A. 信息安全风险管理架构：

- 信息安全之权责单位为信息中心，负责评估规划、执行及推动资安管理事项，并向同仁不定期倡导信息安全意识。
- 稽核室为信息安全监理之查核单位，定期查核执行缺失，要求受查单位提出相关改善计划并呈报董事会，且定期追踪改善成效，降低内部资安风险。
- 运作模式每年采循环式管理，确保资安可靠度之达成且持续检讨改善。

B. 信息安全管理方案：

信息安全管理方案		
类别	说明	相关措施
权限管理	人员账号、权限管理与系统操作行为	•人员账号权限管理与审核 •人员账号权限定期盘点
存取管控	人员存取内外部系统及数据传输管道之控制措施	•内/外部可存取范围定义管控措施 •操作轨迹记录
外部威胁	内部潜在弱点、中毒管道与防护措施	•主机/计算机弱点检测及更新措施 •档案与信件病毒防护与恶意软件检测 •防火墙防护与恶意软件检测
系统可用性	系统可用状态与服务中断时之处置措施	•系统/网络可用状态监控及通报机制 •信息备份措施、本/异地备援机制 •定期灾害复原演练
教育训练及倡导	不定期资安风险案例倡导	•不定期资安风险案例倡导

C.信息安全政策：

宏泰电工秉持维护公司之信息安全理念，对于公司所储存或传递之数据应作周全保护与防范，以杜绝毁损、计算机病毒、泄漏、滥用与侵权等事件。

本公司信息安全政策如下：

1. 信息安全措施，应符合政府法律之规范与公司信息安全政策及内控管理办法之相关要求；所有信息安全控制或程序之开发、修改及建置，须符合并遵循信息内控管理办法之机制。
2. 公司所有人员和供货商、客户，如需公司提供信息服务，均须依规定程序及指定措施办理信息业务，以维护本政策。
3. 本公司各单位信息资产管理者，必须对其所负责领域或持有之信息资产，建置使用状况之监控程序，以随时发掘系统或单位信息遭滥用的潜在风险，加强数据之机密性、可用性及完整性。
4. 所有人员对于发生安全事件、安全弱点及违反安全政策与程序之虞者，应透过适当通报机制，报告信息安全事件及信息安全弱点。
5. 工作分派应考虑职责分离，职务与责任范围应予区分，以避免信息或服务遭未授权修改或误用。
6. 公司严禁所有人员于公司信息设备上安装、使用、下载非法或未授权之软件。
7. 本公司将定期修订信息安全政策，并贯彻执行，以提升各信息系统所有作业之安全。
8. 任何危害信息安全之行为人，视情节轻重追究其民事、刑事及行政责任与相关惩处。

项目	说明
资安专责人员	已配置资安专责人员两名。
外部防火墙	强化对外网关安全，对外网络网关端采用新世代 Layer7 防火墙。
对外上网线路	强化线路安全，对外上网线路依其服务差异及重要性，已向中华电信申请共 13 条线路之资安服务，与新世代防火墙搭配使用，达到外部双层防御效果。
微软更新	配置 WSUS 更新系统，确保计算机之安全漏洞补强可实时到位，也避免微软发布更新若出现异常时进行控管避免灾难发生。
防毒系统	配置趋势科技最新版本 ApexONE 防毒系统，除一般系统病毒侦测及清除外，强化网页信誉评等、可疑联机侦测阻挡、行为监控及接口设备存取控管..等等防御。
终端计算机(PC、NB)	强化终端计算机安全性管理，逐步汰换早期操作系统计算机，目前 99% 以上终端计算机皆为 Windows 10 (含)以上操作系统。
资安方案	针对灾难备援 3-2-1 架构增设第二实体备援完成，并同步评估脱机云端备援机制并会同中华电信 POC 完成测试，准备进行导入。
教育训练	针对资安人员外训报名台湾金融研训院在线课程，分别为信息安全意识、必备知识与责任(120 分钟)、资安事件说明及预防措施(150 分钟)及上市上柜公司资通安全管控指引说明(90 分钟)；另针对同仁举办年度资安通识倡导教育训练课程(120 分钟)。