附錄一

拍賣網站交易安全機制問卷

親愛的先生、小姐您好：

謝謝您百忙中協助填寫本問卷。這是一份學術研究問卷，目的在於瞭解線上拍賣之使用者對於拍賣網站所提供之交易安全保障是否感到滿意。

近年來，線上拍賣發展迅速，相信有許多人有線上拍賣購物的經驗。然而，在享受網路購物之便利性的同時，使用者往往面臨著隱私外洩、交易無法如預期完成以及網路安全威脅所造成的風險。一個好的線上拍賣交易平台，理論上必須提供良好的隱私、交易完整以及網路安全性的保護。因此，**只要您曾經參與線上拍賣、瀏覽過線上拍賣交易平台、或對於參與線上拍賣有興趣**，本研究希望借重您的經驗，對於目前線上拍賣交易平台所提供之隱私保護、交易完整以及網路安全的保障，提供寶貴的意見。

本問卷採不記名方式，所有資料僅供學術研究使用，敬請安心填答。

敬頌

指導教授：陳錦烽博士
碩士班研究生：范詠嵐
國立政治大學會計系
mail：g1353034@nccu.edu.tw

本問卷使用下列三專有名詞，為了幫助各位瞭解其意義，並順利填寫問卷，簡要說明如下：

1、隱私性：係指個人資訊免於被他人濫用於交易以外用途之情況。

2、完整性：係指買賣雙方交易能夠如雙方期望完成，並且免於詐欺的威脅。

3、安全性：係指個人資料及相關交易資料不會遭到不相關第三者之竊取、竄改。

一、網站的選擇及瞭解

1. 在選擇一個拍賣網站進行交易時，您認為下列因素之重要程度為何？

- 拍賣的物品價格普遍較別處低廉

□非常重要□有點重要□普通□不太重要□非常不重要

- 符合需求之物品選擇多

□非常重要□有點重要□普通□不太重要□非常不重要

- 交易成本低

□非常重要□有點重要□普通□不太重要□非常不重要

- 參與拍賣的買（賣）家人數多

□非常重要□有點重要□普通□不太重要□非常不重要

- 名聲響亮

□非常重要□有點重要□普通□不太重要□非常不重要

- 廣告吸引人

□非常重要□有點重要□普通□不太重要□非常不重要

- 網站對於個人隱私性保護佳

□非常重要□有點重要□普通□不太重要□非常不重要

- 該拍賣網站妥當維持交易完整性

□非常重要□有點重要□普通□不太重要□非常不重要

- 該網站能夠保證傳輸資料的安全

□非常重要□有點重要□普通□不太重要□非常不重要

- 交易平台易於操作

□非常重要□有點重要□普通□不太重要□非常不重要

- 其他考量要因素_____

□非常重要□有點重要□普通□不太重要□非常不重要

2. 您在註冊為一拍賣網站之會員時，您會對該網站的經營政策作何程度的瞭解？ □非常深入 □有點深入 □普通 □非常有限 □不在乎是否了解

以下的問題，請您假想選擇某一拍賣網站作為評估標的。您所選擇的拍賣網站為：□YAHOO！ □eBay □其他：_____

二、網路平台使用面

1. 你所選擇的拍賣網站所提供的交易平台簡單且容易上手操作：
   □非常同意 □有點同意 □普通 □有點不同意 □非常不同意
2. 您在使用該拍賣網站的交易平台時，若遇操作上的困難，可於網站上得到立即的教學或指示：
   □ 非常同意 □有點同意 □普通 □有點不同意 □非常不同意

三、隱私性（Privacy）*係指個人資訊免於被他人濫用於交易以外用途之情況*

1. 在該網站註冊時，您是否會擔心所提供之個人資料遭到盜用？
   □非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
2. 您是否贊同該網站應由會員自行決定所提供之個人資料，而非由網站強制規定？□非常贊同 □有點贊同 □普通 □不太贊同 □完全不贊同
3. 您是否贊同個人資料需要修正時，可由會員自行更改所有的資料？
   □非常贊同 □有點贊同 □普通 □不太贊同 □完全不贊同
4. 您欲註冊為一拍賣網站之會員時，會對該網站所提供的隱私性保護政策進行何程度的瞭解？
   □非常瞭解 □有點瞭解 □普通 □不太瞭解 □完全不瞭解
   （若勾選「完全不瞭解」者，請直接跳答第 6 題。）
5. 您認為該拍賣網站目前所提供的隱私性政策是否完善？
   □非常完善 □有點完善 □普通 □有點不完善 □非常不完善

6. 您是否滿意該拍賣網站對您所提供的隱私性保護？
□非常滿意 □有點滿意 □普通 □有點不滿意 □非常不滿意
7. 您是否信任該拍賣網站會徹底落實其隱私權政策？
□非常信任 □有點信任 □普通 □有點不信任 □非常不信任
8. 當您發現個人隱私性資料有遭到危害之可能性時，是否仍會於該網站交易？
□仍會於該處繼續交易 □暫時不於該處交易□再也不在該處交易

四、完整性（Integrity）

係指買賣雙方交易能夠如雙方期望完成，並且免於詐欺的威脅。

1. 您是否會擔心從事網路拍不交貨的情況？
□非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
2. 在該網站交易時，您是否會擔心賣方謊報商品的品質以及合法性或是寄發與其實際描述不符的商品？
□非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
3. 在該網站交易時，您是否會擔心他人可能有一個以上的帳號，而藉此從事干預拍賣機制之行為（如：哄抬物價...等）？
□非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
4. 在該網站交易時，您對該拍賣網站上買賣方的評價紀錄信任程度為何？
□非常信任 □有點信任 □普通 □有點不信任 □非常不信任
5. 您欲註冊為一拍賣網站之會員時，您會對該網站對交易過程所提供之保障進行何種程度的瞭解？
□ 非常瞭解 □有點瞭解 □普通 □不太瞭解 □完全不瞭解
（若勾選「完全不瞭解」者，請直接跳答第 7 題。）
6. 您認為本拍賣網站目前所提供的完整性政策是否完善？
□非常完善 □有點完善 □普通 □有點不完善 □非常不完善
7. 您是否滿意本拍賣網站對您所提供的完整性政策？
□非常滿意 □有點滿意 □普通 □有點不滿意 □非常不滿意
8. 您是否信任本拍賣網站會徹底執行其完整性政策？
□非常信任 □有點信任 □普通 □有點不信任 □非常不信任
9. 當您於交易時遭到詐欺之後，您是否仍會於該網站交易？
□仍會於該處繼續交易 □暫時不於該處交易□再也不在該處交易

五、安全性（Security）

係指個人資料及相關交易資料不會遭到不相關第三者之竊取、竄改。

1. 在該網站交易時，您是
□非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
2. 在該網站交易時，您是否會擔心自己的註冊資料以及交易資料（包含買賣家評價資訊）會被第三者竊取或竄改？
□非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
3. 在該網站交易時，您是否會擔心當資料傳輸時會被第三者竊取？
□非常擔心 □有點擔心 □普通 □不太擔心 □完全不擔心
4. 您欲註冊為一拍賣網站之會員時，您會對該網站所提供的傳輸過程安全性的保護政策達到何程度的瞭解？

□ 非常瞭解 □有點瞭解 □普通 □不太瞭解 □完全不瞭解

（若勾選「完全不瞭解」者，請直接跳答第 6 題。）

5. 您認為本拍賣網站目前所提供的安全性政策是否完善？
   □非常完善 □有點完善 □普通 □有點不完善 □非常不完善
6. 您是否滿意本拍賣網站對您所提供的安全性政策？
   □非常滿意 □有點滿意 □普通 □有點不滿意 □非常不滿意
7. 您是否信任本拍賣網站會徹底執行其安全性政策？
   □非常信任 □有點信任 □普通 □有點不信任 □非常不信任
8. 當您發現個人資料遭到安全性之危害時，是否仍會於該網站交易？
   □仍會於該處繼續交易 □暫時不於該處交易□再也不在該處交易

六、綜合評量

1. 整體而言，該拍賣網站是值得信賴的。
   □非常同意 □有點同意 □普通 □有點不同意 □非常不同意
2. 整體而言，使用該拍賣網站進行交易是明智之舉。
   □非常同意 □有點同意 □普通 □有點不同意 □非常不同意
3. 基於您過去的經驗以及對網站的瞭解，以後是否仍有意願再次（或開始）於拍賣網站上進行交易？
   □非常願意 □有點願意 □普通 □有點不願意 □非常不願意
4. 基於您過去的經驗以及對該網站的瞭解，您是否願意推薦您的親友於該網站交易？□非常願意 □有點願意 □普通 □有點不願意 □非常不願意

七、基本資料

1. 您過去是否曾於拍賣網站上進行過交易？ □曾 □未曾
2. 過去於拍賣網站上進行的交易次數為？
   □未曾 □1 次 □2~9 次 □10～29 次 □30～49 次 □50 次及以上
3. 您的性別：□男 □女
4. 您的年齡： □18 歲以下 □18 歲（含）～25 歲 □25 歲（含）～30 歲 □30 歲（含）～40 歲 □40 歲（含）～50 歲 □50 歲（含）以上
5. 每週上網時數： □1 小時以下 □1（含）～5 小時 □5（含）～10 小時 □10（含）～15 小時 □15 小時（含）～20 小時 □20（含）小時以上
6. 您的職業：□學生 □軍警 □公、教人員 □商 □工 □農 □自由業 □家管 □其他：_____
7. 您的教育程度： □國中及以下 □高中職 □專科 □大學 □研究所及以上

附錄二

Trust Service Criteria

一、安全性

（一）政策：企業必須訂定並書面化其系統安全性政策。

1、企業需建立並且由指派之個人或小組定期審閱及核准企業之安全性政策。

2、企業之安全性政策必須包含，但不限於下列之項目：

（1） 辨識並且將安全性政策與對授權使用者之相關要求書面化。

（2） 允許接近並定義接近的本質及誰被授權接近。

（3） 避免未授權的接近。

（4） 增加新使用者、變更現有使用者的接近程度，以及移除不存在使用者之程序。

（5） 劃分線上隱私及相關安全之責任。

（6） 劃分系統變更及維護之責任。

（7） 系統元件在使用前必須先行測試、評估及授權。

（8） 聲明如何處理與安全性有關之抱怨，以及使用第三者爭議處理機制之程序。

（9） 處理破壞安全性之事件之程序。

（10）處理未於安全政策中提及之例外情況之條款。

（11）提供支援安全性政策之訓練及其他資源。

（12）辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。

3、企業安全性政策及其之變更、更新之責任必須妥善劃分。

（二）溝通：企業必須向授權使用者溝通其所訂定之系統安全性政策。

1、 企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。

2、 使用者之安全義務及企業對使用者之安全性承諾必須與授權使用

者溝通。

3、 企業安全性政策及其變更、更新之責任必須溝通與企業內對其有責並執行該政策者。

4、 向授權使用者溝通通知企業有關系統安全遭受破壞之情形以及提出抱怨之程序。

5、 影響系統安全之變更必須向會受其影響之管理者及使用者溝通。

（三）程序：企業為依循其政策達成其安全性目標之程序。

1、 存在限制邏輯性接近系統，包括但不限於下列各項：

（1） 新使用者之註冊及授權。

（2） 辨識所有使用者。

（3） 變更及更新使用者資訊之程序。

（4） 准許接近系統特權及允許之程序。

（5） 有機密資訊之輸出需限制分配，僅可予授權使用者。

（6） 限制邏輯接近離線儲存、備份資料、系統及媒體。

（7） 限制接近系統架構、超級使用者功能、主密碼以及安全機制。

2、 存在限制實體接近系統，包括但不限於設備、備份媒體以及其他如防火牆、終端機、伺服器等系統元件之程序。

3、 存在保護系統免於未授權者邏輯接近之程序。

4、 存在保護免於電腦病毒、惡意程式以及未授權軟體破壞之程序。

5、 使用者之辨識及相當之資料於網際網路上傳輸時，使用加密或是相當之安全技術保護之。

6、 存在對破壞安全性事件之辨識、報導及回應程序。

7、 當發生不符安全性政策時必須迅速的辨識並且及時的採取應變措施之程序。

8、 設計、取得、執行、配置、修改及管理與安全性有關之架構及軟體必須與訂定之安全性政策一致，以確保授權之接近以及避免未授權之接近。

9、 存有程序規定個人對影響安全性之系統之設計、發展、建置及操作之責任。

10、 存有保護系統元件，包括與訂定之安全性政策一致之架構之程序。

11、 存有程序規定系統僅可接受授權、經測試且書面化之變更。

12、 存有要求緊急變更需書面化及授權之程序。

（四）監督：企業監督系統並且採取適當之行動以維持其符合安全性之政策。

1、 企業之安全性表現必須定期的檢視並與其所訂定之安全性政策相比對。

2、 可辨識並指出對企業目前達成其安全性政策目標之潛在危害。

3、 監控環境及科技之變更並評估其對企業安全性之影響。

二、可取得性

（一）政策：企業必須訂定並書面化其系統可取得性政策。

1、企業需建立並且由指派之個人或小組定期審閱及核准企業之系統可取得性及相關安全政策。

2、企業之系統可取得性及相關安全政策必須包含,但不限於下列之項目：

（1） 辨識並且將系統可取得性政策與對授權使用者之相關安全要求書面化。

（2） 允許接近並定義接近的本質及誰被授權接近。

（3） 避免未授權的接近。

（4） 增加新使用者、變更現有使用者的接近程度，以及移除不存在使用者之程序。

（5） 劃分可取得性及相關安全之責任。

（6） 劃分系統變更及維護之責任。

（7） 系統元件在使用前必須先行測試、評估及授權。

（8） 聲明如何處理與系統可取得性及相關安全有關之抱怨。

（9） 處理破壞系統可取得性及相關安全事件之程序。

（10）處理未於系統可取得性及相關安全政策中提及之例外情況之

條款。

（11）提供支援系統可取得性及相關安全政策之訓練及其他資源。

（12）辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。

（13）依據與顧客之承諾或其他協定之復原及繼續服務計畫。

（14）監控系統產能以滿足與顧客承諾及約定之系統可取得性。

3、企業系統可取得性及相關安全政策及其之變更、更新之責任必須妥善劃分。

（二）溝通：企業必須向授權使用者溝通其所訂定之系統可取得性政策。

1、 企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。

2、 使用者於系統可取得性及相關安全之義務及企業於系統可取得性及相關安全之承諾必須與授權使用者溝通。

3、 企業系統可取得性及相關安全政策及其變更、更新之責任必須溝通與企業內對其有責並執行該政策者。

4、 向授權使用者溝通通知企業有關系統可取得性及系統安全之破壞情形及提出相關抱怨之程序。

5、 影響系統可取得性及系統安全之變更必須向會受其影響之管理者及使用者溝通。

（三）程序：企業為依循其政策達成其訂定之系統可取得性目標之程序。

1、 保護系統免於遭受中斷運作或是損害系統可取得性風險之程序。

2、 備份、離線儲存、復原及災害回復需符合系統可取得性及相關安全政策之程序。

3、 維持資料備份及系統的完整性以遵循系統可取得性及相關安全政策之程序。

4、 存在限制透過電子商務之邏輯性接近個人資料之程序，包括但不限於下列各項：

（1） 新使用者之註冊及授權。

（2） 辨識所有使用者。

（3） 變更及更新使用者資訊之程序。

（4） 准許接近系統特權及允許之程序。

（5） 限制接近系統架構、超級使用者功能、主密碼以及安全機制。

5、 存在限制實體接近存有保護透過電子商務所收集之個人資訊之企業系統，包括但不限於設備、備份媒體以及其他如防火牆、終端機、伺服器等系統元件之程序。

6、 存在系統免於未授權者邏輯接近之程序。

7、 存在保護免於電腦病毒、惡意程式以及未授權軟體破壞之程序。

8、 使用者之辨識及相當之資料於網際網路上傳輸時，使用加密或是相當之安全技術保護之。

9、 存在對系統可取得性及相關安全破壞事件之辨識、報導及回應程序。

10、 當發生不符系統可取得性以及相關安全政策時必須迅速的辨識並且及時的採取應變措施之程序。

11、 設計、取得、執行、配置、修改及管理與系統可取得性及安全有關之架構及軟體必須與訂定之系統可取得性及相關安全政策一致。

12、 存有程序規定個人對影響系統可取得性及安全之系統之設計、發展、建置及操作之責任。

13、 存有保護系統元件，包括與訂定之系統可取得性及相關安全政策一致之架構之程序。

14、 存有程序規定系統僅可接受授權、經測試且書面化之變更。

15、 存有要求緊急變更需書面化及授權之程序。

（四）監督：企業監督系統並且採取適當之行動以維持其符合系統可取得性政策。

1、 企業之系統可取得性及安全表現必須定期的檢視並與其所訂定之線上隱私與相關安全政策相比對。

2、 可辨識並指出對企業目前達成其系統可取得性及相關安全政策目標之潛在危害。

3、監控環境及科技之變更並評估其對企業系統可取得性及安全之影響。

三、處理之完整性

（一）政策：企業必須訂定並書面化其系統處理完整性政策。

1、企業需建立並且由指派之個人或小組定期審閱及核准企業之處理完整性及相關安全性政策。

2、企業之處理完整性及相關安全性政策必須包含,但不限於下列之項目：

（1） 辨識並且將處理完整性政策與對授權使用者之相關安全要求書面化。

（2） 允許接近並定義接近的本質及誰被授權接近。

（3） 避免未授權的接近。

（4） 增加新使用者、變更現有使用者的接近程度，以及移除不存在使用者之程序。

（5） 劃分系統處理完整性及相關安全之責任。

（6） 劃分系統變更及維護之責任。

（7） 系統元件在使用前必須先行測試、評估及授權。

（8） 聲明如何處理與系統處理完整性及相關安全有關之抱怨，以及使用第三者爭議處理機制之程序。

（9） 處理破壞系統處理完整性及相關安全事件之程序。

（10）處理未於系統處理完整性及相關安全政策中提及之例外情況之條款。

（11）提供支援系統處理完整性及相關安全政策之訓練及其他資源。

（12）辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。

3、企業系統處理完整性及相關安全政策及其之變更、更新之責任必須妥善劃分。

（二）溝通：企業必須向授權使用者溝通其所訂定之系統處理完整性政策。

1、 企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。如果是電子商務系統，則需另於網站上揭露其他的資訊。該資訊包括但不限於下列各項：

（1） 商品或服務之描述：

a、貨品的資料

b、服務的描述

c、資料來源

（2） 其經營電子商務之政策及條約，包含但不限於下列各點：

a、完成交易之時間限制。

b、通知顧客非以平常方式處理訂單或服務之時間限制或程序。

c、運送貨品或服務之一般方式。

d、付款條約。

e、相關之服務費用。

f、取消循環費用。

g、退貨政策以及限制條款。

（3） 企業於其網站上揭露顧客可從何處取得售後服務保障、維修服務以及其他於網站上購買之貨物或服務之相關支援。

（4） 有關解決處理完整性議題之程序。此處理程序可包含顧客交易之任何一環節，包含對商品或服務品質、正確、完整、以及無法適當處理抱怨之抱怨。

2、 使用者之系統處理完整性及相關安全義務及企業對使用者之系統處理完整性及相關安全性承諾必須與授權使用者溝通。

3、 企業系統處理完整性及相關安全性政策及其變更、更新之責任必須溝通與企業內對其有責並執行該政策者。

4、 向授權使用者溝通通知企業有關系統處理完整性之爭議、錯誤或是遺漏、系統安全之破壞以及提出抱怨之程序。

5、 影響系統處理完整性及系統安全之變更必須向會受其影響之管理者及使用者溝通。

（三）程序：企業為依循其政策達成其系統處理完整性目標之程序。

1、 關於完整、正確、及時及授權輸入之程序與訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項。

（1） 檢查每個要求及交易之正確性及完整性。

（2） 在交易處理前取得顧客正面確認。

2、 關於完整、正確、及時及授權系統處理之程序，包括錯誤更正及資料庫管理，需與企業所訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項。

（1） 正確的貨品及數量在要求的時限內送達，服務及資訊亦如顧客要求之提供。

（2） 例外情況需立即與顧客溝通。

（3） 傳入之訊息皆正確及完整的處理並發送至正確的 IP 位址。

（4） 輸出之訊息皆正確及完整的處理並發送至網際網路服務提供者之存取點。

（5） 當訊息於服務提供者之網路傳輸時，必須確保其密封完整。

3、 關於完整、正確、及時及授權輸出之程序，需與企業所訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項。

（1） 企業於處理交易前向顧客列示售價及其他相關之成本、費用。

（2） 發出交易帳單。

（3） 立即更正帳單或付款錯誤。

4、 有追蹤資料從來源輸入至最後處置之程序。

5、 存在限制邏輯性接近系統，包括但不限於下列各項：

（1） 新使用者之註冊及授權。

（2） 辨識所有使用者。

（3） 變更及更新使用者資訊之程序。

（4） 准許接近系統特權及允許之程序。

（5） 輸出僅限分配予授權使用者。

（6） 限制邏輯接近離線儲存、備份資料、系統及媒體。

（7） 限制接近系統架構、超級使用者功能、主密碼以及安全機制。

6、 存在限制實體接近系統，包括但不限於設備、備份媒體以及其他如防火牆、終端機、伺服器等系統元件之程序。

7、 存在保護系統免於未授權者邏輯接近之程序。

8、 存在保護免於電腦病毒、惡意程式以及未授權軟體破壞之程序。

9、 使用者之辨識及相當之資料於網際網路上傳輸時，使用加密或是相當之安全技術保護之。

10、 存在對破壞安全性事件之辨識、報導及回應程序。

11、 當發生不符系統處理完整性及相關安全性政策時必須迅速的辨識並且及時的採取應變措施之程序。

12、 設計、取得、執行、配置、修改及管理與安全性有關之架構及軟體必須與訂定之系統處理完整性及相關安全性政策一致，以確保授權之接近以及避免未授權之接近。

13、 存有程序規定個人對影響處理完整性及安全性之系統之設計、發展、建置及操作之責任。

14、 存有保護系統元件，包括與訂定之系統處理完整性及相關安全性政策一致之架構之程序。

15、 存有程序規定系統僅可接受授權、經測試且書面化之變更。

16、 存有要求緊急變更需書面化及授權之程序。

（四）監督：企業監督系統並且採取適當之行動以維持其符合安全性之政策。

1、 企業之安全性表現必須定期的檢視並與其所訂定之安全性政策相比對。

2、 可辨識並指出對企業目前達成其安全性政策目標之潛在危害。

3、 監控環境及科技之變更並評估其對企業安全性之影響。

四、線上隱私性

（一）政策：企業必須訂定並書面化其保護由電子商務所蒐集之個人資訊之政策。

1、企業需建立並且由指派之個人或小組定期審閱及核准企業之隱私

及相關之安全政策。

2、企業之線上隱私及相關安全政策必須包含，但不限於下列之項目：

（1） 辨識並且將隱私權政策與對授權使用者之相關安全要求書面化。

（2） 允許接近並定義接近的本質及誰被授權接近。

（3） 避免未授權的接近。

（4） 增加新使用者、變更現有使用者的接近程度，以及移除不存在使用者之程序。

（5） 劃分線上隱私及相關安全之責任。

（6） 劃分系統變更及維護之責任。

（7） 系統元件在使用前必須先行測試、評估及授權。

（8） 聲明如何處理與線上隱私及相關安全有關之抱怨，以及使用第三者爭議處理機制之程序。

（9） 處理破壞線上隱私及相關安全事件之程序。

（10）處理未於隱私及相關安全政策中提及之例外情況之條款。

（11）提供支援線上隱私及相關安全政策之訓練及其他資源。

（12）辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。

（13）提供顧客有關於資訊收集之警告。

（14）提供顧客選擇收集資料的種類。

（15）允許顧客更新、更正其資訊。

（16）述明資料保存及銷毀之政策。

3、企業線上隱私及相關安全政策及其之變更、更新之責任必須妥善劃分。

（二）溝通：企業必須向內部或外部使用者溝通其所訂定之保護個人資料之政策。

1、 企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。

2、 線上隱私及相關安全之義務及承諾必須與授權使用者溝通，並揭露於網站上。這些揭露包含但不限於下列各項：

（1） 特定類型之資訊之蒐集、保存、使用以及分配與第三者之可能性。如果資訊將提供予第三者，需揭露第三者隱私政策及控制可靠性之限制，否則則代表該第三者之政策及控制可靠性與企業相當或是更勝於企業。此處所述第三者可能包括：

a、參與完成交易之第三者。

b、與交易無關之第三者。

（2） 顧客有權選擇其提供何資訊以及該資訊之使用及分配方式，而這些選擇並不可影響其交易。

（3） 在收集及傳送電子商務交易所需之敏感性資料時，顧客必須有權選擇是否繼續。

（4） 顧客拒絕提供資訊或是選擇不使用特定資訊之後果。

（5） 收集的個人資料在必要時如何檢視、更正及移除。

3、 如果企業網站使用 Cookies 或是其他追蹤方式，企業必須揭露其使用方式。如果顧客拒絕使用 Cookies，必須揭露其拒絕之後果。

4、 向授權使用者溝通取得支援及通知企業有關線上隱私及系統安全之破壞情形之程序。

5、 企業需揭露當企業無法解決隱私議題時，顧客可採取之請求權程序。這些議題包括收集、使用及分配個人資訊以及企業無法解決這些議題之後果。此解決程序可包含下列特徵。

（1） 管理者顧客不滿企業解決方式時，對於採用特定第三者爭議排解服務或其他法令規定之方式之承諾。

（2） 解決爭議之程序。

（3） 當爭議解決之後，需對個人資訊做何使用及採行哪些步驟。

6、 企業揭露其他需符合之法律、法規或任何企業參與之自我約束計畫之其他隱私策略。

7、 當企業之隱私權政策有變更或廢止之情事時，必須提供顧客清楚且明顯的政策變更警告。

8、 當顧客離開企業隱私權政策所涵蓋之網頁時，必須有適當警告。

9、 企業線上隱私及相關安全政策及其變更、更新之責任必須溝通與企業內對其有責並執行該政策者。

10、 影響線上隱私及系統安全之變更必須向會受其影響之管理者及使用者溝通。

（三）程序：企業為依循其政策達成其隱私目標之程序。

1、 企業之程序規定個人資訊僅提供予與交易相關之個體,除非顧客再提供資訊之前有接收到明顯的警告。若於提供資訊實無清楚之警告，在提供資訊予第三者前亦必須取得顧客之同意。

2、 企業之程序規定經電子商務收集之資料僅由員工使用於企業經營。

3、 企業於收集、製作或保存個人資訊時，有編篡及驗證之程序。

4、 企業有取得認證或表示將資料提供予之第三者,其資料保護及隱私政策與企業所揭露之隱私政策一致之程序。

5、 下載之檔案及資訊於使用者電腦上儲存、變更或複製前，必須取得顧客之同意。

（1） 如果顧客指出其不希望使用 Cookies，則企業必須控制確保 Cookies 並未存於顧客之電腦。

（2） 企業要求顧客允許其於顧客電腦上儲存、變更或複製資訊。

6、 揭露之隱私政策廢止或變更時,企業必須有適當的程序依循其提供資訊當時之政策保護個人資訊，或是取得顧客依循新政策之同意。

7、 存在限制透過電子商務之邏輯性接近個人資料之程序,包括但不限於下列各項：

（1） 新使用者之註冊及授權。

（2） 辨識所有使用者。

（3） 變更及更新使用者資訊之程序。

（4） 准許接近系統特權及允許之程序。

（5） 禁止顧客、個人或其他企業接近不屬於其本身之機密資料。

（6） 機密性資料之接近僅限於有相關職責之授權員工。

（7） 有機密資訊之輸出需限制分配，僅可予授權使用者。

（8） 限制邏輯接近離線儲存、備份資料、系統及媒體。

（9） 限制接近系統架構、超級使用者功能、主密碼以及安全機制。

8、 存在限制實體接近存有保護透過電子商務所收集之個人資訊之企業系統，包括但不限於設備、備份媒體以及其他如防火牆、終端機、伺服器等系統元件之程序。

9、 存在保護電子商務系統免於未授權者邏輯接近之程序。

10、 存在保護免於電腦病毒、惡意程式以及未授權軟體破壞之程序。

11、 使用最少128位元之加密或其他相關安全技術以保護使用者於網際網路傳輸其辨識資料及其他個人資料。

12、 存在對隱私及相關安全破壞是件之辨識、報導及回應程序。

13、 當發生不符線上隱私以及相關安全政策時必須迅速的辨識並且及時的採取應變措施之程序。

14、 設計、取得、執行、配置、修改及管理與線上隱私及安全有關之架構及軟體必須與訂定之線上隱私及相關安全政策一致。

15、 存有程序規定個人對影響線上隱私及安全之系統之設計、發展、建置及操作之責任。

16、 存有保護系統元件，包括與訂定之線上隱私及相關安全政策一致之架構之程序。

17、 存有程序規定系統僅可接受授權、經測試且書面化之變更。

18、 存有要求緊急變更需書面化及授權之程序。

（四）監督：企業監督系統並且採取適當之行動以維持其符合保護個人資訊之政策。

1、 企業之隱私及安全表現必須定期的檢視並與其所訂定之線上隱私與安全政策相比對。

2、 可辨識並指出對企業目前達成其隱私及安全政策目標之潛在危害。

3、 監控環境及科技之變更並評估其對企業線上隱私及安全之影響。

五、機密性

（一）政策：企業必須訂定並書面化其保護資訊機密性之政策。

1、企業需建立並且由指派之個人或小組定期審閱及核准企業之系統機密及及相關之安全政策。

2、企業之機密及安全保護必須包含，但不限於下列之項目：

（1） 辨識並且將機密性及對授權使用者相關安全要求書面化。

（2） 允許接近並定義接近的本質及誰被授權接近。

（3） 避免未授權的接近。

（4） 增加新使用者、變更現有使用者的接近程度，以及移除不存在使用者之程序。

（5） 劃分線上隱私及相關安全之責任。

（6） 劃分系統變更及維護之責任。

（7） 系統元件在使用前必須先行測試、評估及授權。

（8） 聲明如何處理與機密性及相關安全有關之抱怨。

（9） 處理破壞機密性及相關安全事件之程序。

（10）處理未於機密性及相關安全政策中提及之例外情況之條款。

（11）提供支援機密性及相關安全政策之訓練及其他資源。

（12）辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。

3、企業機密性及相關安全政策及其之變更、更新之責任必須妥善劃分。

（二）溝通：企業必須向內部或外部使用者溝通其所訂定之保護機密資訊之政策。

1、 企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。

2、 機密性及相關安全之義務及承諾於機密性資料提供時，必須與授權使用者溝通。這些溝通包含但不限於下列各項：

（1） 資訊如何分類為機密資訊。

（2） 授權如何接近機密資訊。

（3） 如何使用機密資訊。

（4） 如果資訊提供予第三者，需揭露第三者機密性策略及控制之限制，否則則代表企業信賴第三者之機密性策略予其相當或更勝之。

（5） 機密性政策需符合相關法律與法規。

3、 企業機密性及相關安全政策及其變更、更新之責任必須溝通與企業內對其有責並執行該政策者。

4、 向授權使用者溝通通知企業有關機密性及系統安全之破壞情形及提出抱怨之程序。

5、 影響機密性及系統安全之變更必須向會受其影響之管理者及使用者溝通。

（三）程序：企業為依循其政策達成其機密性目標之程序。

1、企業程序規定機密資訊僅揭露與規定於機密性及相關安全政策內者。

2、企業有取得認證或表示將資料提供予之第三者,其機密性政策與企業所揭露之機密性及相關安全政策一致之程序。

3、揭露之機密性政策廢止或變更時,企業必須有適當的程序依循其提供資訊當時之政策保護機密資訊，或是取得顧客依循新政策之同意。

（1） 新使用者之註冊及授權。

（2） 辨識所有使用者。

（3） 變更及更新使用者資訊之程序。

（4） 准許接近系統特權及允許之程序。

（5） 禁止顧客、個人或其他企業接近不屬於其本身之機密資料。

（6） 機密性資料之接近僅限於有相關職責之授權員工。

（7） 有機密資訊之輸出需限制分配，僅可予授權使用者。

（8） 限制邏輯接近離線儲存、備份資料、系統及媒體。

（9） 限制接近系統架構、超級使用者功能、主密碼以及安全機制。

4、 存在限制邏輯性接近機密資料之程序，包括但不限於下列各項：

5、存在限制實體接近特定之系統,包括但不限於設備、備份媒體以及其他如防火牆、終端機、伺服器等系統元件之程序。

6、存在保護系統免於未授權者邏輯接近之程序。

7、存在保護免於電腦病毒、惡意程式以及未授權軟體破壞之程序。

8、使用最少 128 位元之加密或其他相關安全技術以保護使用者於網

際網路傳輸其辨識資料及其他機密資料。

9、存在對機密及相關安全破壞是件之辨識、報導及回應程序。

10、 當發生不符機密性以及相關安全政策時必須迅速的辨識並且及時的採取應變措施之程序。

11、 設計、取得、執行、配置、修改及管理與機密性及安全有關之架構及軟體必須與訂定之機密性及相關安全政策一致。

12、 存有程序規定個人對影響機密性及安全之系統之設計、發展、建置及操作之責任。

13、 存有保護系統元件，包括與訂定之機密性及相關安全政策一致之架構之程序。

14、 存有程序規定系統僅可接受授權、經測試且書面化之變更。

15、 存有要求緊急變更需書面化及授權之程序。

（四）監督：企業監督系統並且採取適當之行動以維持其符合機密性政策。

1. 企業之機密及安全表現必須定期的檢視並與其所訂定之機密性與安全政策相比對。
2. 可辨識並指出對企業目前達成其機密及安全政策目標之潛在危害。
3. 監控環境及科技之變更並評估其對企業機密性及安全之影響。