目錄Table of content

1. 目的PURPOSE

本規定之目的為使上詮光纖通信(以下簡稱上詮)於資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件造成之損害。
The purpose of this regulation is to enable Shangquan Optical Fiber Communications (hereinafter referred to as Shangquan) to report promptly and in accordance with procedures when an information security incident occurs, and to take necessary contingency measures and establish an incident learning mechanism to reduce the damage caused by the incident.

2. 範圍SCOPE

本公司之資訊安全事件管理
Our company's information security incident management.

3. 權責RESPONSIBILITY

3.1. 系統資訊管理處部門人員System Information Management Department

研擬資通安全事件通報流程。須執行資通安全事件之分析及處理。
Develop a notification process for information security incidents. Analysis and handling of information security incidents must be performed.

3.2. 系統資訊管理處主管 Head of System Information Management Office

需針對申請人經申請人主管審核後之資訊事件調查表，負有分配、調查、處理責任，並於系統資訊管理處人員，完成事件處理進行督導作業。
It is necessary to be responsible for the distribution, investigation, and processing of the information incident investigation form reviewed by the applicant's supervisor, and to supervise the completion of incident handling by the system information management office personnel.

3.3. 通報人員 Notifying Personnel

所有人員，發現疑似資通安全事件時，皆負有即時通報之責任。
All personnel are responsible for reporting suspected IT security incidents immediately.

3.4. 通報人主管Notifier Supervisor

審核通報人通報內容是否確實符合相關單位要求。
Review whether the content reported by the notifier actually meets the requirements of the relevant unit.

3.5. 外部人員 Outsiders

確定事件影響範圍，並評估損失。協助資通安全事件之通報、處理及分析作業。
Determine the scope of the incident and assess the damage.Assist in the reporting, processing and analysis of information security incidents.

4. 名詞定義DEFINITION

4.1. 資訊安全事件等級Information Security Incident Level

4.1.1. 資通安全事件依影響等級區分為4個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」。
Information security incidents are divided into 4 levels according to the level of impact. From severe to least, they are "Level 4", "Level 3", "Level 2" and "Level 1".

(a)4級事件，符合下列任一情形者：
Level 4 events, those who meet any of the following Circumstances:

機密資料遭洩漏。Confidential information leaked.

關鍵業務系統或資料遭嚴重竄改。
Critical business systems or data have been seriously tampered with.

影響範圍為全公司電腦及網域。
The scope of impact is company-wide computers and network domains.

關鍵業務系統運作停頓，無法於 4 小時內回復正作。
The operation of key business systems is suspended and cannot be restored within 4 hours.

(b)3級事件，符合下列任一情形者:
Level 3 events, those who meet any of the following circumstances：

敏感資料遭洩漏。Sensitive information leaked.

關鍵業務系統或資料遭竄改。
Critical business systems or data have been tampered with.

影響範圍為樓層電腦及網域。
The scope of impact is floor computers and network domains.

關鍵業務運作遭影響或系統停頓，於 4 小時內可回復正常運作。
If critical business operations are affected or the system is suspended, normal operations can be restored within 4 hours.

(c)2級事件，符合下列任一情形者:
Level 2 events meet any of the following circumstances：

限閱等級資料之關鍵業務系統或資料遭洩漏。
Critical business systems or data withrestricted access level datahave been leaked.

關鍵業務系統或資料遭輕微竄改。
Critical business systems or data have been slightly tampered with.

影響範圍為部門電腦及網域。
The scope of impact is department computers and network domains.

關鍵業務運作遭影響或系統效率降低，於 2 小時內回復正常運作。
If key business operations are affected or system efficiency is reduced, normal operations will be restored within 2 hours.

(d)1級事件，符合下列任一情形者:
A level 1 event meets any of the following circumstances：

非關鍵業務系統或資料遭洩漏。
Non-critical business systems or data were leaked.

非關鍵業務系統或資料遭竄改。
Non-critical business systems or data have been tampered with.

影響範圍為個人電腦。Affected scope is PC.

非關鍵業務運作遭影響或短暫停頓可立即於 1 小時內修復。
Non-critical business operations that are affected or temporarily suspended can be repaired immediately within one hour.

4.2. 文件編號定義File number definition

ISM 02 YY MM XXX

ISM：資訊安全英文簡稱ISM(Information Security)

02：資訊安全事件information security incident

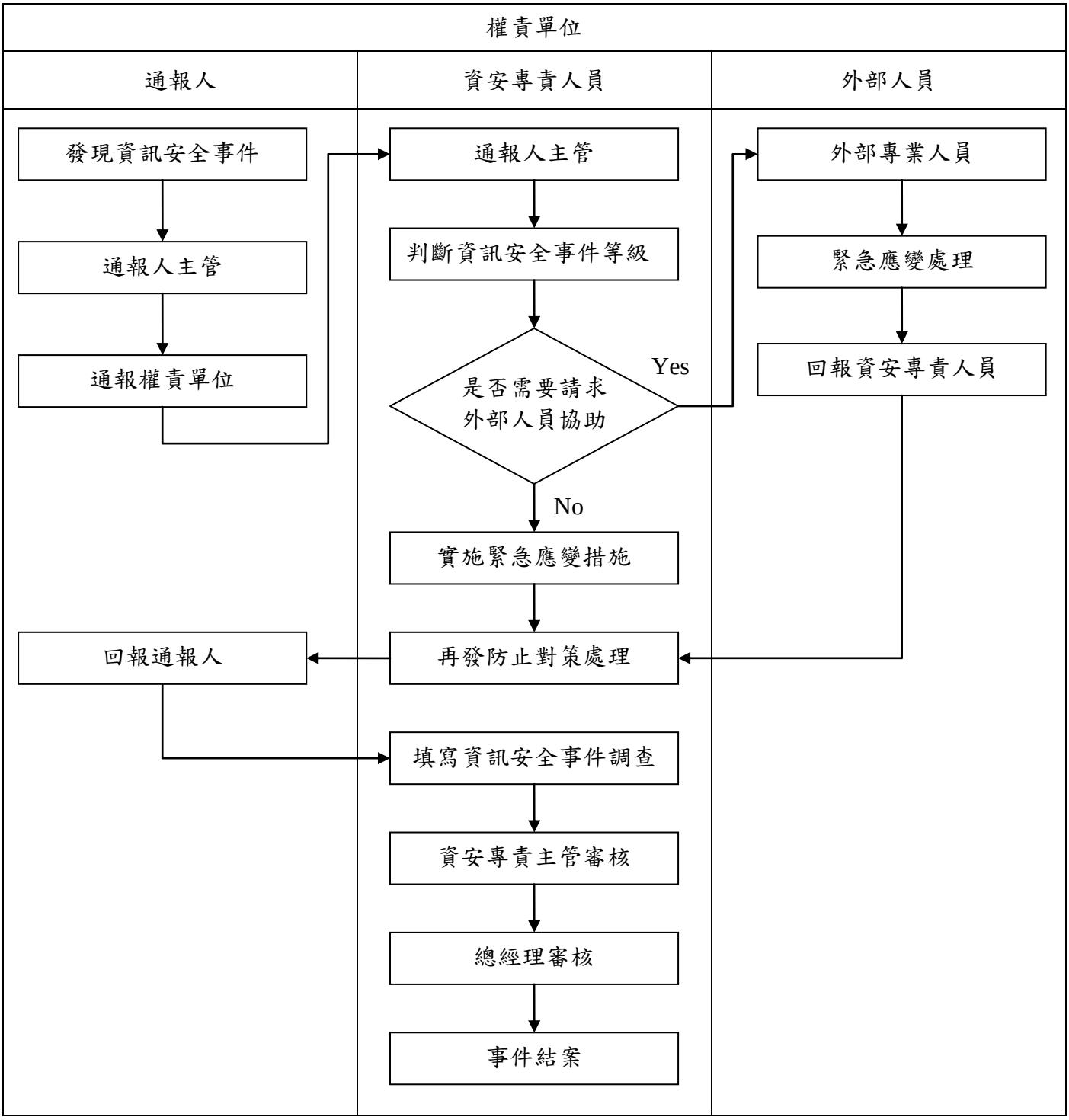
YY：年份years

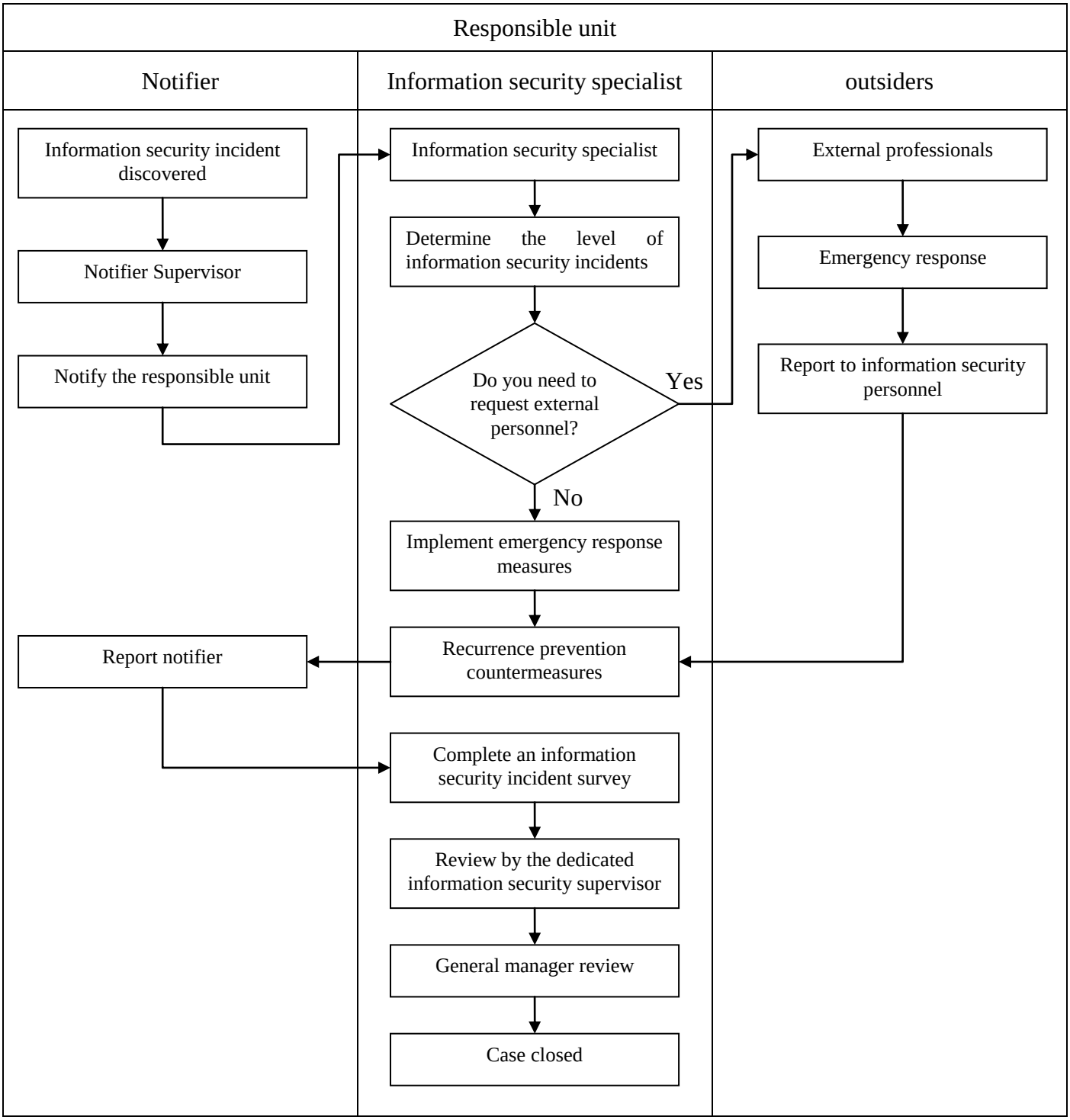
MM：月份month

XXX：流水號serial number

5. 流程圖FLOWCHART

資訊安全事件通報與應變作業流程
Information security incident reporting and response procedures





6. 作業內容OPERATION PROCEDURE

6.1. 處理及復原程序 Treatment and recovery procedures

6.1.1. 立即通報Notify immediately：

發現安全事件後，立即通報相應的安全負責人、IT部門或公司安全小組。確保通報的信息是清晰、具體、包含事件的相關細節，並填寫資訊安全事件調查表申請人欄位後，交由部門主管進行審核。

When a security incident is discovered, immediately notify the appropriate security manager, IT department, or corporate security team. Ensure that the reported information is clear, specific, and contains relevant details of the incident. After filling in the applicant field of the information security incident survey form, submit it to the department supervisor for review.

6.1.2. 資安專責人員調查處理Investigation and handling by specialized information security personnel:

資安專責人員接獲通報後，應立即前往相應地點進行調查，並判斷事件類別、分級、與影響範圍，進行緊急處理後，將會進行討論損失評估與擬定再發防止對策，完成後填寫資訊事件調查表受理人欄位，交由資安專責主管與總經理審核。

After receiving the notification, the information security personnel should immediately go to the corresponding location to investigate and determine the type, classification, and impact scope of the incident. After emergency treatment, they will discuss loss assessment and formulate recurrence prevention countermeasures. After completion, fill in the information The recipient field of the incident investigation form shall be submitted to the dedicated information security supervisor and general manager for review.

7. 相關文件 REFERENCES

N/A

8. 附件 RECORD

資訊安全事件調查表 Information Security Incident Questionnaire(A-B-W00-23-003-01)