信息等级：重要
受控状态：受控
文件编号：CM-IM-005-V1.0

信息安全策略

版本号：V1.0

发布日期：2020年06月15日

蝉鸣科技（西安）有限公司

变 更 履 历

版本	变更内容	编制人/ 创建日期	审核人/ 审核日期	批准人/ 批准日期	备注
V1.0	**文档建立，初次发布**	人力行政中心 2020.06.15	刘瑞青 2020.06.15	张威 2020.06.15	

目 录

1. 信息资源保密策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	保密策略是用于为信息资源用户建立限制的机制。通过一定权限管理以区分内外部用户的信息资源的访问。		
目 的	该策略的目的是明确用户对信息资源沟通的保密需求。		
适用范围	该策略适用于使用信息资源的所有人员。		
术语定义	略		
信息资源保密策略	■ 在公司内部保存和控制的电子文件应该得到控制，只有得到授权的人员才能访问； ■ 为加强信息安全，IT 管理员可以记录和评审信息系统中存储和传递的任何信息。为了达到此目的，IT 管理员还可以捕获任何用户活动，如通讯记录以及访问的网站； ■ 为了商业目的，客户方将信息委托给公司内部保管，那么 IT 管理员的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和安全性。 ■ 用户必须向适当的管理者报告公司内部计算机安全的任何薄弱点，可能的误用事故或者相应授权协议的违背情况； ■ 在未经授权或获得明确同意的情况下，用户不可以尝试访问公司内部系统中包含的任何数据或程序。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

2. 网络访问策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	网络基础设施是提供给所有信息资源用户的中心设施。重要的是这些基础设施（包括电缆以及相关的设备）要持续不断的发展以满足需求，然而也要求同时高速发展网络技术以便将来提供功能更强大的用户服务。		
目 的	该策略的目的是建立网络基础设施的访问和使用规则。这些规则是保持信息完整性、可用性和保密性所必需的。		
适用范围	该策略适用于访问任何信息资源的所有人。		
术语定义	略		
网络访问策略	■ 用户不可以以任何方式扩散或再次传播网络服务。未经研发中心批准不可以安装路由器、交换机或者无线访问端口； ■ 在未经研发中心批准的情况下，用户不可以安装提供网络服务的硬件或软件； ■ 需要网络连接的计算机系统必须符合信息服务规范； ■ 下用户禁止私自下载、安装或运行安全程序或应用程序去扫描系统的安全薄弱点，如，口令破解程序、监听器、网络绘图工具、或端口扫描工具。即使网络管理人员因工作需要必须使用以上工具时，也应取得研发中心批准。 ■ 在局域网上进行文件共享时必须指定访问权限，敏感信息严禁使用 everyone 权限。 ■ 任何员工在访问网络资源时必须使用专属于自己的帐号 ID,不得使用他人的帐号访问网络资源。 ■ 网络分为办公网络和生产环境网络，办公网络又分为日常办公网络和专用访问网络 ■ 生产环境网络与办公环境网络宜进行分割，以确保访问的控制。 ■ 不得从生产环境下载拷贝等操作 ■ 只能从公司指定办公网络（公司专门的网络通道）访问远程的服务器		

	■ 修改远程服务器的内容必须要提前申请报告，且要有详细的操作步骤 ■ 网络管理人员拥有网络基础设施并对其负责，而且还要对基础设施的发展和增加进行管理； ■ 为了提供稳固的网络基础设施，所有电缆必须由研发中心或被认可的合同方安装； ■ 所有连接到网络的硬件必须服从研发中心的管理和监控标准； ■ 在没有研发中心批准的情况下，不能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研发中心的批准； ■ 支持协议的网络地址由研发中心集中分配、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研发中心负责。这包括与外部网络的连接； ■ 在未获得研发中心书面授权的情况下，部门不得使用防火墙；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

3. 访问控制策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	应根据业务和安全要求，控制对信息和信息系统的访问。		
目 的	该策略的目的是为了控制对信息和信息系统的访问。		
适用范围	该策略适用于进行信息和信息系统访问的所有人员。		
术语定义	略		
访问控制策略	■ 公司内部可公开的信息不作特别限定，允许所有用户访问； ■ 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用户方可访问； ■ 公司网络、信息系统根据业务需求访问，访问人员提出申请，经研发中心认可，实施后用户方可访问； ■ 研发中心安全管理员按规定周期对访问授权进行检查和评审； ■ 访问权限应及时撤销，如在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； ■ 用户不得访问或尝试访问未经授权的网络、系统、文件和服务； ■ 远程用户应该通过公司批准的连接方式； ■ 在防火墙内部连接内部网络的计算机不允许连接 INTERNET ，除非获得研发中心的批准； ■ 用户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； ■ 在信息网、外联网安装新的服务（ 包括软件和硬件 ）必须获得研发中心的批准； ■ 用户不得私自撤除或更换网络设备。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

4. 物理访问策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	技术支持人员、安全管理员、IT 管理员以及其他人员可能因工作需要访问信息资源物理设施。对信息资源设施物理访问的批准、控制以及监控对于全局的安全是极其重要的。		
目 的	该策略的目的是为信息资源设施物理访问的批准、控制、监控和删除建立规则。		
适用范围	该策略适用于组织中负责信息资源安装和支持的所有人员，负责信息资源安全的人员以及数据的所有者。		
术语定义	略		
物理访问策略	■ 所有物理安全系统必须符合相应的法规，但不仅限于建设法规以及消防法规； ■ 对所有受限制的信息资源设施的物理访问必须形成文件并进行控制； ■ 所有信息资源设施必须依据其功能的关键程度或重要程度进行物理保护； ■ 对信息资源设施的访问必须只授权给因职责需要访问设施的支持人员和合同方； ■ 授权使用卡和/或钥匙访问信息资源设施的过程中必须包括设施负责人的批准； ■ 拥有信息资源设施访问权的每一个人员都必须接受设施应急程序培训，并且必须签署相应的访问和不泄密协议； ■ 访问请求必须发自相应的数据/系统所有者； ■ 访问卡和/或钥匙不可以与他人共享或借给他人； ■ 访问卡和/或钥匙不需要时必须退还给信息资源设施负责人。在退还的过程中，卡不可以再分配给另一个人； ■ 访问卡和/或钥匙丢失或被盗必须向信息资源设施的负责人报告； ■ 卡和/或钥匙上除了退回的地址外不可以有标志性信息；		

	■ 所有允许来宾访问的信息资源设施都必须使用签字出/入记录来追踪来宾的访问； ■ 信息资源设施的持卡访问记录以及来宾记录必须保存，并依据被保护信息资源的关键程度定期评审； ■ 在持卡和/或钥匙的人员发生变化或离职时，信息资源设施的负责人必须删除其访问权限； ■ 在信息资源设施的持卡访问区，来宾必须由专人陪同； ■ 信息资源设施的负责人必须定期评审访问记录以及来宾记录，并要对异常访问进行调查； ■ 信息资源设施的负责人必须定期评审卡和/或钥匙访问权，并删除不再需要访问的人员的权限； ■ 对限制访问的房间和场所必须进行标记，但是描述其重要性的信息应尽可能少。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

5. 供应商访问策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	供应商在支持硬件和软件管理以及客户运作方面有重要作用。供应商可以远程对 数据和审核日志进行评审、备份和修改，他们可以纠正软件和操作系统中的问题，可以监控并调整系统性能，可以监控硬件性能和错误，可以修改周遭系统，并重新设置警告极限。由供应商设置的限制和控制可以消除或降低收入、信誉损失或遭破坏的风险。		
目 的	该策略的目的是为减缓供应商访问组织资产带来的风险。		
适用范围	该策略适用于所有需要访问组织的供应商。		
术语定义	略		
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： ✧ 安全策略； ✧ 保密策略； ✧ 审核策略； ✧ 信息资源使用策略。 ■ 供应商协议和合同必须规定： ✧ 供应商应该访问的信息； ✧ 供应商怎样保护信息； ✧ 合同结束时供应商所拥有的信息返回、毁灭或处置方法； ✧ 供应商只能使用用于商业协议目的的信息和信息资源； ✧ 在合同期间供应商所获得的任何信息都不能用于供应商自己的目的或泄漏给他人。 ■ 应该向研发中心提供与供应商的合同要点。合同要点能确保供应商符合策略的要求 ； ■ 为供应商分配类型，如 IT 基础组件运维服务、系统维护服务、网络维护服务等； ■ 需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		

	访问的权限； ■ 供应商访问信息的人员范围仅限于工作需要的人员，授权需获得研发中心的批准； ■ 供应商权限人员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，工作结束后应该立即注销访问权限及清空资料； ■ 针对与供应商人员交互的组织人员开展意识培训，培训内容涉及基于供应商类型和 供应商访问组织系统及信息级别的参与规则和行为； ■ 如适合可与供应商就关系中的信息安全签署保密或交换协议； ■ 每一个供应商必须提供在为合同工作的所有员工清单。员工发生变更时必须在 24 小时之内更新并提供； ■ 每一个在组织场所内工作的供应商员工都必须佩带身份识别卡。当合同结束时，此卡应该归还； ■ 可以访问敏感信息资源的每一个供应商员工都不能处理这些信息； ■ 供应商员工应该直接向恰当的人员直接报告所有安全事故； ■ 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； ■ 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； ■ 必须对供应商访问进行唯一标识，并且对其进行的口令管理必须符合口令实施规范和特殊访问实施规范。供应商主要的工作活动必须形成日志并且在管理者需要的时候可以访问。日志的内容包括但不仅限于：人员变化、口令变化、项目进度重要事件、启动和结束时； ■ 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，并在 24 小时内提交一份返回或销毁的书面证明； ■ 在合同或邀请结束时，供应商必须立即交出所有身份识别卡、 访问卡以及设备和供应品。由供应商保留的设备和 / 或供应品必须被管理者书面

	授权； ■ 要求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。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

6. 雇员访问策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	雇员工作在信息安全区域，工作中需要使用公司的各种信息处理设施，需要访问公司的各种信息资产,因此每一个雇员有义务和责任保护好公司信息资产的安全。		
目 的	本策略未访问本公司信息资源的全体雇员，这种访问是出于业务需要的，涉及物理和行政安全管理需求的网络连接、雇员的职责及信息保护的准则。		
适用范围	该策略适用于公司的任何雇员，雇员对信息资源的访问，包括信息处理设施设备和技术资源。		
术语定义	略		
雇员访问策略	■ 雇员必须遵守相应的策略、操作标准以及协议，包括但不仅限于： ✧ 《信息资源保密策略》; ✧ 《病毒防范策略》; ✧ 《可移动代码防范策略》; ✧ 《信息交换策略》; ✧ 《清洁桌面和清屏策略》; ✧ 《网络访问策略》; ✧ 《便携式计算机安全策略》; ✧ 《互联网使用策略》; ✧ 《电子信息策略》。 ■ 雇员在意识到有安全事件发生时应该第一时间向上层领导报告; ■ 雇员应该直接向恰当的人员直接报告所有安全事故; ■ 雇员必须遵守所有适用的变更管理程序; ■ 当雇员离职时，必须确保所有敏感信息在 24 小时内被收回或销毁; ■ 在合同结束时，雇员应该将所有信息返回或销毁，并在 24 小时内提交一份返回或销毁的书面证明，并由资产责任人签字认可;		

	■ 在合同结束时，雇员必须立即交出所有身份识别卡、访问卡以及设备和供应品。由雇员保管的设备和 /或供应品的回收必须由资产责任人签字认可； ■ 要求雇员必须遵守所有规定和审核要求。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

7. 设备及布缆安全策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	网络基础设施是向所有信息资源用户提供服务的中心设施。这些基础设施（包括电源馈送和数据传输的电缆以及相关的设备）需要持续不断的发展以满足用户需求,然而同时也要求网络技术高速发展以便将来能够提供功能更强大的用户服务。		
目 的	■ 该方针的目的保护设备免受物理的和环境的威胁，减少未授权访问信息的风险。防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断； ■ 为了安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会； ■ 为了保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断，应有足够的支持性设施（供电、供水、通风和空调等）来支持系统； ■ 为了保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏，电源馈送和数据通讯的电缆必须确保安全； ■ 为了确保设备持续的可用性和完整性，设备应予以正确地维护； ■ 为了对组织非现场设备采取安全措施，要考虑工作在组织场所以外的不同风险； ■ 为了确保涉密信息不泄露，在存储介质销毁之前，任何敏感信息和注册软件已被删除或安全重写； ■ 为了确保涉密信息不泄露，设备、信息或软件在授权之前不应带出组织场所。		
适用范围	该方针适用于网络设备设施的建设和维护人员。		
术语定义	略		
设备及布	■ 设备安置和保护方针 ✧ 设备应进行适当安置，以尽量减少不必要的对工作区域的访问；		

缆安全策略	✧ 应把处理敏感数据的信息处理设施放在适当的限制观测的位置，以减少在其使用期间信息被窥视的风险，还应保护储存设施以防止未授权访问； ✧ 要求专门保护的部件要予以隔离，以降低所要求的总体保护等级； ✧ 应采取控制措施以减小潜在的物理威胁的风险，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； ✧ 对于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）要予以监视； ✧ 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； ■ 支持性设施方针 ✧ 支持性设施应定期检查并适当的测试以确保他们的功能，减少由于他们的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，必须使用支持有序关机或连续运行的不间断电源（UPS）； ✧ 电源应急计划要包括 UPS 故障时要采取的措施。UPS 设备和发电机要定期地检查，以确保它们拥有足够能力，并按照制造商的建议予以测试； ■ 布缆安全方针： ✧ 进入信息处理设施的电源和通信线路宜在地下，若可能，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；
- ✧ 对于敏感的或关键的系统，更进一步的控制考虑应包括：
  - ＊ 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子；
  - ＊ 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；
  - ＊ 使用纤维光缆；
  - ＊ 使用电磁防辐射装置保护电缆；
  - ＊ 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；
  - ＊ 控制对配线盘和电缆室的访问；

■ 设备维护方针

- ✧ 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者维护人员应该是足够可靠的；
- ✧ 应遵守由保险策略所施加的所有要求。

■ 组织场所外的设备安全方针

- ✧ 无论责任人是谁，在组织场所外使用任何信息处理设备都要通过管理者授权；
- ✧ 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，若可能宜伪装起来；
- ✧ 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；
- ✧ 家庭工作的控制措施应根据风险评估确定，当适合时，要施加合适的控制措施，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办公室的安全通信；
- ✧ 足够的安全保障掩蔽物宜到位，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。 ■ 设备的安全处置和再利用方针 ✧ 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破坏、删除、覆盖信息，而不能采用标准的删除或格式化功能； ✧ 包含敏感信息的已损坏的设备可能需要实施风险评估，以确定这些设备是否要进行销毁、而不是送去修理或丢弃。 ■ 资产移动方针 ✧ 在未经事先授权的情况下，不允许让设备、信息或软件离开办公场所； ✧ 应明确识别有权允许资产移动，离开办公场所的雇员、承包方人员和供应商人员； ✧ 应设置设备移动的时间限制，并在返还时执行符合性检查； ✧ 若需要并合适，要对设备作出移出记录，当返回时，要作出送回记录； ✧ 应执行检测未授权资产移动的抽查，以检测未授权的记录装置，防止他们进入办公场所。这样的抽查应按照相关规章制度执行。应让每个人都知道将进行抽查，并且只能在法律法规要求的适当授权下执行检查。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

8. 变更管理安全策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	信息资源基础设施正在逐步扩大并且越来越复杂。越来越多的人依赖网络、更多的客户服务机构、未升级和扩展的管理系统以及更多应用程序 。由于信息资源基础设施之间的互相依赖程度越来越高,因此有必要加强变更管理过程。 有时每一个信息资源组成部分需要暂停运行，按计划进行升级、维护或调整，另外也可能由于为计划的升级、维护或调整而导致暂停运行。管理这些变更是提供坚固的、有价值的信息资源基础设施的关键组成部分。		
目 的	该策略的目的是以一种合理的、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，以降低对用户群的负面影响，增加信息资源的价值。		
适用范围	该策略适用于安装、操作或维护信息资源的所有人员。		
术语定义	略		
变更管理安全策略	■ 对信息资源的每一次变更，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程序； ■ 所有影响计算机环境设备的变更(如空调、水、热、管道、电)需要向变更管理过程的领导者报告，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； ■ 所有事先有计划的变更申请必须按照变更管理程序的规定提交，以便研发中心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研发中心的正式批准； ■ 指定的研发中心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； ■ 在变更管理程序实施前，必须完成对所有客户的通知；		

	■ 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： ✧ 变更的提交和执行日期； ✧ 所有者和保管者信息； ✧ 变更的特性； ✧ 成功或失败的标志。 ■ 所有信息系统必须遵照上述规定进行信息资源的变更。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

9. 病毒防范策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	计算机安全事故的数量以及由业务中断服务恢复所导致的费用日益攀升。实施稳固的安全策略，防止对网络和计算机不必要的访问，较早的发现并减轻安全事故可以有效地降低风险以及安全事故造成的费用。		
目 的	该策略的目的是描述计算机病毒、蠕虫以及特洛伊木马防御、检测以及清除的要求。		
适用范围	该策略适用于使用信息资源的所有人员。		
术语定义	略		
病毒防范策略	■ 所有连接到局域网的工作站必须使用研发中心批准的病毒保护软件和配置； ■ 病毒保护软件必须不能被禁用或被绕过； ■ 病毒保护软件的更改不能降低软件的有效性； ■ 不能为了降低病毒保护软件的自动更新频率而对其进行更改； ■ 与局域网连接的每一个文件服务器必须使用研发中心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安全事故的病毒，必须向研发中心报告。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

10.可移动代码防范策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	未经授权的移动代码危害信息系统，应实施对恶意代码的监测、预防和恢复控制，以及适当的用户意识培训。		
目 的	该策略的目的阻止和发现未经授权的移动代码的引入，实施对恶意代码的监测、预防和恢复控制。		
适用范围	该策略适用于使用信息资源的所有人员。		
术语定义	略		
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评审；无论出现任何未经验收的文件或者未经授权的修改，都要进行正式调查。 ■ 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，检测应包括： ✧ 在使用前，对存储媒体，以及通过网络接收的文档进行恶意代码检测； ✧ 在使用前，通过信息服务器对电子信息附件及下载文件进行恶意代码检测； ■ 研发中心负责恶意代码防护、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。 ■ 研发中心应制定并实施文件化的程序，验证所有与恶意软件相关的信息并且确保警报公告的内容准确详实。管理员应当确保使用合格的信息资源，防止引入真正的恶意代码。所有用户应有防欺骗的意识，并知道收到欺骗信息时如何处置。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或		

	顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

11.信息备份安全策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	电子备份是一项必需的业务要求,能使数据和应用程序在发生意想不到的事件时得以恢复，这些事件包括：自然灾害、系统磁盘故障、间谍活动、数据输入错误或系统操作错误等。		
目 的	该策略的目的是设置电子信息的备份和存储职责。		
适用范围	该策略适用于组织中负责信息资源安装和支持的所有人员,以及负责信息资源安全的人员和数据所有者。		
术语定义	略		
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； ■ 供应商提供的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供应商每年进行评审； ■ 为了容易识别介质和 / 或关联系统，备份介质至少应该被标注下列信息： ✧ 系统名； ✧ 创建日期； ✧ 敏感度分级［以相应的电子记录保持法规为基础］; ✧ 包含的信息。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

12.技术脆弱性管理策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	为防止技术脆弱性被利用，应建立对应技术脆弱性的管理机制，主动补充脆弱性，增加信息安全控制。		
目 的	该策略的目的是及时得到现用信息系统技术脆弱性的信息,评价公司对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。		
适用范围	该策略适用于访问信息资源的所有人。		
术语定义	略		
网络配置安全策略	■ 研发中心要定义和建立与技术脆弱性管理相关人员，负责脆弱性监视、脆弱性风险评估、打补丁、资产追踪和任意需要的协调责任； ■ 技术脆弱性负责人要制定时间表对潜在的技术脆弱性的通知做出反映； ■ 一旦潜在的技术脆弱性被确定，技术脆弱性负责人要识别相关的风险并采取措施；这些措施可能包括对脆弱的系统打补丁和/或应用其他控制措施； ■ 技术脆弱性负责人应定技术脆弱性需要解决的紧急程度； ■ 如果有可用的补丁，则要评估与安装该补丁相关的风险（脆弱性引起的风险要与安装补丁带来的风险进行比较）； ■ 在安装补丁之前，要进行测试与评价，以确保它们是有效的，且不会导致不能容忍的负面影响；如果没有可用的补丁，要考虑其他控制措施，例如： 1） 关闭与脆弱性有关的服务和功能； 2） 调整或增加访问控制措施，例如在网络边界上添加防火墙（见13.1）； 3） 增加监视以检测实际的攻击； 4） 提高脆弱性意识； ■ 息安全小组要定期对技术脆弱性管理过程进行监视和评价，以确保其有效性和效率；		

	■ 处于高风险中的系统要首先解决；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

13.信息交换策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	在组织之间交换信息和软件应当遵守根据交换协议所制定的正式的交换方针，并且应当服从所有相关的法律。		
目 的	保持在组织内部及任何外部机构之间所交换的信息和软件的安全。		
适用范围	该策略适用于进行信息交换的所有人员。		
术语定义	略		
信息交换策略	■ 不能在公共场所或者敞开的办公室、没有屋顶防护的会议室谈重要密信息。 ■ 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用户不得损害本局的利益，如诽谤、骚扰、假冒、未经授权的采购等。 ■ 不得将包含敏感信息的讯息放在自动应答系统中。 ■ 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。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

14.运输中物理介质安全策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	物理介质是信息资源的载体，在运送过程中必须对其安全进行管理。建立该方针是为了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。		
目 的	略		
适用范围	该方针适用于在组织安全边界外运输组织物理介质的所有人员。		
术语定义	略		
运输中物理介质安全策略	应考虑下列方针以保护不同地点间传输的信息介质： ➢ 应使用可靠的运输单位或人； ➢ 授权的送信人列表应经管理者批准； ➢ 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； ➢ 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： ✧ 使用可上锁的容器； ✧ 手工交付； ✧ 防篡改的包装（它可以揭示任何想获得访问的企图）； ✧ 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。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

15. 电子信息策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	信息资源是组织的资产，必须对其进行有效地管理，因而建立该策略是为了： ✧ 确保员工知晓在电子消息传输过程中的操作方法； ✧ 明确电子消息使用过程中的责任。		
目 的	为了建立某公司的电子消息使用规则，保证电子消息的合理发送、收取和存储。		
适用范围	该策略适用于被批准的、能够通过电子消息工具发送、收取和存储信息的所有人员。 电子消息工具包括：电子邮件、QQ、微信、公司论坛、FTP 等。		
术语定义	略		
电子信息策略	■ 下列行为是策略所禁止的： ✧ 发送或者转发虚假、黄色、反动信息； ✧ 发送或者转发宣扬个人政治倾向或者宗教信仰； ✧ 发送或者转发发送垃圾信息； ✧ 发送或者转发能够引起连锁发送的恐吓、祝贺等信息； ✧ 发送口令、密钥、信用卡等的敏感信息； ✧ 用个人信息处理设备收发公司内部信息； ✧ 用公司外部账号发送、转发、收取公司敏感信息； ✧ 在非授权情况下以公司的名义发表个人意见； ✧ 发送或者转发可能有计算机病毒的信息； ✧ 使用非授权的电子信息收发软件； ■ 下列行为是策略所要求的： ✧ 每位员工都有一个电子消息工具账号，账号密码必须符合口令策略的相关规定； ✧ 用电子消息工具经过外部网络发重要密信息必须经过加密，加密必		

	须符合加密策略的相关规定； ✧ 发送电子消息时必须有清楚的主题； ✧ 电子消息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 ✧ 公司有权对职员的电子消息工具进行监视和记录； ✧ 公司有权对电子消息工具的内容进行存储备份以用于法律目的；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

16.信息安全监控策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	信息安全监控是确保安全实践和控制被恰当执行和有效实施的一种方法，监控活动包括对下列内容的评审： ✧ 防火墙日志 ✧ 用户帐户日志 ✧ 网络扫描日志 ✧ 应用程序日志 ✧ 数据备份和恢复日志 ✧ 其他类型的日志以及出错日志 .		
目 的	该策略是为了确保信息资源控制措施被适当、有效地实施并且不被忽视。安全监控的其中一个好处就是较早的发现破坏行为或新的薄弱点。这样会有助于在破坏发生前阻止破坏行为或薄弱点，最起码能够减小潜在的影响。其他好处包括：审核符合性、服务层监控、业绩测量、划定责 任以及容量策划。		
适用范围	适用于负责信息资源安全、现有信息资源的操作以及负责信息资源安全的所有人员。		
术语定义	略		
信息安全监控策略	■ 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。在可能的地方可以开发安全底线和工具，监控： ✧ 电子信息通信 ✧ 局域网通信、协议以及设备清单 ✧ 操作系统安全参数 ■ 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： ✧ 防火墙日志 ✧ 用户帐户日志 ✧ 网络扫描日志		

	✧ 系统出错日志 ✧ 应用程序日志 ✧ 数据备份和恢复日志 ✧ 网络打印机和传真日志 ■ 下列内容应该由负责的人员每年至少检查一次： ✧ 口令的难猜测程度 ✧ 未经授权的网络设备 ✧ 未经授权的个人网络服务器 ✧ 未受保护的共享设备 ✧ 未经授权使用的调制解调器 ✧ 操作系统和软件许可 ■ 发现的任何问题都应该向研发中心报告，进行进一步的调查。 ■ IT 管理员自身的工作由管理者代表进行审查和监督。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

17.特权访问管理策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	与普通用户相比，技术支持人员、安全管理员、IT 管理员可能有特殊的访问账户权限要求。这些管理性的特殊访问账户的访问等级比较高 ，因此对这些账户的批准、控制和监控对于整个安全程序极其重要。		
目 的	该策略的目的是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	该策略适用于拥有、或者可能会需要信息资源特殊访问权限的人员。		
术语定义	略		
特权访问管理策略	■ 所有管理性的 / 特殊访问账户在获得账号前，应签署一份不泄密协议； ■ 所有管理性的 / 特殊访问账户的用户必须接受培训并获得授权； ■ 每一个使用管理性的 / 特殊访问账号的个人都必须避免滥用权力，并且必须在研发中心的指导下使用； ■ 每一个使用管理性的 / 特殊访问账号的个人必须以最适宜所执行的工作的方式行使账号权力 ； ■ 每一个管理性的 / 特殊访问账户必须满足口令策略的要求； ■ 共有的管理性的 / 特殊访问的账号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： ✧ 必须被授权； ✧ 创建的日期期限必须明确； ✧ 工作结束时必须删除。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

18. 口令控制策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	用户授权是控制信息资源访问者的一种方式。对访问进行控制是任何信息资源所必须的。未经授权的人员访问到信息资源可能会引起信息保密性、完整性共和可用性的丢失，导致收入、信誉的损失或经济困难。		
目 的	该策略的目的是为用户鉴别机制建立创造、分发、保护、终止以及收回的规则。		
适用范围	该策略适用于任何信息资源的使用者。		
术语定义	略		
口令控制策略	■ 所用用户都必须拥有唯一的、专供其个人使用的用户帐号 ID（用户 ID）； ■ 所有用户不得使用他人的用户进行信息资源的访问； ■ **所有口令，包括计算机登录、文件系统、网络等口令，都必须依据研发中心规定的下列规则建立和执行：** ✧ 必须定期更改（最长 90 天）； ✧ 必须符合规定的最小长度（6 位字符）； ✧ 必须符合复杂度要求，即数字+字母+特殊符号的组合，例如：203aa# ✧ 必须不能是可以轻易联想到的帐号所有者的特性：用户名、绰号、亲属的姓名、生日等； ✧ 必须不能用字典中的单词或首字母缩写； ✧ 必须保存历史口令，以防止口令的重复使用。 ■ **服务器、应用系统、网络设备的管理员特殊权限用户的口令除以上要求需要满足外，还有特殊要求：更改周期缩短为 60 天，密码长度不少于 8 位。** ■ 用户的帐号口令必须不能泄露给任何人； ■ 如果怀疑口令的安全性，应立即进行更改； ■ 管理员不能为了使用信息资源规避口令； ■ 用户不能通过自动登录的方式绕过口令登录程序；		

	■ 计算机设备如果无人值守必须启动口令保护屏保或注销； ■ 用户在首次登录时必须更改口令。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

19.清洁桌面和清屏策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	应该实施清除桌面和清除屏幕方针，以降低对文件、介质以及信息处理设施未经授权访问或破坏的风险。		
目 的	该策略的目的是防止对信息和信息处理设施未经授权的用户访问、破坏或盗窃。		
适用范围	该策略适用于公司所有员工。		
术语定义	略		
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口令，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 5 分钟； ■ 传真机由研发中心负责管理，并落实责任人。 ■ 打印或复印公重要密信息时，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。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

20.互联网使用策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	在信息资源管理策略的规定中，信息资源是对组织有价值的重要资产。建立该策略是为了达到下列目的： ✧ 确保符合相应的、与信息资源管理相关的法令、规章以及要求； ✧ 建立谨慎的、合理的互联网使用惯例； ✧ 向使用互联网或者企业内部网络的员工告知他们应负的职责。		
目 的	该策略的目的是规范互联网以及公司内部网络的使用,确保信息资源不会被泄漏、篡改、破坏。		
适用范围	该策略适用于有权访问任何信息资源而又可以访问互联网以及公司内部网络的所有人员。		
术语定义	略		
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； ■ 互联网访问权限只授权给总经理、副总经理、IT 管理员，其他用户需访问互联网必须在公司公共的上网区域访问互联网，且必须遵守相关规定。 ■ 所有用于访问互联网的软件必须都经过研发中心批准，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研发中心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源使用策略； ■ 对用户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源使用策略； ■ 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； ■ 偶尔使用互联网访问的人员必须仅限于授权用户，不能延伸到家庭成员或其他熟人； ■ 偶尔使用必须不造成费用损失； ■ 偶尔使用必须不能干扰员工的正常工作任务； ■ 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； ■ 所有文档和文件——包括私人文档和文件，必须符合记录公开要求，并且可以依照本策略访问到； ■ 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。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

21.便携式计算机安全策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	便携式计算机设备的功能和应用越来越广泛。其小巧的“体型”和强大的功能使人们期望其替代传统的桌面设备。然而，这些设备的便携特性也会给使用他们的组织增加安全暴露。		
目 的	该策略的目的是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。这些规则是保持信息保密性、完整性和可用性所必需的。		
适用范围	该策略适用于使用便携式计算机设备访问信息资源的所有人。		
术语定义	略		
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源； ■ 便携式计算机设备必须有口令保护； ■ 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，SSID 不广播。 ■ 需要连接互联网的计算机系统必须符合信息服务标准； ■ 对无人看守的便携式计算机设备必须实施物理保护，必须放在带锁的办公室、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在公司办公区域内使用； ■ 非授权便携式计算机禁止加入公司域；		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

22.事件管理策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	计算机安全事件的数量以及由其导致得业务中断和服务恢复所需的费用日益增长。实施可靠的安全策略，防止对网络和计算机不必要的访问，提高用户的安全意识以及及早检测并减轻安全事件，可有效的降低风险以及安全事件的成本。		
目 的	该策略的目的是描述处理计算机安全事件的要求。安全事件包括，但不仅限于：病毒、蠕虫、特洛伊码、未经授权使用计算机账号和计算机 系统以及如在电子信息策略、信息资源使用策略以及互联网策略中规定的对信息资源不恰当的使用。		
适用范围	该策略适用于使用任何信息资源的所有人员。		
术语定义	略		
信息资源保密策略	■ IT 管理员的成员此方面任务和职责的优先权要高于其正常的职责； ■ 在怀疑或确定发生安全事件的任何时候都必须遵循适当的事件管理程序，例如病毒、蠕虫、恶作剧信息等； ■ 研发中心负责通知信息安全经理以及 IT 管理员，启动适当的事件管理活动，包括事件管理程序中规定的恢复活动； ■ 在事件调查过程中，研发中心负责确定要搜集的实物和电子证据； ■ IT 管理员提供的用于监控安全事件破坏的技术资源应该被维修并降低其潜在的薄弱点； ■ 研发中心与信息安全经理合作确定是否需要对安全事件进行广泛的沟通，沟通的内容以及怎样最好的将沟通的内容共享； ■ IT 管理员应提供响应的技术资源，用于和系统卖方沟通新问题或薄弱点，并与卖方共同消除或减轻薄弱点； ■ 研发中心在 IT 管理员的协助下，负责启动、完成并文件化事件调查过程； ■ 研发中心负责向下列部门或人员报告： ✧ 信息资源相关部门		

	✧ 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 ■ 研发中心负责与外部组织以及法规强制部门的协调沟通； ■ 在不牵涉到法律强制的地方，研发中心可以向信息安全经理建议惩戒措施； ■ 在牵涉到法律强制的地方，研发中心负责与法律强制部门的联络。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

23.个人信息使用策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	对个人信息的隐私加以保护。		
目 的	该策略的目的是保护个人信息的隐私，符合相关的法律、法规和合同条款的要求。		
适用范围	该策略适用于使用和保存个人信息的人员。		
术语定义	略		
个人信息使用策略	■ 只对业务上必需的最小限度的信息采取合法且公正的方法进行收集，原则上，在向信息所有者说明使用目的并征得同意后再行收集。 ■ 严禁用于收集目的以外的用途。 ■ 个人信息的所有者要求对自己的个人信息进行明示、修改、删除和停止使用时，在进行严格的本人确认后，应尽快予以施行。 ■ 当将与个人信息有关的事宜对外委托处理时，要求施行与在本公司内同等程度的管理。 ■ 当接受外部委托进行有关个人信息的处理时，要遵守委托方的个人信息管理准则。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

24.业务信息系统使用策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	业务信息系统主要是与我公司业务相关的使用软件系统。		
目 的	该策略的目的是为了规范化我们对业务系统的操作，从而降低由此引起的公司财产的损失。		
适用范围	该策略适用于所有业务信息系统操作相关的人员。		
术语定义	略		
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，对于不熟悉的人员应该尽量避免使用。 ■ 对于不熟悉的人员如果需要使用业务信息系统时，需要进行使用前的培训。 ■ 对于需要使用业务信息系统的人员需要提出申请，并且通过研发中心认可后才可以允许使用。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

25.远程工作策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	远程工作是使用通信技术手段使在组织场所外固定地点的人员可以进行远程进入公司网络工作。		
目 的	该策略的目的是确保远程工作及设施的信息安全。		
适用范围	该策略适用于通过远程工作方式访问任何信息资源的所有人。		
术语定义	略		
远程工作策略	■ 远程工作的方式必须获得研发中心的批准，并获得研发中心的授权，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和地点，严禁在公共计算机设备（例如网吧）上进行； ■ 远程工作人员范围仅限于工作需要的人员，内部远程工作人员必须获得部门负责人的书面授权，并获得研发中心的批准； ■ 远程工作人员不得将远程工作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接受研发中心的相关配置和监控； ■ 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，并符合《用户访问控制程序》； ■ 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。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		

26. 安全开发策略

发布部门	研发中心	生效时间	2020 年 06 月 15 日
介绍	建立软件和系统开发规则，并应用于组织内的开发		
目 的	该策略的目的是宜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	该策略适用于开发管理系统、应用系统过程中，同时开发也可能发生在应用中，例如办公应用、脚本、浏览器和数据库等。		
术语定义	略		
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、运营环境想隔离，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； ■ 对开发者就系统开发技术的脆弱性应进行培训，已应对开发过程中遇到是的处理，对培训情况需进行验证。		
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。		