第 4046 號公告　　保險業條例 (第 41 章)

保險業監管局現依據《保險業條例》(第 41 章) 第 133(1) 條，刊登《網絡安全指引》(指引 20)。

上述指引將於 2020 年 1 月 1 日起開始實施。

2019 年 6 月 28 日　　保險業監管局行政總監張雲正

第 4046 號公告　　保險業條例 (第 41 章)

保險業監管局現依據《保險業條例》(第 41 章) 第 133(1) 條，刊登《網絡安全指引》(指引 20)。

上述指引將於 2020 年 1 月 1 日起開始實施。

2019 年 6 月 28 日　　保險業監管局行政總監張雲正

指引 20

網絡安全指引

保險業監管局

目錄 **頁數**

1. 引言

1.1 本指引由保險業監管局（“保監局”）依據《保險業條例》（第41章）（“該條例”）第133條發出。保監局的主要職能是規管與監管保險業，以保障現有及潛在的保單持有人。本指引旨在訂明獲授權保險人在網絡安全方面應達到的最低標準，以及保監局在評估保險人的網絡安全框架的成效時所採用的一般指導原則。

1.2 網絡風險是保險人所面對最主要的業務運作風險之一，尤其是關乎保險人以數碼和線上形式運作的業務。網絡安全事故可導致保險人財務損失、業務中斷、聲譽受損，並為其帶來其他負面影響。因此，本指引要求獲授權保險人建立具防衛力的網絡安全框架，以保障其業務數據及其現有或潛在的保單持有人的個人資料，並確保業務持續運作。

2. 釋義

2.1 在本指引中，除文意另有所指外：

(a) “關鍵系統”就獲授權保險人而言，指某個系統，而該系統的故障會令該保險人的業務運作受到重大干擾，或對該保險人向其現有或潛在的保單持有人所提供的服務造成重大影響；

(b) “網絡風險”指以電子方式，包括技術工具和平台（例如電腦系統、手機應用程式、互聯網及電訊網絡等），在傳輸、儲存、使用或處理數據的過程中所產生的任何風險。當中的風險包括數據違規與洩露、數據損失、由網絡安全事件造成該等數據的實體損壞、因濫用和在未獲授權的情況下存取數據而產生的欺詐行為、數據儲存與傳輸引致的法律責任、以及該等數據的可用性、完整性和機密性；

(c) “網絡安全”指關乎獲授權保險人的系統和業務運作上的保安的策略、政策、標準、常規、科技及創新。網絡安全包含以下各項的活動：降低威脅、減少安全漏洞、阻嚇、

國際性協作、事故應變、防衛及恢復等活動；

(d) “網絡安全事件”指威脅到獲授權保險人的系統安全的事件，包括數據在電子形式下洩露、拒絕服務攻擊、入侵受保護的資訊系統或數據資產、惡意破壞或竄改數據、濫用資訊系統、大規模感染惡意軟件、網站竄改、以及影響聯網系統的惡意程式；

(e) “海事相互保險人”指獲授權保險人只經營其成員間相互承保對方（指船東、承租人或經營船舶者或其他與航運業務有關的人士）與海事相關的風險的保險業務；

(f) “相關事件”指符合以下情況的系統失靈或網絡安全事件：對獲授權保險人的業務運作有嚴重且廣泛影響或對該保險人向其現有或潛在的保單持有人提供的服務造成重大影響；

(g) “系統”指任何數據、硬件、軟件、網絡、或屬於資訊科技基礎設施一部分的其他資訊科技部件；

(h) “系統失靈”指由網絡風險引致獲授權保險人的任何關鍵系統的故障。

2.2 除另有規定外，本指引中所使用的字詞及其涵義與該條例中該等字詞的涵義相同。

3. 本指引的效力和適用範圍

3.1 除專屬自保保險人和海事相互保險人外，本指引適用於所有獲授權保險人在香港或從香港經營的保險業務。

3.2 本指引應與該條例的相關條文、其他相關條例，以及根據該條例及其他相關條例訂立或發出的任何其他規則、規例、守則、通函及指引一併閱讀。

3.3 本指引不具法律效力及不應被詮釋為可凌駕於任何法律條文。不遵從本指引所載述的條文本身不會使獲授權保險人

在司法或其他法律訴訟中被起訴。然而，任何的不遵從可能會令保監局對適用於本指引的獲授權保險人的董事或控權人是否持續為適當人選有所影響。保監局亦可能參照本指引以考慮有否發生可能有損保單持有人或潛在的保單持有人利益的作為或不作為（儘管保監局會考慮與此相關的任何事項之所有資料、實際情況及影響）。

3.4 本指引旨在協助獲授權保險人識別和紓減網絡風險，其中所載的規定並非詳盡無遺，亦不構成專業意見。保險人應採取充足及有效、並與其業務的規模、性質和複雜程度相稱的網絡安全措施。保險人如對網絡安全或本指引相關的任何事宜有任何疑問，應尋求專業意見。

4. 網絡安全策略與框架

4.1 獲授權保險人應制訂和維持網絡安全策略與框架，而該策略與框架應以紓減與其業務性質、規模和複雜程度相稱的相關網絡風險而建構。該網絡安全策略與框架應經由該保險人的董事局審批。

4.2 保險人在制訂網絡安全策略與框架時，應考慮其業務性質、規模、複雜程度和風險狀況，並可參考或以科技及現有最佳並切實可行的質量保證標準作基準。該等標準的例子可包括國際標準化組織所訂立的資訊保安管理系統（ISO/IEC 27001），以及美國國家標準與技術研究院（National Institute of Standards and Technology）發出的《提升關鍵基礎設施網絡安全的框架》（Framework for Improving Critical Infrastructure Cybersecurity）。

4.3 網絡安全框架應清楚界定該保險人的網絡安全目標及對相關人員或系統使用者的能力要求。該網絡安全框架應包含清晰明確的流程及所需的技術，以管理網絡風險及適時將網絡安全策略傳達予所有使用者。

4.4 保險人應定期檢討並更新其網絡安全策略，以確保該策略在其業務經營模式和外在營商環境(包括外部網絡風險情況)發生重大轉變時仍然適用。例如，保險人應最少進

行每年一次的網絡安全策略檢討，或於該保險人發生網絡事故或外部發生重大網絡事件而有可能影響該保險人時，或於使用新系統或現時系統有重大改變時，保險人亦應檢討其網絡安全策略。

5. 管治

5.1 獲授權保險人的董事局應承擔網絡安全監控的整體責任，並清楚訂明有關網絡安全監控的職責、匯報和上報制度，以確保該保險人內部確實執行問責機制。董事局應培養公司上下對網絡安全持有強烈的警覺意識和責任感。

5.2 董事局應就該保險人的網絡風險設立已經清楚界定的風險偏好和容許限額，並監察相關網絡安全計劃的設計、實施和成效。董事局可成立指定的管理團隊，以監察並推行網絡安全措施和監控工作。該指定的管理團隊成員應具備掌握與管理網絡風險的適當技能和知識。如董事局成立指定的管理團隊，兩者皆有責任監察該保險人的網絡安全策略與框架的設計、實施和成效評估，並確保這些策略與框架不斷與時並進。

6. 識別、評估及控制風險

6.1 保險人應識別網絡風險，並評估紓減措施的成效，以便在董事局或其指定的管理團隊所訂定的風險偏好和容許限額的範圍內，抵禦並管理網絡風險。保險人應設立整體網絡風險管理計劃的自我評估工具，作為企業風險管理計劃的一部分。該評估應涵蓋：

(i) 識別業務職能、活動、產品和服務，並備存其資訊資產和系統配置的流動存貨紀錄或列表，包括與其他內部和外部系統之間的互相連接和對這些系統的依賴，以及就其相對重要性釐定優先次序；

(ii) 就每項被識別的職能、活動、產品和服務，評估源於使用者、流程與科技、及相關數據的固有網絡風險；

(iii) 分析網絡風險對業務的影響，即透過識別各種威脅、安全漏洞、可能性和影響，從而決定可能發生的風險和應變該等風險的緩急次序。

6.2 保險人應定期檢討網絡風險應對程序，並在組織與經營結構和系統有重大改動時評估該等程序有否必要作出變更。例如，保險人應每年進行一次檢討或於系統作出重大改動後進行檢討。

7. 持續監察

7.1 保險人應建立系統性監察程序，以便能及早偵測網絡安全事件、定期評估內部管控程序的成效、以及在適當情況下更新其風險偏好和容許限額。

7.2 保險人應制定有效的監察措施，當中包括網絡監察、測試、內部審計和外部審計等。

7.3 作為監察程序的一部分，保險人應管理在實地和遠程存取資訊資產時所需的身份和驗證資料。保險人應識別潛在網絡風險的信號，或監察在其系統中是否已發生確實違規情況。

7.4 保險人應最少每年測試一次其網絡安全框架的所有組成部分，以決定其整體成效。保險人可使用一個或多個最新的方法和常規，例如安全漏洞評估、情景為本的測試及滲透測試。

8. 應變與恢復

8.1 保險人應制訂一個網絡安全事件應變方案，涵蓋網絡安全事件的各種情景和相應的應變策略，以便在該等情景中維持並恢復各項關鍵功能和必要活動。應變方案亦應包括須向董事局或其指定的管理團隊上報該等應變和恢復活動的準則。

8.2 如發生網絡安全事件，保險人應評估該事件的性質、範圍和影響，並採取所有即時切實可行的措施，以控制該事件並紓減其影響。

8.3 保險人應通知內部持份者和外部持份者（如適用），並在有需要時考慮採取聯合應變行動。為此，保險人應最少每年進行一次事件應變演習。

8.4 在偵測到相關事件後，保險人應在切實可行範圍內盡快向保監局匯報該事件和相關資料，惟在任何情況下，該保險人須在偵測到該事件後的72小時之內向保監局匯報。

8.5 在業務運作恢復穩定後，保險人應在相關事件的恢復過程中，識別並紓減所有被利用的安全漏洞，並就該安全漏洞加以糾正以避免同類事件再發生。

9. 共享資訊與培訓

9.1 保險人應制定收集和分析相關網絡風險資訊的程序，並參與資訊分享小組（例如資訊共享平台），適時分享資訊，以便能即時採取適當預防措施，打擊本地和國際性的網絡攻擊及其他形式的網絡風險。

9.2 隨著網絡風險和安全漏洞急速演變，相應的網絡安全最佳常規和技術標準亦不斷進化。保險人應因應其面對的網絡風險的類別和程度，就網絡安全意識和網絡安全的最新發展，安排所有系統使用者接受充分培訓。保險人宜提升其員工（尤其是負責網絡安全和系統的員工）的專業勝任能力。

10. 生效日期

10.1 本指引自2020年1月1日生效。

2019年6月