希华晶体科技股份有限公司
资讯安全作业管理办法

一、目的：建立公司资讯作业管理之各项作业方式，使各部门电脑资讯作业能正常运作，以确保资讯系统之正确执行。

二、适用范围：本办法适用于本公司『电脑管理资讯系统』及相关作业之管理。

三、名词定义：无。

四、作业办法：

4.1 组织、职责及教育训练：

4.1.1 资讯单位

A. 经营管理资讯系统规划、设置及维护。
B. 资讯软、硬体及相关周边设备之评估、建议、请购、安装、测试及维护。
C. 资讯作业制度办法之制、修订。
D. 参与各项作业资讯化之系统分析、设计及测试。
E. 资讯系统及资料安全维护。
F. 资讯使用者教育训练之协助。
G. 其他有关资讯系统相关业务之处理。

4.1.2 资通安全推动组织及人力、物力与财力资源

A. 成立资通安全小组负责资通安全相关业务之推动、协调、监督及审查资通安全管理事 项，设置专责主管 1 人及专责人员至少 1 人，小组成员及工作职掌填应写「资通安全 小组成员及职掌表」(附件十八)呈 总经理核准，人员异动或增减时亦同。
B. 资通安全主管负责资通安全小组任务之推动、协调、监督及审查。
C. 资通安全专责人员协助资通安全主管推动及执行资通安全工作。
D. 资通安全主管应考量资通安全政策及目标，据以规划建置、执行、维持及持续改善资通安全相关工作，并适时检讨所需之人力、物力与财力资源。

4.1.3 职责划分

A. 资讯单位负责资讯系统之软、硬体管理、故障排除与资讯安全及系统维护。
B. 使用单位负责例行资讯作业管理及系统需求之提出。
C. 资讯作业使用权限由各使用单位提出，经资讯单位确认后设定使

用。

D. 电脑操作人员离职时，单位主管应对其所保管之资讯相关文件及磁片、磁带、帐号、电脑硬体暨周边设备等安排办理移交，依「离免停退、职务移交管理办法」办理。

4.1.4 资讯安全宣导与教育训练

A. 每年定期以公告、电子邮件或其他适当方式对使用资讯系统之人员进行资讯安全宣导，以提升使用者安全意识，降低资安风险。

B. 资讯安全专责主管及专责人员，每年应接受适当之资讯安全专业课程训练或资通安全职能训练。

4.1.5 资讯人员之任用由资讯单位负责遴选，任用后之考核、升迁悉依公司「工作规则」办理。

4.2 资讯安全政策制定及评估：

4.2.1 资通安全政策及目标

A. 订定资通安全政策及目标呈 总经理核准，并每年检讨其适切性。

B. 资通安全政策应透过教育训练、内部会议、张贴公告或其他方式向所有人员进行宣导，并每年检视其重要性是否有效传达员工。

4.2.2 资讯安全评估对象

A. 资讯设施及系统提供者。

B. 使用者。

C. 管理者、系统维护者。

D. 其他有关人员。

4.2.3 由内部稽核人员不定期抽查，检查人员是否遵守「员工任用管理办法」中之「资讯作业规定」。

4.2.4 员工如违反资讯安全相关规定，依「工作规则」作业办法处理。

4.2.5 新购资讯产品（如电脑软体、硬体、通信及管理措施等），应将安全性列入评估，以免影响既有的资讯安全措施。

4.2.6 资料保存依「品质记录管理作业办法」实施办理。

4.2.7 电子资料或设备之销毁

设备故障或报废时，应做适当处置(例如：硬碟需格式化或物理性破坏、光碟片破坏性销毁...等)，以确保公司资讯不外流。

4.2.8 机密文件销毁

各单位机密性文件销毁，由保管单位依需求销毁日执行销毁。

4.3 电脑系统安全管理：

4.3.1 由各单位依其作业订定操作说明书或以书面、电子或其他方式载明之，以确保员工能正确及安全操作使用电脑系统，便于工作移转交接、维护的依据。

4.3.2 如果遭遇非预期的电脑系统作业技术问题时，由需求部门提出并通知资讯单位支援。

4.3.3 资讯系统发展及测试作业应将正式区及测试区分开处理，降低可能的风险，以减少作业软体或资料遭意外窜改，或是未经授权存取的机率。

4.3.4 电脑主机系统之效能、磁碟使用率、记忆体容量、档案储存，印表机、其他输出设备及通信系统之使用状况等，由资讯单位人员随时注意及观察分析系统的作业容量，以避免容量不足而导致电脑当机。

4.4 网路安全管理：

4.4.1 安装防毒软体并定期自动更新病毒码，以确保系统不被电脑病毒感染。

4.4.2 使用网路防火墙来堵隔非法入侵。若个人因工作必要需求使用即时通讯软体或私人网路邮箱，或是需开放／拒绝网路服务或通讯埠，应填写「防火墙设定申请书」(附件一)送单位主管同意及 总经理核准后，交由资讯单位进行设定。

4.4.3 使用网路监控设备监控人员网路行为，以确保网路安全，调阅其纪录资料应填写「资料调阅申请书」(附件二)送交单位主管同意及 总经理(含)以上核准后，方可进行调阅。

4.4.4 基于网路安全之考量，整体电脑网路规划为独立之内部网段、非军事区网段（DMZ）及外部网段，其间以网路防火墙区隔。

4.4.5 网路防火墙之安全控管相关设定应经常检讨，并作必要之调整，以确定发挥应有的安全控管功能。

4.4.6 办公室以外之员工采用 VPN 方式或透过网路防火墙 SSL VPN 方式远端网路连线作业，申请 SSL VPN 连线作业程序依 4.4.2 办理。

4.4.7 为避免外部非法入侵，公司架设网路防火墙、电子邮件过滤系统及电脑防毒软体，以确保资讯安全。

4.5 系统开发及程式修改控制：

4.5.1 本公司 ERP 资讯系统开发及程式修改由资讯单位自行维护，若采委外方式处理则由资讯单位统筹按下列阶段实施。

A. 使用者提出系统需求。
B. 资讯单位进行可行性评估。
C. 委外公司选定。
D. 系统需求及细部规格检讨拟定。
E. 程式编号及测试。
F. 系统测试。
G. 教育训练安排。
H. 正式上线。

4.5.2 资讯系统程式之修改由需求单位填写「程式修改需求申请单」（附件三）提出申请，经单位主管确认并会办相关单位意见后，送请资讯单位评估相关作业事项及意见，申请单需经资讯单位核准后方予执行。

4.5.3 修改后的程式测试由需求单位验收及资讯单位主管复核无误后才可使用。

4.5.4 资讯单位需将系统程式修改记录登录「系统程式修改明细表」（附件四）并作程式备份保存。

4.5.5 系统需求拟定应与使用单位充分参与讨论。

4.6 编制系统文书之控制：

4.6.1 资讯系统主要说明书、操作手册、训练教材等系统文件，保存于系统中方便使用者随时参阅，资讯单位制作备份磁带保存，不另列印文件。

4.6.2 存放于系统中之文件随软体公司之版本变更作业一并更新，资讯单位亦需将备份资料更新。

4.6.3 除系统内存放之系统说明书、操作手册、训练教材外，资讯单位亦应针对不足部分编制相关说明文件。

4.6.4 资讯单位对资讯系统版本更新状况应保留记录，制订操作文件之修废需依『文件及资料管理办法』办理。

4.6.5 系统原版程式及文件由资讯单位建立「软体明细表」（附件五）保管，软体部分并需建立备份。

4.6.6 文件、硬体、软体之借用，依「软体管理办法」处理。

4.6.7 软体授权数控管由各单位编列预算采购。软体的安装由需求单位填写「软体安装申请单」(附件六)经单位主管同意，并经副总级(含)以上主管核准后，交由资讯单位进行软体异动。

4.6.8 电脑硬体设备异动由异动单位至 ERP 系统输入资料并申请固定资产异动后，发起表单签核流程，依表单流程完成核准同意，再交由资讯管理人员至电脑设备维护作业程式进行硬体资料之异动。

4.7 程式及资料之存取控制：

4.7.1 程式之修改需依规定程序办理，资讯单位对修改内容应保留记录。

4.7.2 程式及档案区只允许资讯单位及资讯单位授权人员进入，一般使用者只允许执行应用程式。

4.7.3 电脑系统使用权限依工作权责划分，由需求单位提「TIPTOP 使用权限申请表」（附件七）经资讯单位确认后设定使用，

若有跨单位需求者，则需会办相关单位同意才可开放权限。

4.7.4 为确保电脑系统变更作业流程明确划分权责，程式人员应定期将正式区异动之程式列表「程式修改需求清单」(附件八)，并呈交资讯主管复核，以确保所异动之程式皆经申请及适当核准。

4.7.5 系统异常存取之稽核，资讯单位应定期复核异常存取记录与高权限帐号之存取记录，并追踪是否有企图非法进入系统或未经授权存取或修改资料之异常状况。

4.7.6 申请电脑系统使用帐号，由需求人员至 BPM 系统填「使用者帐号使用申请表」(附件九)，申请 PLM 系统使用权限则填写「PLM 系统权限申请表」(附件十)，经核准后设定使用。

4.7.7 定期审查使用者帐号，对于已停用或超出六个月以上未登入之帐号，以电子邮件或其他适当方式通知本人及其直属主管，经确认后不再使用的帐号即予以删除。

4.8 资料输出入之控制：

4.8.1 资料输入时应做核对并留下可供确认的记录。当发生错误时，由使用单位先行分析错误类别。

A. 资料本身错误或输入错误：
由使用单位权责人员更正错误资料，并通知相关单位。

B. 系统异常或程式错误：
由使用单位填写「系统问题反应单」(附件十一)记录错误讯息，经单位主管确认后交由资讯单位分析异常原因并处理之。

4.8.2 系统资料经由使用权限设定之管制，避免机密性或敏感性资料遭不当使用。

4.8.3 机密性或敏感性资料输出不成功需重新输出时，原印制未完成之输出报表应确实作废销毁。

4.8.4 输出资料产生时，应依相关办法对其使用联数加以控制。

4.8.5 输出资料使用后若无保存需要时，应予销毁。

4.9 资料处理之控制：

4.9.1 日常作业资料由各使用单位依工作权责控制管理。

4.9.2 资讯单位定期检视维护各项资讯系统、设备及帐号。

4.10 档案及设备之安全控制：

4.10.1 设定系统密码，除资讯单位及资讯单位授权人员外，其余人员禁止进入程式档案区。

4.10.2 系统程式、应用程式等资料每日执行备份并记录「TIPTOP GP 备份管理表」(附件十二)。

4.10.3 系统资料(含作业系统或应用软体的日志档)每日执行备份并记录「资讯资料备份管理表」(附件十三)，备份磁带轮替使用，并由资讯单位保管。

4.10.4 磁带、磁片保存原则

A. 存放于通风、阴凉、干燥之处，避免阳光直接照射，并远离磁场或火源。

B. 磁片应保持直立状况，不可折迭或压损。

C. 使用磁片应装入封套，放置阴凉地点且避免潮湿。

4.10.5 系统主机应加装 UPS 不断电系统。

4.10.6 系统主机开关机程序遵循操作说明书内容操作。

4.10.7 系统软、硬体以与供应商签订维护合约为原则，实施定期维护保养，确保系统正常运作。

4.10.8 系统软、硬体设置区域应有空调系统及适当之消防设施。

4.10.9 电脑设备异常时，由发生单位通知资讯单位处理，并建立「系统问题反应单」。

4.10.10 病毒防护

邮件主机安装防毒软体，藉由软体所提供之自动更新病毒码与即时防护来防止电脑病毒入侵，资讯单位不定期检查系统主机及使用者电脑作追踪处理。

4.10.11 使用者密码管理

A. 使用者密码预设值与使用者帐号相同。

B. 使用者密码长度最少 6 个字元。

C. 使用者最少每六个月应变更通行密码。

D. 若登入系统错误超过设定次数，系统将会锁定使用帐号而无法登入，需通知资讯单位权责人员解除锁定后，才能重新登入系统。

4.10.12 系统备援计划

A. 经由网路或其他媒介，定期备份重要电脑主机系统环境(含电脑作业系统及其所有应用软体)至适当资料储存媒体存放。

B. 当提供资讯系统服务的电脑因硬体设备或软体原因故障时，能即时将主机系统环境的备份还原至系统备援主机，以确保资讯系统服务持续运作不中断。

4.11 电脑周边设备之购置、使用及维护：

4.11.1 资讯系统各项软硬体需求由资讯单位统筹规划，使用者参与评估后依『采购管理办法』规定请购。

4.11.2 使用单位需求之电脑周边设备，由使用单位提出请购。

4.11.3 资讯单位应建立「电脑周边主要设备清单」(附件十四)，作为系统维护参考之用。

4.11.4 使用单位购入或异动硬体设备，应将购入设备规格或异动内容通知资讯单位登录「电脑周边主要设备清单」。

4.11.5 资产管理权责单位应定期盘点清查资产，并将盘点结果通知资讯单位更新「电脑周边主要设备清单」。

4.11.6 资讯系统暨伺服器主机维护合约由资讯单位负责处理。

4.12 系统复原计划制度及测试程序之控制：

4.12.1 复原准备

系统复原所需之系统软体、应用软体及系统资料备份磁由资讯单位保管。

4.12.2 复原实施

由资讯单位视状况自行处理或请软、硬体厂商配合处理。

4.12.3 复原测试

A. 复原实施后之作业系统测试由资讯单位执行。

B. 复原实施后之应用程式测试由使用者及资讯单位共同测试。

4.13 电脑机房管控：

4.13.1 电脑机房之伺服器维护详阅各操作说明书。除负责机房业务有关人员外，其他未经资讯单位许可人员禁止进入电脑机房。

4.13.2 电脑机房需应规划放置适当消防器材，以避免意外灾害之发生。

4.13.3 电脑机房温度应维持在 18℃至 25℃，相对湿度维持在 50%至 70%，当机房温度>28℃或相对湿度>80%，则应检查冷气空调、除湿机器或排水设施等设备，并维护调整之。

4.13.4 上班时间由资讯单位每日进行点检并填写「电脑机房点检表」(附件十五)，下班时间由守卫人员监控系统并巡视机房内相关设施，并随时监看环控系统注意机房内温湿变化，若发现异常现象，应即时通知相关人员处理。

4.13.5 为避免电脑机房内主机机柜对高架地板负载过重，所导致的崩坏倒塌或物体破裂、坠落、滚落之风险，对负载过重之机柜下方，应增加铁片分散负荷重力，以减少意外风险的发生。

4.14 风险评估：

4.14.1 资讯单位应定期进行资讯系统安全相关风险评估，并填写「资通安全风险评估表」(附件十六)。

4.14.2 名词定义

A. 危害性：1~9 分，风险危害影响程度越高，评分越高。

B. 发生频率：1~9 分，风险发生频率程度越高，评分越高。

C. 风险等级评分 = 危害性评分 × 发生频率评分。

风险等级	低度风险	中度风险	高度风险
评分	1~24	25~49	50~81

4.14.3 高度风险控制改善

当资通安全风险项目等级评定为高度风险时，应拟议管理面或技术面控制措施，并填写于「资通安全风险评估表」之【降低风险控制措施】栏位，以管制降低风险。

4.15 委外管理：

4.15.1 本公司委外办理资通系统之建置、维运或资通服务之提供时，应考量委外厂商之专业能力与经验、委外项目性质及资通安全需求，以选任适当的委外厂商。

4.15.2 选任委外厂商时应考量其办理受托业务之相关程序及环境，是否具备完善之资通安全管理措施或通过第三方验证，且是否配置经适当之资格训练、拥有资通安全专业证照或具有类似业务经验之资通安全专业人员。

4.15.3 监督要求委外厂商执行受托业务时，若有违反资通安全相关法令或发生资通安全事件时，应立即通知本公司并采行补救措施。

4.15.4 与委外厂商签订委外服务契约时，应审查确认契约中之保密条款，并要求委外厂商之业务执行人员签署「委外厂商执行人员保密同意书」(附件十七)。

4.15.5 委外关系终止或解除时，应确认委外厂商已返还、移交、删除或销毁因履行委托契约而持有之资料。

4.16 资安事件通报及应变：

4.16.1 通报作业程序

A. 若发现疑似重大资通安全事件时，由发现人员依事件状况迅速通报资安事件通报窗口，并告知直属单位主管。

B. 资通安全小组收到通知后，依事件影响范围及损害程度评估，研判是否为重大资通安全事件。

C. 若研判为非重大资通安全事件时，则将判定结果回复发现人员并协助处理及解决问题。

D. 若研判为重大资通安全事件时，则依事件之影响程度通知权责单位主管。

E. 若事件处理有需要系统维护或设备保固的外部厂商之协助，应立即以事先已约定方式通知协力厂商联络窗口处理。

4.16.2 应变处置

A. 事前建置资讯安全系统及整体防护架构，增加防御能力，以减少资安事件发生机率，降低资安事件损害程度。

B. 平日随时汇集整理各项资安相关文件，在资安事件发生时可立即参考并处置，以提升应变作业效率。

C. 一旦发生重大资安事件，应于最短作业时间内控制并复原资安事件所造成的损害。

D. 资安事件紧急应变处置后，应进行讨论并研拟适当之预防及矫正措施。

4.17 核心业务及营运中断事件：

4.17.1 核心业务

核心业务	核心资通系统	机敏性资料等级（高/中/低）	系统复原时间目标（RTO）	资料复原时间点目标（RPO）
产品生产	SFT	高	6 工时	24 小时
产品销售	ERP	高	8 工时	24 小时
客户往来	MAIL	中	8 工时	24 小时
内部流程	BPM	低	12 工时	24 小时
人力资源	HRM	高	16 工时	24 小时

4.17.2 营运中断事件

营运中断事件	发生机率（高/中/低）	影响程度（大/中/小）
伺服器主机故障	低	大
资料储存设备故障	高	大
电力供应中断	中	大
天然灾害(地震、台风…)	低	大
联外网路线路中断	中	中
骇客入侵	低	中
电脑中毒	中	中
使用人员操作错误	中	小

使用人员蓄意破坏	低	小
其他意外事件	低	小

五、相关文件：

5.1 离免停退、职务移交管理办法 AMD-P-026
5.2 工作规则 AMD-P-003
5.3 员工任用管理办法 AMD-P-025
5.4 资讯作业规定 AMD-164
5.5 品质记录管理作业办法 TMG-P-004
5.6 文件及资料管理办法 TMG-P-002
5.7 软体管理办法 TMG-P-017
5.8 采购管理办法 PCD-P-002

六、附件：

6.1 防火墙设定申请书	TMG-056	附件一
6.2 资料调阅申请书	TMG-057	附件二
6.3 程式修改需求申请单	TMG-022	附件三
6.4 系统程式修改明细表	TMG-023	附件四
6.5 软体明细表	TMG-021	附件五
6.6 软体安装申请单	TMG-058	附件六
6.7 TIPTOP 使用权限申请表	TMG-018	附件七
6.8 程式修改需求清单	TMG-052	附件八
6.9 使用者帐号使用申请表	TMG-063	附件九
6.10 PLM 系统权限申请表	TMG-061	附件十
6.11 系统问题反应单	TMG-019	附件十一
6.12 TIPTOP GP 备份管理表	TMG-062	附件十二
6.13 资讯资料备份管理表	TMG-026	附件十三
6.14 资讯周边主要设备清单	TMG-020	附件十四
6.15 电脑机房点检表	TMG-055	附件十五
6.16 资通安全风险评估表	TMG-064	附件十六
6.17 委外厂商执行人员保密同意书	TMG-065	附件十七
6.18 资通安全小组成员及职掌表	TMG-066	附件十八