及改善計劃，避免同類事故再次發生。

四、持續優化本澳網絡安全防護能力

上述兩份通用性網絡安全技術規範作為營運者履行《網絡安全法》義務所需要採取的具體措施及開展各類網安活動的基本依據，能夠指導營運者建立一個事前規劃、事中執行、事後檢討及

改善的網絡安全管理閉環，逐步提升其網絡安全管理水平。隨著《網絡安全法》及兩份技術規範的有序落實執行，將能持續優化本澳總體的網絡安全防護能力，有效防範各類相關風險，確保關鍵基礎設施的資訊網絡和電腦系統能正常、安全運作，持續服務社會。