用户访问控制程序

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

1 范围

对公司各种应用系统的用户访问权限（包括特权用户及第三方用户）实施有效控制，杜绝非法访问，确保系统和信息的安全。

适用于公司的各种应用系统涉及到的逻辑访问的控制。

2 职责

2.1 公司各相关部门负责本部门所使用系统的访问权限的分配、审批。

2.2 行政公关部网络管理员负责访问权限的控制和实施。

2.3 公司各部门负责向网络管理员及时通知人事变动情况。

3 程序内容

3.1 访问控制策略

a) 公司内部可公开的信息不作特别限制，允许所有用户访问。

b) 公司内部部分公开信息，经相应的管理责任人认可批准，网络管理员开设访问帐号和设置访问权限后，用户方可访问。

c) 用户不得访问或尝试访问未经授权的网络、系统、服务和文件。

d) 相关部门经理及项目经理填写［系统权限登记表］，确定访问规则后，由网络管理员门开设访问帐号和设置访问权限。

e) 用户访问权限变更时，相关部门经理及项目经理填写［系统权限登记表］，及时向网络管理员提出变更，由网络管理员门负责变更访问权限。

3.2 用户访问管理

3.2.1 权限申请

3.2.1.1 授权流程

- 申请人申请——所在部门经理或项目经理确定访问规则——网络管理员开设访问帐号和设置访问权限；
- 所有用户，包括第三方人员均需要履行访问授权手续；
- 相关部门经理或项目经理根据工作或项目需要，确定其部门或其项目用户需要访问的系统和访问权限，向网络管理员提交［系统权限登记表］后，由网络管理员开设访问帐号和设置访问权限。

3.2.1.2 ［系统权限登记表］应对一下内容予以明确：

- 权限申请人员；
- 权限申请理由；
- 访问权限的范围和级别；
- 访问权限有效期。

3.2.2 权限变更

3.2.2.1 对发生以下情况的用户，对其访问帐号和权限应从系统中予以注销：

- 内部用户劳动合同终止时；
- 内部用户因为岗位调整，不再需要此项访问服务时；
- 第三方访问合同终止时；
- 其他情况下必须予以注销访问权限的情形。

3.2.2.2 由于用户变换岗位等原因需要变更访问权限时，部门经理或项目经理应重新向网络管理员提交［系统权限登记表］，按照本程序 3.2.1 的要求履行授权手续。

3.2.2.3 人力资源部应及时将用户人事变动情况及时通知各部门，网络管理员根据用户所在部门或项目要求对其访问权限进行变更。

3.2.2.4 特权用户因故暂时不能履行特权职责时，根据工作需要可以经其直接领导批准，将特权临时转交指定人员；特权用户返回工作岗位时，收回临时特权人员的特权。

3.2.3 用户访问权限的维护和评审

3.2.3.1 域管理员权限的评审

3.2.3.2 一般用户权限的评审和维护

3.2.3.2.1. 对于任何权限的改变(包括权限的创建、变更以及注销)，各部门应进行记录，填写［系统权限登记表］包括：

- 权限开放 / 变更 / 注销时间；
- 变更后权限范围。

3.2.3.2.2. 各个部门经理或项目经理与网络管理员一起按时对其部门或其项目用户访问权限进行检查，发现不恰当的权限设置，应及时予以调整。

3.2.3.2.3. 各个部门经理或项目经理与网络管理员一起按时对特权用户访问权限进行检查，发现过期的权限设置，应及时予以注销。

3.2.3.2.4. 各个部门应对访问权限的检查结果予以记录，填写［系统权限检查表］。

3.3 用户口令管理

3.3.1 网络管理员应按照以下过程对被授权访问该系统的用户口令予以分配：

分配给用户一个安全口令，并通过安全渠道传递给用户，且对用户口令进行严格管理。

3.3.2 口令的选择和使用要求

所有计算机用户在使用口令是应遵循以下原则：

1） 保守口令的机密性，避免保留口令的字面记录、明文存储或明文网络传递。

2） 任何时候有迹象表明系统口令可能收到损害，要及时更换口令。

3） 用户口令最小长度 6 位， 不要采用姓名、电话号码、生日等别人容易猜测或得到的口令，不要用连续的数字或字母群。

4） 在任何自动登录过程中，不要包含口令。

5） 口令应妥善保存，不要共享个人用户口令。

4 加密控制

通过对重要文档、网络传递数据、口令、源代码等重要信息资产进行加密控制，实现对资产保密性的保护。

4.1 **密码设置**

4.1.1 密码设置原则：

1） 不能直接使用公司信息，如 FHYJ；

2） 不能使用真实单词；

3） 不同的数据分别设置不同的加密密码；

4） 需定期更换加密密码；

5） 密码复杂度要求：暴力破译密码运算时间大于密码定期更换时间（以 SUPER π 104 万位 100 秒的运算标准）；

6） 管理员不能为了方便使用信息资源规避密码。

4.2 **密码存储**

系统管理员须定期更换系统密码，以防止密码的重复使用；

4.3 **密码使用**

a) 密码或含有密码的文件应妥善保管，不能将密码写在纸上随意摆放在桌面上；用户的帐号密码必须不能泄露给任何人；系统管理员不能询问用户的帐户密码；

b) 发送邮件时，加密文件和解密密钥因分两封邮件发送，以降低被盗用的威胁；

c) 用户只能使用自己权限范围内的账号密码，不能随意更改自己的权限；不能通过任何途径将密码泄露给他人。

4.4 **密码变更、废除、销毁及恢复**

发生以下情况时，需要变更废除密码：

1） 密码损毁、遗失、被盗；

2） 密码有安全隐患；

3） 人员离职；

4） 导入、更换新系统，需要重新分配密码；

5） 到期更换密码。

5 相关文件和**记录**

［系统权限登记表］	保存部门：行政公关部	保存期限：2 年
［系统权限检查表］	保存部门：使用部门	保存期限：1 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