受控副本章	
发放编号	003
有效版本	A 版 0 次
实施日期	2010-05-01
使用部门	管理者代表

介质及信息交换管理程序

1 范围

为了对信息介质进行控制和物理上的保护以及对信息交换活动实施有效控制，以防止信息或交换的信息遭受未授权泄露、修改、备份、移动、误传、截取或销毁等，特制定本程序。

本程序适用于对信息介质及信息介质处置的管理和公司各部门及员工在信息交换过程中的活动。

2 职责

2.1 行政公关部

a) 负责电话、打印机、复印机等IT周边设备信息交换、物理介质运送等控制活动。

b) 负责对管理信息网络信息介质处置与计算机电子信息交换控制活动。

c) 负责介质涉密使用的管理和记录。

2.2 介质使用部门和使用者

由部门负责管理的介质，由该部门领导指定专人负责保管。个人使用的介质由本人负责保管与本部门的信息交换活动。

3 程序

3.1 介质和信息交换策略

3.1.1 任何信息设备，如：计算机、交换机、打印机、传真机、复印机等，都需要介质进行存储，当存储设备或介质需要转移或销毁时，如果处理不当，很容易造成信息泄漏。必须按规定执行处置。

3.1.2 介质分为一般介质和可移动介质，一般介质是指文件档案、计算机存储介质，可移动介质是指 U 盘、移动硬盘、数码相机、光盘、磁带、软盘和打印的媒体等。

3.1.3 介质处置原则

当不再需要时，介质应该按照正式的程序可靠、安全的处置，使敏感信息泄露给未经授权的人员的风险最小化。

3.1.4 为信息交换安全，不要暴露敏感信息，避免电话被偷听或截取，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。制作应用系统之间的接口、协议时，不能影响双方应用系统的正常运行。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。

3.2 介质处置与信息交换控制措施

3.2.1 敏感信息介质的处置应该与信息的敏感程度相一致，介质的敏感程度应考虑风险评估的结果。

3.2.2 在使用电子通信设施进行信息交换时，所考虑的控制包括：

a) 防止交换的信息被截取、备份、修改、误传以及破坏；

b) 保护以附件形式传输的电子信息；

c) 所有业务信件和消息的保持和处置，要符合相关的法律法规。

3.2.3 介质处置应考虑下列原则：

a) 将所有的存储介质都应安全的收集和处置。

b) 信息介质的处置前应该识别需要安全处置的项目。

c) 销毁方式一般分为一般格式化、低级格式化、粉碎。

d) 对无敏感信息的介质作一般格式化即可，在保证质量的基础上重新分配和使用。

e) 保存有敏感信息的存储介质应当得到安全的存放和处置。对于含有敏感信息的介质应采用低级格式化，再进行粉碎。

f) 应对含有敏感信息的存储介质的处置做出记录，以备审查。

g) 销毁的介质在处理后宜保存三个月后再作处理。

3.2.4 使用传真的人员应注意避免下列问题：

a) 未经授权对传真机内部存储的信息进行访问，获取信息；

b) 故意的或无意的传真机程序设定，向特定的号码发送信息；

c) 向错误的号码发送文件和信息，或者拨号错误，或者使用存储在机器中的号码是错误的。

3.2.5 处置措施可以是：

a) 软盘：文件删除后，采用低级格式化，再进行粉碎。

b) 硬盘：文件先做删除，低级格式化，粉碎报废。循环使用的硬盘，低级格式化后，拷入大量数据，覆盖无用信息后，高级格式化，再使用。

c) 光盘：一次性光盘，粉碎。可擦写光盘，格式化后再使用。

d) Cmos芯片：粉碎。

e) Flsh卡：报废后粉碎。

f) 可擦写芯片：删除文件，粉碎。

3.3 可移动介质处理

3.3.1 介质管理

可移动介质领用须经本部门领导批准，行政公关部应建立[可移动介质授权使用清单]。

3.3.2 复制和移出

向可移动介质拷贝涉密信息，或将可移动介质带离开本公司需要获得本部门领导的批准，并在[可移动介质涉密使用记录]上记录存储的信息、用途、批准人、操作人等相关信息。

3.3.3 重复使用

对能够重复使用的可移动介质需要重复使用，被授权操作者首先必须确认可移动介质中的涉密信息或重要信息已经安全清除，其次要严格控制在可移动介质的厂家指出的可重复使用的次数之内，确保其存贮信息的安全、可靠性。

3.3.4 保存

可移动介质的的保管部门应按介质要求的保存环境来保存含有涉密信息或重要信息的可移动介质，各部门应对含有涉密信息或重要信息的可移动介质妥善保管，防止丢失，有任何异常必须向部门领导汇报，并根据部门领导的指示对异常情况作相应的处理。

3.3.5 废弃

可移动介质应经过部门领导认可，需确保信息的保密性，能进行删除操作的，将涉密信息或重要信息进行删除。需要废弃的介质统一送到行政公关部，由行政公关部统一进行安全销毁处理，并做好[可移动介质处置记录]。

3.4 交换协议

3.4.1 网络管理员建立与外部团体交换信息和软件的协议。交换协议考虑下列方面：

a) 控制和通知传输、发送和接收的管理责任；
b) 通知传输发送人、发送方和接收方的程序；
c) 确保可追溯性和无否定性的程序；
d) 第三方委托保管协议；
e) 发生安全事件的责任和义务，如丢失数据；
f) 记录和读取信息和软件的技术标准；
g) 保护敏感物品，例如密钥，所需要的任何特别控制措施。

3.4.2 应保护被传输的信息和物理介质，并作为制定交换协议的参考。

3.4.3 任何协议包含的安全内容都应该反映所涉及的业务信息的机密性。

3.4.4 协议可以是电子形式的也可以是书面的，对于敏感信息，应该考虑对信息交换使用特殊的机制，但是必须与组织和协议类型相协调。

3.5 物理介质的传递

3.5.1 在将信息资产带出公司时，对包含信息的介质应进行保护，防止未经授权的访问、误用或破坏。

3.5.2 在进行信息介质的传递时，需考虑下列原则：

a) 应当使用可靠的传递手段和经过授权的快递公司，并报请总经理批准；
b) 存储介质的包装应足以保护其中的内容免受任何在转运过程中可能出现的物理损伤；
c) 需要时，应采用专门的控制措施来保护敏感信息免受未经授权的公开或者修改。

3.6 电子讯息和电子邮箱

3.6.1 电子讯息中包含的信息应该被适当的保护。

3.6.2 电子讯息需考虑的安全问题包括：

a) 保护信息防止未经授权的访问、修改或者服务被否认；
b) 确保正确的地址和传输；
c) 服务的可靠性和可用性；
d) 法律方面的考虑，例如电子签名；
e) 在使用外部公共服务前获得批准，如即时通信、文件共享等。

3.6.3 公司员工应根据业务要求申请公司电子邮箱，填写[电子邮箱申请表]，经本部门负责人审核，报行政管理中心负责人批准，电子邮件系统管理员填入[电子邮箱一览表]，统一管理。

3.6.4 电子邮箱的使用策略，按《资产识别管理程序》进行。电子邮箱的使用限制如下：

a) 禁止用户群发附件大于10M的邮件。
b) 对内发送邮件时，单封邮件限额为小于20M，对外发邮件时，建议单封邮件小于5M，以避免对方无法接收过大的附件。

c) 不得私自利用电子邮箱向同行业公司发送含附件邮件。

3.6.5 员工离职时，由其所在部门更换此邮箱密码，并报网管备案。

3.6.6 行政公关部安全管理员负责每半年检查一次电子邮件系统的授权使用情况，填写[电子邮箱使用情况检查记录]。

3.6.7 行政公关部电子邮件系统管理员负责电子邮箱系统的日常维护，并监控员工使用公司电子邮箱的情况。

3.6.8 行政公关部安全管理员负责监控员工在公司网络使用个人电子邮箱的情况。

3.6.9 当发生或疑似发生信息安全事件时，应对职工使用公司电子邮箱的情况、在公司网络使用个人电子邮箱的情况以及传送的内容进行存储备份。

3.7 业务信息系统

行政公关部应保护与信息系统互联相关的信息。必须考虑下列原则：

a) 了解信息在不同部门共享时，重要系统（如财务系统、web信息共享服务器）中的薄弱点；

b) 通信系统中信息的薄弱点，例如录音电话或会议电话、电话的保密性、传真件的储存、公开邮件、邮件的分发；

c) 管理信息共享的策略和适当的控制；

d) 如果信息系统不能对敏感的业务信息提供适当等级的保护，就从中排除这些信息；

e) 限制访问与特定个人有关的日志信息，例如在敏感工程中工作的人员；

f) 允许使用该信息系统的员工、签约方和业务伙伴的范围，以及可以访问该系统的地点；

g) 把选择的设备限制在特定的用户范围内；

h) 对信息系统上信息的备份和保存；

i) 应变要求和安排。

3.8 其他

3.8.1 信息交换中能够通过电子通信传播的恶意代码的检测和防范按《恶意软件控制程序》进行。

4 相关文件和记录

《恶意软件控制程序》

[可移动介质授权使用清单]	保存部门：行政公关部	保存期限：2 年
[可移动介质涉密使用记录]	保存部门：行政公关部	保存期限：2 年
[可移动介质处置记录]	保存部门：行政公关部	保存期限：2 年
[电子邮箱一览表]	保存部门：行政公关部	保存期限：2 年
[电子邮箱使用情况检查记录]	保存部门：行政公关部	保存期限：2 年
[电子邮箱使用申请表]	保存部门：行政公关部	保存期限：2 年

附加说明：

本标准由湖南丰汇银佳科技有限公司提出。

本标准由湖南丰汇银佳科技有限公司行政公关部起草。

起草：郑安武　　审核：杨彬　　批准：刘熙　　日期：2010-04-28