信息安全管理制度

1.目的

信息是企业存在和发展的重要基础。为规范企业信息管理，保障信息安全，明确信息安全管理的程序、职责、义务和权限，特制定本制度。

2. 职责

2.1 网络管理员（委外）：负责依公司的系统安全规定和部门业务要求，对网络进行维护管理、计算机维护及故障处理等，保证系统安全运行。

2.2 系统管理员（安全员）：负责策划和制定公司信息安全策略、监督安全规定的实施，提出改善要求，确保信息系统满足公司业务安全要求。负责加解密授权管理、用户申报、开通访问授权和机房管理、数据备份。

3．定义与术语

3.1 公司信息分类：

1. 技术信息：产品图纸、制造技术、主要存在于技术部。
2. 质量信息：主要保存在质管部。
3. 商务信息：主要存在于采购部、经营部。
4. 财务信息：主要存在于财务部。
5. 人事信息：公司员工及为公司服务的特殊技能人才信息资料。
6. 密码信息：个人登录、开机密码及IT管理员密码。
7. 内部运作其他信息：包括设备、基础设施、工程等信息资料。

以上信息，根据信息秘密程度，分为可公开信息和保密信息。公司任何员工均不可将公司保密信息（文件）以任何方式传递、泄露给非授权人。

1. 公开信息：此类信息、文件可从公司公开渠道所获取，如公司广告、网站中所涉及的公司名称、地址、经营产品等。
2. 秘密信息：不可从公开渠道所能获取的信息，如产品技术文件，包括产品图纸、客户文件、工艺技术规范等；人事行政文件、管理程序和规范、生产经营统计信息和其他记录、文件等。

3.2信息管理风险及危害

3.2.1 来自企业外的风险

a. 病毒和木马风险

b. 黑客攻击风险

3.2.2来自企业内的风险

a. 文件外发传输，包括电子邮件、打印外发、传真等。

b. 存储设备的风险，通过移动存储介质将文件资料拷贝出公司，包括带有保密信息的存储介质维修泄密，如相机、U盘、硬盘等维修。

c. 即时通讯，如QQ截图、FeiQ、MS LYNC、网络飞鸽等。

3.2.3风险行为

a. 上网行为风险。接收病毒邮件、访问不良网站传染病毒或安装插件，导致泄密或电脑系统的崩溃。

b. 用户密码风险。包括用户密码和管理员密码。密码泄漏可导致非授权人访问或篡改、窃取信息资料。

c. 办公/区域风险。在办公区域随意堆放保密文件、公开谈论工作内容导致泄密。

d. 机房设备风险。主要包括服务器、UPS电源、网络交换机等。这些风险来自防 盗、防雷、防火、防水。机房故障，可能会损坏机房设施，造成业务中断。

4．信息安全措施

4.1上网行为管制

根据各部门涉及的信息需求，由公司保密主管领导决定、公司信息技术管理员实施公司电脑上网授权，包括允许访问网址、下载和安装的软件。电脑使用人员不得自主下载、安装非授权软件。

各业务部门若需要查阅资料和其他目的需要查看特定网站或安装软件，需要由部门主管审查、保密主管领导批准，方可由网络管理员开通。

4.2 文件外发管制

需要拷贝公司的文件资料并带出公司时，需要经过授权人批准，解密后方可带出。

图纸、资料等技术质量类电子文件，如果需要外发，统一由解密权限人员解密后再外发。其中，若给委外加工方的技术文件，应经公司转换，并消除客户有关产品型号、编号等信息后方可外发。

授权解密人员对自己的解密文件进行审查，并对解密行为负责，符合外发要求后方可解密外发。

4.3 计算机应用软件安装与维护

根据工作性质，公司统一规定允许安装的应用软件，并由系统管理员统一安装。员工必须从共享于服务器中的应用软件及升级版本安装，不得安装网络下载或其他渠道软件版本。必须而共享软件中没有的，由计算机管理员负责安装和升级。

系统管理员负责保证所安装软件的安全性。

4.4 计算机设备安全管理

4.4.1 采购、安装与维护：

计算机及其他涉密数码产品采购、安装和使用，应通过网络管理员审查、主管领导批准。任何人不得使用个人电脑、PAD、U盘等接入公司网络。非网络管理人员（包括外来维修人员）不得处置、维修公司电脑、硬盘和其他有涉密信息的数码产品。产品维修及报废处置应建立维修处置记录，相关人员签名存档。

电脑初始安装由系统管理员负责，必须安装规定的安全软件，以保证电脑安全运行。

计算机时钟设置：必须设置成与internet同步，操作人员不得更改计算机日期和时间，以保证计算机文件信息的准确性。

下班后所有不再使用的计算机，应关闭主机电源，以防止意外。

发现由以下等个人原因造成硬件的损坏或丢失的，其损失由当事人如数赔偿：违章作业；保管不当；擅自安装、使用硬件和电气装置。

4.4.2 杀毒软件：

统一由网络管理员安装杀毒软件，并负责定期维护，包括升级以及故障处理。用户使用的杀毒软件和防火墙已经设置好自动调度更新和病毒库升级，每日定时杀毒，使用者也应经常手动扫描杀毒。非管理员不得修改防火墙和杀毒软件设置。

4.4.3 信息资料备份

涉及公司产品技术、质量和财务等保密信息的，应在数据服务器中保存备份文件。

网络管理员负责服务器安全运行，并维护和定期备份服务器文件。

员工离职时，须交回全部技术文件资料等保密文件，并经部门负责人确认。部门负责人联系网络管理员对该员工电脑进行保密检查，确保无泄密后签字认可。

4.4.4 密码管理

每个员工拥有一个公司内部计算机登录帐户和自己的密码。使用者须妥善保管好自己的帐户和密码。帐户及密码设置后通知管理员备案。所有员工必须在所使用的计算机中设置开机密码和屏幕保护密码。为了保护公司的信息资产，设置密码时应注意：密码至少有6个字符长；密码必须包含以下任二部分：字母A-Z或a-z，数字0-9，特殊字符，例如 $ ，-等。

员工密码每三个月至少更新一次。

密码包括：

开机密码、邮箱登录密码、ERP登录密码。

USB Key管理：交由网络管理员锁到密码箱保存。任何人不得将此带出公司。

4.5 机房管理

参照《信息系统安全等级保护基本要求》GB/T22239-2008要求，由人力资源与行政办负责公司网络系统和计算机服务器（机房）管理。建立计算机机房出入、操作登记。

非授权人不得操作服务器。

为保护计算机及网络系统安全，须满足以下要求：

1. 计算机房建筑接地电阻不大于4欧姆;
2. 温度 不高于30度；湿度 不大于70%;
3. 电源：配置稳压器和过压防护设备；
4. 设置访问用户权限，并及时删除废除用户；
5. 服务器数据备份，每周五下午进行备份。

5．记录与支持性文件

5.1 加解密授权审批表

5.2 计算机及其他数码产品登记表

5.3 主机（服务器）操作登记表

5.4 机房出入登记表

5.5 授权加解密人员保密承诺书

5.6 计算机初始配置要求

5.7 硬盘及其他存储介质领用（维修）登记