文件编号及版本：

Document Number and Revision

ZAE-QP-007 Rev · 0

文件题目：Document Title

IT 管理控制程序

IT Management Control Procedure

批准（ Approvals）

Responsible（负责）	Name（名字）	Signature（签名）	Date（日期）
Originator（制作）	Guglus Zhang	Guglus	2010.3.2
Department Leader（部门负责人）	Albert Yang	Albert	2010.3.3
Management Representative（管理者代表）	Gianluca Paolazzi		2010/03/04
General Manager（总经理）	Jimmy Lam		2010/03/15

页码 (Page	1	2	3	4	5	6	7
版本号. (Rev. No)	0	0	0	0	0	0	0
页码 (Page.	8	9	10				
版本号 (Rev.	0	0	0				

生效日期 Effective date： Mar 1, 2010

更改历史（Revision History）：

更改（Revision）From To	日期（Date）	更改内容（Revision Description）	更改人（Changed by）	复核人（Checked by）
0	Mar 1, 2010	New Document	Guglus Zhang	Albert Yang

目录（**CONTENTS**）

1.0 目的：Purpose

通过预防未授权访问数据及滥用`破坏`丢失数据的发生，为 ZAE 创造良好的 IT 环境，以维护系统的数据安全性及保密性；

To create an environment within ZAE that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data.

2.0 范围：Scope

该文件适用于所有 ZAE 信息设备使用者，关于他们的授权范围，以及使用方法；

Apply to users of the IT facilities as regards to their scope of authority, the kind of tool exploited and the way of its utilization in ZAE

3.0 定义：Definition

无 None

4.0 参考文件：Reference Document

无 None

5.0 责任：Responsibility

5.1 行政部负责个人电脑使用的管控。
AD responsible for the PC utilization's control and management.

5.2 行政部负责局域网使用的管控。
AD control and manage the LAN utilization

5.3 行政部负责密码及服务访问管理。
AD manage the password and access service.

5.4 行政部负责电子邮件及互联网使用的管控。
AD responsible for the e-mail and Internet utilization's control and management.

5.5 行政部负责电话系统使用的管控。
AD control and manage the telephone system utilization.

6.0 资格及培训：Qualification and Training

负责 IT 管理的人员须具有大学以上学历及两年以上相关工作经验；

IT administrator should graduate from college with two years related working experience.

7.0 程序：Procedure

7.1 个人电脑之使用：Personal Computer utilization

7.1.1 公司直接或间接分配给职员的个人电脑，**只能用于工作之用**。不同目的的电脑工具使用皆可能是效率降低，维护成本，甚至安全威胁的诱因。电脑设备作为公司之资产应放置于良好环境状态中。（笔记本电脑尤其应小心保管）

The company Personal Computer (PC), directly or indirectly assigned to the employee, must **only be used for working purposes**. The utilization of the computer tools for different aims may contribute to cause inefficiency,

maintenance costs, and moreover security threats. The computer device must be kept in good condition (special care must be taken of the laptop-computer) being part of the company estate.

7.1.2 所有电脑须由 ICT 技术员或外包商定期检查维护；
All of the PCs are subject to a fixed-term check carried out whether by an ICT technician or by an external deputy in charge of the maintenance of the IT devices.

7.1.3 登入电脑需输入密码，该密码由持有者妥善保管，不得告知任何他人。使用者无系统管理员明确允许不得私自设置开机密码；
Logging in to the computer is protected by a password, which must be kept secret by the holder with the best care. No one else but him is supposed to know the password. The user is not allowed to set a password at the initial boot (BIOS), without an explicit authorization of the system administrator.

7.1.4 系统管理员为 IT 设备维护或确保其正常运行之目的，可以进入任何用户之数据，包括邮箱及其他任何信息，系统管理员应为所看到的个人数据严格保密；
The system administrator has the faculty to enter the data of every user, including the email archive and whatsoever information needed for the maintenance and correct running of the IT devices. The sight of the personal data by the system administrator is strictly confidential and limited to the lowest necessary for the maintenance of the computer tools.

7.1.5 电脑使用者严禁在电脑设备上私自安装任何软件。
The user is not allowed to install any kind of software on the PC device.

7.1.6 电脑使用者严禁私自更改电脑的原有设置，除非经系统管理员特别允许；
The user is not allowed to change the original setting of his PC, unless specifically authorized by the system administrator.

7.1.7 每天下班前或长时间离开办公室时须关闭电脑，以防已进入系统的电脑被他人滥用。每台电脑都需启动屏幕保护程序并为其设置密码保护；
The PC must be switched off every night before leaving the office and every time the user being away from the device for a relatively long time. Leaving an unattended logged in computer may allow a third party to use the PC improperly, without being possible afterward to ascertain the author of the abuse. For security reasons a screensaver protected by password must always be set.

7.1.8 除非经系统管理员特别允许，电脑使用者严禁私自增加使用其他存储或通讯外设（如 modem, CD-RW 等）。任何掌握保密数据的使用者不允许用同一系统账号在不同电脑登入；

The user is not allowed to enrich the PC device with any storage and communication device (such as, …), unless clearly authorized by the system administrator. All the users in charge of the treatment of confidential data are not allowed to log in different machines by using the same account

7.1.9 使用者要使用来自公司外的任何文件，应立即联系系统管理员检查是否被病毒感染。尽量不使用外来存储媒体，如确需使用，须先用防病毒软件查杀每个文件
Each user must pay attention to every file created outside the company, immediately contacting the system administrator in case there could be any possibility of a virus infected. The user is not allowed to introduce in the company any unknown or not connected to the company device (such as floppy, CD-ROM, DVD, etc., …); being strictly necessary to introduce it, the user must always check the files by using the anti virus software loaded in each machine.

7.1.10 电脑使用者严禁查看，存储，传播任何有关暴力，色情，种族，宗教，信仰，商贸及政治团体等字眼的文件。
The user is not allowed to file documents containing outrageous and sexual, religious, race, ethnic origin, opinion, trade union and political membership discriminatory documents.

7.2 局域网之使用: LAN utilization

7.2.1 系统管理员任何时候一旦在 PC 或局域网中发现对局域网不安全的文件，可立即删除该文件。如使用者需要存储大容量文件到局域网中，请通知系统管理员；
The system administrator may remove at any time any file considered dangerous for the safety of the LAN, both in the single PC and in the LAN units. It is advisable the user to inform the system administrator in case a big amount of data should be stored in the LAN units.

7.2.2 建议定期（每三个月）清理资料夹，删除没用和陈旧的文件。尤其注意重复的文件：应避免存储同一文件的不同版本。如确实需要，请联系系统管理员把它存到别的存储媒体（如光盘或磁带）；
It is advisable to proceed to a periodical (every three months) clear out of the archives, deleting all the unused and obsolete files. Special care must be paid to the duplication of the files: the user should avoid to save different version of the same file. In case it would be necessary, the user may ask the system administrator to save the data in another storage unit (CD-ROM or tape).

7.2.3 除非文件拥有者允许，使用者不允许查看局域网中其他用户的文件，或与其无关的文件；
The user is not allowed to look at the folders available in the LAN belonging to other users, or in general documents not related to his activity, unless expressly

authorized by the owner of the file (or his deputy)

7.2.4 系统管理员将定期清理用于用户间临时共享文件的空间，因此不得将此资料夹用于存储文件，以免造成文件丢失。
The shared spaces are kept periodically cleared by the system administrator (service folders) where used for the temporary file sharing between users. It is for this reason forbidden to use these folders as file storage, it is possible to loss data.

7.3 密码及服务访问管理：Password and service access management

7.3.1 每一用户以唯一用户名为标识来访问局域网，但不同服务他可以有不同密码。所有密码由用户自己设置。用户应妥善保管好密码；
Each user can be identified by a unique username to access the LAN, though he might hold different passwords to access different services. All the passwords are set user. User need keep well for password.

7.3.2 用户一旦发现自己的密码被泄露，应立即更改；
Once user found the password was reveled, he/she must immediately modified.

7.3.3 用户密码由字母，数字，符号组成，长度至少八位，密码每隔 42 天必须更改一次。
The password minimum length is 8 characters, including letter, numeral, and symbol. Each password must be modified per 42 Days.

7.4 电子邮件及互联网使用：E-mail and Internet utilization

7.4.1 公司分配给使用者的电子邮箱应视为工作之工具。每个邮箱使用者应负责正确使用该电子邮箱；
The mail box assigned by the company to the user must be considered as a working tool. Each holder of a mail box is responsible for the correct use of it.

7.4.2 避免与公司无关及与工作无关的邮件在职员间产生或传播。应定期删除电子邮箱中不用的档案，尤其是包含大容量附加文件的邮件。电子邮箱不应视为文件夹，附加文件应保存到文件夹中；
It is advisable to avoid messages unrelated to the company, to the job to be conducted, and be communicated between employees. The mail box must be kept in order, periodically deleting all the unused documents, especially the mail containing huge attachments (the mail box shouldn't be considered as a file archive, the attachments must be saved on a disk).

7.4.3 使用者打开邮件附件前必须检查它，应避免直接运行邮件之附件。当用户收到包含未知附件的邮件时，不要打开它并把邮件删除；

It is compulsory to check the file attached to the email before opening them; it is advisable to avoid the direct execution of the attachments from the mail client. In case a user would receive an email containing unattended attachments or being the sender unknown, it would be advisable to delete the email, without opening any related attachment.

7.4.4 禁止发送 Internet 地址链。如有使用者收到这种信息，应直接删除它。使用者不能打开这种信息的附件或回复邮件；
It is forbidden to send Internet chains. In case the user receives such a message, it must be directly deleted. The user must not open the attachments of these messages or reply to them.

7.4.5 如邮件中有明显的或隐蔽的类似病毒特征的建议，不得将此邮件转发给他人；
Messages containing explicit or concealed advice regarding the presence of a virus, must not be forwarded to anyone

7.4.6 系统管理员已为每个用户的邮箱设定最大容量。最好在 ICT 技术员指导下把旧的邮件归档到个人邮件夹中。如无 ICT 技术员指导而建个人邮件夹所导致的数据丢失，ICT 技术员概不负责；
Each user's mailbox has a maximum capacity defined by the system administrator. It is advisable to file the old emails in personal mail folders, whose activation must be followed by a ICT technician or his deputy. In case the user would decide to create a personal mail folder, without any supervision, the ICT department is not to be considered responsible for any loss of information.

7.4.7 为避免重复，使用者应避免收件人地址中输入发信人的地址。系统会自动保存已发送邮件，因此不必额外保存该邮件；
In order to avoid duplications, the user must avoid all the messages in which the addressee equals the sender (including CC, BCC). The sent emails are systematically saved by the system, so it is useless to save another copy of the mail.

7.4.8 Internet 用户应遵守国家相关法律使用互联网，严禁使用公司网络资源做工作以外的事。用户访问的每条 Internet 信息将被系统记录，公司总经理可随时检查上网记录，并有权处罚非法 Internet 访问的使用者。
Internet user should observe the country's relevant law to use the Internet, it is not allowed to use company's network resource to do something have no business with the work. The system will record every Internet access activity, general manager will check the Internet access record at any time and punish the lawless Internet user.

7.5 电话系统使用：Telephone system utilization

7.5.1 公司根据职员工作需要分配给使用者相应的电话拨号权限。每个电话使用者应负责正确使用该电话，不得用公司电话拨打私人电话；
The company assigns appropriate phone rights to staff according to his work demand. Each user is responsible for the correct use of it, private phone making is not allowed.

7.5.2 行政部门根据工作环境和各部门的需要可将外线电话用户设置有权码，使用者应妥善保管密码，离开办公室或下班时记得将自己的分机闭锁，以防他人盗打。电话记费系统将记录每个分机打出的每通外线电话，每月底由行政部门清查各分机电话清单。职员应为从自己分机拨出的工作以外电话付费。
AD department will set an authentification code for each external phone user. For your protection, user should keep well your password and lock your extension when you leave your office. The phone toll system will record every external call, these records will be checked by AD department at the end of month. The staff must pay for the phone call from his extension except the working call.

7.6 数据备份作业：（服务器位于 ZIS，所以数据由 ZIS 相关人员统一备份）。
Backup the server's system data (Service lie at ZIS, the backup of server's system data is done by ZIS).

7.6.1 服务器系统数据备份作业：Backup the server's system data

7.6.1.1 系统数据备份之目的在于一旦服务器或操作系统发生损坏无法修复而必须重新安装时，可由备份数据还原，使系统得以在最短时间内恢复；
The purpose of the system data backup is to recover the system as soon as possible when the server or operation system is damaged and need to reinstall.

7.6.1.2 每日由 ICT 人员将服务器主机管理系统整个备份至磁带中，妥善存放并检查每一次备份状况纪录并将检查结果记录在《数据备份纪录表》以确保备份数据完整性.数据备份周期为一周；
The operator backup the server operation system to magnetic tape everyday, then place the tape in safe location and check backup log and record the check result of each backup, and backup circle is 1 week.

7.6.2 个人数据于文件服务器中之备份: Backup the personal data in file server
ICT 部门于服务器内均有设定一使用者专属之磁盘空间供使用者备份文件。各使用者应定期更新服务器内个人数据之备份文件；
ICT department configure a privacy disk place for each user to backup his personal working file on file server. Every user should update his file on server termly.

7.6.3 邮件数据之备份：Daily backup the mail data
使用者需定期整理个人之电子邮件档案并删除不重要或与工作无关之档案。ICT 人员每日将邮件服务器中之用户邮箱备份至磁带中，妥善存放. 数据备份周期为

一周。
The user should clean up his mail box periodically, delete the files that unuseful or hove no business with the work. ICT operator daily backup the user's mail box on exchange mail server to tape, and place the tape in safe location. Backup circle is 1 week.

7.6.4 数据库数据备份：Backup the data-base
数据库内之数据为每日由使用者使用 ERP 等工作产生，每天不断的增加与异动，所以每日必须由 ICT 人员并同系统数据同时备份，且须将备份作业完整纪录下来以确保备份数据完整性。数据备份周期为一周。SAP 系统的数据中心位于意大利，所以数据由意大利相关人员统一备份.
The data in data-base is produced by user's daily working on ERP or others, they are increased and modified day by day, so it must daily backup by ICT operator together with system data, and should record the total backup operation. Backup circle is 1 week. And SAP data center is located at Italy, so backup of SAP data is perform by ICT of Italy.

7.6.5 媒体管理：Backup media's management
ICT 操作人员应当为每盒备份用的磁带适当标示，以便日后查找。每天把备份好数据的磁带放到磁带盒，磁带盒应放置于防潮防水避免阳光直射的安全场所。
ICT operator should identify every tape to look for it conveniently in the future. Place the tape into the tape box after the backup finished, and the tape box should place in a safe location that is moisture proof, rainproof, and against the direct sunshine.

8.0 记录 Record

8.1 Internet 访问记录数据库， 由 ICT 部门保存，保存期为半年
Internet Access Record Database should be remained by ICT department for half an year.

8.2 《数据备份记录表》由 ICT 部门保存，保存期为一年
"Data Backup Record" should be remained by ICT department for one year.