博瑞達應用材料股份有限公司
資訊安全管理辦法

規章編號：PAM-10110

發佈日期：20250711

第一章 总则

一、目的

为建立信息安全管理制度，保护博瑞达集团信息资产的机密性、完整性及可用性，降低信息风险，确保业务持续营运，特订定本办法。

二、适用范围

本办法适用于博瑞达集团(以下简称本公司)全体员工、契约人员、外包厂商及使用公司信息资产之人员。

三、信息安全政策

本公司致力于建立完善之信息安全管理制度，确保信息资产的机密性、完整性与可用性。信息安全管理应纳入公司治理与日常营运流程中，并符合相关法令与利害关系人之期望。全体同仁应共同维护信息安全，防范内外部威胁与弱点，以降低资安风险。

四、信息安全目标

1. 每年至少进行一次资安自我检查，改善率达 100%。
2. 所有操作系统与应用程序，重大弱点修补完成率达 95% 以上。
3. 遇资安事件，通报与处置时间不得超过 4 小时。
4. 每年全体人员资安训练覆盖率达 100%。

五、信息安全原则

信息安全管理应遵循以下原则：

1. 最小权限原则。

2. 持续改善原则。
3. 信息资产风险导向管理原则。
4. 员工资安意识与责任并重。

六、法令与契约遵循要求

本公司推动信息安全管理制度，应遵循下列国内外法令、政策与契约义务，以确保信息资产的机密性、完整性与可用性，并符合对利害关系人之承诺与责任：

1. 公开发行公司建立内部控制制度处理准则
2. 上市上柜公司资通安全管控指引
3. 个人资料保护法
4. 本公司与客户、合作伙伴、委外厂商间所签署之契约中涉及信息安全、保密、个人资料处理、服务水平协议（SLA）等条款

第二章 组织与责任

一、信息安全管理架构

本公司信息安全管理由下列人员共同负责执行与监督：

1. 总经理
2. 资安管理委员会：由总经理指派一位副总级主管担任主委，召集两位一级主管组成。
3. 资安执行小组：由信息单位及各部门主管推派之代表组成，信息单位主管担任资安专责主管。

二、各角色职责

1. 总经理：

   （1）核定信息安全政策与目标。
   （2）支持资安资源分配与制度推动。

2. 资安管理委员会：

   （1）核定资产识别与风险评估结果。
   （2）监督信息安全管理事项执行情形。
   （3）监督重大资安事件处理。

3. 资安专责主管：

   （1）集团信息安全政策之拟订。

（2）定期检讨资安执行情形与改善建议。
（3）主导资安事件通报与应变。

4. 资安执行小组

（1）撰写与维护资安管理文件。
（2）执行风险评估与控制措施。
（3）监控系统安全状况与异常事件。
（4）规划并执行资安教育训练。

三、外部支持

遇信息安全专业不足或需要进行资安稽核、弱点扫描、事故鉴识等事项时，得委托外部专业机构协助办理。

第三章 资产识别与风险管理

一、核心业务识别

本公司之核心业务定义如下：

核心业务	**业务内容简述**	业务失效影响说明	最大可容忍中断时间
报价与接单	接收客户订单、制作报价单并与客户往返确认报价与数量	无法实时报价或接单将导致客户流失、商机丧失，损害公司营收与商业信誉	24H
客户关系管理	管理客户联络信息、交易纪录与商务需求	客户数据遗失将影响后续交易、客服作业与客户信任，造成客源流失	24H
出货与物流追踪	出货安排、物流公司联系、货物追踪、报关与运输文件处理	出货延误或数据错误将影响合约履行、引发客诉与索赔，影响公司信用与客户关系	24H
付款与收款处理	处理 TT 汇款、L/C 开状、信用证处理与财务文件传递	延误或错误将导致收款失败或客户违约，甚至产生金钱损失与法律风险	24H

二、信息资产分类与清册

为有效管理信息资产，本公司依资产性质分类如下，并建立信息资产清册（由 MIS 维护）：

资产类型	说明	管理单位
硬设备	服务器、笔电、网络设备等	MIS
软件系统	ERP、BPM、CRM、邮件系统、资安工具等	MIS
资料资产	客户资料、财务报表、配置文件等	各部门
云端服务	Azure、SaaS 平台等	MIS
文件与纪录	合约、政策文件、稽核纪录等	各部门

信息资产清册应每年定期盘点与更新，并标注资产之拥有者、用户、机敏性等级。

三、机敏性数据识别

本公司将下列信息列为机敏性数据，需加强保护：

- 客户个人资料（如姓名、联络方式、帐户信息）
- 公司财务与营运数据
- 系统管理账号与密码
- 威胁侦测与分析报告
- 尚未公开之产品规划与技术文件

四、风险评估原则

信息安全负责人应每年至少办理一次信息安全风险评估，针对公司关键信息资产、系统、网络与外包作业进行评估，评估项目应涵盖潜在威胁、脆弱点、现行控制措施与风险影响程度。

五、风险评估流程

风险评估应依下列步骤进行：

1. 资产盘点：确认评估范围内之信息资产。
2. 威胁与弱点识别：分析可能影响资产之威胁来源与系统弱点。
3. 风险分析：依据资产价值、威胁可能性与冲击程度，评估风险等级（高、中、低）。
4. 风险处置建议：针对高风险项目，采取以下一种或多种处理方式：
   (1) 风险降低（如加强控管、修补弱点）
   (2) 风险接受（经管理阶层同意）
   (3) 风险移转（如保险、委外）
   (4) 风险回避（如取消高风险作业）
5. 文件化与存查：完整记录评估结果与处置建议，存档至少三年。

六、风险再评估时机

遇下列情形之一时，应进行临时性风险再评估：

1. 系统或设备环境重大变更。
2. 发生重大资安事件后。
3. 新系统或新服务上线前。
4. 法规或营运环境重大变更时。

第四章 系统开发与维运安全

一、系统开发安全

为确保本公司自行开发或委外开发之系统具备基本资安防护能力，应遵循以下原则：

1. 安全设计原则：系统设计时间即应纳入资安需求，如访问控制、数据加密、日志记录、错误处理等。
2. 权限最小化：系统账号与功能模块应依用户职责设定最小必要权限。
3. 程序代码管理：开发人员应使用版本控制工具（如 Git），并避免将机敏信息写入程序代码中。
4. 测试与验证：系统上线前应进行功能测试与资安测试（如 OWASP TOP 10 等基本安全性检查）。

二、系统维运安全

本公司信息系统之日常维运应符合以下安全管理措施：

1. 账号与密码管理：
   (1) 仅授权人员得申请系统账号。
   (2) 密码原则须符合「IT 用户规章」《伍、系统安全》第一条之规定。
   (3) 离职或职务异动人员之账号应实时停用或调整权限。
   (4) 使用云端服务(如 Azure、SaaS 平台…等)时，应启用多因素验证与访问控制。
2. 日志记录与监控：
   (1) 关键系统应保留存取与异常行为日志，保存期限至少 6 个月。
   (2) MIS 每半年应定期检视日志，发现异常应立即通报。
3. 变更管理：
   (1) 系统设定或程序异动应经主管核准，并保留异动纪录。
   (2) 重大变更应安排非上班时段进行，并备妥还原机制。
4. 备份与还原：

（1）关键数据每日备份，并定期测试还原功能。
（2）备份数据应限制存取，并与主系统分离保存。

第五章 资通安全与防护措施

一、系统更新与弱点修补

1. 所有操作系统与应用程序应定期更新安全修补。
2. 留意资安情资与威胁讯息(如：订阅 TWCERT/CC 电子报)，于高风险弱点公告后 30 日内完成修补。
3. 修补纪录须予以保存至少一年。

二、网络安全防护

1. 防火墙应设置于网络边界，限制未授权存取。
2. 提供外部存取服务的主机应设置于 DMZ 区域。
3. 外部网络、DMZ 与内部网络之间的网络通讯，皆须经过防火墙。
4. 集团各分公司或办公据点与总公司之间的网络通讯，需透过 Site to site VPN 进行联机。

三、远程访问管理

1. 远程访问适用对象

本公司远程访问服务系提供予因工作需要需于非公司网域环境联机之人员使用，包含：

（1）本公司正式任用之员工。
（2）经信息主管核准之委外厂商人员，且具项目或维运需要者。

2. 远程访问授权与管理

（1）申请远程访问服务者，须经部门主管及信息安全负责人核准。
（2）员工使用 Azure Entra ID 进行登入。
（3）委外人员应申请个人账号登入，并记录存取行为，严禁共享账号。
（4）远程访问应采取多因素验证机制。
（5）须依最小权限原则设定，限缩可远程访问之系统与资源范围。
（6）对委外人员之联机授权应设定明确期限与目的，项目结束或人员离任应即终止账号。

四、特权账号管理

1. 特权账号定义

特权账号系指拥有系统管理、数据库管理、网络设备设定或其他可变更系统核心设定与用户权力之账号，包含但不限于：

（1）操作系统（如 Windows/Linux）之 Administrator 或 root 账号。
（2）数据库管理账号（如 sa、oracle）。
（3）网络设备（如交换器、防火墙）之管理账号。
（4）云端平台（如 AWS、Microsoft 365）管理账号。
（5）第三方委外厂商所申请之维护专用账号。

2. 账号使用原则

（1）特权账号仅限经授权之人员使用，使用时须基于维运、设定或必要性操作。
（2）禁止使用特权账号从事日常性作业，如一般文书、浏览网页或收发邮件。
（3）特权账号不得由多位管理者共同使用，应以个别名义登入。

3. 账号异动与停用

（1）特权账号如不再使用，应立即停用或删除，并留存纪录。
（2）员工异动或离职时，其所使用具之特权账号须实时停权。

第六章 资通安全事件通报与应变

一、资安事件定义

1. 资安事件系指任何可能危害本公司信息资产之机密性、完整性或可用性之异常情况，包括但不限于：

（1）恶意软件感染（如病毒、勒索软件）
（2）未经授权之存取或异常登入行为
（3）资料外泄
（4）系统异常或服务中断
（5）云端服务或委外厂商之服务异常而影响本公司营运作业
（6）他人通报之信息安全问题

2. 资安事件分级

依照资安事件影响的严重性划分为四个等级：

分级	定义

一级	影响部分信息设备，组织仍可持续营运
二级	非核心业务受影响，组织仍可持续营运
三级	部分核心业务受影响
四级	组织核心业务停摆

二、通报原则

1. 员工如发现可疑或已知资安事件，应立即通报资安执行小组。
2. 资安事件一经发现，须于 4 小时内完成通报，并记录事件概要。
3. 通报方式可透过公司既有通讯机制（如 Email、电话、即时消息等）。
4. 若资安事件符合法令应通报条件，应依规定向主管机关完成通报。

三、应变处理流程

资安事件应依下列步骤进行应变处理：

1. 初步确认与分类：

   （1）信息人员确认事件真伪、影响范围与初步性质（如是否涉及数据泄漏、服务中断）
   （2）依资安事件分级定义进行事件等级分类，并依等级由资安专责主管决定是否启动重大应变程序
   （3）若判定为资安事件，须立即通知母公司资安管理单位。
   （4）若判定为三级以上重大事件，应立即通知高阶管理层。

2. 实时处置：

   （1）隔离受影响系统（如关闭网络、账号冻结、停止服务）。
   （2）防止扩散与进一步损害（如封锁来源 IP、停用漏洞服务）。

3. 调查分析：

   （1）厘清事件来源、触发原因与受影响范围。
   （2）汇整相关日志、系统记录、存证信息
   （3）必要时可请求外部资安厂商或顾问协助处理。

4. 复原与恢复：

   （1）受影响系统应重新安装操作系统。
   （2）修补漏洞或错误设定。
   （3）如需使用备份数据进行数据还原，应确认备份文件并未受事件影响。
   （4）进行安全性检测，确认系统已无风险。
   （5）恢复系统服务与正常营运。

（6）加强防护机制（如变更密码、修补软件）。

5. 后续报告与改善

（1）填写完整《资安事件应变纪录表》与调查报告。
（2）提报管理阶层，研拟改进措施。
（3）定期追踪改善进度并存查。

四、纪录与追踪

1. 所有资安事件应留存完整纪录，包括发现时间、通报者、处理流程、调查报告与预防改善作为。
2. 纪录保存不得少于三年。
3. 信息负责人每半年应汇整资安事件报表，供内部稽核与管理决策参考。

第七章 资安教育训练与倡导

一、年度训练

1. 公司每年至少办理一次信息安全教育训练，提升全体人员资安意识。
2. 信息单位成员每年应接受信息安全专业课程训练。

二、新进人员训练

新进人员须于到职时签署「IT 使用者规章」，于 3 个月内接受信息安全基本训练。

三、日常倡导

资安执行小组应定期推送电子邮件倡导资安观念（如钓鱼邮件识别、防社交工程等）。

第八章 委外管理

一、委外原则

1. 仅委托具备专业能力与良好信誉之厂商。
2. 与外部厂商签订信息系统开发、维护或代管服务时，应在合约中明定资安义务，包括资料保密、存取限制、资安事件通报机制等。
3. 应视委外服务类型，于契约中纳入适当之服务水平协议（SLA），如：系统可用性、响应时间等。

4. 涉及机敏数据之委外作业，应签署保密协议（NDA）。

二、委外管理

1. 应定期进行委外厂商信息安全稽核，检视委外作业之资安风险与执行情形。
2. 发现厂商违反资安规范时，应立即通报并采取补救措施。
3. 委外契约终止或解除时，厂商应依合约规定返还、移交、删除或销毁所有与本公司相关之数据与账号。

第九章 稽核与持续改善

一、自我检查与稽核

每年至少办理一次信息安全自我检查，并汇整改善建议；必要时得委托第三方进行资安稽核。

二、缺失追踪

稽核发现之缺失，信息安全负责人应列管追踪，直至完成改善为止。

三、绩效管理

1. 资安执行小组每年应汇整信息安全绩效指针执行情形，形成分析报告。
2. 针对未达标者应检讨原因，必要时纳入年度改善计划。
3. 每年应进行绩效指标的检讨与修正，以反映风险趋势或法规要求的变化。

四、管理阶层参与

管理阶层应定期（至少每年）审阅信息安全执行情形(含绩效指标)与风险状况，并提供资源与决策支持。

五、政策修订

本办法应每年至少检讨一次，必要时得依实际需求修正。

第十章 附则

本办法经总经理核定后施行，并公告全体人员遵循。

相关文件

1. 信息资产清册

2. 资产风险评估汇总表
3. 资安风险改善计划表
4. IT 使用者规章
5. 资安事件应变纪录表