

笙科电子股份有限公司
113 年度信息安全管理执行情形

資通安全管理之信息揭露

报告人：资安管理代表蔡合掌执行副总

董事会报告日期：113 年 12 月 25 日

Contents

1 資通安全管理策略與架構	錯誤! 尚未定義書籤。
1.1 資通安全政策	錯誤! 尚未定義書籤。
1.2 資通安全風險管理架構	錯誤! 尚未定義書籤。
1.3 具體管理方案	錯誤! 尚未定義書籤。
1.3.1 資通安全管理審查會議之審查結果	錯誤! 尚未定義書籤。
1.3.2 年度資訊作業查核	錯誤! 尚未定義書籤。
1.4 投入資通安全管理之資源	錯誤! 尚未定義書籤。
2 重大資通安全事件	錯誤! 尚未定義書籤。

1 资通安全管理策略与架构

叙明资通安全政策、资通安全风险管理体系、具体管理方案及投入资通安全管理之资源等。(法规依据：年报准则第18条第6款第1目)

1.1 资通安全政策

笙科电子股份有限公司的信息安全政策涵盖本公司及海内外子公司，是以「一、**建立符合法规之信息安全管理规范**；二、透过全员认知，达成信息安全人人有责的共识；三、**保护公司信息的机密性、完整性与可用性**；四、**提供安全的生产环境**，确保公司业务之永续营运」为指导准则。并以**防毒、防骇、防漏三大资安防护主轴为目标**，建立防火墙、入侵检测、防毒系统及诸多内控系统，以提升公司在防御外部攻击以及确保内部机密信息防护的能力。

笙科电子股份有限公司已导入并建立完整的信息安全管理系统（ISMS, Information Security Management System），从系统面、技术面、程序面降低企业资安威胁，建立符合客户需求的信息安全保护环境，并不断地进行「计划—实施—查核—行动」（PDCA, Plan-Do-Check-Act）循环以持续改善。

「**计划阶段**」着重资安风险管理，为了强化信息安全，笙科电子股份有限公司自民国112年导入**ISO27001信息安全管理体系**，使信息系统皆能在标准的管理规范下运作，降低因人为疏失所造成的安全漏洞及生产异常，也透过年度的复审作业，不断持续改善。

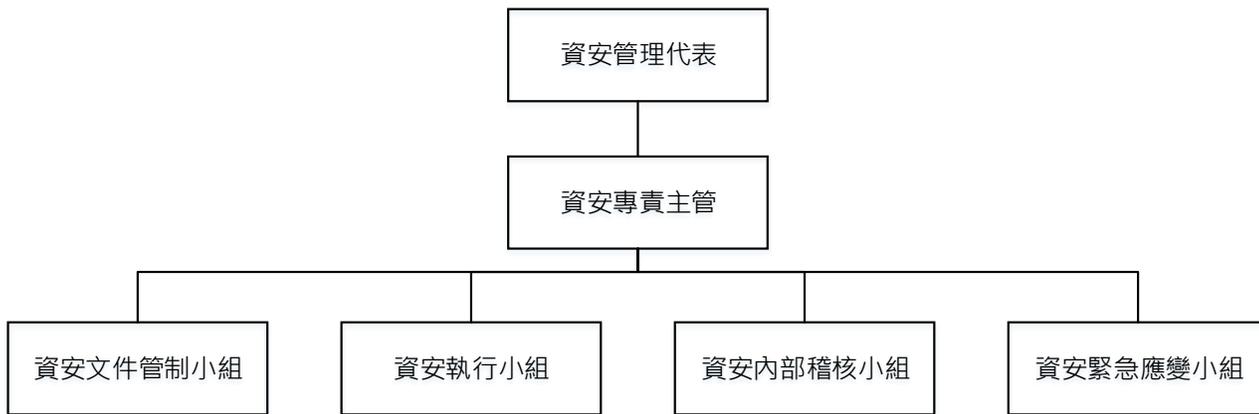
「**运行时间**」建构多层资安防护机制，持续**导入新资安风险控管技术**，以智能化／自动化机制提升各类资安事件之侦测及响应处理程序的效率，并强化信息安全及网络安全保护流程，以维护公司重要资产的防护。

「**查核阶段**」定期监控资安管理指标成效，及上述管理系统**每年第三方复审稽核**，另委由知名的资安厂商进行**渗透测试**，以确保持续提升资安管理及防御能力。

「**行动阶段**」检讨与持续改善，**透过年度的复审作业，不断持续改善**，提升资安管理及防御能力。

1.2 资通安全风险管理体系

笙科电子股份有限公司在民国112年成立「**资通安全管理委员会**」负责执行信息作业安全管理规划，建置与维护信息安全管理体系，统筹信息安全及保护相关政策制定、执行、风险管理与遵循度查核。



资通安全管理委员会组织结构

- 资安管理代表：由「执行副总」担任。
- 资安专责主管：由「信息服务部主管」担任。
- 资安紧急应变小组：由「信息服务部员工」担任。

委员会每年向董事会报告资通安全管理审查会议之审查结果。

1.3 具体管理方案

为达资安政策与目标，建立全面性的资安防护，推行的管理事项及具体管理方案如下：

- 法令遵循及导入国际资安认证标准：笙科电子股份有限公司推行信息安全相关的 ISO27001 认证标准及法规，作为达成各项风险管理的方法与检验依据。公司内部亦成立对应的「资通安全管理委员会」，专责推动各项标准化作业，降低生产营运的风险。
- 提升资安防御能力：定期进行资安系统脆弱度分析及渗透测试，并加以补强与修护，以降低资安风险。建立网络安全事件应变计划，依事件严重度等级进行影响和损失评估，采取对应的通报及复原行动。
- 增进网络安全：整体信息系统网络安全区域优化，增加重要主机特权账号登入多因子认证防护。
- 教育训练：进行全员资安教育训练与不定期社交工程钓鱼邮件测试，以提升资安意识，使资安的运作在高阶主管与各部门的支持下，落实到每一位员工身上。

1.3.1 资通安全管理审查会议之审查结果

编号	稽核项目	稽核发现	改善策略
4	其它	Window 7 操作系统过于老旧，微软已不提供漏洞修补，有资安疑虑。	已于 2024 完成将有联网能力计算机之 Windows 操作系统更新至 Windows 10、11

1.3.2 年度信息作业查核

于 113 年 11 月，由勤业众信联合会计师事务所对本公司进行信息作业查核。查核结果如下表。

编号	查核项目	发现与风险	建议	改善策略				
(1)	系统变更控制	<p>发现事项： 经查核发现 贵公司 Workflow ERP 主机 (CORPAP03) 及 AD 主机(CORPDC01)所在之 Windows 操作系统未安装微软今年度释出之重大更新，且未定期评估是否需要更新。</p> <p>风险： 如未适时进行安全性更新，且未依系统状况做出评估，恐导致漏洞无法实时修补，且易遭外部攻击／威胁之风险。</p>	<p>建议 贵公司</p> <p>应定期评估微软发布之重大更新是否需更新，若评估不需安装，则须留存评估纪录及主管核准纪录。</p>	<p>目前计划采用 patch 更新系统(Ivanti)，每月做一次更新，系统预定 2024 年 12 月底会启用上线。</p>				
(2)	存取安全控制	<p>发现事项： 经查核发现 贵公司 Workflow ERP 系统链接之 MS SQL 数据库以下账号未套用 Windows 密码有效天数设定，亦无人工定期变更密码：</p> <table border="1" data-bbox="212 1213 699 1331"> <thead> <tr> <th>账号</th> <th>上次变更密码日期</th> </tr> </thead> <tbody> <tr> <td>sa</td> <td>2022/03/17</td> </tr> </tbody> </table> <p>风险： 若密码强度不足，恐导致系统账号较为容易被盗用，进而提升数据遭窜改之风险。</p>	账号	上次变更密码日期	sa	2022/03/17	<p>建议 贵公司</p> <p>为强化信息安全，应评估于不影响系统运作之前提下，以人工方式定期变更密码(至少一年一次)。</p>	<p>依建议每年以人工方式修改密码。 (已于 12/5 更新密码)</p>
账号	上次变更密码日期							
sa	2022/03/17							

1.4 投入资通安全管理之资源

- 建立符合法规之信息安全管理规范
 - 导入 ISO27001 信息安全管理体糸
 - 相关会议开会次数：5 次
 - 成立「资通安全管理委员会」
 - 资通安全管理委员会人员总数：20 人

➤ 资安执行小组上外训课程

IT Home 所举办之 CYBERSEC 2024 台湾资安大会

- 保护公司信息的完整性与可用性
 - 建立软件修补程序系统，用以管理、更新软件修补程序
投入资金 NT\$320,000
 - 更新磁盘主机(存放所有虚拟机、M 数据、ERP 数据、电子签核系统数据...)
投入资金 NT\$700,000
- 提供安全的生产环境
 - 扩充机房 UPS(不间断系统)并增加电源回路
投入资金 NT\$69,720
 - 机房 UPS(不间断系统)电池组更换
投入资金 NT\$65,000
 - 机房 UPS(不间断系统)加固工程
投入资金 NT\$35,175
- 防毒、防骇
 - 防病毒软件授权
投入资金 NT\$630,000
 - 更新 Windows 操作系统
 - 更新 Windows 操作系统，投入资金 NT\$448,000
 - 执行所有服务器弱点扫描-渗透测试
投入资金 NT\$138,000
 - 执行社交工程演练，加强员工资安意识，避免执行恶意电子邮件。
投入资金 NT\$138,600

2 重大资通安全事件

本年度无重大资通安全事件发生。