TISAX 信息安全策略

1. 信息资产保密策略	
目 的	明确为保障信息资产的保密性应当采取的管理措施。
适用范围	使用信息资产的所有人员。
信息资产保密策略	■ 为了管理信息系统并加强其安全，资讯部门可以记录、评审，同时也可以使用其信息系统中存储和传递的任何信息。 ■ 在符合法律要求的情况下，为保证信息系统的安全，资讯部门可以捕获任何使用者的活动，如访问的网站； ■ 为了商业目的，第三方将信息委托给公司内部保管，那么公司所有工作人员都必须尽最大的努力保护这些信息的保密性、完整性和可用性。客户的数据应该保密，并且对这些数据的访问也应该依据商业需求进行严格限制； ■ 使用者必须向本部门的信息安全接口人、资讯部门或管理层报告公司内部计算机安全的任何薄弱点，比如可能的误操作事故或者未授权访问的情况； ■ 在未经授权的情况下，使用者不得尝试访问公司内部系统中的任何数据或程序。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 信息安全管理手册》、《TISAX 信息资产控制管理程序》、《TISAX 访问控制管理程序》

2. **网络访问策略**	
目 的	建立网络基础设施的访问和使用规则，以保持信息完整性、可用性和保密性。
适用范围	访问任何信息资产的所有人。
网络访问策略	■ 未经资讯部门批准，不得私自安装路由器、交换机、集线器或者无线访问端口； ■ 计算机系统必须加入域控，方可访问公司网络； ■ 用于发现或揭露系统安全薄弱点的应用程序由资讯部门统一安装，使用者不得私自下载、安装或运行。例如，未经资讯部门批准，不得运行密码破解程序、监听器、网络绘图工具、或端口扫描工具； ■ 未经资讯部门批准，不得以任何方式更换网络硬件； ■ 在 Office365 企业云盘上共享文件时必须指定访问权限； ■ 网络访问账号应当实名且唯一，任何员工不得使用他人的账号访问； ■ 办公网络与生产环境网络应当进行隔离。 ■ 远程工作应通过 VPN 等公司允许的连接方式访问公司内部信息资源
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《企业网络资讯安全管理办法》

3. **访问控制策略**	
目 的	为了控制对信息和信息系统的访问。
适用范围	访问信息和信息系统的所有人员。
访问控制策略	■ 公司内部可公开的信息不作特别限定，允许所有使用者访问； ■ 公司内部部分公开信息，根据业务需求访问，访问人员提出申请，经访问授权管理部门认可，访问授权实施部门实施后使用者方可访问； ■ 公司网络、信息系统根据业务需求访问，访问人员提出申请，经本部门负责人、资讯部门管理员认可、授权后方可访问； ■ 资讯部门系统管理员应按规定周期对访问权限进行检查和评审； ■ 访问权限应及时撤销，如：申请访问时限结束时、员工聘用期限结束时、第三方服务协议中止时； ■ 未经相应管理员授权，使用者不得访问或尝试访问网络、系统、文件和服务； ■ 远程工作应通过 VPN 等公司允许的连接方式访问公司内部信息资源； ■ 未经资讯部门批准，不得以任何方式私自安装路由器、交换机、代理服务器、无线网络访问点(包括软件和硬件)等。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 访问控制管理程序》

4. **物理环境访问策略**	
目 的	为物理环境访问建立批准、控制、监控和删除规则。
适用范围	所有人员。
物理访问策略	■ 所有物理环境必须符合相应的法规，包含且不限于建设法规以及消防法规； ■ 对所有受限制的物理区域的访问必须形成文件并进行控制； ■ 所有物理区域必须依据其功能的关键程度或重要程度进行安全防护； ■ 所有受限制的物理区域访问必须依职责授权，且应当获得该区域负责人的批准； ■ 拥有物理区域访问权的所有人员都必须接受相应应急程序培训，并签署相关安全须知和保密协议； ■ 个人门禁卡/访客证不得与他人共享或借给他人； ■ 个人门禁卡/访客证不再使用时应当及时归还； ■ 个人门禁卡/访客证丢失或被盗时必须及时向该区域负责人报告； ■ 个人门禁卡/访客证不得轻易被非授权复制； ■ 所有受限制的物理区域的访问记录（包括外来人员）必须保存； ■ 人员离职或调岗时，区域负责人必须及时向门禁权限负责单位提出申请删除其访问权限； ■ 外来人员访问必须由专人陪同； ■ 受限制的物理区域的区域负责人必须定期评审人员进出记录，并要对异常访问进行调查； ■ 受限制的物理区域的区域负责人必须定期评审访问权限，并删除无效权限；

	■ 对受限制的物理区域必须进行隔离标记。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《门禁管制办法》《安全评估程序》《厂区进出管理办法》

5. **供应商访问策略**	
目 的	为降低供应商访问公司资产带来的风险。
适用范围	供应商及所有参与供应商管理过程的人员。
供应商访问策略	■ 供应商必须遵守相应的策略、操作标准以及协议，包括但不仅限于： 1. 信息资产保密策略； 2. 网络访问策略； 3. 访问控制策略。 ■ 供应商协议和合同必须规定： 1. 供应商可以访问的信息； 2. 供应商应当怎样保护信息； 3. 合同结束时，供应商所拥有的信息归还、毁灭或处置方法； 4. 供应商只能使用用于商业协议目的的信息和信息资产； 5. 在合同期间，供应商所获得的任何信息都不能用于非合同目的。 ■ 资讯部门应当参与协助供应商信息安全年审，确保供应商符合策略的要求；

	■ 应当对供应商进行分类，如 IT 基础组件运维服务、系统维护服务、网络维护服务等，并定义不同类型供应商可以访问的信息类型，以及如何进行监视和工作访问权限； ■ 供应商的访问权限仅限于工作需要，且由相关管理部门批准授权； ■ 供应商不得将已授权的身份识别信息和相关设备透露、借用给其他人员，工作结束后应当立即注销访问权限及清空资料； ■ 供应商必须提供参与合同工作的人员清单，人员发生变更时必须在 24 小时之内更新并提供； ■ 在公司场所内工作的供应商都必须佩带身份识别卡； ■ 供应商在发现安全事故的时候应当及时向 TISAX 信息安全执行办公室报告； ■ 如果供应商参与安全事故管理，那么必须在合同中明确规定其职责； ■ 供应商必须遵守所有适用的更改控制过程和程序； ■ 供应商定期进行的工作任务和时间必须在合同中规定。规定条件之外的工作必须由相应的管理者书面批准； ■ 供应商访问账号必须实名且唯一，其所有密码必须符合密码规范。 ■ 当供应商员工离职时，供应商必须确保所有敏感信息在 24 小时内被收回或销毁； ■ 在合同或邀请结束时，供应商应该将所有信息返回或销毁， ■ 在合同或邀请结束时，供应商必须立即归还所有身份识别卡、访问权限、设备和供应品。由供应商保留的设备和/或供应品必须被相关管理者书面授权； ■ 供应商必须遵守所有规定和审核要求，包括对供应商工作的审核； ■ 在提供服务时，供应商使用的所有软件必须进行相应的清点并许可。

责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 访问控制管理程序》《IT 第三方管理程序》

6. **员工访问策略**	
目 的	为访问公司信息资产的全体员工提供物理和行政安全管理、职责和信息保护的准则。
适用范围	全体员工。
员工访问策略	■ 员工必须遵守相应的策略、操作标准以及协议，包括但不仅限于： 1. 《信息资产保密策略》; 2. 《病毒防范策略》; 3. 《恶意代码防范策略》; 4. 《信息交换策略》; 5. 《清洁桌面和清屏策略》; 6. 《网络访问策略》; 7. 《便携式计算机安全策略》; 、 8. 《互联网使用策略》; 9. 《电子邮件策略》。 ■ 员工在意识到有安全事件发生时应当立即向上层领导、本部门信息安全接口人或资讯部门报告;

	■ 员工必须遵守所有适用的变更管理流程； ■ 当员工离职或调岗时，必须在 OA 系统上发起《工作交接单》，确保： 1. 所有的工作数据被完整交接； 2. 身份识别卡、设备等被收回，并由相关资产负责人确认； 3. 所有访问权限被收回，并由相关资产负责人确认。 ■ 员工必须遵守所有规定和审核要求。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 访问控制管理程序》、《TISAX 信息安全事件管理程序》

7. **设备及布缆安全策略**	
目 的	保护设备在公司场所内外免受物理和环境的威胁，减少因未授权访问造成的风险，防止因设备的丢失、损坏、失窃等情况造成的公司运营活动的中断。
适用范围	设备设施的建设和维护人员。
设备及布缆安全策略	■ 设备应进行适当安置，以尽量减少不必要的访问； ■ 处理敏感数据的信息设备应当采取视线保护措施，以减少在其使用期间信息被窥视的风险，还应保护其物理环境以防止未授权访问； ■ 要求专门保护的部件要予以隔离； ■ 应采取控制措施以避免潜在的物理威胁，例如偷窃、火灾、爆炸、烟雾、水（或供

	水故障)、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏； ■ 应监视可能对信息处理设施运行状态产生负面影响的环境条件（例如温度和湿度)； ■ 所有建筑物都应采用避雷保护； ■ 应保护处理敏感信息的设备，以减少由于辐射而导致信息泄露的风险。 ■ 应定期检查和测试 UPS 等支持性设施，确保其功能正常，减少由于设施故障或失效带来的风险。应按照设备制造商的说明提供合适的供电； ■ 对支持关键业务操作的设备，尽量使用支持有序关机或连续运行的不间断电源（UPS)； ■ 进入信息处理设施的电源和通信线路应当在地下或提供足够的可替换的保护； ■ 网络布缆要免受未授权窃听或损坏，例如，利用电缆管道或使路由避开公众区域； ■ 为了防止干扰，电源电缆要与通信电缆分开； ■ 使用清晰的可识别的电缆和设备记号，以使处理失误最小化，例如，错误网络电缆的意外配线； ■ 用文件化配线列表减少失误的可能性； ■ 对于敏感或核心系统，更进一步的控制考虑应包括： 1. 在检查点和终接点处安装铠装电缆管道、上锁的房间或盒子； 2. 使用可替换的路由选择和/或传输介质，以提供适当的安全措施； 3. 使用光缆； 4. 使用电磁防辐射装置保护电缆； 5. 对于电缆连接的未授权装置要主动实施技术清除、物理检查。

	■ 要按照供应商推荐的服务时间间隔和规范对设备进行维护； ■ 只有已授权的维护人员才可对设备进行修理和服务； ■ 要保存所有可疑的或实际的故障以及所有预防和纠正维护的记录； ■ 当对设备安排维护时，应实施适当的控制，要考虑维护是由场所内部人员执行还是由外部人员执行；当需要时，敏感信息需要从设备中删除或维护人员应当签署保密协议； ■ 在办公场所外使用任何信息处理设备都要通过相关管理者授权； ■ 离开建筑物的设备和介质在公共场所不应无人看管。在旅行时便携式计算机要作为手提行李携带； ■ 应当有足够的安全保障掩蔽物，以保护离开办公场所的设备。安全风险在不同场所可能有显著不同，例如，损坏、盗窃和截取，要考虑确定最合适的控制措施； ■ 家庭工作时，应当采取合适的控制措施，例如，可上锁的存档柜、清理桌面策略、对计算机的访问控制以及与资讯部门的安全通信； ■ 制造商的设备保护说明要始终加以遵守，例如，防止暴露于强电磁场内； ■ 包含敏感信息的设备在物理上应予以摧毁，或者采用使原始信息不可获取的技术进行破坏、删除或覆盖； ■ 包含敏感信息的已损坏的设备应当销毁； ■ 对国际派遣人员应当采取相应的培训，培训内容包括安全意识、派遣地当局合法检查的应对措施、前往安全敏感度高的国家的应对措施； ■ 设备转移应当形成记录； ■ 应对未授权资产的移动进行抽查，检测未授权的记录装置，防止其进入办公场所。

	这样的抽查应按照相关规章制度执行且只能在法律法规要求的适当授权下执行。全体员工应当知晓相关规章制度。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《门禁管制办法》《安全评估程序》《厂区进出管理办法》

8. **变更管理安全策略**	
目 的	以一种合理的、可预知的方式管理变更，以便员工和客户能进行相应的计划。变更需要事先严格计划、仔细监控并要进行追踪评价，以降低对使用者群的负面影响，增加信息资产的价值。
适用范围	安装、操作或维护信息资产的所有人员。
变更管理安全策略	■ 对信息资产的每一次变更，如操作系统、计算机硬件、网络以及应用程序都要服从变更管理策略，并且必须遵守变更管理流程； ■ 所有影响计算机环境设备的变更(如空调、水、热、管道、电)需要向变更过程中的管理者报告，并与之协调处理； ■ 无论是事先有计划的变更还是事先无计划的变更必须都提交书面的变更申请； ■ 所有事先有计划的系统变更申请必须按照变更管理流程的规定提交，以便资讯部门有足够的时间评审申请，确定并重新评审潜在的失败，并决定申请被批准还是延期执行；

	■ 每一个事先计划的变更申请在执行前必须受到资讯部门的正式批准； ■ 指定的资讯部门领导在下列情况下有权拒绝任何申请：不充分的策划、不充分的删除计划、变更的时间等会对关键的业务过程造成负面影响，或者会造成没有充分的资源可用； ■ 在变更管理流程实施前，必要时需通知客户； ■ 每一次变更必须进行变更评审，无论是计划还是未计划的，成功的还是失败的； ■ 所有变更必须保留变更管理日志，必须保留的日志包括但不限于下列内容： 1. 变更的提交和执行日期； 2. 所有者和保管者信息； 3. 变更的特性； 4. 成功或失败的标志。 ■ 所有信息系统必须遵照上述规定进行变更。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 项目实施管理程序》、《信息系统变更管理程序》

9. **病毒防范策略**

目 的	描述计算机病毒、蠕虫以及特洛伊木马防御、检测以及清除的要求。
适用范围	使用信息资产的所有人员。

病毒防范策略	■ 所有连接到局域网的工作站必须使用资讯部门批准的病毒保护软件和配置； ■ 病毒保护软件不得被禁用、卸载、被绕过； ■ 病毒保护软件的更改不能降低软件的有效性； ■ 不得私自更改病毒保护软件的自动更新频率； ■ 与局域网连接的每一个文件服务器必须使用资讯部门批准的病毒保护软件，并要进行设置检测、清除可能感染共享文件的病毒； ■ 由病毒保护软件不能自动清除并引起的安全事故，必须向本部门负责人、本部门信息安全接口人或资讯部门报告。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《企业网络资讯安全管理办法》

10. **恶意代码防范策略**	
目 的	阻止和发现未经授权的恶意代码的引入，实施对恶意代码的监测、预防和恢复控制。
适用范围	使用信息资产的所有人员。

可移动代码防范策略	■ 禁止使用未经授权的软件。 ■ 防范经过外部网络或任何其它媒介引入文件和软件相关的风险，并采取适当的预防措施。 ■ 定期对支持关键业务过程的系统中的软件和数据进行检测； ■ 安装并定期升级防病毒的检测软件和修复软件，定期扫描计算机和存储介质。 ■ 资讯部门负责恶意代码防护、使用培训、病毒袭击和恢复报告。 ■ 为从恶意代码攻击中恢复，需要制定适当的业务持续性计划。包括所有必要的数据、软件备份以及恢复安排。 ■ 所有使用者应有防欺骗的意识，并知道收到欺骗信息时如何处置。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 运维管理规范》

11. **信息备份安全策略**	
目 的	设置电子信息的备份和存储职责。
适用范围	资讯部门 DBA 及 Infra 组。
信息备份安全策略	■ 信息备份周期和方式必须依据信息的重要性以及数据所有者确定的可接受风险确定； ■ 场所外备份存储必须达到信息存储的最高等级；

	■ 场所外备份存储区的物理访问控制的实施必须满足并超过原系统的物理访问控制，另外备份介质必须依据信息存储的最高安全等级进行保护； ■ 必须建立并实施对电子信息备份成功与否的验证过程； ■ 必须对场所外备份存储区每年进行评审。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 运维管理规范》

12. **网络配置安全策略**	
目 的	为网络基础设施的维护、扩展以及使用建立规则。
适用范围	访问信息资产的所有人。
网络配置安全策略	■ 资讯部门对网络基础设施进行管理并作为最终负责部门； ■ 为了提供稳固的网络基础设施，所有电缆必须由资讯部门或被认可的合同方安装； ■ 所有网络连接设备必须按照资讯部门批准的规范进行配置； ■ 所有连接到网络的硬件必须服从资讯部门的管理和监控标准； ■ 未经资讯部门批准，不得对活动的网络管理设备的配置进行更改； ■ 网络基础设施支持一系列合理定义的、被认可的网络协议。使用任何未经认可的协议都必须经过资讯部门的批准；

	■ 支持协议的网络地址由资讯部门集中分配、注册和管理； ■ 网络基础设施与外部供应商网络的所有连接都由资讯部门负责； ■ 资讯部门的防火墙必须按照防火墙实施规范文件进行安装和配置；
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 运维管理规范》、《企业网络资讯安全管理办法》

13. **信息交换策略**	
目 的	保持公司内部与任何外部机构之间所交换的信息和软件的安全。
适用范围	所有人员。
信息交换策略	■ 不能在公共场所、敞开的房间或没有屋顶防护的会议室谈论机密信息。 ■ 对信息交流应作适当的防范，如不要暴露敏感信息，避免被通过电话偷听或截取。 ■ 员工、合作方以及任何其他使用者不得损害本局的利益，如诽谤、骚扰、假冒、未经授权的采购等。 ■ 不得将敏感或关键信息放在打印设施上，如复印机、打印机和传真，防止未经授权人员的访问。 ■ 做应用系统之间接口、协议时，不能影响双方应用的正常运行；在实施之前应充分考虑应用系统的资源是否足够；保证数据交换的权限最小化。 ■ 在进行与相关方信息交换时，需提前指定双方的信息交换人员、交换方式、交换

	保密方法，以防止信息的泄露。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 信息安全交流管理程序》

14. **运输中物理介质安全策略**	
目 的	确保包含信息的介质在组织的物理边界以外运送时，防止未授权的访问、不当的使用或毁坏。
适用范围	所有人员。
运输中物理介质安全策略	■ 应考虑下列策略以保护不同地点间传输的信息介质： 1. 使用可靠的运输或送信人； 2. 包装要足以保护信息免遭在运输期间可能出现的任何物理损坏，并且符合制造商的规范（例如软件），例如防止可能减少介质恢复效力的任何环境因素，例如暴露于过热、潮湿或电磁区域；

	3. 若需要，应采取专门的控制，以保护敏感信息免遭未授权泄露或修改；例子包括： 3.1 使用可上锁的容器； 3.2 手工交付； 3.3 防篡改的包装（它可以揭示任何想获得访问的企图）； 3.4 在异常情况下，把托运货物分解成多次交付，并且通过不同的路线发送。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 信息资产控制管理程序》

15. **电子邮件策略**	
目 的	建立公司的 Email 使用规则，保证 Email 的合理发送、收取和存储。
适用范围	所有人员。
电子邮件策略	■ 下列行为是策略所禁止的： 1. 发送或者转发虚假、黄色、反动信息； 2. 发送或者转发宣扬个人政治倾向或者宗教信仰； 3. 发送或者转发发送垃圾信息； 4. 发送或者转发能够引起连锁发送的恐吓、祝贺等信息； 5. Email 附件大小超过限制 20M； 6. 发送密码、密钥、信用卡等的敏感信息； 7. 用公司外部账号发送、转发、收取公司敏感信息；

	8. 在非授权情况下以公司的名义发表个人意见； 9. 发送或者转发可能有计算机病毒的信息； 10. 使用非授权的电子邮件收发软件； ■ 下列行为是策略所要求的： 1. 經申請核可的员工都有一个 Email 账号，账号密码必须符合密码策略的相关规定； 2. 用 Email 经过外部网络发送机密信息必须经过加密，加密必须符合加密策略的相关规定； 3. 发送 Email 必须有清楚的主题； 4. Email 的处理和存储必须符合信息的分类、标识和存储策略的相关规定； ■ 管理授权 1. 公司有权对职员的 Email 进行监视和记录； 2. 公司有权对 Email 的内容进行存储备份以用于法律目的；
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 运维管理规范》

16. **信息安全监控策略**	
目 的	确保信息资产控制措施被适当、有效地实施并且不被忽视。
适用范围	负责信息资产安全、现有信息资产的操作以及负责信息资产安全的所有人员。
信息安全监控	■ 自动检测工具会对检测到的破坏行为或薄弱点利用进行实时通知；

策略	■ 在检查破坏行为以及薄弱点被利用情况时可以使用下列文件： 1. 防火墙日志 2. 使用者账户日志 3. 网络扫描日志 4. 系统出错日志 5. 应用程序日志 6. 数据备份和恢复日志 ■ 下列内容应该由负责的人员每年至少检查一次： 1. 密码强度 2. 未经授权的网络设备 3. 未经授权的个人网络服务器 4. 未受保护的共享设备 5. 操作系统和软件许可
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 运维管理规范》

17. **特权访问管理策略**	
目 的	为具有特殊访问权限的账号建立创建、使用、控制及其删除的规则。
适用范围	拥有信息资产特殊访问权限的所有人员。

特权访问管理策略	■ 所有管理性的/特殊访问账户的使用者必须接受培训并获得授权； ■ 所有管理性的/特殊访问账号的使用者都必须避免滥用权力，并且必须在资讯部门的指导下使用； ■ 所有管理性的/特殊访问账号的使用者必须以最适宜所执行的工作的方式行使账号权力 ； ■ 所有管理性的/特殊访问账号必须满足密码策略的要求； ■ 共有管理性的特殊访问账号的密码在人员离职或发生变更时必须更改； ■ 当因内外部审核、软件开发、软件安装或其他规定需求而需要特殊访问账号时，账号： 1. 必须被授权； 2. 创建的日期期限必须明确； 3. 工作结束时必须删除。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 访问控制管理程序》

18. **密码控制策略**	
目 的	为秘密鉴别信息建立创造、分发、保护、终止以及收回的规则。
适用范围	所有人员。
Password control strategy 密码控制策略	■ 所有密码，包括初始密码，都必须依据资讯部门规定的下列规则建立和执行： 1. 必须定期更改（最长 90 天）； 2. 必须符合资讯部门规定的最小长度（8 位字符）； 3. 必须符合复杂度要求，即数字+字母大小写的组合，例如：u4P083ak 4. 必须不能是可以轻易联想到的帐号所有者的特性：使用者名、绰号、亲属的姓名、生日等； 5. 必须保存历史密码，以防止密码的重复使用。 ■ 特殊权限使用者的密码除以上要求需要满足外，还有特殊要求：密码长度不少于 14 位。 ■ 首次登录时必须更改密码； ■ 账号密码必须不能泄露给任何人； ■ 如果怀疑密码的安全性，应立即进行更改； ■ 使用者不能通过自动登录的方式绕过密码登录程序； ■ 计算机设备如果无人值守必须启动密码保护屏保或注销； ■ 不得以任何形式记录密码。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 访问控制管理程序》

19. **清洁桌面和清屏策略**	
目 的	防止对信息和信息处理设施未经授权的使用者访问、破坏或盗窃。
适用范围	该策略适用于公司所有员工。
清洁桌面和清屏策略	■ 含有涉密信息或重要信息的文件、记录、磁盘、光盘或以其它形式存贮的媒体在人员离开时，应锁入文件柜、保险柜等； ■ 所有计算机终端必须设立登录密码，在人员离开时应该锁屏、注销或关机； ■ 在结束工作时，必须关闭所有计算机终端，并且将个人桌面上所有记录有敏感信息的介质锁入文件柜； ■ 应清洁电脑屏幕，确保不放置重要信息在电脑桌面上。 ■ 计算机终端应设置屏幕密码保护，屏保时间不大于 15 分钟； ■ 打印或复印公司机密信息时，打印或复印设备现场应有可靠人员，打印或复印完毕即从设备拿走。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 信息资产控制管理程序》

20. **互联网使用策略**	
目 的	规范互联网以及公司内部网络的使用，确保信息资产不会被泄漏、篡改、破坏。
适用范围	所有人员。
互联网使用策略	■ 提供给授权使用者的互联网浏览软件只能用于公司业务； ■ 所有用于访问互联网的软件必须都经过资讯部门批准，并且必须结合卖方提供的安全补丁； ■ 从互联网下载的所有文件必须通过资讯部门批准的病毒检测软件进行病毒扫描； ■ 访问的所有站点都必须符合信息资产使用策略； ■ 对使用者在信息资产上的所有活动都必须进行记录并评审； ■ 所有 Web 站点上的内容都必须符合信息资产使用策略； ■ 不能通过 Web 站点访问攻击性的或骚扰性的资料； ■ 私人的商业广告不能通过 Web 站点发布； ■ 互联网不可以用于个人私利； ■ 在不能确保资料只被授权的人员或组织使用时，数据不能通过 Web 站点获取； ■ 通过外部网络传送的所有敏感资料都必须经过加密； ■ 电子文件必须服从适用其文件类型的保存规则，必须依照部门记录保存方案进行保存； ■ 文档和文件的发送或接受必须以不引起法律责任或阻碍的方式进行； ■ 使用互联网应遵循法律法规要求，并不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法

	犯罪活动。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《企业网络资讯安全管理办法》、《IT 运维管理规范》

21. **便携式计算机安全策略**	
目 的	建立移动计算机设备的使用规则及其与互联网的连接规则。
适用范围	所有人员。
便携式计算机安全策略	■ 只有被批准的便携式计算机设备才能用来访问信息资产； ■ 便携式计算机设备必须有密码保护； ■ 存储在便携式计算机设备中的重要数据应定期备份； ■ 无线传输设备必须设定复杂化密码。 ■ 对无人看守的便携式计算机设备必须实施物理保护，必须放在带锁的资讯部门、抽屉或文件柜里，或者锁在桌子或柜子上； ■ 非授权便携式计算机禁止加入公司网络；
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 运维管理规范》、《TISAX 访问控制管理程序》

22. **事件管理策略**	
目 的	描述处理信息安全事件的要求。
适用范围	所有人员。
信息资产保密策略	■ 在怀疑或确定发生安全事件时都必须遵循适当的事件管理程序，例如病毒、蠕虫、恶意邮件等； ■ 所有员工都有义务在发现信息安全事件时向各部门信息安全接口人或资讯部门报告，由 TISAX 信息安全管理委员会启动事件管理程序； ■ 在事件调查过程中，信息安全管理委员会负责确定要搜集的实物和电子证据； ■ 资讯部门应当维护用于监控安全事件破坏的技术资源； ■ TISAX 信息安全管理委员会负责启动、完成并记录事件调查过程； ■ TISAX 信息安全管理委员会负责向下列部门或人员报告： 1. 信息资产相关部门 2. 在有关事件响应的法律、法规和/或规章中要求的地方、省、国家有关部门 ■ TISAX 信息安全管理委员会负责与外部组织以及法规强制部门的协调沟通； ■ 在涉及到客户的信息安全事件中，信息安全管理委员会应当与相关部门协商与客户的沟通事宜； ■ 在触犯法律法规的情况下，信息安全管理委员会应当向法务部报告。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 信息安全事件管理程序》

23. **业务信息系统使用策略**	
目 的	规范化员工在业务系统上的操作。
适用范围	所有人员。
业务信息系统使用策略	■ 加强保护业务信息系统免受网络安全风险的干扰； ■ 公司业务信息系统的使用人员应该有熟练的操作技巧； ■ 相关人员使用业务系统前应当进行操作培训。 ■ 因工作需要访问业务系统的人员应当提出申请并经过资讯部门批准、授权。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 项目实施管理程序》

24. **远程工作策略**	
目 的	确保远程工作过程中的信息安全。
适用范围	所有人员。
远程工作策略	■ 远程工作的方式必须获得资讯部门的批准、授权，任何部门和个人不得私设可以远程访问的接口； ■ 远程工作应仅限于申请的设备，严禁在公共计算机设备（例如网吧）上进行； ■ 远程工作人员不得将相关身份识别信息和设备透露、借用给其他人员，工作结束后

	应该立即注销并断开远程连接； ■ 远程工作的相关通信和设备必须由资讯部门进行配置和监控； ■ 远程工作的访问权限不允许超过该人员在公司内部网络的正常访问权限； ■ 外部供应商需要连接本公司网络进行系统维护或故障诊断应该签订保密协议，明确对方的保密责任和相关安全要求；远程访问时要做好记录，维护结束后立即断开连接。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 访问控制管理程序》、《企业网络资讯安全管理办法》

25. 安全开发策略	
目 的	确保进行信息安全设计，并确保其在信息系统开发生命周期中实施。
适用范围	开发人员
远程工作策略	■ 保证开发环境的安全，做到开发环境、测试环境、生产环境相隔离，权限单独控制； ■ 制定软件开发周期的安全指南，包括软件开发方法的安全、开发程序的安全编码指南； ■ 收集并编写系统的安全需求； ■ 在软件的里程碑设置时考虑安全的检查点；

	■ 建立安全知识库，记录意外开发中遇到的安全问题解决经验； ■ 对开发者进行安全意识培训，培训内容包括但不限于系统开发技术的脆弱性。
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《IT 项目实施管理程序》

26. 数据保护策略	
目 的	为维护环旭电子股份有限公司（以下称“环旭电子”）及其客户、合作厂商人员、访客、网站使用者、投资人或股东、求职者及员工等个人资料所有人之个人信息（下称简称“个人信息”），环旭电子依据所适用国家或者地区之隐私权及个人信息保护相关法律法规，制定相应的隐私权及个人信息数据保护政策(下称“数据保护政策”）作为环旭电子合规管理遵循依据，环旭电子依循该等数据保护政策管理个人信息资料搜集、处理及利用等相关作业，并要求环旭电子之供应商、承包商、外部顾问等合作厂商依循环旭电子之数据保护政策落实合规管理，共同实践隐私权及个人信息资料保护，以确保个人信息所有人权益。
适用范围	环旭电子股份有限公司及其客户、合作厂商人员、访客、网站使用者、投资人或股东、

	求职者及员工等
数据保护策略	1. 环旭电子可能基于下列特定目的搜集、处理及利用个人信息资料: (a). 业务营运 (b). 商业行销 (c). 安全管理 (d). 网站维护及沟通 (e). 求职者招聘及面试与管理员工或为员工提供服务 (f). 履行法定义务所必要 (g). 依法协助公务机关执行法定职务所必要 (h). 主张、行使或保护USI法律权利所必 2. 不会主动搜集、处理及利用特种个人资料，包含病历、医疗纪录、健康检查及犯罪前科等，但下列情况除外： (a). 适用法规明文规定 (b). 履行法定义务所必要，且有适当安全维护措施 (c). 依法协助公务机关执行调查不法行为、预防犯罪发生或侦查犯罪案件等法定职务所必要 (d). 经个人信息资料所有人同意 3. 环旭电子搜集、处理及利用个人信息资料不得逾越特定目的之必要范围，并应确保个人信息资料之搜集、处理及利用与特定目的具有正当合理之关联性。个人信息资料所有人得请求停止搜集、停止处理、停止利用、删除或销毁环旭电子搜集、处理及利用之个人信息资料，环旭电子应依循执行。

	环旭电子应采取合理必要措施维护个人信息资料正确性，并主动或依个人信息资料所有人之请求予以补充或更正。 4. 环旭电子留存个人资料时间不得逾越特定目之必要范围所需合理期间，并且在个人信息资料留存期间内，环旭电子应采取适当安全维护措施，对于个人信息资料存取、处理、传输、留存、读取权限、相关传输及储存设备之资讯安全进行完整管控，防止个人信息资料之毁损、灭失、窃取、泄漏或未经授权读取、复制、使用、窜改，以确保个人信息资料安全。 5. 在不逾越原搜集、处理及利用个人信息资料之特定目的之必要范围内，环旭电子位处不同国家之关系企业间可能进行跨境传输及使用个人资料时，应遵循环旭电子之数据保护政策及传输地区所适用之隐私权及个人信息资料保护适用法规管理跨境传输及使用。 6. 环旭电子要求新进人员须完成隐私权及个人信息资料保护教育宣导课程，并定期向所有员工宣导隐私权及个人信息资料保护相关法规及合规管理作业指引，以强化合规意识。 7. 环旭电子除进行年度风险评估及内部合规稽核外，亦不定期执行供应商合规稽核及透过外部独立单位稽核本公司隐私权及个人信息资料保护管理措施，以确保相关作业符合环旭电子数据保护政策及隐私权及个人信息资料保护相关适用法规。
责任	环旭电子对于违反隐私权及个人信息资料保护行为采取零容忍政策。若经调查发现确有涉入违反本政策或隐私权及个人信息资料保护相关适用法律法规之情事，环旭电子将立即检讨改善管理措施，并依照适用纪律规范惩戒涉入违反行为之人员，必要时并

	将依据适用法律法规进行求偿或追诉。 |
引用制度	《TISAX 隐私数据处理管理程序》 《TISAX 隐私影响评估管理程序》 《数据跨境传输政策》 《TISAX 数据主体权利与访问请求管理规定》

27. 样件保护策略	
目 的	降低新品开发信息安全泄露的风险，提高全员原型保护意识
适用范围	1.项目 NPI-SOP 前的样件，包括客户尚未向公众展示和/或以适当形式发布的样件及零部件。 2.适用人员为产品工程、测试工程与项目管理处所有人员及公司内外部与样件开发过程中相关的生产制造、设计验证（可靠性测试）、物流、仓储、借阅和销毁等人员
样件保护策略	■ 工程样件、测试样件的标签名称不得直接使用在售市场的车辆名称，需经过脱名或代号，通过标签应无法轻易看出所属的在售车型名称 ■ 工程样件、测试样件不得存放在无人看守的敞开环境中，应确保无人时样件存放在安全区域 ■ 样件及零部件必须包装、装箱进行运输，以防止样件在公共区域被暴露、窥视和拍照。如果运输过程有特殊要求的，必须根据客户的要求进行。 ■ 样件的异地运输应由客户指定或经公司物流管理部认可的物流公司承运，样件必须包装完好不得暴露，且应拒绝未经授权的检查。如若运输过程中样件丢失或者信息泄露，应即刻向物流管理部经理报备，并由物流管理部报至项目经理，由项目经理向客户报告

	■ 工程样件、测试样件借用仅限公司内部人员，向产品工程部借用样件时应表明借用部门、用途、是否破坏样件、是否归还等信息，获得部门内主管级或以上领导同意后可借用，需要归还的样件应在承诺归还的日期内归还，不需要归还的样件在使用结束后应按照公司报废流程自行报废。 ■ 工程样件、测试样件报废应遵守公司《废料、废品处理管理制度》，填写《报废单》，经部门主管以上领导签字后，应将报废的样件拆解到无法拆解的程度，并运输至指定报废地点，由专人进行破坏，报废单随实物转交给废品管理员进行报废。 ■ 工程样件、测试样件的对外技术展示应遵守样件相对应客户有关展示的规定。 ■ 与样件有关的从业人员或供应商应确保已签订《员工保密协议》或《供应商保密协议》，在从事与样件有关的活动时应遵守保密协议中的规定。 ■ 公司外部人员进入产品工程部所属区域或可靠性测试实验室须填写《访客登记表》，并获得部门主管级以上领导同意，外来人员访问期间应严格遵守《访客管理规定》，受访人应全程陪同
责任	违背该策略可能导致：员工以及临时工被解雇、合同方或顾问的雇佣关系终止、实习人员和志愿者失去继续工作的机会；另外， 这些人员还可能遭受信息资产访问权以及公民权的损失，甚至遭到法律起诉。
引用制度	《TISAX 信息安全交流管理程序》