江门市红十字会
信息安全制度汇编

目录

江门市红十字会信息安全管理办法.....- 1 -
江门市红十字会信息安全等级保护工作指南.....- 9 -
江门市红十字会信息系统应急预案管理制度..... - 13 -
江门市红十字会信息安全事件通报流程.....- 29 -
江门市红十字会信息安全自查工作流程.....- 38 -
江门市红十字会信息安全组织及职责规定.....- 41 -
江门市红十字会信息技术外包管理制度.....- 48 -
江门市红十字会备份与恢复安全管理制度.....- 53 -
江门市红十字会信息系统补丁管理指南.....- 58 -
江门市红十字会信息系统恶意代码防范管理指南....- 62 -
江门市红十字会信息系统项目建设管理制度..... - 66 -
江门市红十字会信息系统网络配置安全指南..... - 76 -
江门市红十字会信息资产管理制度..... - 84 -
江门市红十字会机房安全管理制度..... - 91 -
江门市红十字会介质安全管理指南..... - 94 -
江门市红十字会网站管理指南.....- 97 -
江门市红十字会人员安全管理制度.....- 100 -
江门市红十字会软件安装管理流程.....- 103 -
江门市红十字会软件开发管理制度.....- 106 -
江门市红十字会审批管理制度..... - 111 -
江门市红十字会用户标识与口令管理指南..... - 115 -
江门市红十字会用户个人信息数据分级防护管理规定- 120 -
江门市红十字会用户信息收集及使用规定..... - 130 -

江门市红十字会信息安全管理办法

第一章 总则

第一条 为提高江门市红十字会网络与信息系统的安全防范能力，指导和规范单位网络与信息安全（以下简称信息安全）检查和信息通报工作，保障信息安全，根据国家的有关法律法规以及江门市红十字会的相关管理规定，参照国家信息安全管理与技术标准，结合江门市红十字会实际，特制定本办法。

第二条 本办法适用于江门市红十字会信息安全整体工作，包括信息安全规划、建设、运维和管理。

第三条 本办法所称信息安全是指网络和计算机系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统能够连续可靠正常地运行，保持信息服务不中断。信息安全的核心是确保网络和信息系统的保密性、完整性、可用性、可控性和可审查性。

第二章 引用文件与标准

第四条 主要依据的文件如下：

1、《中华人民共和国网络安全法》

2、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号）

3、《中华人民共和国计算机信息系统安全保护条 例》（国务院 147 号令）

4、《信息安全等级保护管理办法》(公通〔2007〕43 号）

第五条　主要参考的标准如下：

1、ISO/IEC 27000:2009 信息技术、安全技术、信息安全管理概述与术语

2、ISO/IEC 27001:2013 信息技术、安全技术、信息安全管理体系要求

3、GB/T 22080-2008 信息技术、安全技术、信息安全管理体系要求（对应 ISO/IEC 27001:2005 ）

4、ISO/IEC 27001:2013 信息技术、安全技术、信息安全管理规范

5、ISO/IEC 27002:2013 信息技术、安全技术、信息安全管理实用规则

6、ISO/IEC 27003:2017 信息技术、安全技术、信息安全管理实施指南

7、ISO/IEC 27005:2005 信息技术、安全技术、信息安全风险管理

8、GB/T 25058-2010 信息安全技术、信息系统安全等级保护实施指南

9、GB/T 22239-2008 信息安全技术、信息系统安全

等级保护基本要求

第三章 目标、方针和原则

第六条 单位网络与信息安全工作整体目标是：

1、确保信息和信息系统的完整性、保密性、可用性、时效性、可审查性和可控性，确保信息内容的合法性，切实保护股份单位合法权益。

2、保证网络与信息系统的物理环境、设备设施和运行环境的安全。

3、提高全体员工的信息安全意识、安全专业素质以及安全管理与服务水平。

4、提高单位信息系统的可用性和灾难恢复能力，为业务的可持续性运行提供保障。

第七条 信息安全是江门市红十字会安全生产的重要组成部分。江门市红十字会信息安全工作采取积极防御、综合防范的方针，坚持保障信息安全与促进信息化发展相协调、管理与技术统筹兼顾的原则，实行统一协调、分级管理、分工负责。

第八条 信息安全工作按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，单位各部门对本单位的信息安全负主体责任。各部门应按照“责任到位、措施到位”的信息安全工作总体要求，采取有效措施做好信息安全工作。

第四章 信息安全管理制度基本要求

第九条　应针对安全管理人员或操作人员执行的日常管理操作建立操作规程。

第十条　制订总体安全方针和安全策略、安全管理制度、人员操作规程，形成由安全政策、管理制度、操作规程等构成的全面的信息安全管理制度体系。

第十一条　办公室负责安全管理制度的制定。

第十二条　安全管理制度应具有统一的格式，并进行版本控制。

第十三条　单位信息安全领导小组应负责组织相关人员对制定的安全管理制度进行论证和审定。

第十四条　安全管理制度应通过OA系统的方式发布。

第十五条　办公室应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

第五章 信息安全管理内容

第十六条　单位应建立并落实信息安全经费保障制度，落实风险评估、等级保护测评等专项经费。按照统一规划、统一建设、安全运行的原则建立和完善安全保障措施。

第十七条　人员安全管理包括对内部雇员和外部人员访问管理两方面，确保其理解其在信息安全方面的职责。内部人员应当从任用之前、任用中、任用的终止或变化三

种阶段制定相应的控制措施。任用前应包括审查方面的要求，任用中应包括信息安全宣传教育、信息安全绩效考核和信息安全奖惩纪律等内容，任用终止或变化阶段应制定各种权限及时撤销、保密协议相关的要求。

第十八条　单位的信息资产要指定所有者与责任人，并对责任人赋予相应的职责，确保所有信息资产都可以核查。建立并落实信息技术产品安装、使用管理制度，确保对信息安全设备、网络设备、服务器、终端设备、软件等信息技术产品的安全可控。

第十九条　单位网络与信息系统的安全建设和服务，应按国家信息安全服务管理相关要求、技术规范和实施程序，由符合要求的信息安全服务机构承担。单位要与外包服务方签订服务合同及安全保密协议，明确安全责任，特别是远程在线服务带来的安全风险。

第二十条　信息安全和信息化建设工作应当遵循同步规划、同步建设、同步实施、同步发展的原则。

第二十一条　建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与补丁修复、口令更新、配置文件备份和外部连接的授权和批准等方面做出规定，以审视网络系统的安全性，降低网络系统存在的安全风险，确保网络系统安全可靠地运行。

第二十二条　单位生产信息系统应实行物理隔离。物

理隔离是指内部网不直接或间接地连接公共网。

第二十三条　单位应基于业务和安全需求，制定访问控制策略，并明确用户职责，加强用户访问控制管理。单位应加强对移动办公和远程办公的管理。加强对网络系统、操作系统、应用系统的访问控制，如在各单位网络边界设置合适的接口，采取有效的用户和设备验证机制，控制用户访问，隔离敏感信息。同时监控对系统的访问和使用，记录并审查事件日志。

第二十四条　应加强对信息系统的应用、服务、端口的安全管理，及时更新病毒库及系统补丁，实施漏洞扫描、病毒木马检测。

第二十五条　应加强对系统远程访问的控制和管理，需要远程技术支持和服务的，应与服务提供方签订信息安全保障协议。

第二十六条　单位应基于业务连续性的需求，制订安全运维制度，包括：漏洞管理、基线配置、网络安全等。

第二十七条　单位应按照等级保护二级的标准加强对网站的安全管理，采取安全措施防止网站被挂马、篡改，发生网页篡改事件时要及时处置。加强对网上信息发布的审查和内容安全的管理，监督网上信息并及时清理有害信息。

第二十八条　单位应加强对电子邮箱使用的安全管

理，不得使用非工作邮箱、即时通信等工具传递工作文件，不得在非涉密计算机、打印机、移动存储等设备上处理涉密文件或数据。

第二十九条　包含 U 盘、移动硬盘、数码相机、光盘、磁带、软盘、其他可存储信息数据的电子设备以及含有重要资讯的资料（卡片、稿纸等）等在内的介质，应做好领用登记。使用时应根据工作范围划分使用级别，严格控制使用权，严禁非法、越权使用。报废时应使用不可恢复的清除方式彻底删除存储介质内的软件、数据等信息，并做好废弃处置记录。

第三十条　应制定和完善网络与信息系统应急处置预案，每年至少开展一次应急演练，并对演练情况进行评估，针对演练中发现的问题，补充修订应急预案。

第三十一条　应建立重要信息系统灾难备份与恢复制度，建设灾备系统，保证关键业务的连续性。

第三十二条　重要信息系统按实际情况可选择实时备份和每周备份一次等。

第三十三条　为了确保所有人员意识到网络与信息安全的威胁和利害关系，并具有在日常工作过程中具备相关的能力，应对内部员工及外部人员进行安全程序和正确使用信息系统的培训，以尽量降低可能的安全风险。

第三十四条　办公室负责组织单位范围内的信息安

全检查工作，要制定信息安全检查的各项细则，定期开展信息安全检查工作。

第三十五条　单位信息安全实行等级保护制度，应按照《信息安全等级保护管理办法》和相关技术标准，建立等级保护细则。

第三十六条　新建、改建的信息系统应首先确定安全保护等级，同步建设符合该等级要求的信息安全防护设施。向公共网络提供服务的信息系统，应重点提出安全要求。

第三十七条　单位信息安全信息通报工作按照“谁主管谁负责，谁运营谁负责，谁使用谁负责"的原则进行通报，并加强各部门信息安全信息共享和协调管理。

第三十八条　各部门发生信息安全事件时，应及时进行处置，并按规定进行通报。

第三十九条　单位对各部门信息安全工作进行年度讲评和总结，对在信息安全保障工作中成绩显著和有突出贡献的单位、部门和个人给予表彰和奖励。对瞒报、缓报、谎报信息安全事件和推诿责任的行为，单位将根据有关规定进行处理。对发生信息安全事件并造成重大影响的单位、部门和个人进行通报批评。

江门市红十字会信息安全

等级保护工作指南

第一章 总则

第一条 目的：信息系统安全等级保护是国家信息安全保障工作的基本制度、基本策略、基本方法。开展信息系统安全等级保护工作不仅是加强国家信息安全保障工作的重要内容，也是一项事关国家安全、社会稳定的政治任务。为加强江门市红十字会(以下简称江门市红十字会) 的信息安全等级保护工作，特制定本工作指南。

第二条 使用范围：适用于江门市红十字会涉及的信息系统系统。

第三条 职责：由江门市红十字会办公室负责此规定的执行。

第二章 等级保护管理

第四条 江门市红十字会信息安全按照《信息安全等级保护管理办法》(公通字[2007]43 号)和相关技术标准，建立等级保护制度。

第五条 等级保护标准：按照《信息安全技术信息系统安全等级保护定级指南》(GB / T2240-2008)，组织开

展定级工作，《系统定级报告》报信息科技部备案。

第六条　信息系统安全保护等级分为五个等级，从第一级到第五级逐级增高。等级保护定级为三级（含）以上的信息系统属于关键信息基础设施。

1、第一级为自主保护级，适用于一般的信息系统，其受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益；

2、第二级为指导保护级，适用于一般的信息系统，其受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全；

3、第三级为监督保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；

4、第四级为强制保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害；

5、第五级为专控保护级，适用于涉及国家安全、社会秩序和公共利益的极端重要信息系统，其受到破坏后，会对国家安全造成特别严重损害。

第七条　等级保护定级为二级(含)以上的信息系统，由办公室向公安网监部门申请《系统等级保护备案证书》。

第八条　《系统定级报告》经公安网监部门审核批准后，由公安网监部门颁发《系统等级保护备案证书》。办公室妥善保管好该证书，以备公安机关查验。

第九条　信息安全保护等级确定后，信息系统管理部门应按相应等级要求开展安全建设或整改工作。新建、改建的信息系统应首先确定安全保护等级，同步建设符合该等级要求的信息安全防护设施。

第十条　新建、改建的等级保护定级为二级（含）以上的信息系统建设完成后，必须进行验收测评，测评合格后方可投入使用。《验收测评报告》报办公室备案。

第十一条　等级保护定级为二级的信息系统必须每年至少进行一次安全自查；等级保护定级为三级的信息系统必须每年至少进行一次安全自查和安全测评；等级保护定级为四级的信息系统必须每半年至少进行一次安全自查和安全测评；等级保护定级为五级的信息系统必须依据特殊安全要求进行安全自查和安全测评。

第十二条　经测评信息系统安全状况未达到安全保护等级要求的，信息系统管理部门必须进行整改，整改后再次进行安全测评，直至测评合格。

第十三条　必须按程序选择公安网监部门推荐的等

保测评机构进行安全测评。

第十四条　各信息系统的《自查评估报告》和《安全测评报告》报信息部备案。

江门市红十字会信息系统

应急预案管理制度

第一章 总则

第一条 为减少江门市红十字会信息安全事件对业务的影响，保证业务连续性，特制定本制度。

第二条 适用范围：适用于江门市红十字会。

第三条 职责：由江门市红十字会信息安全工作领导小组负责此规定的执行。

第二章 组织机构

第四条 由江门市红十字会信息安全工作领导小组统一指挥信息安全应急预案的制定、审核、检查落实工作，由信息安全工作领导小组办公室负责具体实施。

第五条 信息安全领导小组办公室应急响应主要职责：

1、拟订或者组织拟订单位应对信息安全突发事件的工作规划和应急预案并组织实施。

2、督促检查各处室应急预案的执行情况，并给予指导。

3、督促办公室信息安全突发事件监测、预警工作情

况，并给予指导。

4、汇总有关信息安全突发事件的各种重要信息，进行综合分析，并提出建议。

5、监督检查、协调指导办公室及各部门信息安全突发事件预防、应急准备、应急处置和事后恢复与重建工作。

6、组织制订信息安全常识、应急知识的宣传培训计划和应急救援队伍的业务培训、演练计划，并督促落实。

第三章 应急预案要求

第六条 各项应急处理工作要求：

1、各部门按要求成立应急小组，制定应急预案。

2、业务部门应急工作要求：

1）应急小组由业务部门负责人和业务骨干组成，其中业务部门负责人任组长，制定本部门在信息系统故障，全部或部份不能运行的情况下的应急预案，准备手工业务处理方案。

2）预案要求做到在无信息系统支持下的独立完成相关业务工作。

3）应急预案启动时，相关人员必需按预案要求到达现场。

3、办公室门应急工作要求：

1）应急小组由办公室负责人和技术骨干组成，制定和实施信息系统技术应急预案。

2） 监控计算机网络系统运行状态，向信息化应急领导小组办公室及时报告异常情况；

3）分析确定异常状况的性质、影响范围和延续时间，提出进入紧急状态请求；

4）在应急状态下，具体实施技术应急方案，排除技术故障，恢复系统正常运行；

5）在业务人员协助下完成系统复原后的数据恢复工作；

6）总结、分析事故原因，向信息安全工作领导小组办公室提出事故总结、分析及处理报告。

第七条　信息安全事件分级及通报

各应急小组按照单位信息安全事件通报流程的规定，判断事件级别，并按要求通报。

1、一级/特别重大

信息安全事件造成信息安全数据泄露，主要系统中断一天以上；

2、二级/重大：

信息安全事件造成重点系统业务中断 120 分钟以上；

3、三级/较大：

信息安全事件造成系统业务中断 60 分钟以上，并且未造成业务系统数据损坏、丢失；或者产生较大的社会影响；

4、四级/一般：一般告警级别以上信息安全事件，信息安全事件造成系统业务中断少于 60 分钟，并且未造成业务系统数据损坏、丢失；或者产生一般的社会影响。

第四章 应急预案启动流程

第八条 启动应急预案的条件

当发生信息安全事件，影响业务系统正常运行，经信息安全工作领导小组批准，启动信息安全应急预案。

第九条 资源保障

1、应急队伍

应急队伍由单位各相关部门应急小组、外包维护单位人员组成。

2、硬件配备

加强硬件设备的运行维护，配备了适当比例的备份设备，应用服务器、数据库服务器、核心交换机、核心防火墙均有备份设备。机房采用备用 UPS 供电系统，在市电停电的情况下，可保证机房设备供电 4 个小时。

3、软件与资料配备

1）做好系统软件定期维护工作。

2）做好备份的管理和检查工作，确保备份完整、能用。

3）建立了适应安全需要的、版本齐全的操作系统、数据库软件、应用系统程序。保持与运行系统一致的升级

计划。

4）备有各种技术应急预案、异常情况处理流程、应急物资清单和相关单位、部门及主管领导联系方式。

第十条　做好技术储备与保障，办公室应急小组在平时应加强技术储备与保障管理工作，建立信息系统保障应急管理机构与专家的日常联系和信息沟通机制，认真听取专家意见和建议。适时组织相关专家和机构分析当前通信网络安全形势，开展信息系统保障的现场研究，加强技术储备。

第十一条　应急处理流程

信息安全事件的应急处理应遵循严格的审批制度，并按一定的操作流程执行，具体流程如下：

1、故障上报。办公室初步对故障情况诊断，确定故障类型及可能的处理时间，当判断为重大信息安全事件和较大信息安全事件发生时，办公室负责人应立即报告信息安全工作领导小组。

2、在接到应急响应请求后，信息安全工作领导小组全体成员应在 30 分钟内全部到达事件现场；研究决定并宣布进入应急状态，启动应急预案。并通知相关外包维护单位。

3、信息安全工作领导小组现场研究指定一名现场指挥；一旦指定，全体运行值班人员和现场技术人员都要服

从现场指挥的领导。

4、技术应急小组制定并实施完成现场处置技术方案。按照预案优先的原则，优先执行技术应急处理预案，在无预案的情况下，技术方案由现场指挥集思广益，予以确定。在实施技术应急预案时，记录方案实施的过程。

5、信息安全工作领导办公室做好信息安全事件的宣传舆论疏导工作，按规定通报上级有关部门，请求给予必要的帮助，正确引导舆论，减少负面影响，维护江门市红十字会的形象。

6、当信息安全工作领导小组确定启动业务应急处理方案时，业务应急小组负责具体实施业务应急处理方案，行使各自职权，协助组织实施业务应急方案。

第十二条　系统恢复流程

1、当信息系统恢复正常后，信息安全工作领导小组办公室进行检查评估。

2、评估情况报信息安全领导小组，由信息安全工作领导小组根据评估情况，决定是否恢复系统操作，发出解除应急状态通知。

3、办公室门启动各业务系统。

4、业务部门接到通知后正常办理业务。

5、由现场指挥组织，针对在应急处理工作中故障发生情况、处理过程、处理结果以及遇到的问题在 24 小时

内汇总，形成信息安全事件处理结果报告，提交信息安全工作领导小组，并归档保存。

第十三条　后期处置

1、情况汇报和经验总结

应急任务结束后，信息安全工作领导小组应做好安全事件中各种设施损失情况的统计、汇总，及任务完成情况的总结与汇报，不断改进应急工作。

2、奖惩评定及表彰

为提高应急工作的效率和积极性，按照有关规定，对应急过程中表现突出的单位和个人给予表彰，对保障不力，造成损失的单位和个人进行惩处。

第五章 应急预案管理

第十四条　应加强对网络系统网络安全和信息系统保障应急的宣传教育工作，应对系统相关的人员进行应急预案培训。

1、应急预案的培训应至少每年举办一次；

2、应每年一次对应急预案进行演练，由信息安全工作领导小组决定演练时机；

3、在计算机系统发生重大变动及新的应用系统投产时，对应急预案进行培训和演练；

4、应组织当系统完全不可用时的手工操作演练。

第十五条　应急演练按如下步骤进行：

1、确定应急响应演练的目标；

2、确定应急响应演练的范围；

3、制定应急响应演练的方案；

4、调配应急响应演练所需的各项资源；

5、协调应急响应演练过程中涉及的部门和单位；

6、组织进行应急响应演练；

7、评估并通报应急响应演练结果；

8、总结经验并提出对应急预案的更新建议及其它整改措施；

9、更新应急预案，实施整改工作。

第十六条　应急工作监督检查制度

信息安全工作领导小组办公室应每年一次对信息系统应预案的实施、培训和演练情况进行监督和检查。

第十七条　更新

1、本预案由信息安全工作领导小组负责更新；,

2、预案坚持周期性的评审原则，每年一次，根据需要及时进行修改；。

3、在每次应急响应过程结束之后，应针对应急响应工作过程中遇到的问题，分析应急响应预案的科学性和合理性，针对预案中的问题进行修改；

4、修改后的预案经评审通过后发布生效。

第六章 附件

附件：预案库：

1、病毒安全紧急处置措施

1.1 当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。

1.2 对该设备的硬盘进行数据备份。

1.3 启用反病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。

1.4 如发现反病毒软件无法清除该病毒，应立即向办公室负责人报告。

1.5 设备技术负责人在接到通报后，召集技术应急小成员，研究解决方案。

1.6 经技术人员确认确实无法查杀该病毒后，应作好相关记录，并联系有关厂商咨询解决方案。

1.7 需立即使用该计算机设备的，可采用系统恢复等方式重装操作系统，重装完毕后需对计算机进行全面检查后方可连入网络。

2 信息系统遭受破坏性攻击的紧急处置措施

2.1 重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将它们保存于安全处。

2.2 一旦软件遭到破坏性攻击，应立即向办公室负责人报告，并立即断开受攻击的服务器，系统停止运行。通知各业务部门准备应急预案。

2.3 办公室负责人接到报告后，应召集技术应急小组成员 30 分钟内赶到机房，了解攻击情况，并通知相关外包维护单位联络人。

2.4 属于严重或较大信息安全事件时，设备技术负责人应立即向信息安全工作领导小组办公室汇报攻击情况。

2.5 信息安全工作领导小组办公室根据接到的报告，按信息安全事件报告流程要求通报。

2.6 信息安全工作领导小组根据实际情况启动相应的应急预案。

2.7 技术应急小组成员应保护现场，了解攻击范围和损坏情况，检查日志等资料，确认攻击来源。必要时联系外包维护单位、其他技术支持单位，要求提供技术支持。

2.8 对攻击情况等做好记录。

2.9 在分析完成后，进行信息系统恢复和数据恢复。组织业务部门应急小组进行系统测试。

2.10 将信息系统恢复情况报告信息安全工作领导小组，按指示恢复信息系统运行。

3 数据库安全紧急处置措施

3.1 各数据库系统要至少准备两个以上数据库备份。

3.2 一旦数据库出现故障，影响信息系统运行，重启服务、服务器无法排除故障，应判断为数据库严重故障，值班人员立即向办公室负责人报告，同时暂停信息系统运

行，通知各业务部门准备应急预案。

3.3 办公室负责人接到报告后，应召集技术应急小组成员 30 分钟内赶到机房，并通知相关外包维护单位联络人，检查数据库系统，判断损毁情况及修复时间，如需较长时间（2 小时以上）修复或遇到无法解决的问题，立即向软硬件提供商请求支援。

3.4 属于严重或较大信息安全事件时，设备技术负责人应立即向信息安全工作领导小组办公室汇报攻击情况。

3.5 信息安全工作领导小组办公室根据接到的报告，按信息安全事件报告流程要求通报。

3.6 信息安全工作领导小组根据实际情况启动相应的应急预案。

3.7 系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

3.8 如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。

3.9 如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

3.10 数据恢复完成。组织业务部门应急小组进行系统测试。确认数据完整性。

3.11 将数据恢复情况报告信息安全工作领导小组，按指示恢复信息系统运行。

4 广域网外部线路中断紧急处置措施

4.1 广域网主、备用线路中断一条 后，有关人员应立即启动备用线路接续工作，同时向办公室负责人报告。

4.2 办公室负责人接到报告后，应召集技术应急小组成员 30 分钟内赶到机房，了解中断情况，并通知相关外包维护单位联络人。

4.3 技术应急小组到达现场后，应迅速判断故障节点，查明故障原因。

4.4 如属我方管辖范围，由网络管理员立即予以恢复。如设备损坏并无替代备品或遇无法恢复情况，立即向有关厂商请求支援。

4.5 如属运营商管辖范围，立即与运营商维护部门联系，请求修复。

4.6 如果主、备用线路同时中断，值班人员应立即向办公室负责人报告，并通知相关业务部门准备应急预案。

4.7 办公室负责人接到报告后，召集技术应急小组成员在 30 分钟内赶到机房，了解判断情况。

4.8 网络安全员应立即判断故障节点,查明故障原因，如主、副线路在短时间内无法恢复，办公室负责人应立即向信息安全领导小组办公室报告情况。

4.9 信息安全工作领导小组办公室根据接到的报告，

按信息安全事件报告流程要求通报。

4.10 信息安全工作领导小组根据实际情况启动相应的应急预案。

4.11 技术应急小组应尽快与外包维护单位、运营商维护部门联系，研究恢复措施，向信息安全领导小组上报恢复方案。

4.12 恢复方案批准后尽快完成网络恢复。

4.13 网络恢复后组织测试，恢复系统运行。

5 局域网中断紧急处置措施

5.1 局域网中断后，网络管理员应立即判断故障节点，查明故障原因，并向办公室负责人报告。向业务部门通报受影响的区域，准备应急预案。

5.2 办公室负责人接到报告后，应召集技术，准备应急小组成员 30 分钟内赶到现场，了解中断情况，应迅速判断故障节点，查明故障原因。

5.3 如属路由器、交换机等网络设备故障，应更换备件，如无备件，立即与设备提供商联系取得支持。

5.4 如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调试畅通。如遇无法解决的技术问题，立即向有关厂商请求支援。

5.5 如属线路故障，通报综合办公室检查相关线路，要求提供解决方案。

5.6 如无法在短时间（1 小时）内解决，应先研究替代措施，并向信息安全领导小组办公室报告。

5.7 信息安全工作领导小组办公室根据接到的报告，按信息安全事件报告流程要求通报。

5.8 信息安全工作领导小组根据实际情况启动相应的应急预案。

5.9 网络恢复后测试稳定性，并报告信息安全领导小组办公室，通知业务部门网络恢复正常。

6 设备安全紧急处置措施

6.1 小型机、服务器等关键设备损坏后，有关人员应立即向应立即向办公室负责人报告，通知各业务部门准备应急预案。

6.2 办公室负责人接到报告后，应召集技术应急小组成员 30 分钟内赶到机房，了解受损情况，并通知相关外包维护单位联络人。

6.3 属于软件系统损坏，启用备用系统，保证业务正常开展，同时安排研究原系统损坏原因，排除人为破坏、病毒攻击等因素后，安排恢复系统。

6.3 属于硬件损坏时，启动备用系统，保证业务正常开展。联系硬件厂商、维修供应商提供服务。

6.4 无法提供备用系统时应立即向信息安全工作领导小组办公室汇报有关情况。

6.5 信息安全工作领导小组办公室根据接到的报告，按信息安全事件报告流程要求通报。

6.6 信息安全工作领导小组根据实际情况启动相应的应急预案。

6.7 服务器维修完成后，由技术应急小组安排测试，正常运行后替代备用系统或通知业务部门重新使用系统。

7 外电中断后的设备紧急处置措施

7.1 外电中断后，值班人员应立即切换到备用电源。

7.2 值班人员应立即查明原因，并向办公室负责人汇报。

7.3 如因单位内部线路故障，联系办公室等相关部门迅速恢复。

7.4 如果是供电局的原因，应立即与办公室或相关供电部门联系，了解停电原因及时间。

7.5 如果供电局告知需长时间停电，应做如下安排：

1）预计停电 1 小时以内，由 UPS 供电。

2）预计停电 1 小时以上，关掉非关键设备，确保各主机、路由器、交换机供电。

3）预计停电 2 小时以上：

（1）办公室负责人应立即向信息安全领导小组办公室报告情况。

（2)信息安全工作领导小组办公室根据接到的报告，

按信息安全事件报告流程要求通报。

（3）信息安全工作领导小组根据实际情况启动相应的应急预案。

7.6 恢复供电后，按顺序恢复机房供电。

江门市红十字会信息安全事件通报流程

第一章 总则

第一条 为规范江门市红十字会安全事件的报告与处理程序，减少信息安全事件所造成的损失，并采取有效的纠正与预防措施，特制定本流程。

第二条 适用范围：适用于江门市红十字会的信息安全事件管理工作。

第二章 职责

第三条 办公室负责江门市红十字会信息安全事件通报工作的组织、指导、协调和日常管理工作。信息安全通报工作按照“谁主管谁负责，谁运营谁负责，谁使用谁负责"的原则进行通报。各部门负责本部门内制度的落实。

第四条 办公室负责确定信息通报渠道、联系方式和通报内容。对各单位部门报送的信息安全信息进行整理。同时，向各部门通报信息安全工作情况以及安全预警和病毒攻击等信息。

第五条 各部门应建立信息安全信息通报制度，落实通报责任，向办公室报备本部门信息安全事件通报工作的分管领导、和联络员及联络方式（如人员及联系方式发生变化，应在 1 个月内报备）。

第三章 安全事件定义、分类

第六条　信息安全事件定义

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件。

第七条　信息安全事件分类

将信息安全事件分为 7 类：有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件。

1、有害程序事件：指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序事件包括计算机病毒事件、蠕虫事件、木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 7 个子类。

2、网络攻击事件：指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等 7 个子类。

3、信息破坏事件：指通过网络或其他技术手段，造

成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等 6 个子类。

4、信息内容安全事件：指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件。信息内容安全事件包括以下 4 个子类，违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件等 4 个子类。

5、设备设施故障：指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事件和其它设备设施故障等 4 个子类。

6、灾害性事件：指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

7、其他信息安全事件：指不能归为以上 6 个基本分类的信息安全事件。

第八条　信息安全事件分级

根据信息安全事件所影响业务的重要性，业务损失程度与处理信息安全事件所需的资源，以及造成的社会影响综合评定，信息安全事件分为一级（特别重大）、二级（重大）、三级（较大）、四级（一般）四个级别。

1、一级/特别重大

信息安全事件造成信息安全数据泄露，主要系统中断一天以上，导致造成重大信息安全事件的情况有：

1）自然灾害导致中心机房主要设施遭受毁灭性破坏，形成灾难性故障，持续一天以上不能修复；

2）关键设备的重大故障引起的业务中断，如业务系统主机、存储设备、网络核心设备（交换机、路由器）两套热备的设备同时故障，持续一天以上无法修复；

3）市电供电系统停止 8 小时以上；

4）遭受恶意攻击形成灾难性故障，业务数据被破坏；造成重要系统业务中断 4 小时以上，或者影响的范围涉及三个以上系统；

5）因严重的存储设备故障或数据库崩溃等原因，造成业务数据丢失；损坏、丢失，并且无法恢复；

6）业务系统或网络被破坏或损坏，并且预计在 4 小时内无法恢复；

7）重要数据泄露，产生特别重大的社会影响。

2、二级/重大：

信息安全事件造成重点系统业务中断 120 分钟以上，导致重大信息安全事件的情况有：

1）主机系统两套设备同时发生故障，无法在 120 分钟内修复；

2）出现网络系统故障，无法在 120 分钟内恢复；

3）遭受恶意攻击形成系统故障，关键业务中断、系统瘫痪、关键数据丢失或核心信息被窃密等，从而在社会稳定或公众利益等方面造成重大不良影响以及造成一定程度经济损失；

4）业务系统数据部分损坏、丢失，可以通过备份进行恢复。

5）软件系统故障，如核心业务的数据库系统出现无法使用的故障、操作系统软件故障，系统无法运行；

6)机房附属设备故障：如 UPS 同时故障、空调故障，引起机房、主机温度、湿度异常，超过临界值；防系统出现故障,持续 24 小时不能修复等。

7）市电供电系统出现异常故障超过两小时；

3、三级/较大：

信息安全事件造成系统业务中断 60 分钟以上，并且未造成业务系统数据损坏、丢失；或者产生较大的社会影响。导致较大信息安全事件的情况主要有：

1）因设备故障，业务系统切换到备用系统运行；

2）数据备份过程中发现设备故障，不能正常完成数据备份；

3）网络系统故障：骨干网络设备、安全设备（路由器、交换机、防火墙等）故障，需启用备用设备；

4）磁盘阵列出现可修复性磁盘损坏（少数磁盘坏）；

5）UPS 故障；

4、四级/一般：一般告警级别以上信息安全事件，信息安全事件造成系统业务中断少于 60 分钟，并且未造成业务系统数据损坏、丢失；或者产生一般的社会影响。导致一般信息安全事件的主要原因有：

1）单条 线路故障；

2）百骨干网络设备故障；

3）单台服务器软件系统故障，可一小时内排除故障；

第九条　在接收到信息安全事件处理任务时，维护单位应对信息安全事件优先级进行预判，对于一、二级信息安全事件，应立即按规定通报信息安全领导小组，并由信息安全领导小组办公室按规定向上级有关部门汇报。对于三、四级信息安全事件，应立即向单位分管信息安全领导汇报。

第十条　系统中断信息安全事件处理流程

发现和报告：

1、各个信息管理系统使用者，在使用过程中如果发现系统中断安全事件，任何情况下用户均不应尝试验证弱点，应向信息管理系统维护者报告；

2、各个信息管理系统维护者，在维护过程中接到或发现系统中断安全事件，应立即进行可用性检查。

3、如事件会影响或已经影响业务系统的使用，按规定向信息系统管理人员报告并通知相关业务人员留意系统故障或暂停使用。尽量将对业务系统的影响降至最低。

4、发现人尽量不要改变现状，应保护好事件的现场。

分析：

1、信息系统管理人员接到报告以后，相关管理人员须第一时间赶赴现场并通知技术支持人员。

2、经技术支持人员、管理员分析后判断事件级别，并按规定向单位信息安全领导小组报告。

响应：

相关管理人员组织确定事件解决方案，对安全事件进行迅速、有效的处理。包括采取以下适当措施：

1、采取措施防止事态的进一步扩大；

2、对于事件的响应和处理应遵循以下次序：保护人员的生命与安全、保护敏感的设备和资料、保护重要的数据资源、防止系统被损坏、将遭受的损失降至最小；

3、组织商讨事件解决方案，准备事件处理工作，排

除故障，恢复系统或服务，必要时启动应急预案。

4、填写《信息安全事件记录》，记录处理过程。

评价：

对于信息安全事件，在故障排除或采取必要措施后，由办公室组织对实施情况进行跟踪验证，验证结果记入《信息安全事件记录》。

备案：

办公室将《信息安全事件记录》及其他相关文件存档备案。

第十一条　后期工作

1、对于发生一、二级信息安全事件时，在应急处置工作结束后，信息安全领导小组应立即组织有关人员和专家在有关部门和单位的配合下，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失情况，总结经验教训，并制定防止再次发生的补救措施，写出调查评估报告；

2、对于发生一、二级信息安全事件，信息安全领导小组根据有关规定，对有关责任人员做出处理。

3、对于安全事件及时报告和响应的人员，给予相应奖励。

4、对于三、四级安全事件责任人进行批评教育，给予相应惩罚。

第十二条　各部门要按照保密工作的有关规定，做好信息安全信息通报的保密工作。涉密信息必须通过机要渠道，严禁使用明电、明文方式通报。

江门市红十字会信息安全自查工作流程

第一章 总则

第一条 为保证江门市红十字会现有信息安全管理制度和各项安全措施能被严格、有效地执行，安全管理员能及时掌握信息安全管理制度的执行情况并有计划、有针对性地开展安全审核和检查活动，特制定本流程。

第二条 本流程适用于各项针对江门市红十字会各项信息安全管理制度和安全措施的制定、维护、执行情况的安全审核和检查活动。

第三条 由办公室负责本制度的制定、执行。

第二章 信息安全审核和检查管理制度

第四条 信息安全管理员组织全面安全审核和检查（每年一次）；

第五条 信息安全检查内容：

1、安全技术措施检查

1）现有安全技术措施的有效性，包括物理、主机、网络、应用和数据安全策略的有效性；

2）安全配置与安全策略的一致性：抽查防火墙、入侵检测系统的配置等是否与安全策略设置的一致；

2、安全管理制度

1）现有安全管理制度的有效性，检查安全管理制度是否符合单位管理要求；

2）各项安全管理制度的执行情况：按各项安全制度逐条 进行检查。

3） 对重要业务应用系统的日常运行情况和维护工作的记录进行检查，并记录检查结果；

4）对系统软件，包括操作系统、数据库、中间件、网管软件等软件的日常维护进行检查，并记录检查结果；

5）对主机、存储、网络等重要设备的日常运维记录进行系统检查，并记录检查结果；

6）对备份系统，对照相关备份制度检查备份记录；

7）对安全系统，如 IDS、IPS、审计系统等进行日常记录的检查；

8）对所有日常维护记录进行全面检查，检查是否漏填或填写不符合要求的情况。

9）采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

第三章 安全检查流程

第六条 安全管理员负责协调、安排进行安全检查的时间，制定安全检查计划，确定参与安全检查的人员和检查的内容，填写《安全检查计划表》；

第七条　相关人员根据《安全检查计划表》，分别对安全技术措施和安全管理制度进行检查，填写《安全检查表》；

第八条　组织召开安全审核会议，汇总安全检查数据；组织召开评审会议，邀请相关责任人及各级主管领导，必要时邀请相关专家，对安全检查、管理制度的有效性等进行评审，形成《安全检查报告》和《整改通知单》；

第九条　对安全检查结果进行通报，根据安全检查发现的问题督促相关责任人进行安全整改；

第十条　对整改结果进行复查，并填写相应的《不符合项记录表》。

第十一条　检查人员的要求：检查人员应秉公办事，认真履行职责，坚持执行检查、记录、报告制度。如因玩忽职守，造成严重后果者，追究相关人员责任。

江门市红十字会信息安全组织及职责规定

第一章 总则

第一条 为提高江门市红十字会网络与信息系统的安全防范能力，指导和规范单位网络与信息安全（以下简称信息安全）检查和信息通报工作，保障信息安全，建立自上而下的信息安全工作管理体系，建立健全相应的组织管理体系，以推动信息安全工作的开展。根据国家和有关法律法规的相关管理规定，参照国家和行业信息安全管理与技术标准，结合江门市红十字会实际情况，特制定本规定。

第二条 本规定适用于江门市红十字会的信息安全组织机构和重要岗位的管理。

第二章 规范性引用文件

第三条 下列文件中的条 款通过本标准的引用而成为本标准的条 款。 凡注明日期的应用文件， 其随后的所有的修改单或修订版均不适用于本标准（不包括勘误、通知单） ，然而，鼓励根据本标准达成协议的各方研究可以使用这些文件的最新版本。凡未注日期的引用文件，其最新版本适用于本标准：

1、《信息安全技术 信息系统安全保障评估框架》

（GB/T 20274.1-2006 ）

2、《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）

3、《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）

第三章 组织机构及职责

第四条 单位成立网络安全与信息化领导小组，是信息安全的最高决策机构，下设办公室，负责网络安全与信息化领导小组的日常事务，其最高领导由单位主管领导担任。

第五条 网络安全与信息化领导小组负责研究重大事件，落实方针政策和制定总体策略等。职责主要包括：

1、根据国家和行业有关信息安全的策略、法律和法规，批准单位信息安全总体策略规划、管理规范和技术标准；

2、确定单位信息安全各有关部门工作职责，指导、监督信息安全工作。

3、统一指挥信息安全应急响应工作。

第六条 网络安全与信息化小组下设办公室：负责信息安全、应急处理工作。办公室主任由单位办公室负责人担任。

第七条 网络安全与信息化领导小组办公室的主要

职责包括：

1、 贯彻执行单位网络安全与信息化领导小组的决议，协调和规范单位信息安全工作； 根据网络安全与信息化领导小组的工作部署，对网络安全与信息化工作进行具体安排、落实；

2、 组织对重大的网络安全与信息化工作制度和技术操作策略进行审查， 拟定网络安全与信息化总体策略规划，并监督执行；

3、 负责协调、督促各职能部门的网络安全与信息化工作， 参与信息系统工程建设中的安全规划，监督安全措施的执行；

4、 组织信息安全工作检查，分析信息安全总体状况，提出分析报告和安全风险的防范对策；

5、 负责接收各部门的紧急网络安全与信息化事件报告，组织进行事件调查，分析原因、涉及范围，并评估安全事件的严重程度，提出信息安全时间防范措施；及时向网络安全与信息化工作领导小组和上级有关部门、单位报告信息安全事件。

6、 跟踪先进的信息安全技术，组织信息安全知识的培训和宣传工作。

7、 审定单位网络与信息系统的安全应急策略及应急预案；

8、 决定相应应急预案的启动，负责现场指挥，并组织相关人员排除故障，恢复系统；

9、 每年组织对信息安全应急策略和应急预案进行测试和演练。

第八条　关键岗位：设置信息系统的关键岗位并加强管理，配备安全主管、安全管理员、机房管理员、数据库管理员、系统管理员、网络管理员、应用开发管理员、安全审计员、安全保密管理员要求各自独立。安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。要害岗位人员必须严格遵守保密法规和有关信息安全的管理规定。

第九条　安全主管主要职责有：

1.负责本单位整体信息安全管理工作，根据单位的战略，对本单位的信息安全体系进行整体规划；

2.梳理、评估单位信息安全管理水平，推进信息安全管理体系建设，从物理安全、网络安全、应用安全、信息安全、运营安全、业务连续性及容灾等多个角度设计本单位安全架构；

3.监督并控制本单位信息安全风险，预防并处理信息安全事件，杜绝重大信息安全事故的发生；

4.负责协调本部门和其他部门的信息安全工作，督促各项信息安全工作的开展和落实。

第十条　安全管理员主要职责有：

1.负责在本职能范围内宣传发布信息安全相关制度；

2.负责报告信息安全管理现状；

3.负责协调日常的信息安全监督检查活动；

4.负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

5.负责一般安全事件与紧急事件的汇报；

6.参与信息安全相关制度的制订；

7.协助组织、计划对本单位、部门工作人员的安全技能培训和信息安全教育培训。

第十一条　机房管理员主要职责有：

1.负责计算机机房防火、防水、防静电、防雷击和防辐射等安全设施的管理；

2.负责计算机机房的内部装修，落实电磁波防护等技术规范与技术要求；

3.负责计算机机房配电系统、空调系统的维护与管理；

4.负责计算机机房的进出口的控制及监控系统和门禁系统的维护与管理；

5.负责对计算机机房安全性的检查，发现问题或隐患及时整改意见和书面报告。

第十二条　数据库管理员主要职责有：

1.负责数据库系统的管理和维护工作，进行数据备份

和恢复测试，保证其安全、可靠、正常运行；

2.负责本单位的数据库服务器的管理工作，做好数据库的运行记录，当数据库出现故障时，迅速协同相关人员一同解决；

3.负责数据库系统的建设，做好服务器的维护、数据库软件的安装、数据库的建立工作，定期对数据进行备份；

4.负责对备份的存放介质进行管理；

5.负责数据库服务器的安全防范管理工作。

第十三条　系统管理员主要职责有：

1、 负责系统的运行管理，实施系统安全运行细则；

2、 严格用户权限管理，维护系统安全正常运行；

3、 认真记录系统安全事项，及时向信息安全人员报告安全事件；

4、 对进行系统操作的其他人员予以安全监督。

第十四条　网络管理员的主要职责有：

1、 负责网络的运行管理，实施网络安全策略和安全云心细则；

2、 安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行；

3、 监控网络关键设备、网络端口、网络物理线路，防范黑客入侵，及时向信息安全人员报告安全事件；

4、 对操作网络管理功能的其他人员进行安全监督。

第十五条　应用开发管理员主要职责有：

1、负责在系统开发建设中,严格执行系统安全策略，保证系统安全功能的准确实现；

2、 系统投产运行前，完整移交系统相关的安全策略等资料；

3、 不得对系统设置“后门”；

4、 对系统核心技术保密等。

第十六条　安全审计员负责对设计系统安全的事件和各类操作人员的行为进行审计和监督，主要职能包括：

1、 按操作员证书号进行审计；

2、 按操作时间审计；

3、 按操作类型审计；

4、 事件类型进行审计；

5、 日志管理审计等。

第十七条　安全保密管理员负责日常安全保密管理活动，主要职责有：

1、 监视全网运行和安全告警信息

2、 网络审计信息的常规分析

3、 安全设备的常规设置和维护

4、 执行应急中心指定的具体安全策略

5、 向应急管理机构和领导机构报告重大的网络安全时间等。

江门市红十字会信息技术外包管理制度

第一章 总则

第一条 为了规范信息技术外包服务，有效利用外部优秀专业资源，达到降低成本、提高效率、发挥核心竞争力和增强单位应变能力，特制定本制度。

第二条 、本制度适用于单位将部分信息技术工作委托给专业服务单位、由其按照服务水平协定的要求进行管理、运营、维护的外包服务，包括应用系统的开发、测试与维护，网络通讯管理及维护，机房管理及监控，设备维修及维护，及其它与信息技术相关的咨询服务等。

第二章 外包管理组织

第三条 信息技术外包管理小组由单位办公室相关实施、协调人员组成。

第四条 外包管理小组主要职责：

1、负责外包前对行业实施情况、自身信息化需求进行调查研究，识别信息技术的核心竞争能力，在收益、成本和风险之间进行平衡并进行信息系统外包决策。

2、制定信息系统外包的建设技术标准，设计外包方案，避免重复投资与信息孤岛。

3、评价外包服务商的技术等级、发展能力，选择合

适的外包服务商。

4、签署外包服务合同，对外包服务过程进行全面监督、协调和控制。

5、处理与现有外包服务商的外包关系，监督并审议通过外包服务商的技术决策。

6、积累外包经验并帮助制定未来的外包决策，谈判并推行未来的外包合同，使 IT 整体战略与单位业务整体战略保持一致。

第三章 外包范围的确定

第五条 信息技术外包范围由外包管理小组根据信息系统规划需要，通过对实现目标、实施策略、资源及人力资源状况和安全要求等综合分析后确定。

第六条 确定外包项目时，应充分考虑单位业务特点以及对实时性和安全性的要求。

第七条 外包项目确定后，应根据外包成本的影响因素选择合适的外包方式，以保证较低的外包成本获得较高的外包收益。

第四章 外包服务商的选择

第八条 外包服务商由信息技术外包管理小组根据其技术实力、经营状况、社会信誉等因素进行综合评定后确定。

第九条 评定外包服务商的技术实力时应确定外包

服务商是否具有信息技术方面的资格认证，提供的信息技术产品是否拥有较高的市场占有率，是否能够提供足够的安全防范措施，具有对偶发事件的应对能力。所选择的外包服务商，应该具有较强的咨询能力和较高的服务水准。

第十条　评定外包服务商的经营状况时要分析外包服务商提供的已审计的财务报告等财务指标，考察外包服务商从事外包业务的时间、市场份额以及波动因素，评估外包服务商的技术费用支出等成本控制能力。

第十一条　评定外包服务商的社会信誉时应了解其信誉和服务水平等信息，包括是否具有良好的业界口碑，是否通过相关国际质量体系认证，是否有 IT 外包服务经验及成功案例，是否具备规模化的服务体系和专业团队等。

第五章 外包服务合同的管理

第十二条　外包服务合同由外包管理小组统一负责制定、审核、签署、保管和监督实施。

第十三条　应高度重视外包服务合同的制定工作。

1、外包服务合同内容要尽量详实、明确，必须清晰地指出外包服务的范围与职责，明确规定服务水平协议、服务流程，强调外包服务商对外包资源的安全性、保密性以及对数据备份和交易记录保护的责任。

2、外包服务合同应具有充分的弹性，具备应对技术、业务和策略目标方面可能出现变化的灵活性。

3、外包服务合同应当详细描述服务内容、费用及其计算办法，并对任何与合同规定条 件不符的费用变化进行具体的限制，给出外包服务的价格标准和服务质量标准，详细规定违约责任等。

第十四条　加强对外包服务合同实施过程的管理。

1、要保持对外包项目进度、成本和质量的监督，定期对外包服务商的工作进行评估，保证外包服务质量符合外包服务合同的相关条 款。

2、在整个外包实施阶段，应根据外包工作内容、工作量以及业务需求的变化，及时对外包服务合同进行补充，保证合同顺利实施。

第十五条　应及时对外包服务合同进行归档，在外包服务合同履行完毕后，应对合同执行情况进行全面评估，总结经验与教训，对出现的问题，提出改进措施，不断完善外包业务。

第六章 外包服务商的管理

第十六条　通过第三方工程监理控制项目的实施过程。

第十七条　在外包服务合同执行期间，应对外包服务商进行持续的关注。关注的主要内容包括：

1、外包服务商的经营状况。

2、外包服务商的服务质量和技术支持水平。

3、外包服务商内部关键人员的变动情况，尤其是服务商高层、提供 IT 服务的关键技术人员情况。

4、外包服务商全面履行合同的情况。

5、应急方案的演练情况。

第十八条　应注重对外包服务商的管理和监督，使日常管理更加高效、到位。具体要求如下：

1、对进入本单位服务的外包服务商工作人员，信息技术外包管理小组可进行必要的考核和审查，保证外包服务工作人员的水平满足工作的需要。

2、督促外包服务商定期或不定期地组织对员工进行业务知识、专业技能、保密及安全制度方面的培训，促进服务水平和保密意识的提高。

3、应与外包服务商及其员工签订安全或保密协议，从制度和法律上防范安全风险。

4、应规范工作流程，实行定期报告制度。要求外包服务商提供周报、月报或重要事项、事件报告等，使外包管理小组能及时掌握各种情况。

第十九条　应对外包服务商的信息进行统一管理，并通过建立外包服务案例库的形式，为单位后续外包服务管理工作提供参考。

江门市红十字会备份与恢复安全管理制度

第一章 目的

第一条 为加强江门市红十字会重要信息的备份保护，以及信息被损坏或丢失时的恢复能力，保证业务系统数据的完整性和可用性，特制定本制度。

第二章 适用范围

第二条 适用于江门市红十字会各种重要信息。

第三章 职责

第三条 由江门市红十字会办公室负责此规定的制定、执行。

第四章 备份管理规定

第四条 数据备份程序

1、确定需要备份的电子数据。收集需要备份的信息资产的相关信息，主要包括信息资产的名称、重要性、资产对系统运行的影响等属性，填写《信息备份识别清单》。

需要检查的信息资产包括：

（1） 生产机上运行的应用系统软件；

（2） 数据库结构(表结构、存储过程、视图、索引、函数等)；

（3） 业务数据；

（4） 系统配置参数；

（5） 日志文件；

第五条　制定备份计划

1、根据《信息备份识别清单》和信息备份安全要求，分别制定《信息备份计划》，备份计划具体包括：

（1） 备份责任人：执行备份操作人员。

（2） 备份方式：采用复制，双系统同步，转储，压缩复制等。

（3） 备份频度

（4） 备份介质类型：光盘、硬盘、磁带等。

（5） 保存期

（6） 存放位置

（7） 介质替换频率

（8） 备份数据运输的方法 :应根据信息重要程度有相应的措施。

（9） 备份文件命名规则：备份文件标识应唯一。

2、备份计划应提交给办公室负责人，经办公室负责人确认并批准后予以实施。

第六条　实施备份计划

1、执行信息《信息备份计划》，检查备份数据的可用性，填写完整的《信息备份记录》。

2、备份责任人应向管理员提交备份结果，包括：备

份介质和备份过程中产生的相关文件，填写《资料交接记录》。

第七条　数据恢复程序

1、数据恢复申请审批

（1）管理员在发现系统的数据有损坏或丢失，并判断需要对数据进行恢复时，应填写《数据恢复记录》，说明发现的问题或解释需要对数据进行恢复的原因。

（2）管理员组织相关的业务人员制订数据恢复的解决方案。解决方案内容应包括：恢复工具、备份资源情况、恢复时间要求、恢复操作过程等。

（3） 管理员在制订好解决方案之后，填入《数据恢复记录》上报给办公室负责人进行审批。

第八条　实施数据恢复

1、经过办公室领导审批之后，由管理员组织按照恢复方案进行数据恢复的操作。备份信息使用前，应检查备份信息的完整性和可用性。操作时应至少有两人在现场，以确保恢复操作的正确无误。恢复时间要根据具体的情况而定。

2、恢复过程完成之后，备份介质安全返还到存放地点，管理员填写《数据恢复记录》中的恢复过程及结果（成功与否）。

第九条　结果检查

1、如果数据恢复成功，则应由业务部进行恢复后的数据检查。业务部检查人员在确定数据恢复无误后，要填写《数据恢复记录》中检查结果部分，并报办公室负责人签字认可。

2、如果恢复不成功，则管理员必须报告办公室负责人，然后会同相关人员制订新的数据恢复解决方案。

第十条　数据恢复的演练

1、管理员应建立定期的《数据恢复演练计划》，并按照计划严格执行恢复程序，以检查和测试备份数据的正确性、完整性和可恢复性，确保在恢复程序规定的时间内完成备份的恢复。

第十一条　信息备份安全要求

1、操作系统数据指操作系统和相关的系统软件以及重要的系统配置信息，操作系统数据备份由系统管理员执行，采用硬盘（光盘、磁带、硬盘）方式备份，要求每季备份一次，保存半年。

2、应用软件指业务系统的源代码和目标代码以及相关的控制文件、说明文档及表格等。应用软件由系统管理员执行，采用光盘（光盘、磁带、硬盘）方式备份，要求每次修改前备份一次，保存半年。

3、数据库系统数据指数据库管理软件以及重要的系统配置信息，数据库系统数据由管理员执行，采用硬盘（光

盘、磁带、硬盘）方式备份，要求每季备份一次，保存半年。

4、应用数据即业务数据，是连续改变的数据。应用数据由管理员按规定执行，采用硬盘（光盘、磁带、硬盘）方式备份，每天进行增量备份，每周至少一次完全数据备份。年末备份数据永久保存。

5、网络数据主要指路由器、交换机、防火墙等网络设备的配置信息。网络数据备份由管理员执行，采用硬盘（光盘、磁带、硬盘）方式备份，网络数据备份每季度备份一次，保存三个月。

6、操作系统软件、数据库系统数据、应用软件、网络数据升级或变更，要求 OA 报办公室负责人审批，按规定在升级或变更前、后分别做备份。备份数据保存三个月。

7、资料管理员对备份介质按照备份文件命名规则分类标识，整齐有序存放。

8、需要永久保存的备份介质应在介质有效期内进行介质替换。

江门红十字会信息系统补丁管理指南

第一章 总则

第一条　目的：为加强江门红十字会信息系统补丁的管理，规范补丁部署流程，保证信息系统补丁及时更新，确保单位信息网络安全稳定的运行，特制定本办法。

第二条　使用范围：适用于江门红十字会涉及的信息系统。

第三条　职责：由江门红十字会办公室负责此规定的执行。

第二章 管理要求

第四条　补丁范围：所涉及的补丁包括操作系统补丁、数据库补丁和应用系统补丁。

第五条　服务器管理员工作职责

1、负责服务器操作系统（含浏览器、办公软件）补丁的管理。

2、负责收集操作系统漏洞信息，跟踪最新补丁信息，评估漏洞威胁、成因和严重性。

3、负责提出操作系统漏洞修补要求和相关防护措施，审批变更计划。

第六条　数据库补丁管理员工作职责

1、负责各数据库补丁的管理。

2、负责收集数据库漏洞信息，跟踪最新补丁信息，评估漏洞威胁、成因和严重性。

3、负责提出数据库漏洞修补要求和相关防护措施，审批变更计划。

第七条　应用系统补丁管理员工作职责

1、负责各应用系统（含中间件）补丁的管理。

2、负责收集应用系统漏洞信息，跟踪最新补丁信息，评估漏洞威胁、成因和严重性。

3、负责提出应用系统漏洞修补要求和相关防护措施，审批变更计划。

第八条　系统开发员工作职责

1、负责搭建测试环境，负责测试补丁和测试结果的记录。

2、负责跟踪最新补丁信息和下载补丁。

第九条　终端维护员

1、负责办公终端计算机设备补丁的安装或分发，负责制订补丁修补计划。

2、负责解决补丁安装或分发过程中出现的问题。

第三章：补丁安装管理

第十条　补丁管理　：

1、服务器补丁由单位办公室统一进行下载、测试和

安装，未经许可，不可私自下载安装。

2、办公终端补丁可通过系统更新或者统一部署的安全软件下载、安装，手动下载的补丁由单位办公室的终端维护员统一下载分发，不得自行下载、安装。

3、补丁来源须为原厂商官方网站或者系统开发人员，对于非法的补丁禁止安装。

第十一条　补丁安装要求:

1、应定期对系统安装安全补丁程序，补丁安装前，应先做好系统和数据备份工作，保证出现问题时可进行回退操作。

2、补丁须经严格测试通过后方可安装，对测试不成功的补丁严禁安装。

3、系统管理员负责对操作系统补丁进行测试，应用系统开发人员负责对应用系统的补丁进行测试 测试中发现的问题应做详细分析，判断发生问题的原因，对应用系统造成影响的，由开发人员解决，如果不能解决，须记录发生问题的环境，暂停安装补丁。

4、对于刚发布的严重等级漏洞（无补丁）或未通过测试的补丁，可采用临时解决办法消除漏洞的威胁或者暂时接受该风险。

5、制订补丁修补计划，须先分析信息资产、IT 系统环境、IT 网络环境和信息资产重要等级，确定需要安装的

补丁和相应严重等级，同时明确修补时间、修补方式和修补范围。

6、补丁安装顺序遵循“资产价值大、威胁等级高优先安装”的原则。对于漏洞级别为严重的补丁，无特殊情况须在补丁发布后一星期内安装。

7、补丁安装完成后应进行全面检查，以确认补丁安装情况，同时制定补丁清单列表。

江门市红十字会信息系统

恶意代码防范管理指南

第一章 总则

第一条 目的：在信息系统常遇到的安全事件中，由恶意代码带来的威胁最为常见，且信息系统的应用中众多的途径都可能引入恶意代码，给系统带来安全风险。为了确保江门市红十字会信息系统安全，特制定本制度。

第二条 适用于江门市红十字会信息系统。

第三条 由江门市红十字会办公室负责此规定的制定、执行。

第二章 管理规定

第四条 办公室对恶意代码等安全相关事项进行集中管理。

第五条 系统管理员对于重大操作系统漏洞以及集中病毒爆发提出预警。通过内网发布或邮件电话等通知客户端及时采取必要措施，并记录相关信息。

第六条 所有用户均应关注病毒警告，及时升级病毒软件。

第七条 在读取移动存储设备上的数据以及网络上

接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

第八条　系统管理员负责对服务器进行恶意代码检测并保存检测记录；网络管理员对网络进行恶意代码检测并保存检测记录。

第九条　应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理。

第三章 管理要求

第十条　网络层防恶意代码

1、应配备相应的安全设备：在内部网与外部网之间，设置防火墙实现内外网的隔离与访问控制。防火墙设置在不同网络或网络安全域之间信息的唯一出入口。

2、防火墙具有以下五大基本功能：过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；对网络攻击的检测和告警。

3、应通过 VLAN 技术实现对内部子网的物理隔离。将安全等级不同、保密要求不同的网段划分到不同的 VLAN 内，限制局域网络安全问题对全局网络造成的影响。

4、对于重要系统网络边界应设置防毒墙，实现在网

络边界处对恶意代码进行检测和清除。

5、应维护恶意代码库的升级和检测系统的更新。

第十一条　服务器防恶意代码

1、使用正版软件，定期更新补丁。补丁更新流程详见《系统安全管理制度》

2、应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

3、主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

4、应支持防恶意代码的统一管理。

5、能够检测对重要服务器的入侵行为。记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间。

第十二条　客户端病毒防护

1、使用正版软件，定期更新补丁，修复操作系统及软件漏洞

2、所有客户端均应安装防病毒软件

3、客户端应定期更新防病毒软件及病毒库

4、客户端机器不执行与工作无关的操作，不访问与工作无关的网站。

5、所有接入系统的移动存储介质、计算机以及邮件均应先查杀病毒后方可使用。

6、发现病毒应及时上报办公室。

第十三条　软件开发管理

1、应严格根据开发需求检测软件质量；

2、应在软件安装之前检测软件包中可能存在的恶意代码或由开发商承诺软件中无恶意代码；

3、应要求开发商提供软件设计的相关文档和使用指南；

4、重要系统应要求开发商提供软件源代码。开发商应承诺软件不存在后门。

江门市红十字会信息系统

项目建设管理制度

第一章 总则

第一条 为加强江门市红十字会信息系统建设步伐，进一步规范信息系统工程项目建设安全管理，参照《信息系统安全等级保护基本要求》，结合江门市红十字会实际情况，特制定本制度。

第二条 本制度适用于信息系统项目申报、建设、实施和验收管理。

第三条 办公室负责信息系统项目建设管理制度的制定和修订。

第二章 项目申报

第四条 项目申报阶段应对信息系统项目及其建设的各个环节进行统一的安全管理规划，确定项目的安全需求、安全目标、安全建设方案，以及生命周期各阶段的安全需求、安全目标、安全管理措施。

第五条 应由项目应用主管部门进行项目需求分析、确定总体目标和建设方案。项目应用主管部门进行项目申报时应填写《信息系统项目立项申请表》，并提交《业务

需求书》和《信息系统项目可行性研究报告》。

第三章 系统定级

第六条 依据国家信息系统安全等级保护定级指南对项目中的系统进行定级，明确信息系统的边界和安全保护等级。

第七条 以书面的形式说明确定信息系统为某个安全保护等级的方法和理由，形成信息系统定级报告。

第八条 组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定，上报上级主管单位和安全监控单位进行审定。

第九条 信息系统的定级结果向本地公安机关进行备案。

第四章 系统安全需求

第十条 安全威胁分析报告：应分析待建计算机系统在生命周期的各个阶段中可能遭受的自然威胁或者人为威胁（故意或无意），具体包括威胁列表、威胁可能性分析、威胁严重性分析等。

第十一条 系统脆弱性分析报告：包括对系统造成问题的脆弱性的定性或定量的描述，这些问题是被攻击的可能性、被攻击成功的可能性。

第十二条 影响分析报告：描述威胁利用系统脆弱性可能导致不良影响。影响可能是有形的，例如资金的损失

或收益的减少，或可能是无形的，例如声誉和信誉的损失。

第十三条 风险分析报告：安全风险分析的目的在于识别出一个给定环境中涉及到对某一系统有依赖关系的安全风险。它取决于上面的威胁分析、脆弱性分析和影响分析，应提供风险清单以及风险优先级列表。

第十四条 系统安全需求报告：针对安全风险，应提出安全需求，对于每个不可接受的安全风险，都至少有一个安全需求与其对应。

第五章 安全可行性

第十五条 项目目标、主要内容与关键技术：增加信息化项目的总体安全目标，并在主要内容后面增加针对前面分析出的安全需求所提出的相应安全对策，每个安全需求都至少对应一个安全对策，安全对策的强度应根据相应资产的重要性来选择。

第十六条 项目采用的技术路线或者技术方案：增加描述如何从技术、运作、组织以及制度四个方面来实现所有的安全对策，并形成安全方案。

第十七条 项目的承担单位及人员情况介绍：增加项目各承担单位的信息安全方面的资质和经验介绍，并增加介绍项目主要参与人员的信息安全背景。

第十八条 项目安全管理：增加项目建设中的安全管理模式、安全组织结构、人员的安全职责、建设实施中的

安全操作程序和相应安全管理要求。

第十九条 成本效益分析：对安全方案进行成本-效益分析。

第二十条 对投入使用的应用软件需要升级改造的，虽不需另行立项，但仍需参照上述方法进行一定的安全性分析，并针对可能发生的安全问题提出和实现相应安全对策。

第六章 安全方案设计

第二十一条 本阶段主要是项目审批单位对项目申报内容进行安全方案的设计，对项目的安全性进行确定，必要时可以聘请外单位的专家参与论证工作。

第二十二条 根据系统的安全保护等级选择基本安全措施，设计安全标准必须达到等级保护相关等级的基本要求，并依据风险分析的结果进行补充和调整必要的安全措施。

第二十三条 应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。

第二十四条 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。

第二十五条 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

第七章 方案论证和审批

第二十六条 本阶段主要是项目审批单位对项目申报内容进行审批，对项目进行安全性论证，必要时可以聘请外单位的专家参与论证工作。

第二十七条 须进行安全性论证和审批。

第八章 项目实施方案和实施过程安全管理标准

第二十八条 信息化项目实施阶段包括 3 个子阶段：概要设计、详细设计和项目实施，本阶段的主要工作由项目开发承担单位来完成，项目审批单位负责监督工作。

第二十九条 在概要设计阶段，系统层次上的设计要求和功能指标都被分配到了子系统层次上，这个子阶段的安全目标是保证各子系统设计实现了总体安全方案中的安全功能。

第三十条 详细设计阶段的安全目标是保证各模块设计实现了概要设计中的安全功能。

第三十一条 项目实施阶段主要目的是将所有的模块（软硬件）集成为完整的系统，并且检查确认集成以后的系统符合要求。

第三十二条 在系统实施阶段需要采购的网络安全设备必须由江门市红十字会进行统一采购。

第三十三条 安全专用产品应具有国家职能部分颁发的信息安全专用产品的销售许可证。

第三十四条 密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位。

第三十五条 在产品采购前，应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

第三十六条 通过上述测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定。通过试运行的设备，才能投入生产系统，正式运行。

第三十七条 产品和服务供应商应达到系统集成商的资质要求：至少要拥有国家权威部门认可的系统一级集成资质，对于较为重要的系统应有更高级别的集成资质。

第三十八条 应符合国家相关法律、法规，按照相关主管部门的技术管理规定对非法信息和恶意代码进行有效控制，按照有关规定对设备进行控制，使之不被作为非法攻击的跳板。

第九章 项目启动

第三十九条 工程启动前需开启工程启动会，办公室相关负责人需和工程实施单位的负责人沟通确认工程里程碑、测试、验收等关键点的时间，并要求工程实施单位的负责人制定工程实施计划。

第四十条 工程实施前需与工程实施单位签订保密协议。

第十章 项目实施

第四十一条 工程实施单位的负责人应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。

第四十二条 工程实施过程中办公室相关负责人需对工程的进度和质量进行把控，定期对工程的实施进度汇报至上级领导。对于工程中的重要操作，需要报告至上级领导审批，经同意后方可操作，并对所有的操作记录备案和归档。

第十一章 项目验收与投产

第四十三条 系统建设完成后，项目承建方要依据项目合同的交付内容向项目应用主管部门进行项目交付。

第四十四条 系统交付要项目实施和应用主管部门的相关项目负责人进行签字确认。

第四十五条 系统交付由项目应用主管部门负责，必须按照系统交付的要求完成交付工作。

第四十六条 项目应用主管单位应委托经国家认可的第三方检测机构对系统进行安全性测试，并出具安全性测试报告。

第四十七条 应制定投产与验收测试大纲，在项目实施完成后，由项目应用主管单位和项目开发承担单位共同组织进行测试。

第四十八条 在测试验收前，根据设计方案或合同要求等制订测试验收方案，测试验收过程中需详细记录测试验收结果，并形成测试验收报告。

第四十九条 测试完成后，项目测试小组应提交《测试报告》，其中应包括安全性测试和评估的结果。不能通过安全性测试评估的，由测试小组提出修改意见，项目开发承担单位应作进一步修改。

第五十条 测试通过后，由项目应用单位组织进入试运行阶段，应有一系列的安全措施来维护系统安全，它包括处理系统在现场运行时的安全问题和采取措施保证系统的安全水平在系统运行期间不会下降。

第五十一条 项目应用主管部门负责系统测试验收的管理，必须按照系统测试验收的要求完成验收工作。

第五十二条 项目应用主管单位应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

第五十三条 项目应用主管部门应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

第五十四条 项目应用主管部门应对负责系统运行维护的技术人员进行相应的技能培训。

第五十五条 项目应用主管部门应提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

第十二章 系统备案

第五十六条 办公室负责管理系统定级的相关材料，并控制这些材料的使用。

第五十七条 应将系统等级和系统属性等资料报系统主管部门备案。

第五十八条 系统建设完成后，应将系统等级及其他要求的备案材料报相应公安机关备案。

第十三章 设备管理

第五十九条 设备的使用均应指定专人负责，均应设定严格的管理员身份鉴别和访问控制，严禁盗用账号和密码，超越管理权限，非法操作安全设备。

第十四章 投产后的监控与跟踪

第六十条 项目投产后还应进行一段时间的监控和跟踪，发现对系统安全有不良影响处，都应在系统设计、配置、运行管理上做相应改进，以保证系统安全、正常运行。

第十五章 等级测评

第六十一条 系统进入运行过程后，三级的系统每年聘请第三方测评机构对系统进行一次等级测评，二级的系统自评估每年测评一次，发现不符合相应等级保护标准要求的及时整改。

第六十二条 系统发生变更时，及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，

发现不符合相应等级保护标准要求的及时整改。

第六十三条 测评机构要选择具有国家相关技术资质和安全资质的单位。

第六十四条 系统的等级测评由办公室负责管理。

第十六章 安全服务商选择

第六十五条 安全服务商的选择必须符合国家的有关规定。

第六十六条 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

第六十七条 选定的安全服务商需提供技术培训和服务承诺，必要的与其签订服务合同。

江门市红十字会信息系统

网络配置安全指南

第一章 总则

第一条 为了加强江门市红十字会网站及信息系统安全管理，规范系统日常操作维护的行为，确保信息系统的安全，特制定本制度。

第二章 使用范围

第二条 适用于江门市红十字会信息系统及网络配置管理。

第三章 职责

第三条 由江门市红十字会办公室负责此规定的执行。

第四章 管理规定

第四条 操作系统安装配置规范：

1、应使用成熟、正版的操作系统

2、在首次使用操作系统时，应对操作系统进行配置管理、网络访问控制、口令管理控制以及屏幕加锁控制。

3、系统安装应遵循最少化安装原则，只安装必需的组件。

4、系统安装后应检查系统默认账户，删除非必须的

默认账户，保留的默认账户应修改默认密码。

5、账户权限授予依据最小化原则，仅授予账户所需的最小权限。

6、对于易受攻击的重要服务器应安装防病毒软件，并定期更新病毒库。

7、对于新安装系统应及时记录服务器相关信息，在相关信息修改后应及时修改服务器基础信息。

8、重要系统应开启系统审计功能。记录系统登录日期、时间、类型等相关信息。审计信息不应被随意删除或修改。在审计信息被删除前应存档保存至半年。

9、对系统运行的服务应该进行严格控制，一些不应该开启的服务或是会带来安全性问题的服务原则上都应该关闭。

原则上应停止如下不需要的服务：

DHCP server services、 WINS Service、 Fax Service、 Bluetooth Support Service、 Indexing Services、Messenger Service、Print Spooler、Remote Registry Service(AD域环境及novell备份服务器除外)、Server（AD 域环境及 novell 备份服务器除外）、Simple TCP/IP Services、 Wireless Zero Configuration、 SMTP/FTP/IIS Admin/WWW Publish （如果需要 IIS 服务，可关闭由 IIS 提供的 SMTP、FTP 服务）

第五条 数据库安全配置：

1、应使用成熟、正版的数据库系统软件。

2、数据库安装应遵循最少化安装原则，只安装必需的组件。

3、对于新安装数据库应及时记录数据库配置信息。在相关信息修改后应及时修改相关的配置信息。

4、在数据库安装后应检查数据库默认账户。删除非必须的默认账户。保留的默认账户应修改默认密码。

5、账户权限授予依据最小化原则，仅授予账户所需的最小权限。

6、重要数据库应根据需要定期备份，详细内容见《信息系统备份管理指南》。

第六条 应用系统安全

1、系统应具备输入数据的确认功能，以确保输入数据的正确性和适用性。

2、重要系统应有专门的登录控制模块对登录用户进行身份标识和鉴别。

3、对于新安装应用系统应及时记录应用系统配置信息。在相关信息修改后应及时修改相关的配置信息。

4、重要系统应提供登录失败处理功能，限制非法登录次数。采取结束会话或自动退出等措施。

5、重要系统用户登录密码设置应符合《用户标识与

口令管理指南》。

6、应具有访问控制功能，用户仅能访问其必须的数据、文件。

7、严格控制系统中的默认账户，默认账户密码可以更改，在系统正式上线后修改所有默认账户的密码。

8、用户权限授予最小化原则，仅授予其完成承担任务所需的最小权限。

第七条 用户管理策略配置

1、各网络设备的所有管理方式均须启用账号/口令登录方式。

2、当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如采取加密传输方式。

3、网络设备账号和口令管理按照《用户标识与口令管理指南》管理细则执行。

4、启动网络设备的登录限制功能，对网络设备的管理员登录地址进行限制。

第八条 访问控制策略

1、网络边界部署访问控制设备，启用访问控制功能。

2、所有与外部系统的连接均要通过 OA 申请审批。

第九条 日志配置策略

1、必须开启所有网络设备，包括路由器、交换机、

防火墙、入侵检测系统等的日志功能，对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

2、准确设置信息处理设备的时钟。

3、记录的日志必须保存半年，任何个人和部门不得以任何理由删除保存期之内的日志。

4、对重要区域、重要网络设备日志文件进行定期备份，并保存备份的日志。

5、必要的时候，邀请外部信息安全专家来对日志记录进行检查分析。

第十条 防火墙安全配置

1、内部办公区域访问外网，按照开放最小化配置的方式访问外网，如有特殊访问需求需通过 OA 申请开通，由办公室负责人审批后方可开放使用，使用期结束后应及时回收使用权限。

2、内部重点服务器区域，原则上不允许访问外网或被外网访问。

3、内部服务器区域，不允许被外网访问，根据业务需要如需外网访问内部服务，须通过 OA 申请开通，经办公室负责人批准，为服务器映射公网 IP 地址及开放端口，使用期结束后应及时回收使用权限。

第十一条 网络交换机安全配置

1、交换机以 VLAN 方式区分各业务单元。

2、交换机须配置访问控制列表，按照业务需求以最小化原则配置。

3、交换机安全配置策略应考虑和周边网络设备的连接的兼容性、安全性、可靠性和可变性。

4、交换机安全配置策略应尽量减少不必要的限定以保证合理的通信能力。

第十二条 升级与打补丁

根据网络设备厂商提供的软件升级版本对网络设备和安全设备进行升级，及时下载安装补丁，重要补丁安装应经过办公室有关负责人批准，避免造成安装补丁后系统不能正常运行。在升级之前要注意对网络设备的相关配置命令以及日志记录进行备份操作。

第五章 系统日常操作管理

第十三条 对运行关键业务的系统进行持续监控。监控系统关键性能参数（如启动参数）、工作状态、占用资源和容量使用情况等内容。

第十四条 不得随意重启业务系统服务器、相关网络设备和安全设备，尽量少安装与业务无关的其它软件。

第十五条 需按照等级保护的要求对各系统进行安全策略设置，并定期根据业务需求对系统策略进行检查调整。

第十六条 对主机系统上开放的网络服务和端口进行检查，发现不需要开放的网络服务和端口时及时通知相关

管理员进行关闭。

第十七条 对系统运行情况进行记录，每月对记录结果进行分析、统计，并形成分析报告向上级汇报。

第十八条 开办交互式栏目的信息系统必须配备关键字过滤措施，防止出现有害信息和非法言论。

第十九条 对系统日志定期进行审计、备份，并定期对运行日志和审计数据进行分析，以便及时发现异常行为。

第二十条 日常操作维护过程中，各管理员应确保信息系统安全、稳定运行，任何升级、补丁安装等变更操作需进行审批，变更操作前需进行备份。

第二十一条 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。

第二十二条 做好系统日常运行维护工作，并及时、准确记录运行管理日志，日常运行维护工作主要包括：制定系统运行维护计划，严格按计划对系统进行维护，并详细记录维护情况；监控系统运行状况，发现异常情况及时向办公室相关人员反映，能够处理的系统故障应及时处理，并对故障产生原因进行认真分析总结等。

第二十三条 任何人不得擅自修改系统参数，确需修改应严格履行审批手续，由系统管理人员实施，实施时应有监督，详细记录系统变更及操作过程，修改后的参数应

记录备案。

第二十四条 任何人不得擅自对业务数据进行修改或恢复操作，需要操作时应严格履行审批手续，由系统管理人员实施，并由有关人员监督执行。系统管理人员进行可能影响业务系统运行的操作前必须先请示办公室相关负责人。

江门市红十字会信息资产管理制度

第一章 总则

第一条 对信息系统资产实施适当的分类与分级，建立资产的清单并加以维护，使用信息资产受到有效的保护。

第二条 使用范围：适用于江门市红十字会信息资产的管理。

第三条 职责：由江门市红十字会办公室负责此规定的制定、执行。

第二章 资产分类

第四条 资产表现形式分类：

江门市红十字会信息资产分为五大类，包括：

1、信息资产：数据、数据文件、合同和协议、系统文档、研究信息、用户手册、培训教材、各类规章制度和操作规程、归档信息、业务信息等。

2、软件资产：操作系统、数据库管理系统、业务系统、办公软件和源程序等。

3、硬件资产：网络设备（交换机、路由器、防火墙、入侵检测系统等）、计算机设备（服务器、个人办公终端设备）、存储设备、传输线路、保障设备（UPS、机房空调、门禁等）、打印机等。

4、服务：计算和通信服务、公用设施，例如：供暖、照明、能源、空调等。

5、无形资产，如组织的声誉和形象。

注释：个人办公终端设备、服务和无形资产不在本管理制度范围之内。

第三章 资产标识

第五条 硬件资产标识 :硬件资产中属于固定资产的由办公室统一进行标识，使用股份单位固定资产标签。不属于固定资产的不用标识。

第六条 软件资产标识

1、软件资产有原件（盘）由使用人负责保管并自行标识；

2、软件资产为电子档案的，不用标识，证书、序列号等标志信息由使用人负责保管；

3、信息系统管理软件的文档（安装软件、安装手册、操作手册、维护手册、开发文档等 ）由办公室安排专人管理，自行标识。

第四章 信息资产管理

第七条 信息资产采购管理：

1、硬件资产采购：由信息系统使用部门提出申请，办公室提供参数、性能要求，按江门市红十字会采购管理规定执行。

2、软件资产采购：信息系统所需操作系统、应用软件、数据库、安全软件、工具软件等的采购必须由所需部门提出申请，对所需软件的用途、型号等进行说明，由办公室提供技术参数要求，按单位采购管理规定执行。

3、信息系统所采购的软件必须是正式版本，严禁使用测试版和盗版软件。

4、应要求应用软件产品供应厂家对以下软件安全性相关内容做出明确商业承诺，必要时，办公室与信息系统实施单位应对所购买的软件产品进行安全性测试，形成安全测试报告。软件安全性相关内容包括：

1)　软件产品应具有时间安全性，到期不出现锁死、自毁等对计算机信息系统造成损害的情况；

2)软件不应含有病毒、后门等恶意代码；

3)　软件产品应对用户输入数据进行验证，以减少用户输入错误的风险和预防包括缓冲区溢出和代码注入等攻击；

4)　软件产品应对软件输出数据进行验证，以确保对所存储信息的处理是正确的且是安全的。

5、软件安装和测试

1）重要的操作系统和主要应用软件必须在办公室人员的监督之下进行安装，注意清理操作系统和应用软件中默认选项。

2）软件安装后，须使用可靠检测软件或手段进行安全性测试，了解其脆弱性，并根据脆弱性程度采取措施，使风险降至最小。

第八条 信息资产档案管理由办公室统一登记造册，设立信息资产管理员，当资产发生变动时随时办理增减变动手续，并定期进行清查工作。

第九条 信息资产实物管理由资产使用人负责管理。

第十条 当信息资产需要在内部流动时，由相关资产使用人填写《固定资产内部转移单》，并在相应的资产清单中作资产变更记录。

第十一条 资产出租或外调：原则上资产不得出租或外调，但如确有此需要，必须提出书面申请、主管领导审批、由资产所属管理者填写《资产转移单》，并在相应的资产清单中作资产变更记录。

第十二条 资产报废：由需报废资产的管理员填写《固定资产报废单》，按单位固定资产报废管理制度执行，并将进行安全资产报废处理，并在相应的资产清单中作资产变更记录。

第十三条 监督：资产管理员对信息资产进行定期清查工作，周期为每年一次，并填写《资产清查记录》。

第五章 资产安全管理

第十四条 各单位部门第一安全责任人是本单位部门

信息资产管理的第一责任人，负责组织本管理办法的贯彻落实。

第十五条 信息资产所属部门的负责人是信息资产责任人，对所属信息资产负直接责任。其主要职责包括：

1、理解各种信息访问活动相关的安全风险；

2、根据单位相关策略确定并检查信息访问权限；

3、针对所属信息资产提出恰当的保护措施。

第十六条 信息资产管理人是受信息资产责任人委托，对信息资产进行日常管理的资产保管者，负责维护已经建立的保护措施。主要职责包括：

1、根据相关策略和信息资产责任人的要求，负责信息资产的维护操作和日常管理事务；

2、负责具体设置信息访问权限；

3、负责所管理的信息资产的安全控制；

4、部署恰当的安全机制，进行备份和恢复操作；

5、按照信息资产责任人的要求实施其它控制。

第十七条 信息资产的使用者，除了单位内部员工，也可能是因为业务需要而访问单位信息的第三方人员。其主要职责包括：

1、向信息资产责任人申请信息访问；

2、按照单位信息安全策略要求访问信息，严禁非授权访问；

3、向相关部门报告隐患、故障或者违规事件；

4、配合信息资产责任人的信息安全检查。

第十八条 各部门应指定本部门信息安全联络员。其主要职责是负责通报本部门的信息安全状况，传达和落实单位信息安全的工作要求。

第十九条 按等级保护要求配备相关技术人员：安全运维管理员、操作系统管理员、网络管理员等。操作系统管理员和网络管理员不得兼任安全运维管理员。其职责分别如下：

1、安全运维管理员：负责对安全管理平台、防火墙、入侵检测、入侵防范、防病毒系统、网络审计系统等安全设备进行管理。执行日常安全运维作业计划，处理安全事件，负责收集安全系统以及安全设备的各项数据。

2、操作系统管理员：负责信息系统设备和系统级别的运行维护和数据的安全管理工作。

3、网络管理员：主要负责网络畅通和网络安全，负责系统安全补丁、漏洞检测及修补，病毒防治等工作，以保证良好的网络设备运行环境。

第二十条 各部门对信息资产的访问权应限制到最低限度，即仅赋予其执行授权任务所必需的权限。重要信息及程序文件应控制在最少人员的范围。

第二十一条 设备外送修理前，需将存贮介质内的应

用程序等与业务相关信息予以删除，必要时应与设备维修厂商签订保密协议。对已修理完毕的，维修人员应进行检验，并对存贮介质中的内容进行安全检查。

第二十二条 远程登录维护必须由资产管理部门批准，做好记录并及时更换口令，严防泄密事件发生。

第二十三条 资产报废时，对存有程序、数据或资料的资产进行不可恢复的清除，防止失密，并做好废弃处置记录。对涉密设备的报废必须按有关保密要求妥善处理。

江门市红十字会机房安全管理制度

第一章 总则

第一条 为确保江门市红十字会机房信息处理设施的安全，防止未经授权的访问，加强机房的安全与管理，做好机房的防火、防盗、防泄露等工作，规范机房的管理。特制定本规定

第二条 使用范围：江门市红十字会机房。

第三条 由江门市红十字会办公室负责此规定的执行。

第二章 机房管理规定

第四条 机房进出管理规定

1、配备机房管理员，对机房的出入、服务器的开机或关机等工作进行管理；

2、严格执行机房出入登记制度，外部人员进入机房须先提出书面申请，经办公室负责人或机房管理员批准后，认真填写《机房出入登记表》后方可进入，机房内的工作由设备技术部人员全程陪同。

3、进入机房人员随身携带的物品应放置到指定位置，禁止随意乱放。

4、设备、介质和物品移入、移出机房要经过机房管理员批准，应填写《机房出入登记表》。

5、任何人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品及其它与机房工作无关的物品进入机房。

6、进入机房的工作人员离开工作区域前，应锁定工作服务器，清理带入的所有个人物品和资料。

第五条 机房工作管理要求

1、机房内严禁吸烟、吃食物、喧哗、嬉戏或进行剧烈运动，保持机房安静。

2、机房内物品摆放整齐，定期打扫机房卫生；机房门窗保持关闭状态，防止外来粉尘污染；机房管理员每年对机房内服务器进行一次彻底除尘。

3、机房内严禁使用软盘、U 盘等移动存储介质。

4、机房管理员负责保管机房钥匙，禁止将钥匙外借；机房管理员负责早晚开关机房门锁，并检查门禁系统的状态；对于遗失钥匙的情况要及时上报。

5、机房管理员应每周检查网络设备、服务器、空调、消防等设备运行状态（如设备指示灯、仪表），及时了解设备运行状态，填写《机房工作日志》；定期检查、整理设备物理连接线路，定期对空调、消防、UPS 等设备进行维护，填写《设备维护记录》。

6、机房管理员负责检查机房的防水、防潮系统，设置合理的温度、湿度。

7、机房管理员负责安排有专业资质的人员定期检查和维护 UPS、空调、消防、通风等设备设施，并填写《设备维护记录》。维护人员应按照安全规程操作，保证人身及设备安全。严禁随意对设备断电、更改设备供电线路，严禁随意串接、并接、搭接各种供电线路，以防造成短路或失火。

8、机房管理员必须严格按照操作规程（操作规程如：温度、湿度等要求）对机房内服务器、网络设备、UPS 电源、空调等重要设备进行操作。

9、在对机房设备设施的配置进行重大更改之前，应首先制定完整解决方案，进行可行性论证后由具备资格的技术人员进行更改和调整，并做好详细的操作记录。解决方案中应考虑到由更改、升级、配置所带来的负面后果，并制定应急预案。

10、出现机房盗窃、破门、火警、水浸等严重事件时，应立即通知机房管理员及相关部门，机房管理员应立即到达现场，协助处理相关事件。

江门市红十字会介质安全管理指南

第一章 总则

第一条 目的：为加强江门市红十字会介质的管理和使用安全，规范介质的使用行为，特制定本制度。

第二条 使用范围： 江门市红十字会涉及的所有介质。

第三条 由江门市红十字会办公室负责此规定的制定、执行。

第二章 管理规定

第四条 介质的范围：

单位涉及的所有介质，包括存储相关信息的 USB 盘、磁盘、硬盘、移动硬盘、光盘等。

第五条 介质分为：涉密介质和非涉密介质。

涉密介质：存储涉密信息介质，由保密员负责管理。

非涉密介质：不存储涉密信息的存储介质。

第三章 介质的安全管理

第六条 对存储介质应进行统一的登记和记录。介质的使用、转移、维修和销毁必须受到严格管理。

第七条 存储介质应贴好标签进行标识，标签必须贴在表面易于辨识的地方，应标注介质编号、介质有效期、截止日期、操作人员、环境名称、内容、用途和数据保存

时间等信息。

第八条 介质保管

1、介质的保管环境要符合介质生产商对介质保管的要求。

2、介质在长期保管时，其保管的地点必须满足防火、防水、防潮、防雷击等要求。电子介质应远离高磁场环境，满足防静电、防磁等方面的安全要求。

3、单位介质由办公室指定专人保管介质，个人保管的介质由员工个人负责介质的存放安全。

4、涉密介质按涉密管理规定执行，由保密员负责管理。

第十条 含有内部信息的存储介质应有严格的外部访问控制，严禁任何人带离工作场所，如需外出进行更换或者维修损坏的介质，需要签订保密协议。

第十一条 重要存储介质应保存在安全的物理环境下，须具有防火、防静电及其他环境保护措施的环境。对于存放重要数据的存储介质应当在异地进行备份。

第十二条 应根据存储介质的使用寿命，制定数据恢复计划，以避免数据丢失。

第十三条 对含有重要数据的存储介质不再使用时，必须执行重复写操作防止数据恢复。对于磁带、光盘、纸质等存储介质进行报废处理时，应采取切碎或者烧毁的方

式进行。

第十四条 介质维护

1、定期检查备份介质是否可用，备份信息是否有效。

2、发现故障的介质由办公室统一处理，如需送出维修首先清除介质中的敏感信息，不能清除信息的介质根据信息的密级采用销毁或其他处理方式（如与维修单位签署保密协议，选择可信维修单位等）。

第十五条 介质销毁

1、移动存储介质确定不再使用时，需由办公室统一销毁，涉密介质由保密办按保密规定负责处理。

2、光盘和软盘如果是可读写的可采用先清除数据，然后采用物理方式销毁。

3、其他存储介质的销毁可以采用多次格式化等方式先清除数据，然后采用物理方式销毁。

4、介质销毁后要在《介质登记表》注明销毁的时间和日期。

江门市红十字会网站管理指南

第一章 总则

第一条 为进一步加强江门市红十字会网站（以下简称“网站” ）的管理与维护，建立规范的信息采集、审核、发布、更新机制，充分发挥网站信息传播、资源共享、宣传引导的作用，结合单位实际，特制订本办法。

第二条 本办法适用于参与单位网站管理的所有业务人员及其他相关人员。

第三条 单位网站建设应严格遵守国家法律法规、行业政策规定，并依据本办法开展网络建设和日常管理工作。

第二章 网站管理机构及职责

第四条 网站管理遵循谁运营谁管理的原则，办公室负责网站防病毒、防黑客攻击网站的规划建设、版面设计、栏目设置等管理工作。

第五条 办公室为网站的正常运行和维护提供技术支持与保障。

第三章 网站版面与栏目维护

第六条 网站版块、栏目设置等内容管理由办公室负责，全面落实管理责任制，指定网站管理员负责管理工作。若需要技术改版，由网站管理员报部门负责人审核通过后，

经领导审批，同意后方可提交外包维护单位执行。

第四章 信息的搜集与发布

第八条 网站所发布的信息实行 “个人提供，部门负责”的原则，所有网页上的图片和文字在发布之前必须认真审阅，确保内容和文字的正确性。网站管理员要做好相关记录。

第九条 办公室负责网站信息的收集和整理，各通讯员根据部门职能、部门最新动态及时向网站管理员提供最新相关信息。

第五章 网站管理

第十一条 任何人未经批准，不得随意发布信息或更改网站页面版式画面及文字内容。

第十二条 网站后台密码由单位网站管理员负责管理，未经批准不准向任何部门或个人泄漏。

第十三条 网站管理员发现单位网站被病毒、黑客袭击或发现网站运行不正常，应及时与网站维护单位联系，及时处理。针对网站运行和维护收到的建议、投诉等，务必及时回复、处理。此事由网站管理员收集，一般转由相关责任部门及时回复，并反馈处理结果。

第十五条 对发布的信息，网站管理员要以电子文档的形式备份后永久保留。

第六章 处罚

第十六条 网站维护要求每月一查，单位应及时更新对应版块内容，以保证单位网站的时效性。

第十七条 凡是以下情况的，将按照有关法律、法规追究其责任：

1、违反规定造成失密、泄密；

2、利用单位网站发布虚假信息，散布谣言，影响单位形象；

3、利用单位网站传播反动、淫秽、不道德以及其他违反国家法律、社会公德的信息；

4、恶意攻击、破坏网站正常工作。

江门市红十字会人员安全管理制度

第一章 目的

第一条 对江门市红十字会人员进行安全管理，降低由人员因素带来的安全风险。

第二章 适用范围

第二条 适用于江门市红十字会人员的管理。

第三章 职责

第四条 由江门市红十字会办公室负责此文件的制定、执行。

第四章 人员管理规定

第六条 人员任用及培训考核

1、人员正式到岗之前（包括岗位调整），由人力资源部和任用人员签订《岗位职责说明书》、《保密协议》，使人员明确相关的安全责任和惩戒措施。

2、年初由办公室制定年度《教育和培训计划》，针对不同岗位制定不同培训计划，培训计划应根据当前和未来的任务制定，内容包括信息安全意识教育、管理制度更新培训、岗位技能和操作规程培训和相关安全知识和技术培训。培训计划中应确定培训目的、培训内容、培训时间、培训方式、培训费用、培训范围；办公室负责人审核培训

计划并批准实施。

3、依据教育和培训计划定期组织培训，培训完成后填写《集体培训活动记录表》、《个人外出学习、培训情况汇报表》。

4、在实际实施过程中如有培训计划的调整，应及时在《教育和培训计划》中注明调整的原因和调整后的安排。

5、定期对各个岗位的人员进行安全技能及安全认知的考核，并填写《人员考核记录》。

6、依据《岗位职责说明书》和《保密协议》，对违反违背安全策略和规定的人员进行处罚。

第七条 离职与解聘

1、离职人员应交接所有工作资料，归还全部正在使用的单位资产（包括各种身份证件、钥匙、徽章以及机构提供的软硬件设备介质等），撤销离职人员对信息和信息处理设施所有访问权，并进行登记备案，填写《离职人员交接表》；如果在工作交接尚未完成时离职，应上报办公室负责人处理，并根据情况采取进一步的措施。

2、应办理严格的离职手续，签订《离职保密协议》。

第八条 外部人员访问管理

1、外部人员未经授权不得使用公司信息资产，包括系统、设备、信息数据等。

2、外部人员访问受控区域应遵守机房和办公环境相

关管理规定。

江门市红十字会软件安装管理流程

第一章 目的

第一条 为有效使用及管理计算机软件资源,并确保单位计算机软件的合法使用，避免人员因使用非法软件，影响江门市红十字会声誉或造成计算机病毒侵害，影响日常工作正常进行，特制定本制度。

第二章 适用范围

第二条 适用于江门市红十字会系统及应用软件的使用管理。

第三章 软件安装及使用管理办法

第一条 各类计算机软件，应依据著作版权者为限，并统一由办公室负责安装保管，信息管理软件及其它专用软件，需通过 OA 进行申请，获准后方可安装。

第二条 严禁个人私自在单位计算机上安装未获授权、非授权单位使用或超过使用授权数量的软件，未经授权或同意，使用者不得擅自在计算机内安装任何软件，经授权同意后方可在计算机内安装合法授权的软件。

第三条 各部门软件分配使用后，保管人或使用人职务变动或离职时，应移交其保管或使用的软件，并办理交接手续。

第四条 禁止员工使用会干扰或破坏网络上其它使用者或节点的软件系统，此种干扰与破坏如散布计算机病毒、尝试侵入未经授权的计算机系统、或其它类似的情形者皆在禁止范围内。

第五条 网络上存取到的任何资源，若其拥有权属个人或非单位所有，除非已经正式开放或已获授权使用，否则禁止滥用或复制使用这些资源。

第六条 禁止员工使用非法软件,或私人拥有的计算机软件安装使用于单位计算机上，也不得将单位合法软件私自拷贝、借于他人或私自将软件带回家中，如因此触犯著作权，则该员工应负全部责任，各部门应妥善保管正版软件，防止软件授权外泄或被非法使用。

第七条 为使软件在计算机中发挥应有的效用，并避免非法软件流入单位，办公室定期或不定期检查，如发现使用非法计算机软件者，除提报于单位外，并追究相应责任。

第八条 管理人员应依据软件本身需求定期备份数据，对于软件数据进行的更新操作必须存档相关数据文件和审批文件。

第九条 设备技术部对于购入的合法软件由专门人员分类保管。软件保管人对软件负保管之责，软件使用者如有使用不当，造成损毁或遗失，应负赔偿责任。

第十条 借用或归还软件，须直接联系软件管理人员，不可私自转借，并不得委任借还。借用软件若有遗失或不正常使用导致损坏，无法正常使用，借用人应负责赔偿。(正常使用的毁损不在此限，但须交回原借用的光盘或磁盘)。

第十一条 软件使用人员如果需要增加或修改软件功能，应与办公室联系，由办公室负责与软件供应商沟通，对相应模块进行升级或更新。

第十二条 各软件系统统一由办公室负责安装，安装到位后，任何人不得擅自删除和更改，如因此项原因导致当前管理软件的故障、报错等各种无法继续操作的情况，将由操作人员承担相关责任。

第十三条 操作人员发现软件系统不能正常运行的，不得擅自对系统进行尝试性修复，请及时通知系统管理人员，由系统管理人员进行检修或做相应的处理。

江门市红十字会软件开发管理制度

第一章 总则

第一条 为规范应用系统开发项目管理流程，及时提供满足管理和业务需求的应用系统，结合公司实际情况，特制定本制度。

第二条 本制度适用于江门市红十字会应用系统开发管理、二次开发管理等工作。

第三条 对于外包开发项目，合作方为软件或服务供应商。

第四条 办公室负责软件开发管理制度的制定和修订。

第二章 开发职责

第五条 需求提交部门职责：

业务部门负责需求的提出、参与需求规格说明书业务部分的制定、参与需求审核及演示版审核、负责用户测试的业务部分、配合安装部署试运行和产品验收。

第六条 办公室职责：

负责受理业务部门提出的需求，进行需求分析，同时需要进行安全分析，主持需求规格说明书、概要设计、演示版的审核；负责质量控制，组织产品验收和正式投产使用；负责软件开发过程中的整体协调工作。

第七条 合作方职责：

负责进行需求分析、概要设计、详细设计、代码编制、测试、安装部署和验收。

第三章 外包软件开发要求

第八条 在外包软件开发过程中，应根据开发要求的技术指标对软件进行功能和性能测试。

第九条 在软件安装之前需检测软件包中可能存在的恶意代码。

第十条 开发单位应提供软件设计的相关文档和使用指南（如需求分析说明书、软件设计说明书、软件操作手册、软件源代码文档等）。

第十一条 开发单位应提供软件源代码，并审查软件中可能存在的后门。

第四章 软件开发工作程序

第十二条 提出需求：业务部门提出开发的应用软件的需求，具体包括：时间要求、功能要求、权限控制、安全要求和业务流程。

第十三条 受理：办公室在接到业务部门的要求后，立即着手安排各项准备工作，制定任务计划，包括人力资源的考虑和时间要求的考虑，向合作方提出开发要求。

第十四条 需求分析：合作方在接到开发要求后，与办公室共同进行需求分析。

第十五条 需求审核：办公室组织业务部门和合作方共同进行需求规格说明书的审核，合作方提供审核所需的材料和需求规格说明书，负责技术问题的解释。业务部门应认真审核需求规格说明书所描述的内容是否符合业务和管理要求，如果不符合要求办公室和合作方重新进行需求分析，直到审核通过为止，业务部门签字认可。

第十六条 概要设计：合作方对审核通过后的需求按软件开发标准开始进行概要设计。

第十七条 概要设计审核：办公室组织业务部门对合作方的概要设计进行审核，包括：是否符合业务部门提出的业务和管理要求，是否符合软件开发标准的要求，结构是否合理。审核未通过，合作方重新进行概要设计。

第十八条 演示版开发：合作方对概要设计通过后的需求进行演示版的开发，完成所有界面设计、业务流程和功能规划。

第十九条 演示版的审核：办公室组织业务部门和合作方共同进行演示版的审核，业务部门要对界面、业务流程和功能划分进行确认，如未达到业务部门的要求，重新进行演示版的开发，直到审核通过为止，业务部门签字认可。

第二十条 详细设计和代码编制：合作方对演示版审核通过后的应用开始进行详细设计和代码编写，并按软件

开发标准文档补充和完善详细设计说明书。合作方对代码编写完的应用产品编写安装维护手册、升级安装手册、用户操作手册、测试用例报告，并进行多种方式的测试，包括：开发人员自身的测试、测试人员的测试，测试环境的测试，测试的内容不仅需要包含功能需求，也需要包含业务系统的安全需求，测试人员在测试完成后应编制测试报告，如果出现 BUG 或者不满足安全需求，要求填写 BUG 记录表，开发人员修订程序代码，直到测试完全通过。

第二十一条 安装部署试运行：办公室根据安排通知合作方开始安装部署试运行事件。由办公室组织业务部门进行安装部署试运行工作，并由业务部门负责用户测试工作。

第二十二条 试运行审核：办公室组织业务部门试运行进行审核，审查测试用例、报告测试报告以及相关的技术文档，对程序中的关键点和安全需求按照测试用例报告进行严格测试，业务部门应配合办公室对应用产品进行试用，验证产品功能是否满足业务和管理要求，如果试用过程中发现不符合业务和管理要求，应认真填写问题反馈意见。如果业务部门反馈意见表明试运行不合格，办公室将要求合作方重新进行代码编写和测试，直到试运行通过。

第二十三条 产品验收：办公室组织业务部门对合作方提交的应用产品进行验收，主要根据试运行用户测试结

果和合同中规定的验收文档和其他要求进行验收工作，办公室负责严格检查技术文档，业务部门负责严格检查业务操作文档，并各自出具验收报告，由办公室汇总项目验收报告后报项目领导小组。若验收不合格，由办公室与合作方重新商定验收时间，择日进行，直到验收通过。

第二十四条 投产上线：在产品正式投产使用前，办公室负责对系统的基础架构平台进行安全检测与评估，安全检测的范围包含但不仅限于：操作系统、数据库、网络、信息系统功能隐患、结构合理性、源代码缺陷、服务能力（压力测试）。办公室确认该系统满足信息安全基线要求后，产品才可以正式的投产使用。

第二十五条 记录归档：办公室在项目结束后将所有记录根据档案管理的要求进行归档工作。

江门市红十字会审批管理制度

第一章 总则

第一条 为加强信息系统相关活动的授权和审批管理，规范审批程序，提高办事效率，保障资源的合理利用，结合江门市红十字会实际情况，特制定本制度。

第二条 本制度适用于江门市红十字会审批管理工作。

第三条 办公室负责审批管理制度的制定和修订。

第二章 职责分工

第四条 各部门承担本部门内各类事项授权和审批的管理工作。

第五条 根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。

第六条 涉及跨部门的重大事项授权和审批，应由江门市红十字会主管信息化与安全工作的领导牵头，各相关部门参与，共同确定审批事项、授权人和被授权人，确定后将结果上报江门市红十字会信息安全领导小组，领导小组审批后通过。

第三章 重要活动审批管理

第七条 信息系统相关重要活动主要包括对网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资

源的变更、操作、访问和接入等内容。

第八条 针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动进行逐级审批。

第九条 严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

第十条 完善系统外部连接管理，保证所有与外部系统的连接均得到授权和批准，并对授权和批准过程进行记录和保存。

第十一条 信息系统变更类事项主要包括以下方面：

(一)调整和更改网络设备、服务器、操作系统等各类设备和系统的配置参数；

(二)设备硬件更换；

(三)网络结构调整、网络连接更改；

(四)应用程序软件包修改；

(五)应用系统新需求/新功能的开发；

(六)系统数据库修改；

(七)产品版本升级；

(八)新技术的使用；

(九)组织策略和规程的更改。

上述变更内容涉及设备、系统自身的变更应由办公室

主管领导进行审核和批准；涉及全网或跨部门的变更应由办公室审核，单位信息安全领导小组审批。

第十二条 应确保信息系统的变更符合本单位总体安全策略要求。

第十三条 信息系统重要操作类事项包括以下方面：

(一)重要服务器、交换机、路由器、网络安全设备的启动、关闭；

(二)系统用户账号的增加、删除和权限修改；

(三)系统漏洞扫描、风险评估和渗透测试。

上述操作事项涉及单个信息系统自身的重要操作应由办公室主管领导进行审核和批准；可能影响骨干网络正常运行、多个业务系统运行或跨部门的操作应由办公室审核，信息安全领导小组审批。

第十四条 本单位机房物理环境的访问应按照《机房管理制度》进行审批管理。

第十五条 本单位系统接入类事项审批要求：

(一)新设备入网应按照机房管理相关办法进行审批；

(二)新业务系统接入，仅涉及单个信息系统的应由办公室主管领导进行审核和批准；可能影响骨干网络正常运行、多个业务系统运行或跨部门的操作应由办公室审核，信息安全领导小组审批。

第十六条 其他信息系统重要活动的审批流程遵照本

单位相关工作流程处理。

第十七条 审批需经过多级审批，对审批过程进行记录并保存审批文档。

第十八 条应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，经过办公室审核，不断调整更新审批事项。

江门市红十字会用户标识与口令管理指南

第一章 目的

第一条 密码是信息系统认证的重要手段，加强密码管理是信息安全的重要组成部分。为了加强江门市红十字会密码管理，确保信息安全，保护江门市红十字会的合法利益，必须建立严格的管理制度，规范密码设置、修改、保存的行为，确保信息系统的安全。

第二章 使用范围

第二条 适用于江门市红十字会所有系统、服务器、主机、数据库密码管理。

第三章 密码管理

第三条 由单位办公室负责此规定的执行。

1、密码管理人员职责

（1）负责密码的日常维护、定期修改

（2）负责陪同、监管其他需要该密码登录系统的维护人员

第四条 管理规定

1、密码管理的范围包括：网络、服务器系统、数据库系统、中间件系统、VPN、应用系统等相关的需要通过密码认证的信息统。为了区分不同的管理要求，我们将密

码管理分为三个大类，分别规范其管理细则：

（1）系统级密码：涉及公共设施如：网络交换机、防火墙、服务器系统、数据库系统、中间件系统、邮件及应用系统的超级管理员等系统管理的账户密码。

（2）VPN 密码：通过 VPN 方式登录系统的账户及密码。

（3）普通用户密码：各应用系统普通使用人员的账户及密码。

2、系统级密码管理细则

（1）确保密码存放在安全的环境中，密码不应在计算机上以未加密的形式进行存储、保管。

（2）明确责任，系统级密码应由专人负责维护管理，

（3）密码由密码管理人负责维护管理。密码管理人不应通过电子邮件、电话、传真、或口头告知等任何方式将密码泄露给第三人。其他人员需要密码执行操作，需要密码管理人员在场输入密码并全程陪同，直至退出系统。

（4）使用密码登录系统后，密码管理人员不应离开登录机器。如需离开，应退出登录后方可离开。系统使用完成后及时退出界面。

（5）机器上不应设置自动保存登录密码功能。

（6）系统级密码应至少定期更换，确保系统安全。

（7）密码应有一定复杂性。重要密码要求最少 6 位

以上；最少包括一个英文字母，一个数字，一个特殊字符；不能与用户相同；不能使用系统缺省密码。

（8）如果系统支持失败锁定功能，系统应设置失败登录次数，超过失败登录次数后，账户自动锁定。

第五条 VPN 密码管理细则

1、办公室应设置专人负责 VPN 密码管理、分配。

2、VPN 开通应由 OA 审批认可后方可开通。审批内容包括：申请人、申请原因、使用时间范围、账户名称等信息。

3、VPN 管理人员根据 OA 审批内容开启 VPN 账户。

4、VPN 账户应有一定复杂性，要求最少 6 位以上；最少包括一个英文字母，一个数字，一个特殊字符；不能与用户相同；不能使用系统缺省密码。

5、在使用时间到期后，VPN 管理人员应及时关闭 VPN 账户。

6、VPN 账户根据 OA 申请单建立有使用时间范围的账户，VPN 管理人员应定期检查 VPN 账户使用情况，对可以停用的 VPN 账户及时关闭 VPN 账户。

7、VPN 的开启、关闭均应保留完整 OA 申请记录。

8、VPN 账户专人专用，同一 VPN 账户不应多人共同使用。

9、VPN 账户使用人应妥善保管密码，密码不应以不

加密的方式保存在计算机上。

10、VPN 登录不能设置为自动保存密码登录。

11、VPN 账户登录后应由该账户使用人操作计算机，在使用过程中不应离开计算机。使用结束后及时退出 VPN 登录。

第六条 普通用户密码管理细则

1、账户使用人应妥善保管密码，密码不应以不加密的方式保存在计算机上。

2、涉及安全等级保护的系统不能设置为自动保存密码登录。

3、用户登录后应由该账户使用人操作计算机，在使用过程中不应离开计算机。使用结束后及时退出系统。

4、账户专人专用，同一账户不应多人共同使用。

5、密码应定期更换，重要的涉密系统要求每季度更换密码。

6、密码应保持一定复杂性。重要的涉密系统要求最少 6 位以上；最少包括一个英文字母，一个数字，一个特殊字符；不能与用户相同；不能使用系统缺省密码。

7、如果应用程序支持失败锁定功能，应设置失败登录次数，超过失败登录次数后，账户自动锁定。

8、涉及到重要涉密系统的应用账户丢失密码或账户锁定后，需通过 OA 提出申请，经批准后由系统管理人员

重新设置密码。用户在获得新密码进入系统后应立刻修改缺省密码。

第七条 应用程序应符合的密码管理规范

1、系统在正式交付使用后，不允许任何未经授权的非法登录。

2、应用用户登录密码在系统中加密存放。系统管理员无法通过应用程序或查询数据库等方式获得用户密码。

3、系统管理员可以重新设置用户密码。

4、应用使用人员可以自己重新设置密码。

5、应用系统具有失败登录多次后账户锁定的功能。

6、密码具有一定的复杂性管理。与用户名相同的或过于简单的密码不允许设定。

7、重要涉密系统密码必须定期更换，否则账户将被自动锁定。

8、重要涉密系统具有密码更换提示功能，在账户锁定前及时提醒用户更换密码。

江门市红十字会用户个人信息

数据分级防护管理规定

第一章 总则

第一条为规范单位产品的信息安全管理水平，保障我单位统业务正常进行，使全体工作人员了解信息安全工作要求，并落实到实际工作中，推动信息安全保障工作的顺利进行，结合单位的实际情况，特制订此管理规定。

第二条本规定适用于江门市红十字会全体工作人员。

第三条江门市红十字会信息安全领导小组负责此规定的制定、落实。

第二章 用户个人信息的定义分类

综合考虑我单位所运营的平台系统中用户个人信息的属性和类型特征，参照 YD/T 2781-2014《电信与互联网服务用户个人信息保护定义及分类》，将平台中用户个人信息分为用户身分和鉴权信息、用户数据和服务内容信息以及用户服务相关信息三类：

1.用户身份和鉴权信息是能够单独或与其它信息结合，对用户自然人身份进行识别，和代替用户自然人属性在信息系统中使用的虚拟身份信息，也包括用户验证身份

的鉴权相关信息；

2.用户数据和服务内服信息是应用系统在提供服务过程中收集的具有用户隐私属性的数据和内容信息；

3.用户服务相关信息是应用系统在服务过程中所收集的服务使用情况及服务相关辅助类信息。

（1）、用户身份和鉴权信息

用户身份及安全信息包括用户自然人身份和表示信息以及用户虚拟身份和鉴权信息两个子类；如下表所示:

子类　范围　信息举例

A1 用户自然人身份和标识信息 A1-1 用户基本资料　姓名、证件类型及号码、年龄、性别、职业、工作单位、地址、宗教信仰、民族、国籍等

A1-2 身份证明身份证、驾驶证、社保卡、护照等证件的影印件等

A1-3 生理标识指纹、声纹、虹膜、脸谱等

A2 用户虚拟身份和鉴权信息　A2-1 普通服务身份标识和鉴权信息　电话号码、账号、邮箱地址、用户个人数字证书以及服务涉及的密码、口令、密保答案等

A2-2 交易类服务身份标识和鉴权信息 各类交易账号和相应的密码、密码保护答案等

（2）、用户数据和服务内容信息

用户数据和服务内容信息包括用户服务内容和资料

数据以及用户设计内容信息两个子类；如下表所示：

子类　范围　信息举例

B1 用户服务内容和资料数据　B1-1 服务内容信息　平台服务内容信息，通过互联网传输的涉及个人信息的数据文件等

B1-2 联系人信息 通讯录、好友列表、群组列表等用户资料数据等

B1-3 用户私有资料数据用户存储、终端等存储用户文字、多媒体等资料数据信息等

B2 用户社交内容信息 B2-1 私密社交内容　对特定用户群体发布的社交信息，如群组内发布内容、设置权限博客内容等

（3）、用户服务相关信息

用户服务相关信息包括服务使用信息和设备信息两个子类；如下表所示：

子类　范围　信息举例

C1 用户服务使用信息 C1-1 业务订购、订阅关系 业务订购、业务注册时间、修改和注销状况信息等

C1-2 服务记录和日志 Cookie、访问记录、终端 session、账单记录等

C1-3 消费信息和账单 停开机、入网时间、在网时间、信用等级、缴费状态等

C1-4 位置信息 用户所在的经纬度、住址信息等

C2 用户设备信息 C2-1 设备信息硬件型号、唯一设备识别码、SIM 卡信息等

第三章 用户个人信息防护的分级

本规定中用户个人信息防护分级的对象是本单位所开发运营的所有互联网应用平台。

用户个人信息保护分级的目标是根据本规定对平台中的用户个人信息保护级别进行划分，以提高平台系统的整体数据安全性。

本单位所开发运营维护的互联网应用平台应按照本规定中规定的分级方法对其提供的应用服务中的用户个人信息进行分级。

本规定中针对不同类型和级别的应用平台提出不同的用户个人信息保护要求，遵循同级别的不同类型服务应当承担同等程度的用户个人信息保护要求的原则。应用系统应按照相应级别的管理要求及技术要求对其提供服务过程中涉及的用户个人信息的收集、存储、转移、使用和销毁等工作流程进行规范化管理。

3.1 级别划分

应用系统用户个人信息保护级别划分的原则:根据应用系统所收集、存储、转移和使用的用户个人信息确定服务的用户个人信息保护级别。本规定按照 YD/T

2781-2014《电信与互联网服务用户个人信息保护定义及分类》中定义的用户个人信息分类，确定应用系统的用户个人信息保护级别。

依据 YD/T 2782-2014《电信和互联网服务用户个人信息保护 分级指南》对应用系统用户个人信息进行级别划分，该标准将互联网服务的用户个人信息保护级别由低到高划分为 1-5 级，服务所收集、存储、转移和使用的用户个人信息敏感性越高，该服务的用户个人信息保护级别就越高。按照用户个人信息保护分级方法确定服务的用户个人信息保护级别后，服务提供方应按照对应级别 所规定的要求在收集和使用个人信息过程中提供相应的保护机制。由于服务内容发生变化而导致收集、存储、转移和使用过程中涉及的用户个人信息发生变化时，应对该服务重新分级。

3.2 分级方法

(1)第 5 级服务的分级方法及基本保护要求

第 5 级服务分级要素包括(以下分级要素依据 YD/T 2781-2014《电信和互联网服务用户个人信息保护定义及分类》的规定):

— AI-2(身份证明):包括但不限于身份证、军官证、护照、驾照、社保卡等影印件;

— AI-3(生理标识):包括但不限于指纹、声纹、虹膜、

脸谱等;

— A2-2(交易类服务身份标识和鉴权信息):包括但不限于各类交易账号和相应的密码、密码保护答案等。

如果应用系统在提供服务过程中涉及第 5 级分级要素，则该服务的用户个人信息保护级别为 5 级。第 5 级服务基本保护要求:第 5 级分级要素应实施严格的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，确保用户个人信息访问控制安全，建立严格的用户个人信息安全管理规范以及数据实时监控机制。例如，在收集、转移和使用用户个人信息时应征得用户同意，在信息的存储以及收集和转移的传输过程应使用高强度的加密措施，保障数据的机密性和完整性，应对信息采取严格的访问控制措施，应定义严格的用户个人信息各生命周期 (包括信息收集、生成、存储、使用、传输和销毁等各个环节)安全管理规范，应设置内部的数据审批流程及制度，并对用户个人信息的 使用进行实时监控及预警。

第 5 级服务中涉及到的其他级别的分级要素，其保护要求见相应级别服务的保护要求。

（2）第 4 级服务的分级方法及基本保护要求

第 4 级服务分级要素包括 (以下分级要素依据 YD/T 2781-2014《电信和互联网服务用户个人信息保护定义及

分类》的规定):

— AI-1(用户基本资料):包括但不限于姓名、证件类型及号 码、年龄、性别、职业、工作单位、 地址、宗教信仰、民族、国籍等;

— B1-2(联系人信息):包括但不限于通信录、好友列表、群组列表等用户资料数据;

— C1-4(位置信息):包括但不限于用户所在的经纬度、住址信息、小区代码和基站号等。

如果应用系统在提供服务过程中未涉及第 5 级服务分级要素，但涉及第 4 级服务分级要素，则该服务的用户个人信息保护级别为 4 级。第 4 级服务基本保护要求:针对第 4 级分级要素应实施必要的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，确保用户个人信息访问控制安全，建立用户个人信息安全管理规范以及数据准实时监控机制。例如，在收集和转移用户个人信息时应征得用户同意，在信息的收集和转移的传输过程应采取必要的加密措施，保障数据的机密性和完整性，应对信息采取严格的访问 控制措施，应定义严格的用户个人信息各生命周期 (包括信息收集、生成、存储、使用、传输和销毁等各个环节)安全管理规范，应设置内部的数据审批流程及制度，并对用户个人信息的使用进行准实时监控及预警。

第 4 级服务中涉及到的其他级别的分级要素，其保护要求见相应级别服务的保护要求。

（3）第 3 级服务的分级方法及基本保护要求

第 3 级服务分级要素包括（以下分级要素依据 YD/T 2781-2014《电信和互联网服务用户个人信息保护定义及分类》的规定):

— A2-1(普通服务身份标识和鉴权信息):包括但不限于电话号码、账号、邮箱地址、用户个人数字证书以及服务涉及的密码、口令、密码保护答案等;

— B1-1(服务内容信息): 平台服务内容信息，通过互联网传输的涉及个人信息的数据文件等;

— B1-3(用户私有资料数据):包括但不限于用户存储、终端等存储用户文字、多媒体等资料数据信息等;

— B2-1(私密社交内容):包括但不限于对特定用户群体发布的社交信息，如群组内发布内容、 设置权限博客内容等;

— C1-2(服务记录和日志): Cookie、访问记录、终端 session、账单记录等；

—C2-1(设备信息): 硬件型号、唯一设备识别码、SIM 卡信息等。

如果应用系统在提供服务过程中未涉及第 4 级、第 5 级服务分级要素，但涉及第 3 级服务分级要素，则该服务

的用户个人信息保护级别为 3 级。

第 3 级服务基本保护要求:针对第 3 级分级要素应实施基本的技术和管理措施，保护用户的知情权和选择权，确保用户个人信息访问控制安全，建立用户个人信息安全管理规范。例如，在收集和转移用户个人信息时应征得用户同意，应对信息采取必要的访问控制措施，应定义用户个人信息各生命周期(包括信息收集、生成、存储、使用、传输和销毁等各个环节)安全管理规范。

第 3 级服务中涉及到的其他级别的分级要素，其保护要求见相应级别服务的保护要求。

（4）第 2 级服务的分级方法及基本保护要求

第 2 级服务分级要素包括（以下分级要素依据 YD/T 2781-2014《电信和互联网服务用户个人信息保护定义及分类》的规定):

C1-3(消费信息及账单): 停开机、入网时间、在网时间、信用等级、缴费状态等。

如果应用系统在提供服务过程中未涉及第 3 级、第 4 级、第 5 级服务分级要素，但涉及第 2 级服务分级要素，则该服务的用户个人信息保护级别为 2 级。

第 2 级服务基本保护要求:针对第 2 级分级要素应实施基本的技术和管理措施，保护用户知情权和选择权，确保用户个人信息访问控制安全。例如，在转移用户个人信

息时应征得用户的同意，应对信息采取必要的访问控制措施。

第 2 级服务中涉及到的其他级别的分级要素，其保护要求见相应级别服务的保护要求。

（5）第 1 级服务的分级方法及基本保护要求

第 1 级服务分级要素包括 (以下分级要素依据 YD/T 2781-2014《电信和互联网服务用户个人信息保护定义及分类》的规定):

C1-1(业务订购关系):包括但不限于业务订购信息、业务注册时间、修改、 注销状况信息等

如果应用系统在提供服务过程中未涉及第 2 级、第 3 级、第 4 级、第 5 级服务分级要素，但涉及第 1 级服务分级要素，则该服务的用户个人信息保护级别为 1 级。

第 1 级服务基本保护要求:针对第 1 级分级要素应实施基本的技术和管理措施确保用户个人信息访问控制安全。例如，应对用户个人信息采取必要的访问控制措施。

江门市红十字会用户信息收集及使用规定

第一章 总则

为了加强单位对用户个人信息收集、使用及相关活动的记录，保护用户的合法权益，维护平台信息安全，我单位开展贯彻《电信和互联网服务用户个人信息保护分级指南》和《信息安全技术个人信息安全规范》国际标准工作。

《电信和互联网服务用户个人信息保护分级指南》和《信息安全技术个人信息安全规范》是企业的法规性文件，是指导企业建立用户个人信息安全管理体系的纲领和行动准则，体现企业对社会的承诺。

第二章 目的

为了使单位对客户信息资源的管理规范化、有效化，单位应按照相应级别的管理要求及技术要求对提供服务过程中涉及的用户个人信息的收集、存储、转移、使用和销毁等工作流程进行规范化管理。

第三章 范围

对于单位产品所涉及的任何个人信息，单位规定明确，除法律、法规规定外，未经用户同意，单位不得收集与用户相关、能够单独或者与其他信息结合识别用户身份的信息，包括用户姓名、出生日期、身份证件号码、住址等身

份信息以及用户使用服务的号码、账号、时间、地点等日志信息，并明确告知用户收集个人信息的方式、内容和途径。

第四章 个人信息安全基本原则

（1）权责一致原则：对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任；

（2）目的明确原则：具有合法、正当、必要、明确的个人信息处理目的；

（3）选择同意原则：向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意；

（4）最少够用原则：处于个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息；

（5）公开透明原则：以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

（6）确保安全原则：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；

（7）主体参与原则：向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

第五章 个人信息的收集

5.1 对个人信息的合法性要求

（1）不得欺诈、诱骗、强迫个人信息主体提供其个人信息；

（2）不得隐瞒产品或服务所具有的收集个人信息的功能；

（3）不得从非法渠道获取个人信息；

（4）不得非法手机法律法规明令禁止手机的个人信息。

5.2 对个人信息的最小化要求

（1）收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现。

（2）自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率。

（3）间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

5.3 收集个人信息时的授权同意

（1）收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则(例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关

情况等)，并获得个人信息主体的授权同意。

（2）间接获取个人信息时：

a）应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

b）应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等；如本组织开展业务需进行的个人信息处理活动超出该授权同意范围，应在获取个人信总后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。

5.4 征得授权同意的例外

以下情形中，个人信息控制者收集、使用个人信息无需征得个人信息主体的授权同意：

（1）与国家安全、国防安全直接相关的；

（2）与公共安全、公共卫生、重大公共利益直接相关的；

（3）与犯罪侦查、起诉、审判和判决执行等直接相关的；

（4）出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；

（5）所收集的个人信息是个人信息主体自行向社会公众公开的，从合法公开披露的信息中收集个人信息的，

如合法的新闻报道、政府信息公开等渠道；

（6）根据个人信息主体要求签订和履行合同所必需的；

（7）用于维护所提供的产品或服务的安全稳定运行所必需的,例如发现、处置产品或服务的故障；

（8）个人信息控制者为新闻单位，且其在开展合法的新闻报道所必需的；

（9）个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；

（10）法律法规规定的其他情形。

第六章 个人信息的保存

6.1 外个人信息保存时间最小化

对个人信息控制者的要求包括：

（1）个人信息保存期限应为实现目的所必需的最短时间；

（2）超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理。

6.2 去标识化处理

收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的

数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。

6.3 个人敏感信息的传输和存储

对个人信息控制者的要求包括：

（1）传输和存储个人敏感信息时,应采用加密等安全措施；

（2）存储个人生物识别信息时,应采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要。

6.4 个人信息控制者停止运营

当个人信息控制者停止运营其产品或服务时,应：

（1）及时停止继续收集个人信息的活动；

（2）将停止运营的通知以逐一送达或公告的形式通知个人信息主体；

（3)对其所持有的个人信息进行删除或匿名化处理。

第七章 个人信息的使用

7.1 个人信息访问控制措施

对个人信息控制者的要求包括：

（1）对被授权访问个人信息的内部数据操作人员，应按照最小授权的原则，使其只能访问职责所需的最少够用的个人信息，且仅具备完成职责所需的最少的数据操作权限；

（2)应对个人信息的重要操作应设置内部审批流程，

如批量修改，拷贝、下载等；

（3）应对安全管理人员、数据操作人员、审计人员的角色进行分离设置；

（4）如确因工作需要，需授权特定人员超权限处理个人信息的，应由个人信息保护责任人或个人信息保护工作机构进行审批,并记录在册；

（5）对个人敏感信息的访问、修改等行为，宜在对角色的权限控制的基础上，根据业务流程的需求触发操作授权。例如，因收到客户投诉，投诉处理人员才可访问该用户的相关信息。

7.2 个人信息的展示限制

涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如，在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

7.3 个人信息的使用限制

对个人信息控制者的要求包括：

（1）除目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户面像；

（2）对所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合识别自然人个人身份，或者反映自然人个人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。

注：加工处理而产生的个人信息属于个人敏感信息的，对其处理应符合本标准对个人敏感信息的要求。

（3）使用个人信息时，不得超出与收集个人信息时所声称的目的具有直接或合理关联的范围，因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。

注：将所收集的个人信息川于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，应对结果中所包含的个人信息进行去标识化处理

7.4 个人信息的访问

个人信息控制者应向个人信息主体提供访问下列信息的方法：

（a）其所持有的关于该主体的个人信息或类型；

（b）上述个人信息的来源、所用于的目的；

（c）已经获得上述个人信息的第三方身份或类型。

注：个人信息主体提出访问非其主动提供的个人信息

时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，做出是否响应的决定，并给出解释说明。

7.5 个人信息的更正

个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。

7.6 个人信息的删除

对个人信息控制者的要求包括：

（1）符合以下情形的，个人信息主体要求删除的，应及时删除个人信息：

a）个人信息控制者违反法律法规规定，收集、使用个人信息的；

b）个人信息控制者违反了与个人信息主体的约定，收集、使用个人信息的。

（2）个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除。

（3）个人信息控制者违反法律法规规定或与个人信息主体的约定，公开披露个人信息，且个人信息主体要求

删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

7.7 个人信息主体撤回同意

对个人信息控制者的要求包括：

（1）应向个人信息主体提供方法撤回收集、使用其个人信息的同意授权，撤回同意后，个人信息控制者后续不得再处理相应的个人信息；

（2）应保障个人信息主体拒绝接收基于其个人信息推送的商业广告的权利，对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回同意的方法。

7.8 个人信息主体注销账户

对个人信息控制者的要求包括：

（1）通过注册账户提供服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且该方法应简便易操作；

（2）个人信息主体注销账户后，应删除其个人信息或做匿名化处理。

7.9 个人信息主体获取个人信息副本

根据个人信息主体的请求，个人信息控制者应为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下个人信息的副本传递给第三方：

（1）个人基本资料、个人身份信息；

（2）个人健康生理信息、个人教育工作信息。

7.10 约束信息系统自动决策

当仅依据系统的自动决策而做出显著影响个人信息主体权益的决定时（例如基于画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制着应向个人信息主体提供申述方法。

第八章：个人信息安全事件处置

8.1 安全事件应急处置和报告

对个人信息控制者的要求包括：

（1）应制定个人信息安全事件应急预案；

（2）应定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程；

（3）发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行以下处置：

a）记录事件内容,包括但不限于：

发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

b）评估事件可能造成的影响,并采取必要措施控制事态，消除隐患；

c）按《国家网络安全事件应急预案》的有关规定及时上报，报告内容包括但不限于：

涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施事件处置相关人员的联系方式；

（4)根据相关法律法规变化情况,以及事件处置情况,及时更新应急预案。

8.2 安全事件告知

对个人信息控制者的要求包括：

（1）应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

（2）告知内容应包括但不限于：

a）安全事件的内容和影响；

B）已采取或将要采取的处置措施；

c）个人信息主体自主防范和降低风险的建议；

d）针对个人信息主体提供的补救措施；

e）个人信息保护负责人和个人信息保护工作机构的联系方式。

第九章 组织的管理和要求

9.1 明确责任部门与人员

对个人信息控制者的要求包括：

（1）应明确其法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等；

（2）应任命个人信息保护负责人和个人信息保护工作机构。

（3）满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作：

a）主要业务涉及个人信息处理，且从业人员规模大于 200 人；

b）处理超过 50 万人的个人信息，或在 12 个月内预计处理超过 50 万人的个人信息。

（4）个人信息保护负责人和个人信息保护工作机构应履行的职责包括但不限于：

a）全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；

b）制定、签发、实施、定期更新隐私政策和相关规程；

c）应建立、维护和更新组织所持有的个人信息清单(包括个人信息的类型、数量、来源、接收方等)和授权访问策略；

d）开展个人信息安全影响评估；

e）组织开展个人信息安全培训；

f）在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为；

g）进行安全审计。

9.2 开展个人信息安全影响评估

对个人信息控制者的要求包括：

（1）建立个人信息安全影响评估制度，定期（至少每年一次）开展个人信息安全影响评估；

（2）个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于：

a）个人信息收集环节是否遵循目的明确、选择同意、最少够用等原则；

b）个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括处理是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等；

c）个人信息安全措施的有效性；

d）匿名化或去标识化处理后的数据集重新识别出个人信息主体的风险；

e）共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；

f）如发生安全事件，对个人信息主体合法权益可能产生的不利影响。

（3）在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，应重新进行个人信息安全影响评估。

（4）形成个人信息安全影响评估报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平；

（5）妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。

9.3 数据安全能力

个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失。

9.4 个人管理与培训

对个人信息控制者的要求包括：

（1）应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查；

（2）应明确内部涉及个人信息处理不同岗位的安全职责，以及发生安全事件的处罚机制；

（3）应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；

（4）应明确可能访问个人信息的外部服务人员应遵

守的个人信息安全要求，与其签署保密协议，并进行监督。

（5）应定期（至少每年一次）或在隐私政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

9.5 安全审计

对个人信息控制者的要求包括：

（1）应对隐私政策和相关规程，以及安全措施的有效性进行审计；

（2）应建立自动化审计系统，监测记录个人信息处理活动；

（3）审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；

（4）应防止非授权访问、篡改或删除审计记录；

（5）应及时处理审计过程中发现的个人信息违规使用、滥用等情况。