供應商的資訊安全管理基準

Ver. 1.03

松下電器產業株式會社

調達本部

資訊安全本部

2006年12月1日

目　錄

Ⅰ・　松下集團的資訊安全基本方針

松下電器產業株式會社以及相關公司（以下，總稱爲“本公司”）的目標在於，按照經營基本方針，透過卓越的技術、產品以及服務，使顧客滿意並取得顧客的信賴。因此，我們要認識到以顧客的資訊、個人資訊、財產資訊爲首的資訊的保護是非常重要的，我們應將資訊安全定位爲經營的重要戰略之一，並按照如下要求加以推進，以努力實現健全的資訊化社會。

1・資訊安全體制

在各組織建立資訊安全的責任體制，透過製定和實施必要的規程，致力于適當的管理。

2・資訊資產的管理

爲了確保資訊的安全，要根據資訊的重要性及其風險明確處理方法，進行適當的管理。

3・教育和培養訓練

對全體董事以及員工，要持續實施資訊安全相關教育和培養訓練，以期提升資訊安全意識並貫徹資訊安全相關各規程。對于違反規程者，要加以懲戒，嚴正處理。

4・提供可讓顧客放心的產品和服務

考慮到被使用的顧客資訊的安全，努力做到提供令顧客放心的產品和服務。

5・遵守法令和持續改善

在遵守相關法令和其它的規範的同時，根據環境的變化持續地加以改善和提升，以確保資訊安全。

Ⅱ・　遵守保密合約

對于與本公司共享的資訊，應按照基本交易合約以及各單項合約中的保密規定，採取萬無一失的措施。　＊ 參見基本交易合約書第 34 條（保密）。

Ⅲ・ 供應商資訊安全基準

1・ 目的

製定該基準的目的在于，本公司作爲以實現健全的資訊化社會爲目標的全球企業，能夠致力于透過推進適當的資訊安全，正確地處理和管理顧客資訊、個人資訊、(技術、品質、產品和服務等方面的)資訊資產，進而不斷地發揮企業的社會責任，特別是在供應商的資訊管理方面，透過本基準的製定，明確相關的工作基準，使得共享本公司機密資訊的供應商能夠遵守基本交易合約以及各單項合約中的保密規定，要求其實施與本公司同等的資訊安全。

透過建立可正確管理和利用資訊的環境，使本公司以及供應商能夠放心、安全且高效地開展工作，實現事業的持續穩定發展和相互繁榮。

2・適用範圍

該基準適用于本公司指定的由共享機密資訊的供應商進行的相應資訊的處理、管理以及其他業務(技術移轉、業務委托、資材購買活動等)。

機密資訊的形態包括文件、電子化資訊、經驗技術、試製品/模具等所有包含機密資訊的物質形態。

關於須進行更加嚴格管理的絕密資訊和重要資訊等，也適用保密合同等追加管理對策。

3・ 對供應商的資源安全要求事項

(1) 建立可有組織地推進資訊安全的體制。

(2) 明確須進行機密管理的資訊，並基于規則進行機密管理。

① 明確由本公司指定的機密資訊以及使用此機密資訊創造出的機密資訊

② 機密資訊的交接相關管理規則
(本公司與供應商之間以及供應商與委託對象之間)

③ 工作部門的訪問管理(物理安全和出入相關管理規則)

④ 資訊資產的帶出、帶入相關管理規則(個人電腦以及同等的客戶機終端(以下簡稱“電腦”)、筆記本電腦、帶攝影功能的手機、PDA、半導體儲存卡和 USB 儲存器等(以下簡稱“電子媒體”)、文件)

⑤ IT 系統的訪問管理(ID 和密碼的管理規則)

⑥ IT 系統(包括電腦)的設置以及廢棄相關管理規則

⑦ 對非法程式和電腦病毒的管理規則

⑧ 爲了確保事業可持續性的備份相關管理規則

(3) 實施保密合同等可防止資訊洩露的人的對策。

① 實施資訊安全的教育和培育訓練

② 與員工等簽訂保密合同書

（4） 明確發生資訊安全事故時的處理方法並加以實施。

① 確立事故報告和處理體制

② 製作事故處理手冊

③ 製定並實施防止事故再次發生的對策

（5） 實施可持續推進改善活動的資訊安全 PDCA。

① 實施自我檢查，以確認資訊安全是否得以正確實施

② 基于自我檢查結果建立改善的體制

4・實施

2007 年 4 月 1 日以後，對于與不符合本基準的供應商間的機密資訊共享（技術移轉、業務委托、資材購買等），由於無法確保資訊資產的適當安全，故將被限制。

5・ 詳細的要求事項

（1） 建立有組織地推進資訊安全的體制。

1-1	建立資訊安全管理相關組織體制。
1-2	製定資訊安全相關規則的書面文件。
1-3	對于組織內的資訊安全實施項目，要明確資訊管理負責人及相關任務和責任

（2） 確定須進行機密管理的資訊，基于規則進行機密管理。

① 明確由本公司指定的機密資訊以及使用此機密資訊創造出的機密資訊

2-1 明確機密資訊	
2-1-11	製作本公司製定的機密資訊以及利用該資訊創造出的機密資訊的管理列表，使機密資訊明確化。。
2-1-22	對于管理列表中的機密資訊進行適當的安全管理。。
2-1-33	由資訊管理負責人定期地對管理列表以及管理的實際狀況進行重審。

② 機密訊息的交接相關管理規則

2-2 對于交換機密資訊的管理	
將與本公司共享的機密資訊，與業務合作伙伴（對于本公司來說的二級以後的供應商等）、委託對象以及派遣相關公司（以上，總稱爲“委託對象等”）之間進行交換時，應基于以下的管理規則進行安全管理。	
2-2-1	製作與供應商共享機密資訊的委託對象等的管理列表。
2-2-2	應與委託對象等簽訂包括如下規定的條款在內的保密合約（或包括了保密條款的合約）。 a.) 成爲保密對象的資訊的範圍 b.) 保密義務期限(也包括無限期) c.) 使用目的的限制 d.) 訪問者應限定爲在業務上須了解該資訊的人員（Need To Know） e.) 對指定重要機密資訊的管理方法 f.) 限制對指定重要機密資訊進行複製 g.) 規定在保密期限期滿後返還或廢棄 h.) 由本公司進行保密相關確認（提問和監查等）措施的規程 i.) 違反合同時的措施（除了損害賠償以外，還要加入可使停止在市場銷售等的條款） j.) 禁止擅自進行再委託

2-2-3	與本公司和供應商一樣，在供應商和委託對象等之間也要製定機密資訊的交換相關規則。 a.) 由本公司交給供應商的資訊，原則上，均作爲內部資訊處理（禁止對第三方公開）。 b.) 須交換和公開機密資訊時，要事先取得本公司的認可后再實施。 c.) 以電子文件的形式發送和接收機密資訊時，要實施加密。
2-2-4	對于供應商和委託對象等，要定期地實施資訊安全的實際狀況調查。
2-2-5	要記錄供應商與委託對象等之間交接機密資訊的情況。 a.) 發生了資訊資產的交接時，要決定與對方交接的規則，製作協議書。 b.) 已進行了實際的通信（交接）記錄並實施了管理。
2-2-6	包括了資訊的返還和回收的規則。 a.) 明確業務結束時的返還和回收的方法、期限及資訊管理負責人等。
2-2-7	要基于規則實施交換、返還和回收。
2-2-8	透過電子商務交易系統、圖紙的交接系統等進行固定的資訊交換時，雙方之間應就步驟和運用方法等的保密對策達成協議並加以實施。 a.) 進行發信/接收，發送/收領及其通知的步驟 b.) 資訊的記錄/讀取、包裝以及傳送相關方法 c.) 數據丟失后的責任以及保證

③ 在工作部門的訪問管理

2-3 物理管理	
進行機密資訊的管理時，對于與本公司共享的機密資訊，要基于以下的物理管理規則進行管理。	
2-3-1	爲了能夠限制無關人員進入公司區域、建築物以及房間內而進行了區域區分。
2-3-2	完善限制進入的物理架構。
2-3-3	只許可須了解資訊的人員進入。 a.) 僅限資訊管理負責人判斷爲在業務上必要的人員/情況下，才允許入室。 b.) 取得出/入室兩者或其中之一的日誌。
2-3-4	必要時，須設置圍牆、ID 卡認証、監視攝影機、感應器等。 ※例子 重要區域 ： 利用監視攝影機監視入口處，出入室管理則透過 ID 卡認証取得日誌。 業務區域 ： 入室管理透過 ID 卡認証取得日誌。
2-3-5	定期地對圖像和進出日誌進行監查。
2-3-6	全體員工在公司內部都配戴姓名卡 。 a.) 要掌握外部人員進入時的狀況。
2-3-7	建立了僅限需要了解資訊的人員訪問機密資訊的體制。 a.) 機密資訊要上鎖保管于文件櫃中。 b.) 對試製品要進行數量管理，並將訪問限制爲最低限度。

④ 資訊資產的帶出/帶入相關管理規則

2-4 帶出、帶入（文件、電子媒體、電腦）以及廢棄的管理。	
2-4-1	禁止在業務目的以外將電子媒體帶入處理機密資訊的場所。 a.) 要帶入時，須得到資訊管理負責人的許可。
2-4-2	在工作中不得使用私人電腦，並且，禁止將私人電腦帶入。
2-4-3	對于工作中需要使用的電子媒體和電腦，製作管理表。
2-4-4	對于工作中需要使用的電子媒體和電腦，製作帶出規則，並加以實施。 a.) 原則上，禁止帶出電腦，對于帶出的電腦要實施加密、設置多重密碼等
2-4-5	決定記載有重要機密資訊的紙張（文件）的廢棄步驟。 a.) 對于機密資料，要用碎紙機進行裁切、溶解或燒毀。
2-4-6	決定了機密資訊以及機密資訊載體的廢棄步驟。 a.) 對于設計資訊等的技術載體，要進行破壞以無法讀取資訊。 b.) 要與處理工業廢品的企業簽訂 NDA 合同。

⑤ IT 系統的訪問管理

2-5 IT 系統的使用者 ID 和密碼的管理	
在對與本公司共享的機密資訊進行電子化管理時，關於對電子化資訊的訪問，應基于以下的管理規則進行安全管理。	
2-5-1	訪問電子化資訊時，每個人要使用自己單獨的 ID 和密碼，並取得誰訪問了與本公司共享的機密資訊的記錄。
2-5-2	製定了 ID 的發行規則。 a.) 用戶不與其他的用戶共用 ID。 b.) 規定 ID 的發行步驟和資訊管理負責人許可。
2-5-3	製定了密碼的管理規則。 a.) 密碼同時包含有英文和數字，在 6 個字符以上。 b.) 密碼須定期地變更，至少要每 30 天變更一次 c.) 不得將密碼借給其他人
2-5-4	要定期地實施 ID 重審。 a.) 對是否存在離職者的 ID、臨時使用的 ID 等、未被使用的 ID 以及不正當的 ID 進行檢查。

⑥ IT 系統（包括電腦）的設置以及廢棄相關管理規則

2-6 電腦、伺服器等 IT 系統的設置以及廢棄的管理	
2-6-1	在與網際網路之間設置合適的防火牆，將業務上必要的資訊設備和電腦連接于安全的公司內部系統內。
2-6-2	已決定了設置 IT 系統時的手續。
2-6-3	已決定了 IT 系統的管理/使用規則。 a.) 資訊要保管在伺服器上，而並非個人電腦裡。

	b.) 人員離開座位時，要將筆記本電腦上鎖保管于辦公桌的抽屜裡、櫃子等中。 c.) 桌上型電腦等的固定式電腦，要用電腦鎖固定在辦公桌等的上面。 d.) 帶出的電腦內的資訊要實施加密，在萬一被盜時，可避免資訊被讀取。 e.) 帶出電腦期間，應隨時帶在身邊。 f.) 對 BIOS、OS、螢幕保護程式設定密碼。 可設定爲，在 5 分鐘內無輸入的狀態下，可透過帶密碼的螢幕保護程式鎖定螢幕。離開座位時，要鎖定螢幕或退出系統。
2-6-4	決定了 IT 系統的廢棄和再使用規則。 a.) 製定了將硬碟內的資訊完全刪除或進行物理破壞的規則。
2-6-5	伺服器設置在了可確保安全的合適場所。
2-6-6	對于伺服器管理場所的出入進行限制。 a.) 保管機密資訊的伺服器設置在實施了安全管理的區域，上鎖管理于帶門的架子上。此外，還進行與此同等的管理。

⑦ 對非法程式和病毒的管理規則

2-7 非法程式的對策	
2-7-1	針對電腦病毒和非法程式，製定了相應的對策和規則。 由系統管理員（或提供單位）指定防病毒軟體（殺毒軟體）的種類和版本等，並加以引進。
2-7-2	實施了病毒和非法程式的對策和規則。 a.) 使防病毒軟體常駐于規定的各設備中，始終確保完全受保護的環境。 b.) 設置爲至少每天更新一次（推薦每隔一定時間進行自動更新）病毒定義。 c.) 對于被保存的所有文件，進行每周掃描一次以上的設定。
2-7-3	製定有病毒對策實施狀況的自我檢查表和體制。
2-7-4	製定相應規則，以使受病毒的危害被控制在最小限度。 a.) 包括感染病毒時的物理處理和報告、通知方法等。
2-7-5	禁止安裝和使用 Peer to Peer 軟體（Winny、Share 等的文件交換軟體）。
2-7-6	定期確認是否安裝了禁止軟體。 a.) 由資訊管理負責人檢查，或使用檢測工具等。

⑧ 爲了確保事業可持續性的備份相關管理規則

2-8 實施備份	
2-8-1	製定了備份的規則。 a.) 對于重要系統，研究了備份的必要性和頻度。 b.) 確保了事業的可持續性。
2-8-2	按照規則定期地實施了備份。
2-8-3	製定備份數據的保管規則，並按照規則實施管理。 a.) 要能夠確認處理機密資訊的資訊系統的所有備份媒體均得以正確的管理。

（3） 實施保密合同等的可防止資訊洩露的人的對策。

① 實施資訊安全的教育和培育訓練

3-1 資訊安全的啓蒙、教育以及培育訓練	
3-1-1	製定資訊安全的教育計畫。 a.) 關於資訊安全，製定有進行員工教育的體制（錄影、指導手冊、研修等），且製定了教育計畫。
3-1-2	對組織責任人或項目主管等的管理者定期實施安全教育，並整理好聽講記錄。
3-1-3	對所有公司員工和派遣員工實施資訊安全教育，此外，委託對象也應對委託進行業務的員工實施同樣的資訊安全教育，並製作聽講記錄。 a.) 在入社、調入和升職等時，均實施資訊安全教育以及定期教育。 b.) 在接收員工時以及接收後，均應適當實施。
3-1-4	製作對規則進行自我檢查的檢查表，由全員實施。
3-1-5	建立可對自我檢查結果的不合格點進行改善的體制。 a.) 組織責任人定期地確認自我檢查結果，當出現不符合規定的事項時，要指導改善並記錄。
3-1-6	自我檢查表中加入了清理桌面（應注意整理整頓，禁止將機密文件放在桌上）、清理螢幕（離開座位時，應設定爲不顯示螢幕或啓用帶密碼的螢幕保護程式）的規則 。

② 與員工等簽訂保密合同書

3-2 與員工等簽訂合同書	
3-2-1	就業規則中有關於保密的條款，取得員工簽署的保密合同書。
3-2-2	派遣員工在上班前應取得保密合同書。 a.) 進行與公司員工等同等的保密管理，並對誓約書進行管理。
3-2-3	委託業務時，委託對象要取得員工簽署的保密合同書。 a.) 委託對象要進行保密管理，並對合同書進行管理。

（4） 明確發生資訊安全事故時的處理方法並加以實施。

① 建立事故報告和處理體制
② 作事故處理手冊
③ 製定並實施防止事故再次發生的對策

4-1	設置了事故發生時的聯絡/處理的資訊管理負責人，建立事故報告體制。 a.) 要建立相應的體制，以在發現資訊安全上的問題或感覺到發生的危險時，或目擊了事件事故或發現了事件事故的痕跡時，能夠迅速向貴公司的資訊管理負責人報告。
4-2	對于與本公司共享的機密資訊，在發現了上述的問題以及事件事故或感覺到發生的危險時，要迅速向本公司通報。 a.) 規定了報告管道、從事故發生到通報爲止的時間等，並加以貫徹。
4-3	完備發生了資訊安全事故時的處理手冊，明確步驟。 a.) 把握受害狀況和使受害影響最小化的緊急處理 b.) 查明原因和暫定措施 c.) 應採取相應措施，以在資訊洩露時可向該第三方報告等，可實現相關者能夠進行自衛和相關處理。 d) 必要時，應進行宣傳處理，向相關政府機關報告
4-4	記錄事故的經過和處理的過程。
4-5	要迅速實施防止事故再次發生的對策，並貫徹周知。

※資訊安全事故的例子：

資訊的洩露、非法訪問、非法獲取、病毒事故、

喪失可用性（系統故障、資料被破壞等）、喪失完整性（資料被篡改、刪除）

（5） 實施可持續地推進改善活動的資訊安全 PDCA。

① 實施自我檢查，以確認資訊安全是否得以正確實施
② 基于自我檢查結果建立改善的體制

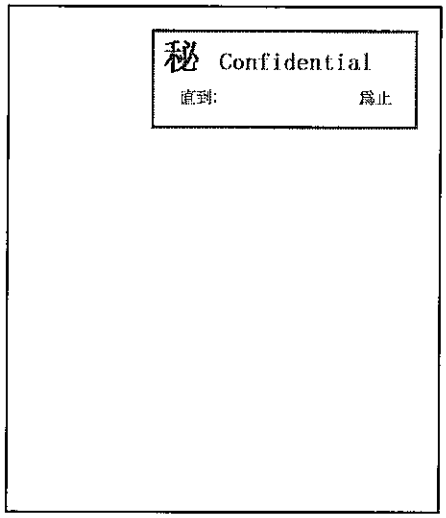
5-1	規定了有組織的資訊安全活動的自主檢查內容。 a.) 透過自主檢查，應可以檢查資訊安全規則是否被遵守。 b.) 包括附則檢查表中的項目。
5-2	有組織地定期實施自主檢查。 a.) 每 6 個月實施 1 次以上的檢查。
5-3	針對自主檢查的結果、明確了的不符合事項，製定了改善計畫。 a.) 由資訊安全擔當者製定包括改善內容、擔當者和時期等在內的改善計畫，取得資訊管理負責人的認可后實施。

附則

1・ 本基準自 2006 年 12 月 1 日開始施行。

2・ 由本公司指定適用本基準的機密資訊的方法。

標誌舉例



按照 1～4 中的任意一種方法進行指定。

1. 在文件的右上角標示了“秘 Confidential”的機密資訊。
2. 在圖片上標示了“秘 Confidential”的機密資訊。
3. 文件名爲
   秘－文件名　或 C-文件名的機密資訊。
4. 另行指定爲機密資訊的機密信資訊。

3・ 檢查表

請使用本檢查表實施自我檢查，並定期報告。

附表 1：供應商資訊安全基準檢查表