浙江宝绿特环保技术工程有限公司

电脑化资讯系统管理循环

2023 年 12 月

目　录

Z-BRT-EP-01 资讯处理部门之功能及权责划分

1.目的

明确规范资讯单位之功能及使用部门之职责划分，确保公司作业电脑化及资料处理之独立性。

2.范围

资讯单位功能及职掌之界定，并明确划分资讯单位与用户部门之权责。

3.权责单位

3.1.资讯单位：在权责划分原则下善尽职责，适当分工并达到控制、勾稽功能。

3.2.使用单位：依实际及未来作业状况向资讯单位提出作业需求。

4.控制重点

4.1.资讯单位应持超然独立之立场执行其职务，并不得逾越未经授权之事宜。

4.2.资讯单位与使用单位应适当划分职责、权限。

4.3.各项电脑及周边设备应经资讯单位签核始可办理异动。

5.程序内容

5.1.资讯单位之功能

5.1.1 设置独立于使用单位以外之专职资讯人员，俾达成下列功能：

5.1.1.1.推展各项应用系统，加强电脑化。

5.1.1.2.促进各部门对电脑软硬件之充分有效使用。

5.1.1.3.发挥电脑作业迅速、省力及连贯作业之特性，提高公司各项作业之效率及质量。

5.1.1.4.运用电脑自动勾稽机能，达到内部控制目标。

5.1.2.协助与电脑相关之自动化工作。

5.2.资讯单位之职责

5.2.1.统筹规划全公司作业及应用系统之安全、运用及系统整合事宜。

5.2.2.全公司电脑软、硬件需求等之审核与验收。

5.2.3.「电脑化资讯系统管理循环」之订定及维护。

5.2.4.灾难回复管理之规划与执行。

5.2.5.设备规划与管理

5.2.5.1.公司电脑及外围设备、软件包之规划、评估与控制。

5.2.5.2.电脑及外围设备、软件包使用之管理、调度及维护。

5.2.5.3.机房空调、电力、不断电系统(UPS)及消防设备之规划与管理。

5.2.5.4.电脑网络与通讯系统之规划、管理。

5.2.6.电脑作业管理

5.2.6.1.机房门禁、操作系统及档案管理。

5.2.6.2.机房电脑主机及各外围设备运转之管理。

5.2.6.3.资讯输出／输入设备使用管制作业。

5.3.职务代理

资讯单位应根据职责划分原则及系统安全控管精神制订职务代理制度，其规范原则请详「职务代理人制度」作业说明。

5.4.与使用单位之职责划分

5.4.1.各使用单位得视本身现行与未来作业情况，提出作业需求。资讯单位则参酌电脑软硬件发展情况与相关部门会商决定开发之优先级后办理。

5.4.2.使用单位自行登录及处理资料者，除因业务需要并经使用单位同意及授权，资讯单位不得擅自变更其资料。

5.4.3.使用单位若有机器移动应依「固定资产—调拨作业」程序办理，并知会资讯单位签核，由资讯单位指派人员陪同使用人员方可移动。

6.相关程序

6.1.「职务代理人制度」

6.2.「固定资产—调拨作业」

7.相关办法

无。

8.使用表报

无。

Z-BRT-EP-02 系统开发及程序修改作业

1.目的

明订应用系统(程序)或软件之购置、开发及修改程序，以确保电脑化作业之软件符合企业及使用单位需求。

2.范围

本作业程序适用于应用系统(程序)或软件之购置、开发及修改程序之申请、审核与验收作业。

3.权责单位

3.1.资讯单位：依照使用单位之需求执行应用系统(程序)或软件之分析、修改、设计、购置、开发等作业。

3.2.使用单位：使用需求之提出及验收。

4.控制重点

4.1.系统软件、应用系统（程序）或软件之委外开发、购置，应依规定之作业程序办理，并考虑使用单位之需求。

4.2.评估纪录等书面文件应经适当签核。

4.3.开发或购置之系统软件、应用系统（程序）或软件之申请需求，应与实际开发或购置之系统相符。

4.4.系统之外购应经核准，并签订合约。

4.5.相关单位与资讯单位应就书面设计与实际设计作最后比对。

4.6.系统测试及修改应设立独立之环境。

4.7.程序变更修改应确实经核准后办理。

4.8.系统修改后，须与使用单位测试其可行性。

5.程序内容

5.1.申请单位因实际作业而有系统开发或程序修改需求时，填写【电脑作业需求单】，检附相关资料，依权限呈核后，送交资讯单位审核，倘决议自行开发／修改者，则依 5.2.程序执行。倘决议委外开发／修改者，则依 5.3.程序办理。

5.2.系统自行开发或程序修改

5.2.1.可行性分析作业

系统开发人员应与相关人员讨论作业现况、系统之需求及收集相关资料。后将分

析、规划结果，可行性方案汇总填入【电脑作业需求单】，视需求可列附件，依权限送呈签核。

5.2.2.系统规划分析之作业程序

系统开发人员依据所收集的资料进行析规划，进而确立系统之规划蓝图、功能细节、操作流程及作业范围，并据此撰写系统规划。过程应会同使用单位或相关单位进行确认。

5.2.3.程序设计作业程序

系统开发人员依系统规划之内容进行程序设计、撰写及布署。

5.2.4.系统测试之作业程序

系统开发人员完成个别程序模块之撰写、编译、布署后应就个别程序模块进行测试工作，测试资料应小心选择，保护及管制，并确认程序是否运作正常或符合需要。重要之资料库应分为测试区及正式区，所有测试工作应于测试区完成后，方可导入正式区使用。

5.2.5.系统建置(转换)及程序修改上线之作业程序

5.2.5.1.系统开发人员会同使用单位及相关单位之主管或关键用户做最终确认。

5.2.5.2.系统开发人员撰写操作手册或技术手册等设定文件及培训资料。

5.2.5.3.系统开发人员会同使用单位及相关单位进行培训，并约定上线时间，测试可行后，使用单位应回复验收情况。

5.2.5.4.上线应由权责人员执行且于上线前确认已备有权责主管复核之【电脑作业需求单】。

5.2.5.5.系统开发人员于计划时间切换系统，并将【电脑作业需求单】、系统规划等其他相关文件按「编制系统文书之控制」作业办理结案归档。

5.3.系统软件、应用系统（程序）或软件之委外开发购置

5.3.1.本公司之整合性管理资讯系统采外购软件者，由资讯单位依据公司需求，经与厂商议价，权责主管核可后购置，并与原开发公司签订长期维护合约，合约内容应注意保固期限、维护服务、教育训练、系统文件及操作方式范围等规范，并考虑机密性、可用性、完整性之适用性；委外开发时亦同。

5.3.2.外购软件或开发之测试、文件准备、用户培训、上线等工作比照 5.2.5 自行开发程序之作业程序办理。

5.4.系统软件、应用系统（程序）或软件委外改版更新(upgrade)或修改

5.4.1.使用单位因业务需要、或供应商定期更新版本、或资讯单位整体规划需求时，应办理系统软件、应用系统（程序）或软件之版本更新或修改。

5.4.2.资讯单位应与原供应商（如合约厂商、原厂保证厂商）联系，安排修改事宜，相关之合约、需求表或采购订单应存档备查。对于提供服务之委外厂商，应于服务合约中适当列明其系统安全政策及权责归属问题，并考虑企业本身之安全需求，拟定测试之机制，以了解委外厂商之政策遵循及其安全控管之适当性。

5.4.3.实际发生费用时，除按「采购及付款循环－付款作业」办理请款外，应加附 5.4.2.之相关附件。

5.4.4.更新或修改之测试、教育训练及验收应比照 5.2.5.项办理之。

5.4.5.新设或修改系统，应于使用前提交使用部门进行模拟测试，经充分讨论及验证后，始可取代旧系统。

5.4.6.相关操作手册、技术手册及设定文件、培训资料等，应按「编制系统文书之控制」作业办理。

6.相关程序

6.1.「编制系统文书之控制」

6.2.「采购及付款循环-付款作业」

7.相关办法

无。

8.使用表报

8.1.【电脑作业需求单】

Z-BRT-EP-03 编制系统文书之控制

1.目的

为利于电脑系统文书资讯之管理，特订定本作业程序。

2.范围

本作业程序适用于电脑系统文书编制及保管之控制。

3.权责单位

3.1.资讯单位：电脑系统文书资讯之管理。

4.控制重点

4.1.资讯单位所有之电脑文书及档案文件应编号列册，并设专人保管。

4.2.资讯单位于新系统开发及进行修改作业时，其相关之电脑文书应同时予以更新。

5.程序内容

5.1.电脑系统文书编制

5.1.1.资讯单位于完成系统测试程序及验收程序后(含新购、版本更新及修改)，将【电脑作业需求单】及操作手册编号存查列管。

5.2.文书资料保管

5.2.1.资讯单位应将各项系统分析、开发及设计文件按序分类归档，对于具机密性资料、文件应特别装柜加锁以避免资料的外泄。

5.2.2.当作业人员因公借阅系统文件纸本原件时，应登记有关事项于【档案资料借阅簿】后方得借用，并依照规定还件日期归还，资料保管人员应定期催讨逾期未还者。

5.2.3.如借阅之文件属于机密或敏感性文件，须经权责主管核准后方可借阅。

6.相关程序

无。

7.相关办法

无。

8.使用表报

8.1.【电脑作业需求单】

8.2.【档案资料借阅簿】

Z-BRT-EP-04 程序及资料之存取控制

1.目的

为建立本公司各用户对系统程序及资料存取之权限及范围，特制定本作业程序。

2.范围

本作业程序适用于网络及个人电脑，其程序及资料之访问控制。

3.权责单位

3.1.资讯单位：对各使用者之需求权限进行设定。

3.2.使用单位：提出权限新增与异动之需求。

4.控制重点

4.1.程序档案的存取使用应依个人权限加以管制。

4.2.重要之系统公用程序、工具及指令应依其用户权限限制其访问权限。

4.3.一般应用系统之用户除执行应用系统外，应无存取系统公用程序、工具及指令之权限。

4.4.程序档案的存取使用均应留下可追踪的纪录。

4.5.权责主管应定期复核相关记录。

4.6.程序及档案应依业务应用及稽核使用加以区分。

4.7.密码不可显示于电脑屏幕上，亦不可未经乱码化即打印于任何报表。

5.程序内容

5.1.网络系统内之存取控制作业

5.1.1.各使用单位主管于建置新的应用管理系统、有新进人员或权限异动时，应依其所辖职员之业务权限，填写【电脑权限申请单】并呈核后，交资讯单位人员设定用户权限。

5.1.2 资讯单位依【电脑权限申请单】创建、赋予、异动或删除账户权限时应注意申请权限之部会权责，有疑义得会同相关单位咨询。

5.1.3.新进人员使用系统时应先按 5.1.1.申请取得新帐户密码方可使用，帐户应具有可识别性，并禁止使用共同帐户。

5.1.4.电脑系统使用单位操作人员因故离职时，离职人员应将【工作移交清册】交资讯单位删除用户权限。

5.1.5.员工离职，其使用代码应立即注销或更新。

5.1.6.对于软硬件厂商维护时使用之使用者代号应限制其访问权限，且不得重复使用。

5.1.7.使用默认密码登入系统时，应要求使用者于登入后立即变更密码。

5.1.8.帐户密码于身份验证时，相关信息不以明文显示与传输，且系统应具备帐户锁定机制。

5.1.9.系统密码应有设定原则，如最低密码复杂度。

5.1.10.权责主管应定期审核帐户与权限之建立、修改、启用、禁用及删除之状况。

5.2.使用个人电脑之存取控制

5.2.1.个人电脑之使用应依岗位需求向资讯单位提出，视情况依『固定资产-调拨作业』或『固定资产-请采购作业』取得个人电脑，并依 5.1.1 申请个人电脑帐户权限后方得使用。

5.2.2.用户所使用之磁盘或软件必须经资讯单位核可认定后，方可于公司电脑上使用或安装，以防止电脑病毒入侵，破坏存档之资料。

5.3.权限控制

5.3.1.资料权限应有分层授权系统，稽核及管理人员无权限更新资料库，应用系统、作业系统及资料库之最高权限管理账号， 由资讯单位最高主管管理，并应定期变更密码。

5.3.2.负责系统或程序上线人员应于执行上线程序时，依系统安全及用户职权之所需设定程序及资料文件之访问权限。

5.3.3.设定系统程序对有权接取某特定档案的程序限制其接取权利。

5.3.4.原则上公司内网不开放远端电脑接入，如有作业需求者，应填写【电脑权限申请单】，经权责主管核准后，交资讯单位设定权限。

5.3.5.资讯单位应不定期检视远端连线状况，避免有非授权人员接入之情况。

6.相关程序

无。

7.相关办法

无。

8.使用表报

8.1.【电脑权限申请单】

8.2.【工作移交清册】

Z-BRT-EP-05 资料输出入之控制

1.目的

确保资料之输出与输入均经适当控制。

2.范围

本作业程序适用于资料输出，输入及错误更正。

3.权责单位

3.1 资讯单位：资料输出入权限之设定及应用程序错误之修改。

3.2 使用单位：外部资料之输入与核对输出报告之正确性。

4.控制重点

4.1.输入作业

4.1.1.若系统支持，应启用稽核记录管理，保留特定事件(如：特权账号所执行之各项活动)之稽核记录。

4.1.2.程序内对输入资料的正确性应有自动核对功能。

4.1.3 错误资料更正，是否依既定程序办理及保留稽核轨迹。

4.1.4 适时审查用户活动、异常或错误之稽核纪录，并适时采取适当行动。

4.2.输出作业

4.2.1.机密性或敏感资料之输出应适当管制。

4.2.2.输出产生时，应留下记录以供追踪查核及稽核所需。

4.2.3.报表输出后应立即分送有关单位。

4.2.4.输出资料使用后，若无保存需要，应经适当的毁弃处理。

4.2.5.输出资料若以磁性媒体保存，应定期检查，以确定在必要时能以报表方式列出。

5.程序内容

5.1.资料输入控制

5.1.1.使用单位应依照系统所需之输入资料，输入异动单据。

5.1.2.各项输入异动单据必须要有配合系统规格的单据号码。

5.1.3.使用单位之主管应就其具有影响性之系统操作功能提出用户权限规范，并确保具有关键性之操作能由训练合格之成员完成，及负责系统运作之结果。

5.1.4.对错误资料之发生原因应进行分析，以期改善。

5.1.5.资料输入人员于收到原始凭证、单据时，应先审核资料内容业经权责主管签核且无异常情形者，方得据以登录。

5.1.6.资料输入完毕后，应即对原始凭证做适当的记号以防止重复输入，并依规定分类存档，原始凭证应依照规定年限妥善保存。

5.1.7.整批资料输入处理时应采下列方式控制：

5.1.7.1.各批次资料予以识别号码。

5.1.7.2.各批次资料数量予以适当限制。

5.1.7.3.总和控制。

5.1.7.4.批次资料的传送登记。

5.1.8.输入处理时，应采下列方式控制：

5.1.8.1.输入错误时，屏幕显示错误讯息，提醒用户更正。

5.1.8.2.系统应依据资料的合理性、存在性及完整性等进行细部检查。

5.1.9.接口系统输入处理时，系统自动调节及结转至系统结转资料文件内。

5.1.10.标准参数及重要主文件资料之输入及更正应经适当授权，并依其职权严格限制其访问权限。

5.1.11.应于程序设计时，加入适当之限制或自动检查输入之原始资料，以防止人员输入错误，及早发现问题。

5.1.12.所有 IT 人员非经授权，不得直接由后台修改资料。

5.2.资料输出控制

5.2.1.输出资料于产生时应注意：

5.2.1.1.依不同单位及人员之需求，供已授权之单位或人员使用。

5.2.1.2.若有输出错误且无需存档之报表应予以销毁。

5.2.1.3.有机密性或敏感资料之输出应设定适当控制。

5.2.2.重要或敏感性之报表打印应有适当之权限设定，输出资料应先确认处理项目、单位无误后再行分送，若分送资料为报表或媒体时，应经主管核准后，方可分送有关单位。

5.2.3.收受单位应于收受报表时，与留存之原始凭证或相关资料检验，资料有误时应会同相关人员查明错误原因，并经权责主管同意后方得修正。

5.2.4.若透过媒体或线路传送资料时，收受单位应打印或查询确认资料的正确性，有误

时应再传送或送交正确之媒体。

5.2.5.系统应产生重要资料键入、主文件变更及系统自动产生交易之审计轨迹报告(如交易明细报告)，以供核对及调节原始输入凭证。

5.3.错误更正之控制

5.3.1.因输入错误，导致报表与其他报表勾稽不平时，经办人员应经主管核准后，输入正确之资料，并附于原始凭证之后备查。

5.3.2.因应用程序错误而造成报表错误，使用单位需填写【电脑作业需求单】送交资讯单位申请修改，其后续作业比照「系统开发及程序修改作业」办理。

5.3.3.若机器故障时，操作人员应通知资讯单位人员通知维修厂商修复。

5.4.软、硬设备报废

5.4.1.有关电脑及磁性储存媒体之报废，为避免个资外泄，使用单位应会资讯单位进行报废媒体之勘验。

5.4.2.使用单位应先自行清空电脑硬盘资料，并将该电脑硬件含硬盘送交资讯单位进行实际勘验。

5.4.3.资讯单位于勘验后，应将机密性、敏感资料及授权软件确实予以移除，实施安全覆写或实体破坏，并确保报废之电脑硬盘及储存媒体储存之资料不可还原，通知使用单位取回可报废的硬盘，以完成最终之财产报废程序。

5.4.4.若欲报废的电脑设备为笔电者，则由使用单位径行将整台笔电送交资讯单位进行前述作业。

6.相关程序

6.1.「系统开发及程序修改作业」

7.相关办法

无。

8.使用表报

8.1.【电脑作业需求单】

Z-BRT-EP-06 资料处理之控制

1.目的

建立软、硬件于资料处理时之控制程序，以确保资料处理之正确性。

2.范围

本作业程序适用于硬件及系统软件于资料处理之控制程序。有关资料处理之输出／入控制依资料输出入之控制作业办理。

3.权责单位

3.1.资讯单位：对于系统开机与系统执行及软、硬件之资料处理进行控制及系统软、硬件异常状况排除。

3.2.使用单位：提出系统使用需求及通报系统软、硬件异常状况。

4.控制重点

4.1.系统运作发生异常时应即修护、排除。

4.2.系统异常之修护、排除过程序应予记录。

4.3.程序中应设定适当之控制功能，确保资料处理的正确性。

4.4.系统应自动检核或产生重要资料之序号。

4.5.制订适当控制处理程序以达到下列目的：

4.5.1.确定所有为系统接受之交易系经系统适当处理。

4.5.2.确定系统内部自动产生之交易系经系统适当处理。

4.5.3.确定交易业已记录于适当之会计期间。

5.程序内容

5.1.硬件于处理资料之控制

5.1.1.相关之硬设备应定期检查，并将检查情形予以记录。

5.1.2.硬设备如有异常现象发生，应根据各项设备使用手册之指示设法排除或是即刻通知厂商前来维修，并作成维修纪录。

5.2.系统开机

5.2.1.各作业权责单位依据规定启动各项电脑系统并记录异常状况。

5.2.2.电脑主机设备如发现不正常情形，应根据各项设备使用手册之指示设法排除或是即刻通知厂商前来维修，并作成维修纪录。

5.3.系统执行

5.3.1.营业时间内相关作业人员应随时掌握各项可能突发之异常现象，以便采取因应之对策。

5.3.2.硬设备如有异常现象发生，应根据各项设备操作手册之指示设法排除或是即刻通知厂商前来维修。

5.4.系统软件于处理资料之控制

5.4.1.一般系统软件系指操作系统及公用程序，通常由厂商提供，若需修改或更版系统软件时，应比照「系统开发及修改作业」办理。

5.4.2.不同使用者应有不同的权限控制，其权限设定比照「程序及资料访问控制」作业办理。

5.5.应用软件于处理资料之控制

5.5.1.对于资料之处理，应于系统作业中，利用程序设定防错机制。其使用等级或权限之设定比照「程序及资料访问控制」作业办理。

5.5.2.为确保处理资料的一致性，若有两个以上应用操作系统同时更新档案资料时，程序中应判断一次只能由一应用系统更改该笔资料，另一应用系统须等该档案已更改完后方能变更该笔资料内容。

5.5.3.处理控制应与输入控制相互配合，于程控中应有适当之检查方式，如：

5.5.3.1.由某一程序处理资料将结果传给另一程序时，应有处理总数之控制以确保资料无遗漏。

5.5.3.2.合理化之检查：如极限值、范围的控制，检查号码、字型型态检查、借贷平衡检查、四舍五入的原则等勾稽方式，以强化资料正确性。

5.5.4.于执行应用软件处理资料时，若有错误发生，应分析是资料或程序错误，若是资料错误应依错误更正程序办理；若程序错误应依程序修改作业程序处理。

5.5.5.系统因故中断，使用单位应立即通知资讯单位协助处理，检查当笔资料应存在、应可进行还原或必须重新输入。

6.相关程序

6.1.「系统开发及修改作业」

6.2.「程序及资料访问控制」

7.相关办法

无。

8.使用表报

无。

Z-BRT-EP-07 档案及设备之安全控制

1.目的

为维护资料文件及各项电脑设备之安全，特制定本作业。

2.范围

本作业适用于资料文件之拷贝、控管及电脑设备、机房之维护、安全控制。

3.权责单位

3.1.资讯单位：依资料文件、电脑设备及电脑机房之安全进行控制。

3.2.使用单位：配合资讯单位订立之使用规则进行档案之存取。

4.控制重点

4.1.档案安全管理

4.1.1.系统应定期做备份，并留存书面记录。

4.1.2.备份资料应指定专人保管。

4.2.设备安全管理

4.2.1.消防设备应定期检查维护。

4.2.2.系统发生异常状况时，应加以了解原因、改进及记录。

4.2.3.各项支持防护设备应定期检查、换新。

4.2.4.用户对其使用或保管之各项电脑设备及外围设备须不定期检查，如有问题时，应通知资讯单位维修。

4.3.机房人员进出应确实管制。

4.4.应定期更新侦测病毒软件之版本，并训练所有人员使用侦测病毒软件侦测外来磁盘之病毒。

5.程序内容

5.1.资料文件之安全控制

5.1.1.资讯单位之统筹控制

5.1.1.1.至少每周备份一次资料，存放之媒体可为网络硬盘、NAS、磁盘等。

5.1.1.2.将平日取用之媒体分别各备两份，分存于不同之地点(不同之厂区)。

5.1.1.3.历史档案之媒体依不同档案性质(系统程序、应用程序、资料文件)定期备份一份存放于其他地点(不同之厂区)。

5.1.2.使用单位对档案之控制

5.1.2.1.为防止公司电脑资讯遭电脑病毒侵入，资讯单位应依职权设定软件安装权限。

5.1.2.2.使用单位对于档案之使用应依照「程序及资料访问控制」作业办理。

5.1.2.3.备份储存媒体除资讯单位外不得调借其他单位。

5.1.2.4.为确保资料完整性，资讯单位当设定控制程序，禁止非经核准之档案存取。

5.1.3.为避免档案资料遭病毒毁损，资讯单位应不定期自动侦测病毒。

5.2.电脑设备之安全控制

为确保系统运作顺畅、安全，资讯单位应对各项电脑设备详加规划与管理，兹将电脑设备分成电脑机器、通讯、支持、电源设备四种，其使用之安全控制管理分述如下：

5.2.1.电脑机器管理：包含电脑主机、终端机、打印机、磁带(碟)机。

5.2.1.1 凡机器设备于购入时，资讯单位应依「采购及付款循环」相关验收作业会同使用单位验收，及依「不动产、厂房及设备循环」办理建档编号。

5.2.1.2.超过保存年限者应列单报废，以避免留存不必要之设备。

5.2.2.通讯设备管理

5.2.2.1.通信网路应保持机密性，防止资料被他人截取。

5.2.2.2.若设备线路发生故障时，应立即检查，以了解线路故障原因，通知厂商或电信公司进行维修。若有重要性资料需立即处理时，应报请主管同意改以人工操作代替之。

5.2.2.3.设备应适当防护，未经授权人员不得接近，且附近不可放置易燃或危险物品。

5.2.3.支持设备管理

5.2.3.1.备有火警设备，以警示有火灾讯息。

5.2.3.2.于明显及重要地点设置灭火器，以便火灾时灭火用。

5.2.3.3.灭火器应定期更换，并有专人负责消防系统之定期检查与维修。

5.2.4.电源设备管理

5.2.4.1.重要设备应装设有不断电设备(UPS)及电源供应器以防止较长时间的停电。

5.2.4.2.应安装自动电压稳定装置。

5.2.4.3.使用的电源要具有电磁式开关及地线接地，以保护电脑设备。

5.3.机房之管制

5.3.1.机房内应设置独立之空调设备以维持机房温度之适当性。

5.3.2.人员进出管制

资讯单位人员应禁止非作业人员进出机房洽公，电脑机房应设置门禁管制，由资讯人员陪同并登录【机房进出记录】才可进入。

5.3.3.操作管理

5.3.3.1.操作机器发生异常时应留下异常记录。

5.3.3.2.机房中所有机器设备操作人员应依操作手册规定启动及操作。

5.3.3.3.系统之控制面板所留下之记录需加以保留并定期由主管检验。

5.3.4.禁止事项

5.3.4.1.非操作人员未经允许，不得携带物品进出机房。

5.3.4.2.非操作人员不得使用电脑机房，若因紧急状况需使用机房设备时，应经权责主管同意。

5.3.4.3.机房内除机台设备及其他必需品外禁止放置可燃物，或散置垃圾及私人物品。

5.3.4.4.机房内禁止吸烟及进用食物饮料。

6.相关程序

6.1.「程序及资料访问控制」

6.2.「采购及付款循环—验收作业」

6.3.「不动产、厂房及设备循环」

7.相关办法

无。

8.使用表报

8.1.【机房进出记录】

Z-BRT-EP-08 硬件及系统软件之购置、使用及维护控制

1.目的

为使硬件及系统软件之购置、使用及维护处理有所遵循，特制定本作业。

2.范围

本作业适用于电脑硬件及系统软件之购置、使用及维护控制。

3.权责单位

3.1.资讯单位：电脑硬件及系统软件之购置、使用及维护等相关控制。

3.2.使用单位：对电脑软、硬件之购置及资讯设备之维修提出需求。

4.控制重点

4.1.电脑软硬件购置、更新应经过管理阶层之书面核准，相关之系统设定文件应适当存档与保管。

4.2.电脑软硬件之使用须设定密码控制，并依操作手册执行。

4.3.电脑软硬件当定期维护并记录。

5.程序内容

5.1.电脑硬件及系统软件之购置

使用单位依业务需求，欲购置电脑硬件及系统软件时，须按照「不动产、厂房及设备循环循环」会同资讯单位办理。

5.2.电脑硬件及系统软件之使用

5.2.1.使用单位对于电脑硬件及系统软件之使用应依照操作手册之说明进行操作。

5.2.2.资讯单位对于电脑硬件及系统软件之维护应依照系统手册办理。

5.2.3.资讯单位应依程序及资料之存取控制之密码控制作业，规范各部门使用软件之权限。

5.2.4.操作控制

5.2.4.1.应于系统设定用户于联机后一定时间内未用电脑时，电脑自动脱机；倘系统无法做此设定，使用者应自行于 PC 内设屏幕保护程序，进入时需再输入密码才可进入；个人电脑不使用时需关机。

5.2.4.2.禁止擅自利用资讯单位系统设备处理与本身业务无关的作业。

5.2.4.3.非办公时间或假日要使用主机，应将使用目的及使用时间事先经权责主

管核准。

5.2.4.4.工作人员按「开关机程序」开机或关机。

5.3.硬体设备及软件维护

5.3.1.资讯单位对于硬体设备应定期维护保养，并记录于【设备检查表】。

5.3.2.公司所有之硬体设备，其型号应列册记录，以利维护作业。

5.3.3.用户对其使用或保管之各项电脑设备及外围设备须不定期检查，如有问题时，应通知资讯单位维修。

5.3.4.各单位欲申请系统设备维修时，应通知资讯单位进行处理，若须外修应通知厂商维修，修毕验收无误后请申请人签名并依「采购及付款循环」规定办理请款。

5.3.5.若通讯设备线路发生故障时，资讯单位应派员立即检查，以了解线路故障原因进行维修。若有重要性资料需立即处理时，应报请主管同意改以人工操作代替之。

5.3.6.外购电脑软件之修改程序比照系统开发及程序修改作业办理。

6.相关程序

6.1.「采购及付款循环—请购作业」

6.2.「采购及付款循环—付款作业」

7.相关办法

无。

8.使用表报

8.1.【设备检查表】

Z-BRT-EP-09 系统复原计划及测试程序之控制

1.目的

确保企业资讯系统遭受不可抗力之灾害或其它人员破坏时，能在最短时间内复原至正常企业营运。

2.范围

本作业程序适用于资讯系统复原计划制度及测试程序之建立、实施与控制等作业。

3.权责单位

3.1.资讯单位：建立及测试资讯系统复原计划，并予以适当维护。

3.2.使用单位：配合资讯单位完成测试资讯系统复原计划。

4.控制重点

4.1.制定系统复原办法并定期修订，检讨内容之完整性与可行性，尤其是人员变动、资源变动等等。

4.2.是否定期确认系统复原所需资源之可用性，包含备援协议之约期、备份资料及系统软件之回复性、备援设备及地点之可用性等等。

4.3.电脑系统及其设计，是否加入适当之预防措施，减低不当破坏之机率。

4.4.系统资料回复后，是否适当测试并比对。

4.5.备份资料应定期执行复原测试，以确保与财务报导有关之重要系统备份资料可用性。

5.程序内容

5.1.资讯单位于日常作业应依档案及设备安全控制之规定进行文件备份。

5.2.使用单位因系统遭受不可抗力之灾害事故、或档案被破坏、或机器故障致资料受损时，应立即呈报部门主管，并通知资讯单位处理。

5.3.资讯单位于事故发生时应参照相关系统复原办法及测试程序作业，予以呈报管理阶层，并分析档案及资料受损情况，及其对企业营运之影响，按其重要性排定应用系统复原顺序及规划应执行之资料复原程序与资料处理范围。

5.4.资讯单位处理情形与方式应及时提出书面报告，经呈报签核并知会相关单位后自行存档。

5.5.资讯部门应就资讯系统之实体环境、作业程序及应用现况进行风险分析，并拟定书面之系统复原办法。风险分析之要素，应包含：

5.5.1.了解资讯系统之弱点、威胁及其对企业营运活动之影响。

5.5.2.界定企业之重要资源、辨认各业务活动之重要性及等待复原最长可容忍时间。

5.5.3.选择符合成本效益的复原策略。

5.5.4.建立分散风险之措施。

5.6.书面资讯系统复原办法，至少包括：

5.6.1.灾变预防准备工作

针对现有资讯系统之安全性,对企业正常营运活动之影响性等进行评估并建立保护及因应措施，包括实体安全、备援协议(reciprocal agreement)、资料备份、分储等，必要时，亦应就重要资讯设备办理保险。

5.6.2.系统故障或异常之紧急应变措施

5.6.2.1.明订一般处理原则，含适当之紧急关机程序、修护申请、程序及替代之人工操作程序，确保将影响减至最低。

5.6.2.2.设定系统自动记载紧急修护代码，并定期之日志复核，确保系统有效、正确运作。

5.6.2.3.记录系统故障或异常之排除、处理之书面记录程序，据以分析、遏止重复发生，及加速应变之处理。

5.6.3.灾后复原工作

5.6.3.1.灾后情况之假设及其基本对策。

5.6.3.2.灾后复原阶段之划分、目标之设定与复原预计时间。

5.6.3.3.复原小组成员与职掌之划分，并适当授权复原小组负责人，足以因应紧急处理。

5.6.3.4.宣告灾变之程序及复原小组之动员方式。

5.6.3.5.明订各阶段复原工作之内容（包括资讯单位及各营业单位复原）及列示重要应用系统回复之优先级。

5.6.3.6.复原工作资源之准备与分配，如日常备份资料之取回、系统软件、应用系统（软件）文件、备援协议之厂商、备援之电脑设备与作业程序及复原地点之安排等，加速复原工作之实施。

5.6.4.系统复原计划之维护

5.6.4.1.配合实际资讯系统、软／硬件更新及人员变动，定期检讨，保持计划之可行性。

5.6.4.2.设立专案文件记录更新情形，并确保复原小组人员保有之系统复原办法。

5.6.4.3.定期演练假设之灾变状况。

5.6.4.4.相关资讯系统复原计划、书面办法应保持其安全性，并于公司外之第三地置放一份。

5.6.5.系统复原计划之测试

5.6.5.1.明订测试之时机，如一定之测试周期或特定事件发生时，并据以设定测试目标。

5.6.5.2.测试应按电脑设备及系统文件实施，使用单位并应参与测试。

5.6.5.3.测试结果应做成书面记录，遇有异常应即反应并修订。

6.相关程序

无。

7.相关办法

无。

8.使用表报

无。

Z-BRT-EP-10 资通安全检查之控制

1.目的

明确规范资讯单位对资讯通讯安全之检查及控制原则，预防资讯资料之泄漏或破坏。

2.范围

本作业程序适用于资讯通讯安全系统之建立、实施与控制等作业。

3.权责单位

3.1.资讯单位：负责安全之建立、实施、倡导与控制。

4.控制重点

4.1.资讯单位应经常性取得资通安全新知，实时建制新的控制。

4.2.资讯单位将资通安全风险倡导告知电脑使用单位。

4.3.各项电脑及外围设备、系统应经申请并授权后方得使用。

4.4.公司资讯如有须对外公告申报时，须经权责主管核准，并依母公司制度办理。

5.程序内容

5.1. 资通安全软硬件之建制

5.1.1.于 internet 及 intranet 之间，应建立防火墙、流量监控、行为监控等网络管理之软硬件。并应设置用户密码授权，防止设定遭到窜改。

5.1.2.电子邮件系统应建置垃圾邮件过滤机制，防止威胁透过电子邮件入侵。

5.1.3.电脑或服务器应设置防火墙、防毒软件，防止病毒入侵。

5.1.4.电脑或服务器使用之应用软件应先经过资讯单位评估，不使用来历不明之软件，防止病毒夹带其中。

5.1.5.电脑或服务器使用之应用软件或操作系统，应不定期更新，以防止黑客透过系统漏洞入侵。

5.2.资通安全之倡导

5.2.1.资讯单位应不定期对资通安全议题进行倡导、文章发布或培训。

5.2.2.资讯单位应透过管理手段对电脑用户进行适当之安全性评估，实时发现危险行为。

5.3.资通安全之控制

5.3.1.资讯单位应拟定适当之检查、规范或评估，以保证资通安全作业执行落实。

5.3.2.资讯单位应经常性关注新型态之资讯风险，实时布置新式安全机制及安全倡导，

保证资通安全不被新型态之威胁入侵。

5.3.3.资讯如有须对外公开时，须经权责主管核准。

6.相关程序

无

7.相关办法

无。

8.使用表报

无。

Z-BRT-EP-11 订定与修订

1.订定：2018 年 2 月 22 日

2.第一次修订：2022 年 8 月 3 日

3.第二次修订：2023 年 12 月 29 日