黄石市大数据信息发展有限公司

安全生产管理制度（试行）

文档版本 V1.0

黄石大数据信息发展有限公司

目录

前言.....1
各级各部门安全生产责任制度篇.....1
成立安全生产小组.....1
总经理（法定代表人）安全责任制.....1
部室负责人责任制.....2
项目安全运维部门负责人安全生产责任制.....3
财务部门安全责任制.....3
办公室安全责任制.....4
安全规章制度篇.....4
办公区域安全生产（暂行）管理办法.....4
第一章 总 则.....4
第二章 消防安全管理.....5
第三章 防盗安全管理.....5
第四章 用电安全管理.....6
第五章 信息网络安全管理.....6
第六章 相关事项.....7
项目施工现场安全生产管理办法.....7
第一章 施工组织设计与专项安全施工方案编审制度.....7
第二章 安全技术措施计划执行制度.....9
第三章 安全技术交底制度.....10
第四章 架体设备安装验收制度.....11
第五章 施工机具进场验收与保养维修制度.....11
第六章 安全生产检查制度.....12
第七章 安全教育培训制度.....13
第八章 伤亡事故快报制度.....15
第九章 考核制度.....17
第十章 项目组安全活动制度.....19
第十一章 门卫值班和治安保卫制度.....20
第十二章 消防防火责任制度.....21
第十三章 卫生保洁制度.....23
第十四章 不扰民措施.....24
信息安全安全生产管理办法.....25
第一章 信息安全方针及安全策略.....25
第二章 信息安全领导机构组成与职责.....31
第三章 安全检查和审核管理.....36
第四章 信息安全培训管理.....41
第五章 第三方安全管理规范.....46
第六章 网络与信息系统安全设计规范.....57
第七章 网络安全管理制度.....62
第八章 恶意代码防范管理.....66

第九章 变更管理程序.....69
第十章 备份与恢复管理.....73
第十一章 介质安全管理制度.....77
第十二章 资产安全管理制度.....80
第十三章 软件开发管理规范.....89
第十四章 代码编写安全规范.....107
第十五章 外包软件开发管理.....111
第十六章 服务商安全管理.....114
第十七章 系统安全管理制度.....116
第十八章 机房安全管理制度.....124
第十九章 安全和监控中心管理.....129
第二十章 主机运维操作规程.....131
第二十一章 系统交付管理.....134
第二十二章 信息系统应急预案管理.....136
第二十三章 安全事件/故障应急响应处理流程.....145
第二十四章 信息安全责任制.....156

前言

认真执行国家有关计算机软、硬件的法律、法规和规章制度，坚持“安全第一，预防为主”的方针，建立“管生产必须管安全”、“谁主管、谁负责”的安全生产管理责任制，设置安全生产管理机构，配备安全生产管理人员，落实各项安全生产制度，保证安全生产必要投入，制定切实可行的安全防范措施，强化企业安全管理自我约束机制，最大限度地为社会提供安全、及时、经济、方便、舒适的软件服务，实现企业价值最大化的目的。

各级各部门安全生产责任制度篇

成立安全生产小组

组长：胡海鹏

副组长：金伟

成员：刘建华、王朋、曹祥林、黄裕文

安全生产领导小组下设办公室，办公室设在公司的综合管理部，综合管理部负责人兼任办公室主任。

总经理（法定代表人）安全责任制

总经理（公司法定代表人），是公司安全生产第一责任人，其主要安全职责为：

1、总经理是本公司安全生产的第一责任人，对本公司的

安全生产工作负全面责任，总经理必须具备与本单位所从事的生产经营活动相应的安全知识和管理能力。

2、建立健全公司安全生产管理机构，按规定配备专职安全人员，形成安全管理网络，在计划、布置、检查、总结、评比生产的同时，要计划、布置、检查、总结、评比安全工作，牢固树立安全第一的思想，把安全工作真正纳入到议事日程。

3、定期召开安全办公会议，组织研究讨论和解决本公司安全的重大问题。

4、领导编制和实施本企业中、长期整体规划及年度、特殊时期安全工作实施计划。建立健全和完善本企业的各项安全生产管理制度及奖惩办法。

5、领导并支持安全管理人员或部门的监察工作。

6、定期组织本公司的安全检查，及时了解个项目的安全生产状况，对重大和危险隐患分别亲自组织解决和亲临现场处理，定期组织开展安全生产竞赛活动，提高职工安全防护意识与安全操作技能。

7、领导、组织本企业有关部门或人员，做好重大事故调查处理的具体工作，监督防范制度的制度和落实，预防事故的发生。

部室负责人责任制

1、部室负责人对总经理负责，对本企业的劳动安全生产和信息、网络保护负全面领导责任。在计划、布置、检查、

总结、评比生产的同时，要计划、布置、检查、总结、评比安全工作。

2、部室负责人必须坚持管生产必须管安全，谁主管谁负责的原则。

3、部室负责人执行生产与安全发生矛盾的时候，生产不行服从安全，也就是不安全不生产。

4、认真贯彻执行劳动保护和安全生产政策、法令和规章制度。

5、制定企业各级部门的安全责任制度等制度，建立健全安全生产的保证体系。

6、定期组织安全检查和开展安全竞赛等活动。

项目安全运维部门负责人安全生产责任制

1、因公司性质特殊，主要生产活动涉及安全方面主要以网络安全和信息安全为主，公司项目安全运维部门负责人对企业安全生产的技术工作负总的责任。

2、负责提出安全技术项目和实施措施，并组织实施。

3、组织对员工进行安全技术教育。

4、负责组织编制生产安全事故应急救援预案，并指导实施。

5、设立专门的安全责任人。

财务部门安全责任制

1、根据企业实际情况及企业安全技术措施实施的需要，按计划及时提取安全技术措施经费、领导保护经费及其他安

全生产所需经费，保证专款专用。

2、按照国家对劳动保护用品的有关标准和规定，负责审查购置劳动保护用品的合法，保证其符合标准。

办公室安全责任制

1、及时传达转发和组织学习党和国家的安全生产方针、政策、文件和规定。

2、协助安全好安全会议，安全检查及其他安全活动等各项工作。

3、宣传党和国家的安全生产方针、政策、法令，及时总结报道安全生产情况及整改情况。

4、及时宣传指导安全生产的先进事迹和好人好事，配合安全活动和安全生产竞赛，做好宣传鼓动工作。

5、配合其他部门做好事故的善后处理工作。

安全规章制度篇

办公区域安全生产（暂行）管理办法

第一章　总　则

第一条：为加强公司安全生产管理工作,增强员工的安全意识,落实各项安全措施,保证公司各项工作顺利开展,本着“预防为主，　杜绝隐忠”的原则，制定本制度。

第二条：本制度中的安全生产管理,包括消防、防盗、用电、项目建设、信息网络安全等方面。

第三条：综合管理部为公司安全生产管理部门，负责安

全防范措施的制订、落实、检查及安全实施的调查、处理等工作；各部门负责人负责本部门的安全生产管理工作。

第四条：本制度适用于公司所有部室。

第二章　消防安全管理

第五条：综合管理部不定期组织消防安全学习,开展多种形式的消防安全宣传教育。

第六条：综合管理部应按照消防法规和消防部门的要求，对设施设备的配置情况进行检查，发现问题立即整改。

第七条：综合管理部应对消防设施设备的性能情况不定期进行检查，确保消防栓、灭火器具等完好、有效，消防通道通畅，消防标语清晰、准确。

第八条：办公楼内严禁存放易燃易爆物品。

第九条：发生小火情应立即采取相应措施。（采用正确的灭火方法并选用适当的灭火工具积极扑救。当密闭的房间内起火，未准备好充足的灭火器材前，不要打开门窗。拨打“119”报警。说清地点、火势、报警人姓名及电话号码。报警后派人去街道路口迎候消防车）

第三章　防盗安全管理

第十条：员工就餐、休息、开会离开办公室 30 分钟以上的应锁门。

第十一条：办公室、会议室不允许供应商进入办公，供应商应在公司指定区域进行办公。

第十二条：员工不得在办公室存放私人贵重物品或大笔现金。公司停车场停车时应关锁门窗，车内不宜存放贵重

物品。

第四章　用电安全管理

第十三条：公司机房和办公区域应根据配电容量配置设施设备，并预留安全空间。

第十四条：员工使用各类设施设备时，应遵守相关的操作程序和要求，禁止违规操作以保障用电安全。

第十五条：除办公设备以外的电力设施设备的维修应交由专人修理，公司人员不得擅自维修。

第十六条：员工不得在办公区域私自用电，不得擅自使用电热器具；下班时间应切断办公设备、空调电风扇等各类电器的电源。

第五章　信息网络安全管理

第十七条：员工必须设置开机密码，员工离开座位时应及时对电脑屏幕进行锁屏，也必须设置屏幕保护（设置等待时间不得超过三十分钟，并且需勾选在恢复时启用登录页面）。

第十八条：员工不得让非公司员工独自操作员工电脑。

第十九条：由安全运维部出具网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。

第二十条：员工离岗（职）时须回收涉及公司业务的全部资料文档，取回工作牌、办公区域钥匙、徽章以及公司提供的软硬件设备，若涉及关键岗位，需对该员工离职前在公司负责相关项目的其他企业或局委办的负责人发出通告。

第六章　相关事项

第二十一条：各部室下班最后离开的员工应检查门窗及电源的安全情况。离开接待室、会议室也要及时关闭门窗和电源。

第二十二条：综合管理部定期检查各类防范设施的完好情况和安全防范措施的落实情况，发现问题及时整改。

第二十三条：出现各类安全问题时，综合管理部根据原因、性质、后果、责任等因素负责处理，并向总经理报告。

第二十四条：违反以上第八条、第十条、第十一条、第十四条、第十五条、第十六条、第十七条、第十八条、第十九条、第二十一条制度的部门或员工，由综合管理部进行记录，并在月底绩效考核中进行扣分，每次扣 1.5 分。

第二十五条：本制度自发布之日起执行。

项目施工现场安全生产管理办法

第一章　施工组织设计与专项安全施工方案编审制度

根据《中华人民共和国安全生产法》、《中华人民共和国劳动法》等法律法规的有关规定，为了从技术上和管理上采取有效措施，防止各类事故发生应制订本办法：

1、安全生产组织设计编审内容

（1）平面布置。在施工组织设计中，必须有详细的施工平面布置图，各种设施布局合理，道路坚实平坦，排水畅通，物料堆放整齐有序，符合安全、文明施工要求。

（2）土方工程。应根据基坑、沟渠、地下室等挖土深度和土质情况，选择合理开挖方法，确定边坡和采用支撑、支

护等，以防坍塌。

（3）编制施工临时用电方案，应按照《施工现场临时用电安全技术规范》进行编制。施工现场的各种电气线路及设备都必须规范，包括架空线安全距离，设置“三相五线制”和三级配电要求设置电箱，使用合格电气设备，采用三级漏电保护及“一机一闸一触保”等措施。

（4）脚手架搭设方案要符合规范，“四口”、“五临边”和立体交叉作业的防护要可靠，安全网（平网、立网）布设合理有效，网要有出厂合格证，不能以次充好，要保证质量。

（5）施工电梯、塔吊、井架位置恰当，牢固性、稳定性好，安全装置齐全、可靠。

（6）防火、防雷、防毒、防爆措施正确、有效。

（7）文明施工，减少噪声，控制烟尘，临街、近居民区工程采用全封闭作业。

2、特殊工程安全技术措施要求

所谓特殊工程是指结构复杂、超高层、跨度大、工艺要求高、所处位置特殊的工程，这些工程应编制单项安全技术措施。如爆破工程、大型吊装、沉箱、沉井、烟囱、水塔工程、特殊架设、超高层脚手架、井架搭设和拆除等，特殊工程的安全技术措施要有设计依据，强度计算，并有详图和文字说明。

3、季节性施工的安全技术措施。

（1）雨季施工，重点防坍塌、防雷击、防触电、防台风等。

（2）夏季施工，重点是做好防暑降温工作。

（3）冬季施工，重点防冻、防滑、防火防中毒等。

4、安全技术措施落实。

（1）开工前，工程项目经理或技术总负责人对施工员、班长和作业人员应进行交底，除口头外，应有书面材料，并履行双方签字手续，并注明交底日期。

（2）项目经理要注重在实施过程中的监督检查。

（3）项目部应建立实施技术措施计划目标管理考核制。

第二章　安全技术措施计划执行制度

安全技术措施计划（执行）是项目施工保障安全的指令性文件，具有安全法规的作用，必须认真编制和执行。

1、编制原则

编制安全技术措施计划要在编制施工计划的同时进行。安全生产技术措施计划的编制与执行要纳入项目建设的议事日程，并必须按设计者、审核者、批准者的会签程序后生效执行（特别是高层或难度大的施工项目）。

编制安全技术措施计划时应考虑到必须与可能、切实掌握好花钱少、效果大的原则，制定出科学、先进、可靠、实用的安全生产技术措施计划。

2、编制依据

编制时必须依据国家发布的劳动保护安全生产法规、法令和各项标准、规范、规章等；注重解决在实践中存在或在检查中发现亟待解决的问题；在技术革新与工艺改革中面临所需的新防护设施问题；针对不安全因素易造成伤亡事故或

职业病主要原因应采取的措施。

3、编制方法

要按照项目施工的实际进行编制，内容符合与安全技术和劳动保护有关的相关法律法规的有关规定。编制必须针对性强，对各种不同的工程结构、施工方法、作业条件等产生各个不相同的不安全因素，采取相应的对策、措施，为此首先要掌握项目工程概况。

4、执行程序

要认真进行分部分项的安全生产技术交底，安全技术措施中的各种安全设置、防护应列入施工任务单，责任落实到个人，并实行验收制度。

第三章　安全技术交底制度

安全技术交底是《建设工程安全生产管理条例》和《建筑施工安全检查标准》的法定工作要求，必须认真执行。

1、交底必须在施工作业前进行，任何项目在没有交底前不准施工作业。

2、交底工作一般在施工现场项目部实施。

3、交底必须履行交底人和被交底人的签字模式，书面交底一式二份，一份交给被交底人，一份附入安全生产台帐务查。

4、被交底者在执行过程中，必须接受项目部的管理、检查、监督、指导，交底人也必须深入现场，检查交底后的执行落实情况，发现有不安全因素，应马上采取有效措施，杜绝事故隐患。

第四章　架体设备安装验收制度

1、施工机械设备的操作人员必须身体健康，并按规定经过安全技术培训，取得操作证后，方可独立操作。

2、施工机械操作人员和配合工作人员，都必须按规定穿戴劳动保护用品，长发不得外露。高处作业必须挂好安全带，不得穿硬底鞋或拖鞋。严禁从高处投掷物件。

3、进场施工机械设备安装后必须按规定进行验收，合格方可使用，做好验收记录，验收人员履行签字手续。

4、施工机械设备应按其技术性能的要求正确使用。缺少安全装置或安全装置已失效的施工机械设备不得使用。严禁使用倒顺开关控制设备。

5、操作人员应熟悉作业环境和施工条件，听从指挥，遵守现场安全规则。当使用施工机械设备与安全发生矛盾时，必须服从安全的要求。

6、严禁拆除施工机械设备的自动控制机构、各种限位器等安全装置及监测、指示、仪表、警报等自动报警、信号装置。其调试和故障的排除应由专业人员负责进行。中小型建筑机械安装就位后，使用之前必须经过验收。

第五章　施工机具进场验收与保养维修制度

1、进场施工机械设备安装后必须按规定进行验收，合格方可使用，做好验收记录，验收人员履行签字手续。验收内容主要是：

（1）安装位置是否符合施工平面布置图要求。

（2）安装地基是否坚固，机械是否稳固，工作棚或操作

台搭设是否符合要求。

（3）传动部分是否灵活可靠，离合器是否灵活，制动器是否可靠，限位保险装置是否有效，机械的润滑情况是否良好。

（4）电气设备是否安全可靠，电阻摇测记录应符合要求，漏电保护器灵敏可靠，接地接零保护正确。

（5）安全防护装置完好，安全、防火距离符合要求。

（6）机械工作机构无损坏；运转正常，紧固件牢固。

（7）机械操作人员持证上岗。

2、机具的保养、维修是杜绝机械事故的关键工作，必须按规范标准和有关规程办。

（1）各种作业施工机械必须由专人负责保养、维修，并落实责任制，做到勤检查、勤保养、勤维修。

（2）严禁机具带病运作，杜绝不安全因素。

（3）不懂机械性能者不准从事保养、维修的工作。

（4）电器设备下班前应拉下闸刀，关闭好电箱，上班前持证上岗者必须检查试车正常后方可运转作业。

第六章　安全生产检查制度

安全生产检查是安全生产职能部门必须履行的职责，也是监督、指导、及时消除事故隐患、杜绝不安全因素的方法途径和有力措施，各级职能部门必须认真抓紧抓好这项工作。

1、检查内容

安全生产检查应根据施工（生产）季节、气候、环境的

特点，制定检查项目内容、标准，一般的检查内容包括检查思想、制度、机械设备装置、安全防护设施、安全教育、培训、操作行为、劳保用品使用、文明施工、伤亡事故处理等等。

2、检查评定标准

安全生产检查的评定标准按照《湖北省建设工程安全生产管理办法》的有关要求作为评定标准打分。

3、检查频率要求

公司除平时不定期抽查外，每年例行安全生产大检查不少于三次。部门每月不少于二次，项目组每周不少于一次自查自改。

4、检查、评比、消化

检查后必须进行评讲活动，每检查一次后出一次《通报》或《简报》，列入档案，并作为目标管理考核依据。对检查出来的不安全因素或事故隐患，出具整改单并落实“三定”工作（定人、定期限、定措施），做到及时复查验收，对整改不力者酌情处罚。

第七章　安全教育培训制度

安全教育是提高全员安全意识、安全素质的保证，必须认真抓好。

1、新人必须经过三级安全教育（公司、部门、项目组）方可参加施工。

2、工人变换工种，须进行新工种的安全技术教育并记录方可参加施工。

3、三级教育的时间一般不能少于50小时。（公司不少于15小时，部门不少于15小时，项目组不少于20小时）

4、特殊工种必须经过安全培训，考试合格后持证上岗作业。

5、定期轮训各级领导干部和安全管理人员，每年至少一至二次，不断提高安全意识、技术素质，提高政策业务水平。

6、安全教育内容是安全生产思想教育，从加强思想路线方针、政策和劳动纪律两个方面进行；从基本施工概况、施工工艺方法、危险区、危险部位及各类不安全因素和有关安全生产防护的基本知识入手，安全技能教育，结合各种专业特点，实施安全操作、规范操作的技能培训，使其熟悉掌握安全操作技术；事故教育可以使其从事故教训中吸取有益的东西，可预防类似事故的发生，法制教育可以激发人们自觉地遵纪守法，杜绝各类违章指挥、违章作业行为，这类教育可以定期或不定期地进行实施。在开展教育活动中，必须结合先进的典型事例进行正面教育，以利取长补短，保障安全生产。安全教育要求体现“六性”，即全员性、全面性、针对性以及成效性、发展性、经常性。

7、要开展好各项安全生产活动，使安全生产警钟长鸣，防范于未然。同时还可以根据施工生产的特点实施好“五抓”的安全教育，即：工程突击赶任务时，工程接近收尾时，施工条件好时，季节气候变化时，节假日前后时这五个环节必须抓紧教育。

8、教育培训形式。安全教育、培训可以根据各自的特点，

采取多种形式进行。如设培训班、上安全课、安全知识讲座、报告会、智力竞赛、图片展、书画剪贴、电视片、黑板报、墙报、简报、通报、广播等等使教育培训形象生动。

第八章　伤亡事故快报制度

按规定做好伤亡事故的报告和处理工作。

1、工伤事故定义

工伤事故指在劳动过程中发生的人身伤害、急性中毒等。

（1）伤亡事故分类。伤亡事故按其伤害程度可分为：轻伤、重伤、死亡、重大伤亡（一次死亡三人以上）事故，按照《工程建设重大事故报告和调查程序规定》即：

一级事故：一次死亡30人以上或经济损失300万元以上。

二级事故：一次死亡10人以上29人以下，经济损失100万元以上300万元以下。

三级事故：一次死亡3人以上9人以下，或经济损失30万元以上不满100万元。

四级事故：一次死亡2人以下或重伤3人以上19人以下，或经济损失10万元以上不满30万元的事故。

（2）事故类别：有物体打击、提升、车辆伤害、机械伤害、起重伤害、触电、淹弱、灼烫、火灾、高处坠落、坍塌、冒顶片帮、透水、放炮、火药爆炸、瓦斯煤气爆炸等其他伤害。

2、事故报告调查程序

（1）事故快报：伤亡事故发生后，负伤者或事故现场有关人员应当立即直接或者逐级上报，企业负责人接到重伤、死亡、重大死亡事故报告后，应立即报告主管部门和当地劳动部门，最迟不得超过24小时，报告内容包括发生事故的单位、时间、地点、伤亡情况和初步分析事故原因等，企业按规定每月填写“职工伤亡事故综合月报表”，并做到准确、及时，可比（如千人重伤率=（重伤人数÷平均职工人数）×103）。

（2）保护好现场，并迅速采取措施，抢救人员和财产，防止事故扩大，因抢救需要移动现场物体时，必须做出标记、拍照、详细记录和绘制事故现场图，伤亡事故现场的清理，如无特殊原因，应经事故调查机关同意。

3、事故调查

企业发生轻伤事故，一般重伤事故，由企业负责人组织安监、工会等部门进行调查，发生一次重伤三人以上或死亡事故由企业主管部门、当地劳动部门、工会组织等部门进行调查，一次死亡三人以上事故由省级有关部门组织调查。

4、事故分析

（1）原因分析，即是直接原因还是间接（管理方面）原因。

（2）事故性质是责任事故，非责任事故还是破坏事故要分清。

5、事故处理

事故处理必须执行“三不放过”的原则，即事故原因没

有查清不能放过；事故责任者和职工群众未受到教育不能放过；没有制订出防范措施不能放过，对发生事故处理一般按事故的轻重大小可分为经济处罚、行政处分和追究刑事责任三种。经济处罚：一是企业内部按企业奖惩办法查处；二是行政执法机关按有关行政法规查处。行政处分：按照干部、职工管理权限对事故责任者以行政处分。查处重大责任事故罪，根据国家有关法律法规规定处理。

第九章　考核制度

为进一步落实“安全第一，预防为主”的方针，考核标准如下：

序号	考核内容	考核对象	考核标准
1	不戴安全帽（每次）	现场负责人、个人	5
2	高空、悬空作业不系安全带（每次）	现场负责人、监理、个人	50
3	施工现场无安全生产牌或制度	项目经理、现场负责人、监理	200
4	安全生产技术措施不编制	项目经理、现场负责人、监理	100
5	安全生产资料不真实、残缺不齐	现场负责人、监理	200
6	强令他人冒险违章作业	指挥者	200
7	安全生产无检查、无活动	项目经理、现场负责人、监理	100

8	高空作业时乱抛材料、工具、杂物	现场负责人、监理、个人	50
9	非操作人员乱开或玩弄机电设备	现场负责人、个人	200
10	作业时穿拖鞋、高跟鞋、塑料底鞋	现场负责人、监理、个人	5
11	无故翻爬井架、脚手架	现场负责人、个人	10
12	不按规定布设安全网	现场负责人、监理	100
13	井架防护每缺一项	现场负责人、监理	50
14	电机设备无接地或接零（每处）	现场负责人、监理	20
15	特种工无证上岗（除停止操作外）	现场负责人、监理、个人	200
16	易燃地区不设灭火设备每处	现场负责人、监理	50-100
17	脚手架未经验收使用	现场负责人、个人	50
18	闸刀无盖或无插头直接电源（每处）	现场负责人、监理	20
19	易燃易爆处吸烟（每人）	现场负责人、个人	10
20	工地发现小孩	现场负责人、监理	50
21	外地工无身份	现场负责人、监理	50
22	乙炔气与氧气存放不符合规定	现场负责人、监理、个人	100
23	打群架	现场负责人、个人	100
24	脚手架子上面嘻闹	现场负责人、个人	5

25	工地进行赌博（没收赌具）	现场负责人、个人	100-200
26	偷窃财物按现价	现场负责人、个人	1-5 倍
27	酒后作业	现场负责人、监理、个人	50
28	发现不满十八周岁的童工作业	现场负责人、监理	3000
29	穿背心、赤膊作业	现场负责人、个人	20

第十章　项目组安全活动制度

搞好安全生产，建立项目组活动制度，安全管理工作做到纵向到底，横向到边，落实项目组安全工作是搞好施工安全的关键基础，增强安全意识和自我保护能力，切实执行本安全生产活动制度。

1、上班前应实行班前安全生产教育交底。

2、交底内容：根据工作内容进行电器、机械设备“四口五临边”防护高处作业、季节气候、防火等各种环节的情况进行有针对性的交底和提出针对性的预防措施。

3、上岗检查，主要查上岗人员的劳动保护情况，查现场的每个岗位的作业环境是否安全无患。

4、上岗检查机械设备的安全保险装置是否完好有效，以及各类安全技术交底措施的落实工作情况等。

5、做好上岗记录，记录好上岗交底主要内容，人员分工情况，记录好上岗检查后存在主要的不安全因素，和采取的相应措施和发生事故苗子、违章情况。

6、检查过程中发现的问题，采取措施作出处理意见，并

付诸实施，并作好记录，作好签字手续。

7、在做好每日上岗活动的基础上，做好安全生产工作小结，表扬先进事例和遵章守纪的先进个人，小结主要经验教训，针对不安全因素，发动全员提出改进措施，从中吸取经验教训，举一反三，做到安全生产警钟长鸣。部门做好监督指导工作。

8、开展班前“三上岗、一讲评”活动，即在班前须进行上岗交底、上岗检查、上岗教育和每周一次的“一讲评”安全活动，及考核措施。

9、班前活动和检查、讲评活动等到应有记录并有考核措施。

第十一章　门卫值班和治安保卫制度

1、施工现场必须安排责任性强，身体健康人员值班，值班人员要协助材料员，做好材料进出的验收，做好施工现场的安全防范工作，加强巡逻检查，严防坏人进行偷盗和破坏活动。

2、施工现场办公室必须门窗完整、安全，钥匙要随身携带，做到人离关窗、上锁，贵重物品（如现金，手表）要随身携带。

3、施工现场的物资要分类堆放，留出通道不要紧靠围墙。

4、材料运出现场，应填写证明，及时清理易燃物；工程竣工及时收回多余材料。

5、高档木材、门窗、瓷砖、钢配件、铝合金、电子电器设备等贵重材料、物资、设施、设备应存放在专门的安全地

点。

6、施工现场配备的消防器材要有专人负责，标明有效期，妥善保管，不得乱丢乱放或移作他用。

7、发生事故或案件，要保护好现场，并及时向公安、保卫部门报告，积极协助公安、保卫部门侦破案件。

8、对施工现场内的一切物资、设备的数量、规格进行查对、登记。经办人员必须出示本人证件，向值班人员和材料员登记签名。

9、个人携带物品进入施工现场，值班人员认为有必要时，有权进行检查，不得拒绝。

10、值班人员、材料员必须坚持原则，不循私情，对违章人员应给予批评教育和纠正。

11、提高警惕，对职责范围内的地区巡视、勤检查，防止发生偷窃或治安灾害事故的发生，发现可疑情况及时报告公安、保卫部门。

第十二章　消防防火责任制度

1、认真做好对工人的安全教育工作，提高安全防火意识，遵守安全操作规程和各项规章制度。

2、木工间、宿舍、仓库及易燃易爆等场所不准使用明火、电炉和高用量电热器，不准在场内吸烟；施工现场必须严格遵守用电消防安全管理规定，防止电气失火。

3、电焊、气割及生产用火时，必须遵守防火安全间距的规定，远离易燃和可燃物，落实防范措施，动火前，必须按级别履行动火审批手续，不准违章使用明火。

4、每天要做好落手清工作，将工作场所的创花、木屑等可燃物必须及时处理掉，并堆放到安全地点，易燃易爆及化工材料必须按规定严格保管和存放，下班后应切断电源闸刀。

5、有专人负责，经常检查工作场所的防火安全，对不安全隐患必须立即采取措施整改，服从管理和监督。

6、人人遵守、注意安全，对无视规章制度，不采取措施整改或违章造成后果的将视情节对当事人及项目部做出处罚，直到清退，触犯法律的由司法部门依法追究法律责任。

7、经常向职工进行安全教育，积极预防火灾、爆炸、中毒等重大治安灾害事故的发生，严格各项规章制度，

8、对油库、易燃、易爆、危险品仓库、木工间、电工间及明火使用场所等重点防火部位，设立必要的消防设施，制订章约、经常检查，发现问题及时督促整改，做到防患未然，如发生火警、火灾应立即报警和组织扑救，把事故消灭在萌芽之中。

9、加强各种灭火器材的管理，根据各种灭火器材的特性，按部位配置并及时换药，做到全面有效。

10、现场临时设施搭建应合理布局，对油库、油漆库、木工间、易燃、易爆及危险品仓库和部位、车辆加油等都必须远离明火，严禁吸烟，宿舍内禁止使用明火、电炉和高用量电热器，禁止擅自私下装拆电器装置。

11、健全义务消防组织，负责一定的业务指导和有条件进行消防训练，提高消防知识和实际消防工作能力。

12、以上各条希望人人遵守，违者给予必要的处罚，直至提请追究法律责任。

第十三章　卫生保洁制度

1、施工区卫生管理

环境卫生管理的责任区为创造良好的工作环境，养成良好的文明施工作风，增进个人身体健康，划分责任区，责任到人，使文明施工保持经常化。

2、环境卫生管理措施

（1）施工现场要天天打扫，保持整洁卫生，场地平整，道路畅通，作到无积水，有排水措施。

（2）施工现场严禁大小便，发现有随地大小便现象要对责任区负责人进行处罚。

（3）施工现场零散材料和垃圾，要及时清理，垃圾临时存放不得超过三天，如违反本条规定处罚工地负责人。

（4）办公室内作到天天打扫，保持整洁卫生，做到窗明地净，文具报告摆放整齐，达不到要求。对当天卫生值班员罚款。

（5）大功率用电器，必须有验收手续。合格后方可使用。

（6）楼内清理的垃圾，要用容器或小推车，用提升栏或电梯等运下，严禁高空抛撒。

（7）为了广大施工人员身体健康，施工现场必须设置保温桶和开水（水杯自备），公用杯子必须采取消毒措施。

3、环境卫生定期检查记录

施工现场的卫生要定期进行检查，发现问题，限期改正。

第十四章　不扰民措施

施工现场防噪声污染的各项措施：

1、人为噪声的控制措施

施工现场提倡文明施工，建立健全控制人为噪声的管理制度。尽量减少人为的大声喧哗，增强全体施工人员防噪声扰民的自觉意识。

2、强噪声作业时间的控制

凡在居民稠密区进行强噪声作业的，严格控制作业时间，晚间作业不超过22时，早晨作业不早于6时，特殊情况需连续作业（或夜间作业）的，应尽量采取降噪措施，事先做好周围群众的工作，并报工地所在的环保局备案后方可施工。

3、强噪声机械的降噪措施

（1）牵扯到产生强噪声的成品，半成品加工、制做作业（如预制构件，木门窗制做等），应尽量放在工厂、车间完成，减少因施工现场加工制作产生的噪声。

（2）尽量选用低噪声成备有消声降噪设备的施工机械。施工现场的强噪声机械（如：搅拌机、电锯、电刨，砂轮机、切割机等）要设置封闭的机械棚，以减少强噪声的扩散。

4、加强施工现场的噪声监测

加强施工现场环境噪声的监测，采取专人管理的原则，根据测量结果凡超过《施工场界噪声限值》标准的，要及时对施工现场噪声超标的有关因素进行调整，达到施工噪声不扰氏的目的。

信息安全安全生产管理办法

第一章　信息安全方针及安全策略

1、总则

（1）目的

为了深入贯彻落实国家信息安全政策文件要求和信息安全等级保护政策要求，加强黄石大数据信息发展有限公司的信息安全管理工作，增强公司全员信息安全意识，切实提高公司信息系统安全保障能力，特制定本方针。

（2）范围

本方针适用于黄石大数据信息发展有限公司安全管理活动。

（3）职责

由公司领导和各部门主管为主体的信息安全领导小组负责本方针文件的审核和修订，由安全运维部为主体的信息安全工作小组负责本方针文件的贯彻和执行。

（4）符合性

本方针文件主要遵循《信息安全技术信息系统安全等级

保护基本要求（GBT 22239-2008）》标准的要求，同时在部分环节也符合以下两个国际标准。

ISO/IEC 27001 信息安全管理体系要求

ISO/IEC 27002 信息技术—安全技术—信息安全管理实践规范

2、信息安全方针

黄石大数据信息发展有限公司总体安全方针为：提高人员信息安全风险意识，确保业务系统安全；强化信息安全管理，坚持以人为本。

3、方针主要内容

（1）主要安全策略

- 信息安全是公司及相关部门正常经营的重要保障，黄石大数据信息发展有限公司将遵照“统一规划、分级管理、积极防范、人人有责”的原则，通过风险评估和风险管理，采取一切可能的措施，加强公司信息安全的建设和管理。
- 公司设立信息安全领导小组，信息安全领导小组是公司信息安全管理的最高机构；安全运维部、运维人员、系统管理员等是公司信息安全日常工作和执行机构，负责公司信息系统及信息安全的日常维护和管理工作。
- 公司全体职工均有参与信息安全管理、保护公司及相关部门信息安全的义务和责任。公司全体职工应积极参加各种形式的信息安全教育和培训，遵守相关国家

法律、法规、部门规章和行业规范，遵守公司信息安全管理制度。

- 承载信息系统的所有软硬件设施及物理环境均应受到适当的保护。
- 采取必要的措施保护公司信息的机密性，以防止未经授权的不当存取；同时应确保信息不会在传递的过程中，或因无意间的行为透漏给未经授权的第三者。
- 采取必要的措施确保公司信息的完整性，以防止未经授权的篡改。
- 采取必要的措施确保公司信息的可用性，以确保使用者需求可以得到满足。
- 采取必要的措施确保公司信息的连续性，以确保业务持续可用。
- 公司相关的信息安全措施或规范应符合现行法令、法规的要求。
- 公司全体员工都有责任通过适当的上报机制，报告所发现的信息安全意外事故或信息安全弱点。
- 任何危及信息安全的行为，都应诉诸适当的惩罚程序或法律行动。

（2）信息安全目标

最大限度保证信息系统的完整性、保密性和可用性免遭破坏。确保每年信息安全重大事故（II 级）的发生频率为可控范围内的最低，目标为“0”次。

（3）信息安全管理框架

黄石大数据信息发展有限公司信息安全管理框架是根据 ISO/IEC 27001《信息安全管理体系要求》中的控制目标和控制项，并结合黄石大数据信息发展有限公司的实际情况所建立的。符合“PDCA”的管理模式。

① P（PLAN）过程是计划过程，指统一规划和设计黄石大数据信息发展有限公司的信息安全目标和安全控制策略，指导黄石大数据信息发展有限公司整体的信息安全管理工作。

② D（DO)过程是执行过程，指黄石大数据信息发展有限公司在开展信息安全工作中需要落实的管理要求，包括信息安全组织制度管理、人员安全管理、系统建设安全管理、信息系统运维管理、变更管理和信息资产安全管理等，指导日常的信息安全管理工作。

③ C（CHECK）过程是检查过程，指黄石大数据信息发展有限公司开展信息安全工作的持续改进机制，通过信息安全风险评估、等级保护测评、检查，监督和审核等方式，指导信息安全管理体系控制要求不断完善。

④ A（ACTION）过程是处置过程，指黄石大数据信息发展有限公司信息安全事件处置和应急预案，通过发现和总结信息安全问题，形成新的管理办法和控制措施，确保信息安全管理体系的适用性和有效性。

黄石大数据信息发展有限公司信息安全管理框架通过 PDCA 各环节的不断完善，实现信息安全管理体系自身的持续改进，从而提高信息安全管理体系的全面性、有效性和适用

性。

（2）信息安全管理原则

① 基于安全需求原则：黄石大数据信息发展有限公司核心业务信息系统根据等级保护要求，定级为三级，安全需求主要参照三级等级保护要求，同时考虑可能受到的威胁及面临的风险分析安全需求，遵从三级等级保护的规范要求，从全局上恰当地平衡安全投入与效果；

② 主要领导负责原则：信息安全领导小组的主要领导确立黄石大数据信息发展有限公司信息安全保障的宗旨和政策，负责提高全员的安全意识，组织有效的安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效；

③ 全员参与原则：与核心业务信息系统相关的所有运行维护人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全；

④ 持续改进原则：安全管理是一种动态反馈过程，贯穿整个安全管理的生命周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性；

⑤ 依法管理原则：信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权

者适时发布准确一致的有关信息，避免带来不良的社会影响；

⑥ 选用成熟技术原则：成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的失误；

⑦ 管理与技术并重原则：坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

第二章　信息安全领导机构组成与职责

1、总则

（1）目的

为更好的实现对黄石大数据信息发展有限公司信息系统的安全管理，促进各项制度、措施的落实，经公司领导研究决定成立以信息安全领导小组为管理机构、信息安全工作小组为执行机构的组织架构，负责全公司信息安全建设及防护。

（2）范围

本标准针对黄石大数据信息发展有限公司信息安全组织建设相关事务，规定了组织框架和角色责任，适用于黄石大数据信息发展有限公司所有纳入到信息安全管理体系范围的组织和个人。

（3）职责

信息安全工作小组负责起草、制定本标准，安全领导小组负责批准、发布本标准。

信息安全组织内相关人员承担本标准定义的相关角色，履行相应的信息安全管理职责。

2、信息安全组织架构

信息安全领导小组负责组织信息化建设总体规划和统筹安排，协调各部门与信息化之间的关系。信息安全领导小组组长由总经理兼任，副组长由副总经理和部门经理兼任。

信息安全领导小组成员如下：

胡海鹏、金伟

信息安全领导小组下设信息安全工作小组，信息安全工作小组人员设置如下：

信息安全工作小组组长：

金伟、王朋

信息安全工作小组副组长：

黄裕文、曹祥林

信息安全工作小组成员：

郑煜、赵睿、李威林、王谦、袁剑

3、机构和组织职责

（1）信息安全领导小组组长职责

组长：负责信息化建设总体规划、设计决策、项目决策、流程决策、人员调配决策以及信息安全事故的应急协调和指挥。

副组长：负责具体项目规划设计、人员召集、组织实施等工作，对工程质量负责，并负责人员培训，流程制定，需求确认，协助实施、安全事故应急响应等具体日程和事务。

（2）信息安全领导小组具体职责

负责审定信息安全建设与应用总体规划、经费预算、技术标准、管理规范及相关政策措施。

① 研究决定信息安全体系建设重大事项，监督信息安全体系规划的实施。

② 及时解决项目建设过程中的决策问题，并对各项工作做出指示

③ 审批发布信息安全方针和管理体系。

④ 审批信息安全规划和项目的批准。

⑤ 提供信息安全资源保证。

⑥ 负责信息安全策略审核及推广。

⑦ 建立与内部/外部专家、权威机构、合作伙伴、供应商之间的沟通渠道。统一控制对外信息发布和通告。

（3）信息安全工作小组组长职责

组长：直接对信息安全领导小组负责，负责信息安全领导小组宏观策略和项目规划的落地执行；在信息化领导小组的领导下，协调工作小组成员完成方案起草，流程收集，需求汇总等工作；协调信息安全工作小组内部人员的工作分配，人员管理等。

副组长：协助信息安全工作小组组长完成宏观策略和项目规划的落地执行，任命信息安全角色和岗位，并明确各信息安全岗位的职责，组织并实施信息安全管理评审，督促各成员统一协作，完成方案起草，流程收集，需求汇总等工作。

（4）信息安全工作小组人员职责

负责系统调试、日常维护、人员培训、人员组织、安全管理等具体工作。具体职责如下：

① 负责信息安全体系建设具体工作实施和推进，与工作小组组长及时沟通并汇报有关情况。

② 负责与咨询公司沟通协调项目实施情况以及项目在公司内部的推进和后续知识转移。

③ 负责安全管理体系的建立并监督信息安全管理制度

的执行。

④ 对信息安全相关项目进行规划和监督，确保信息安全风险评估和管理工作能够落实。

⑤ 制定年度评审计划，确定评审范围和内审内容。

⑥ 负责信息安全策略、标准、流程和制度的编写、审核及推广。

⑦ 制定业务连续性计划。

⑧ 建立与内部/外部专家、权威机构、利益伙伴之间的沟通渠道。统一控制对外信息发布和通告。

4、附录

附 1：信息安全组织相关人员信息表

信息安全相关组织人员信息表

角色	姓名	工作部门	职务	联系电话
信息安全领导小组组长	胡海鹏	公司领导	总经理	15172037405
信息安全领导小组成员	金伟	公司领导	副总经理	13942608441
信息安全工作小组成员	王朋	公司领导	部门经理	18972780088
信息安全工作小组成员	黄裕文	安全运维部	组员	15112629616
信息安全工作小组成员	曹祥林	安全运维部	组员	13972779797
信息安全工作小组成员	郑煜	安全运维部	组员	17771080325
信息安全工作小组成员	赵睿	安全运维部	组员	18507235692
信息安全工作小组成员	李威林	安全运维部	组员	15914043591
信息安全工作小组成员	王谦	安全运维部	组员	17754475335
信息安全工作小组成员	袁剑	安全运维部	组员	15907239067
信息安全岗	王谦	安全运维部	工程师	17754475335
网络管理岗	王谦	安全运维部	工程师	17754475335
文档管理岗	王谦	安全运维部	工程师	17754475335

第三章　安全检查和审核管理

1、总则

（1）目的

为形成信息安全检查和审核长效机制，提高公司全体职工信息安全意识，特制订本规范。

（2）范围

本管理制度适用于黄石大数据信息发展有限公司安全运维部在信息安全管理过程中的周期信息安全检查和审核管理。

（3）职责

安全运维部负责协调，安全运维部安全管理员负责常规的信息系统安全检查和记录。信息安全工作小组负责对全公司信息系统安全抽查，并由安全运维部做好记录。

2、管理细则

（1）安全检查机构分工：

① 日常安全检查由安全管理员负责，安全检查应根据日志中心的安全日志情况，不定期进行，但最少应每季度检查一次。

② 信息安全工作小组可在安全管理员检查的基础上不定期的进行信息安全抽查，或者组织全系统范围内的全面安全检查，但最少应每半年做一次全面的安全检查。

（2）安全检查审核主要内容

① 安全管理员的日常安全检查主要内容包括：系统日常运行情况、系统漏洞、数据备份情况等。

② 信息安全工作小组的安全检查和审核主要内容包括：系统日常运行情况（就安全管理员的日常检查情况进行汇总）、系统漏洞、数据备份情况、现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

③ 信息安全工作小组的安全检查和审核结果如需要可在全系统范围内进行通报，通报内容可以删除敏感信息。

3、附件

附 1 ：信息系统安全检查表单

信息系统安全检查表单

检查 单元	最近 X 月 运行情况	系统漏 洞情况	重要数据 备份情况	故障受 理情况	各项制度 执行情况	其他突出安全问题	检查时间
智慧城管							
智慧环保							
智慧环卫							
网络设备							
终端设备							
等等							

注：安全检查至少每季度一次，每月开始的第一个周末必须完成上月的检查并填写此表单。
检查人员：

附 2：信息安全检查报告及通报

信息安全检查报告及通报

1.检查记录

检查单元	**存在主要问题记录**
业务系统	
云主机	
数据库系统	
网络设备	
终端设备	

2.安全形势、安全风险状况通报

1、简述总体安全形势
2、重点安全问题/问题部门分析

4、改进建议

报告制作部门：安全运维部　　时间：

第四章　信息安全培训管理

1、总则

（1）目的

为提高公司全体职工信息安全意识和信息安全技能,特制订本规范。

（2）范围

本规范适用于黄石大数据信息发展有限公司相关人员的安全意识培训、安全技能培训管理。

（3）职责

安全运维部负责制订各类岗位和人员的信息安全相关培训计划，并按照计划执行各种形式的信息安全培训。各部门主管协助安全运维部开展覆盖本部门范围的相关安全培训，全体职工积极参加安全运维部组织的各类信息安全培训。

2、信息安全意识培训

（1）信息安全意识培训对象

全公司职工都应接受信息安全意识的培训。

（2）信息安全意识培训时机

① 新入职职工在上岗前都应接受信息安全意识培训;

② 针对现有职工，安全运维部应确保每年至少提供一次基础的信息安全意识培训，以确保所有职工都保持必要的信息安全意识。

3、信息安全技术培训

（1）信息安全技术培训对象

信息安全技术培训对象主要是安全运维部技术人员，各部门相关人员。

（2）信息安全技术培训时机

① 技术人员和项目经理在上岗前都应接受信息安全技术培训；

② 针对现有的技术人员，应确保每年至少提供一次基础的信息安全技术培训；

③ 当出现新的信息安全技术时，应确保所有的技术人员参加相应的培训。

4、信息安全管理培训

（1）信息安全管理培训的对象

信息安全管理培训的对象是中层以上管理人员。

（2）信息安全管理培训的时机

① 在信息安全管理体系建设过程中，应对中层以上管理人员进行信息安全管理培训，确保他们理解并支持信息安全管理体系的建设，确保信息安全管理体系的实施顺利进行。

② 应确保每年至少提供一次基础的信息安全管理培训。

5、培训的组织与管理

（1）信息安全年度培训计划

① 信息安全工作小组负责参照以下信息编制黄石大数据信息发展有限公司的《信息安全年度培训计划》。

② 过去一年全公司信息系统内发生的信息安全事件状况。

③ 公司职工在遵守安全程序及规范方面的状况。

④ 《年度信息安全培训计划》应由信息安全工作小组组长批准，并报信息安全领导小组备案。

（2）培训形式

① 内训：在黄石大数据信息发展有限公司内部培训，由黄石大数据信息发展有限公司内部人员或者外聘的讲师进行培训。

② 外训：指根据培训计划和职工发展需求安排职工参加的在黄石大数据信息发展有限公司以外举办的公开课程或阶段课程（包括研讨会、讲座等形式）。

（3）培训实施

① 安全运维部负责根据《信息安全年度培训计划》提前确定培训的时间，参加培训的人员和培训教师。每次培训前，安全运维部将提前至少三天拟定培训通知，并发放各相关部门。

② 提供培训的老师应提前准备教材。

③ 如果培训方式为外聘或者外送，安全运维部应提前与外部机构进行确认，并根据公司相关规定进行申报批准。

④ 安全运维部应准备《培训记录签到表》，培训时所有培训人员应签到。签到表由安全运维部保管，可做为个人绩效评估的参考资料。

（4）培训效果评估

培训之后，应针对培训内容对培训人员做必要的测试，以检验培训的效果。

（5）培训反馈

应设定特定的方式接受学员关于培训的反馈，例如问卷调查、意见邮箱等。逐步完善信息安全培训体系。

6、附件

附 1：年度信息安全培训计划

年度信息安全培训计划

序号	培训名称	培训时间	参与人数	培训内容	备注
1					
2					
3					
4					
5					
6					
7					

编制：　　审核：

批准：　　年　月　日

附 2：年度信息安全培训计划

培训记录签到表

课程名称		课程类别	安全培训
培训机构		培训讲师	
培训时间		培训地点	

课程内容摘要			
培训学员	部门	签名	备注

第五章　第三方安全管理规范

1、总则

（1）目的

为了加强对第三方合作伙伴、人员、系统的安全管理，防止引入第三方给黄石大数据信息发展有限公司带来的安全风险，特制定本管理办法。

（2）范围

本规范适用于黄石大数据信息发展有限公司在信息安全管理过程中对外来人员和第三方人员的行为规范管理。

（3）职责

黄石大数据信息发展有限公司第三方信息安全管理由安全运维部负责，并应按照本办法严格落实。

2、管理细则

（1）解释

本办法所指第三方包括第三方公司、第三方系统、第三方人员：

① 第三方公司是指向黄石大数据信息发展有限公司提供设备、产品、服务的外部公司。

② 第三方系统是指为黄石大数据信息发展有限公司服务或与黄石大数据信息发展有限公司合作运营的系统。这些系统可能不在黄石大数据信息发展有限公司机房内，但能通过接口与黄石大数据信息发展有限公司的系统发生数据交互。

③ 第三方人员是指为黄石大数据信息发展有限公司提供

开发、测试、运维等服务或参与合作运营系统管理的非黄石大数据信息发展有限公司人员。

④ 对第三方公司的信息安全管理应遵循如下原则：“谁主管谁负责、谁运营谁负责、谁使用谁负责、谁接入谁负责”的原则。

（2）总体要求

① 对于与我公司开展合作运营的第三方公司，安全运维部要求其按照公司网络与信息安全的管理规定，严格落实信息安全责任，建立日常安全运维、检查制度，确保不发生信息泄密、重大安全漏洞。

② 安全运维部需要求在我公司开展现场长期服务的第三方公司，在派驻现场设立专职人员，其主要职责包括：负责按照国家及公司的信息安全管理要求，开展派驻现场的安全管理，指导和监督派驻现场人员的信息安全，确保不发生违规行为；接受我公司的监督和考核等。

③ 第三方公司信息安全管理人员发生变更时，应在变更前 1 周将有关变更信息报送黄石大数据信息发展有限公司安全运维部。

④ 安全运维部要督促指导第三方公司及人员遵循黄石大数据信息发展有限公司的安全管理制度和规范，将安全要求作为考核内容，纳入双方合作协议，定期组织对第三方安全检查。

（3）第三方公司及人员管理

① 第三方公司必须与黄石大数据信息发展有限公司签订

保密协议，在协议中明确第三方公司的保密责任以及违约罚则；第三方公司应与其员工签订保密协议，在协议中明确第三方公司员工的保密责任以及违约罚则。

② 第三方公司必须严格遵守黄石大数据信息发展有限公司客户服务的要求和规定。

③ 第三方公司在合作过程中，如不可避免地接触到黄石大数据信息发展有限公司客户资料、病例信息、病人信息、公司经营信息等各类敏感信息及商业秘密（下面简称敏感信息），应保证不损害敏感信息的保密性、完整性、可用性、真实性、可核查性、可靠性、防抵赖性。

④ 第三方人员管理的范畴包括临时人员和长期人员：临时人员指因业务洽谈、技术交流、提供短期和不频繁技术支持服务的人员；长期人员指因从事合作开发、参与项目工程建设、提供技术支持或顾问服务的人员。

⑤ 由第三方公司参与开发并提供服务的业务系统或软件程序，如系统或程序能接触到客户敏感信息，应要求将第三方系统开发文档提交安全运维部留档，文档应注明分发范围，并要求开发人员、测试人员、项目管理人员严格遵守分发控制要求。

⑥ 第三方公司参与或独立开发的业务系统或软件程序，应落实版本管理工作，并主动在上线验收前向安全运维部提交其源代码或代码审计报告、以及安全测试报告，安全运维部进行备案存档。

⑦ 第三方公司应对其参与或独立开发的业务系统或软件

程序源代码进行妥善保管，严格控制第三方人员访问权限，避免代码泄漏。

（4）第三方接入管理

① 第三方人员进入黄石大数据信息发展有限公司核心区域或者登录黄石大数据信息发展有限公司各业务系统操作时，应严格遵守黄石大数据信息发展有限公司的各项安全管理制度和规范。

② 第三方人员工作区域与黄石大数据信息发展有限公司的生产、内部办公、维护区域分离，在安全域中划分独立的第三方用户接入区，如系统开发接入区、系统维护接入区等，并应采用更严格的访问控制策略和管控手段。

③ 第三方用户接入区部署的常驻终端，应有严格的接入认证，并满足黄石大数据信息发展有限公司相关终端安全合规性检查标准。

④ 第三方用户接入区内的非常驻终端，需按照相应申请审批流程向安全运维部申请，并按照黄石大数据信息发展有限公司终端相关安全合规性标准进行检查，获得授权后方可接入，安全运维部应将申请审批记录备案。

⑤ 安全运维部应组织对现场服务的第三方人员终端进行安全审核、检查，不定期抽查。

⑥ 禁止第三方人员在未授权的情况下通过远程方式接入第三方用户接入区，如第三方人员因特殊情况需要通过远程登录，须经过安全运维部审批授权后，临时开通远程登录功能，并及时撤销。远程登录必须通过堡垒机系统等进行集中

认证、授权和审计，应遵循权限最小化原则，控制用户访问的系统及权限。

（5）第三方帐号及权限管理

① 第三方人员需与所属公司签订保密协议，报备安全运维部后，方可申请相关系统帐号（不含超级帐号和系统帐号管理员帐号）、接入或访问黄石大数据信息发展有限公司内部的生产系统以及其他相关信息系统。

② 第三方人员申请新增或变更帐号时，必须符合专人专号原则、权限最小化原则。帐号申请应经过安全运维部审核并批准方可生效，帐号申请授权书应约定使用者、权限、使用期限等事项。

③ 安全运维部授权的第三方人员临时远程接入帐号，其帐号及权限有效期最长不能超过 3 天，帐号到期或者接入任务完成后，应及时删除临时帐号并审核。

④ 第三方人员的帐号口令不得使用弱密码。帐号口令必须是在必要时间或次数内不循环使用。口令不得以任何形式明文存放于可公共访问的设备或物理界面上，保证帐号口令在传输和存储时的安全。

⑤ 在运维和运营环节，由于工作需要在一定时间段内频繁接触敏感信息的第三方人员，必须提前获得安全运维部授权，经审批通过后方可被授予相应权限，安全运维部应备案申请审批记录及事后审计。

⑥ 第三方人员访问黄石大数据信息发展有限公司信息系统时，第三方人员的帐号、认证、授权管理和安全审计应纳

入堡垒机系统集中管控。

3、附件

附 1：第三方人员保密协议

第三方人员保密协议

甲方：

乙方：

为了保护甲乙双方在商业和技术合作中涉及的专有信息（如本协议第 2 条所定义的内容），经友好协商，甲乙双方签订如下协议：

1、签约责任人：双方就专有信息的传授和接受事宜而协调的首要责任人。

（1）甲方责任人：

（2）乙方责任人：

2、专有信息的定义：

本协议所称的“专有信息”是指所有商业秘密、技术秘密、通信或与该产品相关的其他信息，无论是书面的、口头的、图形的、电磁的或其它任何形式的信息，包括（但不限于）数据、模型、样品、草案、技术、方法、仪器设备和其它信息，上述信息必须以如下形式确定：

（1）对于书面的或其它有形的信息，在交付接收方时必须标明专有或秘密。

（2）对于口头信息，在透露给接收方前必须声明是专有信息，进行书面记录。

3、保密义务：

（1）乙方同意严格控制和保护甲方所透露的专有信息。

（2）乙方保证采取一定的保护方法、措施和手段对甲方提供的专有信息进行保密，避免非授权透露、使用或复制甲方专有信息。

（3）乙方保证不向任何第三方透露本协议的存在或本协议的任何内容。

4、使用方式和不使用的义务：

（1）乙方同意如下内容：

①乙方只能为下述目的而使用专有信息：

使用目的：

除乙方的高级职员和直接参与本项工作的普通职员之外，不能将专有信息透露给其它任何人；

②不能将此专有信息的全部或部分进行复制或仿造。

（2）乙方应当告知并以适当方式要求其参与本项工作之雇员遵守本协议规定，若参与本项工作之雇员违反本协议规定，乙方应承担连带责任。

5、例外情况：

（1）乙方保密和不使用的义务不适用于下列专有信息：

①有书面材料证明，甲方在未附加保密义务的情况下公开透露的信息；

②有书面材料证明，在未进行任何透露之前，乙方在未受任何限制的情况下已经拥有的专有信息；

③有书面材料证明，该专有信息已经被乙方之外的第三方公开；

④有书面材料证明，乙方通过合法手段从第三方在未受到任何限制的情况下获得该专有信息。

（2）如果乙方的律师通过书面意见证明：乙方对专有信息的透

露是由于法律、法规、判决、裁定（包括按照传票、法院或政府处理程序）的要求而发生的，乙方应当事先尽快通知甲方，同时，乙方应当尽最大的努力帮助甲方有效地防止或限制该专有信息的透露。

6、专有信息的交回：

（1）当甲方以书面形式要求乙方交回专有信息时，乙方应当立即交回所有书面的或其他有形的专有信息以及所有描述和概括该专有信息的文件。

（2）没有甲方的书面许可，乙方不得丢弃和处理任何书面的或其他有形的专有信息。

7、　否认许可：

除非甲方明确地授权，乙方不能认为甲方授予其包含该专有信息的任何专利权、专利申请权、商标权、商业秘密或其它的知识产权。

8、救济方法：如果发生乙方违约，双方同意如下内容：

（1）乙方应当按照甲方的指示采取有效的方法对该专有信息进行保密，所需费用由乙方承担。

（2）乙方应当赔偿甲方因违约而造成的所有损失，包括（但不限于）：法院诉讼费用、合理的律师酬金和费用、所有损失或损害等等。

9、适用法律：

本协议受中华人民共和国法律管辖，并在所有方面依其进行解释。

10、争议的解决：

由本协议产生的一切争议由双方友好协商解决。协商不成，双方约定本协议纠纷的管辖法院为甲方归属地人民法院。

11、生效及其它事项：

本协议一式四份，甲乙双方各执两份。

甲方：　　乙方：

签字：　　签字：

盖章：　　盖章：

日期：　　日期：

附 2：第三方接入访问申请表

第三方访问申请表

使用人		所属单位	
公司接口部门		联系电话	
申请类型	（☐ 仅访问机房　☐ 访问业务内网　☐应用系统具体权限）		
申请内容 **（详述）**			
安全运维部审批	年　月　日		

注：以下内容仅访问内网和具体应用系统时有安全运维部配合人员填写

访问时段	☐长期　☐临时(　　)
申请人确认	如在网络内做违规操作，占用带宽、感染病毒并传播至业务服务器等影响业务运行或访问与工作无关网站，占用他人 IP 地址等违规操作，入网权限将被回收且对我公司内做通报，追究相关负责人责任。 申请人签字： 年　月　日
开通记录	新增 IP： 操作内容： 负责人员： 年　月　日

附 3：第三方访问登记表

第三方人员访问登记表

注：该表单由当日机房值班员（第三方人员进入机房）或负责第三方人员接入网络的配合人员填写。

访问人	访问地点/内容	陪同人	访问时间	批准人

第六章　网络与信息系统安全设计规范

1、总则

（1）目的

为规范黄石大数据信息发展有限公司信息系统安全设计过程，确保整个信息安全管理体系在信息安全设计阶段即符合国家相关标准和要求，特制订本规范。

（2）范围

本规范适用于黄石大数据信息发展有限公司在信息安全设计阶段的要求和规范管理。

（3）职责

安全运维部负责信息安全系统设计，并会同上级单位、相关部门和有关专家对设计方案进行评审后报信息安全领导小组批准。

2、设计规范

（1）物理机房安全设计

新机房建设根据物理安全主要包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等，该部分内容将主要参考GB/T22239－2008《信息系统安全等级保护基本要求》（以下简称《基本要求》）要求的第三级标准进行建设，建设过程中可以参考的标准主要包括：

GB50174－93《电子计算机机房设计规范》

GB 50057－1994《建筑物防雷设计规范》

GB 2887-88《计算站场地安全要求》

GB 2887-89《计算站场地技术条件》

应从安全技术设施和安全技术措施两方面对信息系统所涉及到的主机房、辅助机房和办公环境等进行物理安全设计，设计内容包括防震、防雷、防火、防水、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等方面。物理安全设计是对采用的安全技术设施或安全技术措施的物理部署、物理尺寸、功能指标、性能指标等内容提出具体设计参数。具体依据《基本要求》中的“物理安全”内容，同时可以参照《信息系统物理安全技术要求》等。

（2）通信网络与区域边界安全设计

网络设计、建设、维护过程中应参考GB/T22239－2008《信息系统安全等级保护基本要求》第三级网络部分要求。对信息系统所涉及的通信网络，包括骨干网络、城域网络和其他通信网络（租用线路）等进行安全设计，设计内容包括通信过程数据完整性、数据保密性、保证通信可靠性的设备和线路冗余、通信网络的网络管理等方面。

通信网络安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置参数等提出具体设计细节。具体依据《基本要求》中“网络安全”内容，同时可以参照《网络基础安全技术要求》等。

对信息系统所涉及的区域网络边界进行安全设计，内容包括对区域网络的边界保护、区域划分、身份认证、访问控制、安全审计、入侵防范、恶意代码防范和网络设备自身保

护等方面。应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。应完善并加强不同网络区域的隔离，根据安全区域和业务系统不同安全域细化不同的 VLAN 和访问控制。

区域边界安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置策略和参数等提出具体设计细节。具体依据《基本要求》中的“网络安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《网络基础安全技术要求》等。

（3）主机系统安全设计

对信息系统涉及到的服务器和工作站进行主机系统安全设计，内容包括操作系统或数据库管理系统的选择、安装和安全配置，主机入侵防范、恶意代码防范、资源使用情况监控等。其中，安全配置细分为身份鉴别、访问控制、安全审计等方面的配置内容。具体依据《基本要求》中的“主机安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《信息系统通用安全技术要求》等。

（4）应用系统安全设计

对信息系统涉及到的应用系统软件（含应用/中间件平台）进行安全设计，设计内容包括身份鉴别、访问控制、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错和资源控制等。具体依据《基

本要求》中的“应用安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《信息系统通用安全技术要求》等。

网络安全的数据库系统主要包括MySQL、Oracle、HBase等业务生产系统数据库服务器群，这些数据库分别为黄石大数据信息发展有限公司各核心业务系统提供数据服务。通常这些数据库系统自身都提供了完善的安全机制，同时如果需要更精细的安全功能也可以通过一些数据库安全增强选件来实现。

（5）备份和恢复安全设计

针对信息系统的业务数据安全和系统服务连续性进行安全设计。设计内容包括数据备份系统、备用基础设施以及相关设施。针对业务数据安全的数据备份系统可考虑数据备份的范围、时间间隔、实现技术与介质以及数据备份线路的速率以及相关通信设备的规格和要求；针对信息系统服务连续性的安全设计可考虑连续性保证方式（设备冗余、应用级冗余）与实现细节，包括相关的基础设施支持、冗余/集群机制的选择、硬件设备的功能/性能指标以及软硬件的部署形式与参数配置等，可参照《信息系统灾难恢复规范》等。

黄石大数据信息发展有限公司网络与信息系统中存储大量重要的数据，网络内分布众多的数据库服务器，这些数据大量集中，且为众多用户直接共享，在黄石大数据信息发展有限公司项目工程中，需要对数据库进行实时的审计监控，以全面保障数据库的安全。

应建立灾备中心，已防止在线系统出现事故、自然灾害时无法恢复，并且建立完毕后，应该每年都进行灾备切换演练，以防止恢复过程出现意外。

（6）建设经费预算和工程实施计划

建设经费预算，根据信息系统的安全建设整改内容提出详细的经费预算，包括产品名称、型号、配置、数量、单价、总价和合计等，同时应包括集成费用、等级测评费用、服务费用和管理费用等。对于跨年度的安全建设整改或安全改建，提供分年度的经费预算。

工程实施计划

根据信息系统的安全建设整改内容提出详细的工程实施计划，包括建设内容、工程组织、阶段划分、项目分解、时间计划和进度安排等。对于跨年度的安全建设整改或安全改建，要对安全建设整改方案明确的主要安全建设整改内容进行适当的项目分解，比如分解成机房安全改造项目、网络安全建设整改项目、系统平台和应用平台安全建设整改项目等，分别制定中期和短期的实施计划，短期内主要解决目前急迫和关键的问题。

方案论证和备案

将信息系统安全建设整改技术方案与安全管理体系规划共同形成安全建设整改方案。组织专家对安全建设整改方案进行评审论证，形成评审意见。第三级（含）以上信息系统安全建设整改方案应报公安机关备案，并组织实施安全建设整改工程。

第七章　网络安全管理制度

1、总则

（1）目的

为规范黄石大数据信息发展有限公司网络信息系统安全管理，特制订本规范。

（2）范围

本规范适用于安全运维部网络管理员和安全管理员对网络系统的日常管理和安全维护行为。

（3）职责

安全运维部日常网络运行维护管理主要由网络管理员和安全管理员负责。

2、管理细则

（1）网络系统维护基本要求

① 日常维护要求：监测节点设备上的告警和控制台的告警显示信息，发现问题并及时处理，为网络稳定运行提供基本保障。

② 定期维护要求：每天对机房、设备、网管及配套设施进行巡视巡检、数据备份等操作。

③ 突发性维护要求：由安全运维部负责协调处理，信息安全领导小组协助配合，并对故障现象和处理过程作详细记录。

④ 对基础数据网设备进行硬件操作时须严格按照规范执行。

（2）网络系统维护具体要求

① 网络配置管理

- 检查当前运行的网络配置数据与网络现状是否一致，如不一致应及时更新。
- 检查缺省启动的网络配置文件是否为最新版本，如不是应及时更新。
- 网络发生变化时，及时更新网络配置数据，并做相应记录。
- 网络配置数据应及时备份，备份结果至少要保留到下一次修改前。
- 对重要网络数据备份应实现异质备份、异址存放。

② 网络运行管理

- 网络资源命名按安全运维部规范进行，建立完善的网络技术资料档案（包括：网络结构，设备型号，性能指标等）。
- 重要网络设备的口令要定期更改，一般要设置八个字符以上，口令设置应无任何意义，最好能包含非数字和字母在内的字符，同时采用大小写混用的方式；口令要存档保存。
- 需建立并维护整个系统的拓扑结构图，拓扑图体现网络设备的型号、名称以及与线路的链接情况等。
- 涉及与外单位联网，应制定详细的资料说明备案；需要接入内部网络时，必须通过相关的安全管理措施，报主管领导审批后，方可接入和接出。
- 内部网络不得与互联网进行物理连接；不得将有关涉密信息在互联网上发布，不得在互联网上发布非法信息；在互联网上下载的文件需经过检测后方可使用，不得下载带有非法内容的文件、图片等。

- 尽量减少使用网络传送非业务需要的有关内容,尽量降低网络流量；禁止涉密文件在网上共享。

（3）备份管理

备份周期：网络管理员对维护的网络设备配置每半年备份一次；日常性维护，网络设备配置文件发生变更前也需要保留备份文件；突发性维护尽可能在可备份情况下进行备份。

备份周期：2 个月和变更后

备份位置：至少需要放在文件服务器，冷备、重要及核心设备须有异地备份。

备份文件命名规则：设备名称+IP 地址(取最后字节)+备份日期

备份方式：可采用手工或自动备份方式。

备份记录：备份时须填写《网络数据备份记录表》，记录备份过程。

3、附件

附 1：网络数据备份记录表

网络数据备份记录表

单位：					
备份设备	备份时间	备份方式	备份位置	备份人员	备份内容
填表说明：					

附 2：网络违规行为记录表

网络违规行为记录表

违规行为详细记录（含违规时间）	处理措施	记录人	记录时间

第八章　恶意代码防范管理

1、总则

（1）目的

为加强对计算机病毒的预防和治理，保护信息系统安全，根据公安部《计算机病毒防治管理办法》以及有关计算机病毒防治的规定，制定本办法。

（2）范围

本管理办法适用于黄石大数据信息发展有限公司所有服务器和终端操作系统。

（3）职责

各计算机终端系统使用人负责本机防病毒客户端的维护，病毒查杀。安全运维部系统管理员负责计算机病毒防治的日常管理工作，负责计算机病毒的监控、处理、汇总、通报、上报等工作，负责计算机杀毒软件的安装、升级、运行、监控和维护等工作。

2、管理细则

① 本办法所称的计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

② 我公司计算机必须安装和使用统一要求的病毒查杀软件或查杀工具，并按要求进行操作和使用，认真做好相关参数设置、病毒升级以及计算机补丁安装等工作。

③ 计算机操作人员要学会病毒查杀软件或查杀工具的安装、使用，按要求做好病毒监控、病毒检查、病毒及操作系

统补丁升级、病毒软件运行状态等工作，未经允许不得关闭病毒监控程序，不得违反规定设置和修改病毒监控条件；不得安装和使用与工作无关的文件、软件及媒体，更不得制作、输入、传播计算机病毒，危害公司信息系统安全。

④ 任何部门和个人在使用购置、维修、接入的计算机设备时，在使用网络下载的或移动介质报送的文件、软件及媒体时，在使用接入上过外网的笔记本、移动介质等设备时，必须坚持“先杀毒后使用”原则，先进行病毒检测，确认无病毒后方可使用。

⑤ 各部门要加强网络安全管理，利用网络传送数据、文件等内容时，要坚持：传输前先检测，数据接收后，先检测后使用的原则，先进行病毒检测，确认无病毒后方可使用。

⑥ 各部门计算机出现异常现象或发现不能清除的病毒时，应立即与网络断开，并停止使用，同时报安全运维部处理。各部门发生因计算机病毒引起的信息系统瘫痪、程序和数据受到严重破坏等重大事故，要保护好现场，并第一时间报告安全运维部。

⑦ 各部门要做好计算机病毒的宣传教育以及培训工作，不断提高计算机操作人员的病毒预防意识和防犯能力。要定期组织计算机病毒防范检查和考核工作，对发现的问题要及时进行处理和整改。

⑧ 对于人为引起的或管理不善造成的计算机病毒传播事件，要追究当事人和领导者的责任，要根据情节和后果，按有关规定进行处理。情节特别严重的、造成后果特别恶劣的

要报公安部门进行处理。

⑨ 各部门要严格遵守本管理办法，不断加强计算机病毒的防治工作，一旦发现违反本管理办法，对使用者及该部门根据情节严重作出相应处罚。

3、附件

附 1：病毒日志汇总分析记录单

病毒日志汇总分析记录单

病毒名称	时间	系统名称	事件描述	跟进方案	完成时间	管理员

第九章　变更管理程序

1、总则

（1）目的

为规范黄石大数据信息发展有限公司各信息系统需求变更操作，增强需求变更的可追溯性，控制需求变更风险，特制定本规程。

（2）范围

本规范适用于黄石大数据信息发展有限公司所有业务信息系统、网络系统的变更管理。

（3）职责

各业务部门信息系统使用和维护人员按照本办法发起和进行各信息系统的变更，安全运维部系统管理员和网络管理员按照本办法发起或受理各信息系统的变更，并就相关变更的执行过程进行控制。

2、管理细则

（4）变更原则

① 当需求发生变化，需对软件包进行修改/变更时，首先应和第三方企业/软件供应商取得联系并获得帮助，了解所需变更的可能性和潜在的风险：如项目进度、成本以及安全性等方面的风险。

② 应按照变更控制程序对变更过程进行控制。

③ 实施系统变更前，应先通过系统变更测试，并提交系统变更申请，由信息安全工作小组审批后实施变更，重大系统变更需提交信息安全领导小组审批后实施。

（5）系统数据变更流程

① 业务经办人员需首先填写《需求变更申请表》，由申请人在申请表中签名，提交至安全运维部；

② 安全运维部分管系统管理员审核该项变更，如审核通过，则填写解决方案，并评估工作量和变更完成时间，最后在“安全运维部意见”处签字认可，提交至安全运维部领导审批；

③ 安全运维部领导需对该项变更的风险和工作量进行确认，审核通过后在“安全运维部领导意见”处签字认可，交安全运维部分管系统管理员安排实施变更；

④ 如果变更由外协公司人员负责实施，业务经办人员需提交一式两份需求变更申请单，一份留安全运维部存档，一份交外协公司保管，作为日后计算工作量的依据。

（6）系统应用变更流程

① 业务经办人员首先填写《需求变更申请表》，由申请人在申请表中签名，经业务部门主管签名同意后，提交至安全运维部；

② 安全运维部分管系统管理员审核该项变更，如审核通过，则填写解决方案，并评估工作量和变更完成时间，最后在“安全运维部意见”处签字认可，提交至安全运维部领导审核；

③ 安全运维部领导需对该项变更的风险和工作量进行审核，审核通过后在“安全运维部领导意见”处签字认可，交安全运维部分管系统管理员安排实施变更；

④ 如果变更由外协公司人员负责实施，业务人员需提交一式两份需求变更申请单，一份留安全运维部存档，一份交外协公司保管，作为日后计算工作量的依据。

3、附件

附 1：系统变更申请表

系统变更申请表

以下内容由发起单位填写

发起人		**日期**		**要求期限**	
联系电话		**单位\部门**			
变更内容或需求目标	☐数据变更　　☐应用变更　　☐网络变更 （如表格无法显示全部内容可附附件做详细说明）				
业务部门主管意见					
分管领导意见					

以下内容由安全运维部填写

系统管理员意见	
领导审批	
承办情况	办理人员签字：

变更任务号：<u>000000000XXX</u>

附 2：变更过程记录

变更过程记录单

变更记录	
变更任务号：	
变更前描述	**变更后描述**
变更实施人：　　年　月　日	

第十章　备份与恢复管理

1、总则

（1）目的

为规范黄石大数据信息发展有限公司存储备份系统管理，加强存储备份工作的日常管理及考核水平，保障系统安全稳定运行，明确管理责任，特制定本办法。

（2）范围

本办法涉及的存储备份系统包括：存储设备、光纤交换机、移动介质、备份软件；管理适用对象包括安全运维部相关运维人员。

（3）职责

系统管理员：负责存储备份系统的管理，包括存储设备的规划和空间分配管理、光纤交换机 Zone 管理、制订备份恢复策略、组织实施备份恢复工作等。

运维人员：负责存储备份系统的日常保养，包括系统日常巡检、故障上报及维护工作许可、并配合系统管理员完成排除故障工作等。

系统集成商和原厂商：负责提供存储备份系统的售后技术支持与服务，包括系统调优并对日常运行维护中的技术难点提供解决方案与支持。

2、管理细则

（1）备份范围和备份方式

① 数据备份范围包括重要云主机系统的操作系统、系统

配置文件、数据文件和数据库。

② 备份方式有全备份（Full）、增量备份（Differential Incremental）、积累备份（Cumulative Incremental）和数据库日志备份（transation log）。

③ 各系统管理员根据自己负责系统的具体情况选择备份方式，基本原则是：保证数据的可用性、完整性和保密性均不受影响，且不破坏业务的连续性。

（2）存储备份系统日常管理

① 存储备份系统由安全运维部安排专人负责管理和日常运行维护，禁止不相关人员对系统进行操作。系统集成商或原厂商须经许可，方可进行操作，并要服从管理、接受监督和指导。

② 任何人员不得随意修改系统配置、恢复数据，如需修改、恢复，须严格执行工作制度，经批准后方可操作。

③ 对系统的变更操作须在系统配置文档中进行记录。

④ 重要系统的数据必须保证至少每周作一次全备份，每天作一次增量备份。

⑤ 应定期（每年）对备份恢复工作进行测试，以确保备份数据的可恢复性。

⑥ 当存储备份系统出现告警或工作不正常，引起应用系统无法访问、系统不能备份时，应立即启动应急预案，恢复系统正常运行，并及时上报。

⑦ 日常巡检管理

■ 当日值班员需每天对存储备份系统进行巡检，巡检内

容须纳入机房值班管理。

- 巡检内容：检查存储设备的电源风扇模块、控制器状态、控制器连接端口、盘柜物理硬盘状态和电池运行是否正常。检查光纤交换机电源模块运行是否正常和各端口连接是否正常。
- 系统需定期（每季度）进行一次健康检查，检查内容及工作方案由系统管理员配合系统集成商和原厂商制定，经批准后方可执行，并提交详细的定检报告。

3、附件

附 1：数据备份记录表

数据备份记录表

备份日期	备份时间	备份方式	存放位置	备份人员	备份内容	备份文件名	备注
填表说明：备份文件名需要填写备份操作所涉及的备份来源设备（或 IP 地址、主机名），避免备份文件冲突							

第十一章　介质安全管理制度

1、总则

（1）目的

为规范黄石大数据信息发展有限公司内部移动存储介质的使用和管理，防止出现因移动存储的使用造成黄石大数据信息发展有限公司网络与信息系统感染病毒、信息外泄等情况，根据黄石大数据信息发展有限公司信息安全建设及保密工作需要，特编制本规定。

（2）范围

本管理程序适用于黄石大数据信息发展有限公司对可移动介质的安全管理。

（3）职责

安全运维部负责全公司移动介质的安全管理，具体管理工作由安全运维部文档管理员负责。

（4）术语、定义及缩写语

下列术语和定义适用于本管理标准。

可移动介质 Removable media

可移动介质主要是指用于记录、存储、拷贝数据信息的移动硬盘、软盘、磁带、光盘、U 盘、存储卡等磁、光及半导体介质载体。移动存储介质包括：软盘、光盘、磁盘、移动硬盘、U 盘、CF 卡、SD 卡、MMC 卡、SM 卡、记忆棒、xD 卡及手机、相机、磁带等。

2、管理内容及要求

（1）可移动介质的使用和登记管理

① 原则上黄石大数据信息发展有限公司内部只能使用由黄石大数据信息发展有限公司统一派发的移动存储设备，禁止外来移动存储设备在我公司内使用，确因工作需要须到指定专用计算机上使用。

② 文档管理员应对可移动介质进行登记管理。登记信息应包含介质类型、重要程度、存放地点等内容。介质重要程度根据存储信息数据类型分为“工作秘密”、“内部公开”、“外部公开”三种类型。

③ 涉及业务信息、系统敏感信息的可移动介质应当存放在带锁的屏蔽文件柜中，对于重要的数据信息还需要做到异地存放。其他可移动介质应存放在统一的位置。

④ 安全运维部对移动存储介质要定期（至少每年一次）进行检查盘点，随时掌握每个移动存储设备的工作状态，监控设备使用过程。

（2）可移动介质的维修管理

① 常规的介质错误或软故障维修由安全运维部文档管理员进行维护处理。

② 移动介质如发生硬件故障、损坏等情况需要外送维修时，必须由文档管理员对介质中的敏感数据进行清除处理，清除处理后的数据必须不可恢复。

③ 对于数据无法识别也无法清除的涉密移动介质可由文档管理员提出申请走介质报废流程。

（3）可移动介质的销毁管理

移动介质的销毁必须经安全运维部同意后由文档管理

员当众销毁，任何人不得自行销毁公司的移动介质。移动介质销毁可参照下述方式进行。

① 移动硬盘：文件先做删除，高级格式化后，低级格式化。报废的硬盘，需要粉碎报废。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。

② U 盘：报废后能正常使用的写入大量数据并格式化后粉碎，不能正常使用的直接粉碎。

③ 光盘：一次性光盘，粉碎。可擦写光盘，格式化后再使用。

④ Flash 卡：报废后粉碎。

3、附件

附 1：介质登记和盘点记录

介质登记和盘点记录

编号	重要程度	存储内容	存放地点	16 年登记状态	17 年盘点状态	18 年盘点状态	19 年盘点状态
1							
2							
3							

附 2：介质销毁登记记录

介质销毁登记记录

介质编号	销毁原因	数据处理情况	经办人签字	批准人签字	时间
1					
2					
3					

第十二章　资产安全管理制度

1、总则

（1）目的

规范黄石大数据信息发展有限公司信息资产的管理、使用和处置，防止其滥用和丢失，保护数据安全。

（2）范围

适用于黄石大数据信息发展有限公司信息资产的管理，包括：获得、分类分级、使用和处置。

（3）职责

投资发展部：主要负责信息资产的采购、入库。

综合管理部：主要负责信息资产的领用、为资产建立台账。

安全运维部：负责使用与处置方法，并监督各部门的执行情况。

各部门：按照相关规定，对信息资产进行有效使用和管理。

（4）术语和定义

信息资产：本文件中的信息资产是指可以存储信息数据的信息载体，包括：硬件、软件、数据（电子数据）、文档（实体信息）、人员、服务设施、其他。

2、管理细则

信息资产的生命周期可分为采购与生成、使用与更新、销毁与废弃三个阶段。

（1）信息资产的获取

软件、硬件设施、服务性设施等的获得主要以采购的方式获得，采购按照有关规定进行采购和验收。

（2）信息资产的分类

① 信息资产的分类

各部门根据业务流程列出信息资产清单并将每项资产的资产类别、信息资产编号、资产现有编号、资产名称、所属部门、管理者、使用者、地点等相关信息记录在资产清单上。资产的分类原则和编号原则如下：

分类原则：

- 硬件
  - 计算机设备：(台式机、笔记本)、（WWW、SMTP、POP3、FTP、DNS）等服务器（含虚拟机）；
  - 存储设备：磁带机、磁盘整列、磁带、光盘、软盘、移动硬盘等；
  - 网络设备：路由器、交换机、HUB、网关、程控交换机等；
  - 传输线路：光纤、双绞线、电话线(布线)、电源线；
  - 安全设备：硬件防火墙、入侵检测、网络隔离设备（如网闸）、负载均衡设备、身份验证、SOC、UTM 等；
  - 办公设备：打印机、复印机、扫描仪、传真机、碎纸机、写字白板、应急照明设备；
  - 保障设备：动力保障设备（UPS、变电设备）、空调、保险柜、文件柜、门禁、消防设施等；
- 软件

- 如：操作系统、办公软件、应用软件、网管软件、杀毒软件、财务软件、开发工具和资源库等。

■ 电子数据

- 存在电子媒介的各种数据资料。如：源代码、数据库数据、各种数据资料、系统文档、运行管理规程、计划、日周月报告、财务报告（电子版本）、用户手册、方案、电子设计图纸等。

■ 实体信息

- 纸质的各种文件。如：传真、电报、财务报告、发展计划、合同、纸张图纸等。

■ 服务性设施

- 如：电源、空调、保险柜、文件柜、门禁、消防设施等。

■ 人员

- 如：公司各级领导、各级正式雇员、临时雇员等。

■ 其他

- 如：公司形象、客户信息等。

② 信息资产的分级

按照信息资产的公开和敏感程度，以及信息资产对系统和组织的重要性，信息资产的分级原则有两个：

对于文档（含电子文档与纸质文档）、介质类的数据载体，按照承载信息本身的公开和敏感程度，该类信息资产拟划分为“工作秘密”、“内部公开”、“外部公开”三级，针对不同级别的资产标识不同的保护等级。

对于其他物理设备，按照其对系统和组织的重要程度，该类信息资产拟划分为“关键资产”、“重要资产”、“普通资产”三级，针对不同级别的资产标识不同的防护等级。

信息资产分级划分具体方法：

- 关键资产：承载、处理或存储公司核心业务信息系统数据，一旦破坏，会对公司的主营业务造成冲击和损害。原则上承载处理业务信息系统数据的资产均应被标识为关键资产。
- 重要资产:对公司某一部门提供服务的信息系统所含资产、或属于业务信息系统的支撑系统的信息系统所含资产，如财务信息系统所有资产、人力资源系统所有资产、OA 办公自动化系统所有资产、防病毒系统所有资产、入侵检测系统所有资产等。
- 普通资产：除上述信息系统以外的信息系统包含资产均可划分为普通资产，如不直接承载、存储业务信息系统的打印机、打码机等。
- 工作秘密：涉及公司明确规定需要保密的信息、业务信息系统数据、公司财务数据、人员工资数据、信息系统账号等的信息数据文档均应划分为工作秘密。
- 内部公开：在公司内部公开,对外保密的信息,向外扩散有可能对公司的利益造成损害的数据文档。
- 外部公开：对社会公开的信息，公用的信息处理设备和系统资源等信息资产。

③ 信息资产的标识

■ 信息资产标注的原则

对不同安全类别的信息进行明确的标识，有助于内部相关人员依照有关信息安全规章制度进行具体操作和处理，从而最大限度地降低人为的误操作带来安全隐患的概率。

a. 所有信息资产安全分类标识必须正确反映该信息的安全防护级别，信息安全工作小组对信息安全分类有最终决定权。

b. 对所有的信息安全分类标识，由信息安全工作小组作定期更新维护。

c. 电子格式的数据和文档采用电子方式进行分类标识。其他形式的资产采用贴标签的方式对信息进行分类标识。

■ 信息资产标注的方法

a. 电子信息

- 电子格式的数据和文档采用电子方式进行分类标识。标识分为“工作秘密、内部公开、外部公开”三个类别。
- 对于电子文档，应在文档的页眉、页脚、或封面开始部分的醒目处进行标识。
- 其他电子信息，如配置信息、备份数据等，如果可以采用电子方式进行标识，则采用电子方式进行标识。
- 对于技术手段上不能进行标识的电子信息，可以在文件名称上加上密级标识，或者采用对信息载体进行物理标签标识等其他方法。
- 如果文档是由已经标识好的电子文档打印出来的，则

不需要再做任何标识。

b. 物理资产

- 采用贴物理标签的方式对信息进行分类标识。

c. 信息资产标注的内容

信息资产分类标识必须包括并不仅限于下列信息：

- 简单描述或内部编号
- 安全类别/重要程度
- 资产管理员

④ 信息资产的识别与汇总

通过业务流程分析，识别各个流程的各类关键信息资产，最终安全运维部汇总《信息资产清单》，并每半年进行一次更新，确保重要信息资产的完备性（重要信息资产没有遗漏和缺失）和准确性（信息资产的保密级别和重要程度能够真实反映信息资产的状态）。

（3）信息资产的使用规范

① 硬件资产的使用规范

- 所有的硬件资产必须明确设备的使用人员/管理人员,明确职责。
- 硬件资产的使用人（或管理人），在使用或管理硬件资产时，要注意硬件资产的安全性、机密性、完整性，防止信息载体的毁坏和信息的泄密，防止信息处理设施的滥用。
- 对设备定期进行维护保养，发生毁坏，丢失等问题时能够及时处置。
- 新硬件设备接入网络按照相关规定处理。

- 当设备迁移时，如果设备中存储有重要信息时候，需事先进行备份；
- 设备迁移完成后，需要检查设备是否损坏；
- 设备迁移出黄石大数据信息发展有限公司时，检查人员在检查时要格外注意，禁止设备中存放重要信息，以防止公司机密信息泄露或泄露的风险增加。
- 离开公司的设备和介质,如客户现场的设备和介质需要有人值守或委派负责人(或者公共场所放置的需要有人值守或监视系统)。
- 在旅行时便携式计算机（笔记本电脑）要作为手提行李携带，若可能宜伪装起来；

② 软件资产的使用规范

- 所有的软件资产必须设置专人管理，明确职责，避免软件资产的丢失，泄密。
- 所有正版软件实体由安全运维部保管，在安装软件时要规定使用权限，防止非授权访问。
- 公司自己开发系统软件的源代码应进行备份。
- 对公司重要系统,如邮件系统,文件服务器系统进行备份。
- 当人员离职或岗位变动，需要回收有关的软件，必要时，由安全运维部人员对离职人员使用的软件进行卸载,删除。

③ 电子数据的使用规范

- 对所有电子数据进行分类/分级,标识未授权人员的访问限制，不同安全级别的数据应存储在不同的区域，按类按级传达，便于信息的安全管理。

- 不同类型的电子文件按照统一规律存放在个人电脑或服务器中，便于整理和查阅以及工作交接时转移。
- 所有电子文件保存在电脑或服务器中，并按照规定的备份频率定期进行备份。
- 对于存于服务器上的电子数据的访问，会根据服务器提供服务的不同与部门／职务的不同，设备不同的访问权限，减少非受权的访问.
- 对于工作秘密级别的电子信息，要由专人管理，存放在受权限控制的路径下。
- 对于内部公开级别的电子信息,其使用要控制在公司内部，禁止带出公司。

④ 实体信息的使用规范

- 所有的工作秘密级的实体信息资料要（通过标签或其它方式）标识出资产的保密级别，分类存放，不同安全级别的实体信息应按类按级传达，便于实体信息的安全管理。
- 对于比较重要的工作秘密实体信息必要时保存在带锁的柜子或保险柜子中，柜子钥匙由专人保管。
- 对于实体信息的保存期限依据备份相关制度进行实施。
- 对于比较重要的实体信息的使用过程,应注意信息的保密，确保信息的完整性和可用性;
- 对于比较重要的实体信息的传输，应采取适当的安全措施加以保护，如专人递送、分散传输等。

3、附件

附 1：信息系统资产清单

信息资产清单

资产编码	资产名称	资产类别	在用部门	IP 地址	重要程度	责任人	用途

附件 2：信息系统资产转移单

信息系统资产转移单

转出部门	转入部门	转移日期	接收人	资产状态

第十三章　软件开发管理规范

1、总则

黄石大数据信息发展有限公司目前的应用系统均为外包开发，但对于外包系统的开发，外包系统商必须按照黄石大数据信息发展有限公司的开发安全规范进行开发，以保证开发系统符合黄石大数据信息发展有限公司信息安全规范需求和信息安全等级保护需求。

在应用外包开发商与黄石大数据信息发展有限公司签订应用外包开发合同时，此协议必须作为外包开发合同的附件对外包开发商的外包开发行为的开发过程进行规范和约束。

如外包开发商的开发过程未按照该规范进行，黄石大数据信息发展有限公司有权拒绝为该开发交付物付款，且保留进一步追究外包开发商违约的权力。

2、应用安全要素

应用软件（或系统，下同）的开发阶段是其生命周期内的一个重要阶段，在此阶段，将主要完成应用软件的需求分析、设计实现及测试等工作，此阶段的工作将极大程度地决定了应用软件本身的安全性，因此，要确保信息安全在此阶段的各个具体工作过程中的贯彻和实施，以便交付具有高安全特性的应用软件，为将来应用软件的安全投产运行奠定坚实的基础。

与信息安全的基本要素一样，应用软件开发过程中要关注的安全要素主要包括机密性、完整性、可用性。

（1）机密性

机密性是指保证只有被授权访问的人才可以获取信息，具体包括身份鉴别、授权、安全通讯等措施。

（2）完整性

完整性是指保证信息和处理方法是正确和完全的，免受非授权、意料之外或无意的更改，具体包括数据校验、审计、安全通讯等措施。

（3）可用性

可用性保证经过授权的用户在需要时可以访问/使用相关信息资产，具体实施手段有灾难备份/恢复、冗余、业务持续性计划等。

3、安全开发过程

应用软件的开发过程一般包括以下阶段：

（1）需求分析阶段

完成挖掘与分析最终用户需求的工作，总结出应用软件所要完成的功能定义及相关要求。

（2）架构与设计阶段

完成应用软件的架构设计及其他必要的详细设计工作。

（3）编码实现阶段

按照设计文档的要求，在具体的基础平台上实现应用软件。

（4）测试阶段

试应用软件中实现的功能是否满足用户的要求。

要在应用软件开发过程中实施安全性，其过程也是相同

的，即将安全性所涉及的具体工作落实到以上过程中，即：

（1）安全需求分析阶段：

对应用系统面临的各种风险、业务安全要求、需要保护的资源以及如何保护等进行分析，同时在一些主要的技术实现的环节提出明确定义的、可衡量的技术安全需求。

（2）安全设计阶段：

按照安全需求的要求和通用的安全设计原则来设计合理的、安全的系统架构，并对一些具体环境所使用的安全技术进行定义。

（3）安全编码阶段：

对安全设计过程中所确定的安全架构和安全技术为基础，参照通用的安全编码要求来编码实现应用软件。

（4）安全测试阶段：

针对系统提供的安全功能进行测试，以确定其正确、恰当地完成了所有功能，同时要以攻击者的身份进行攻击测试，以测试应用软件中是否存在漏洞。

4、安全需求分析

在安全需求分析阶段，主要关注以下几个方面的内容：

（1）风险分析

对目标系统/软件中可能出现的安全风险进行全面分析，并尽量对这些风险进行概率及影响评估。风险分析可以从业务和技术两个角度入手，下面列出（但不限于）了几种可能的要素：

- 误操作

- 人为破坏
- 非授权操作
- 软硬件平台质量及其安全漏洞
- 其它风险

在进行目标系统/软件的风险分析时，要尽量准确地评估各种可能存在的风险点、发生的概率及造成的损失。

（2）业务安全需求

从业务管理、业务风险的角度具体提出系统需实现那些业务控制措施。包含的要素有：

① 交易分类描述系统/软件中如何划分各类不同级别的交易，及每个级别交易操作所需要的权限。

② 帐务控制描述系统/软件中如何控制各类帐务信息的显示、操作等，如普通操作员不能查询总分类帐务及其报表等。

③ 现金相关操作描述系统/软件中如何对与现金相关的操作进行控制，对于现金额度超限的操作如何控制等。

④ 信息归属相关操作对于交易/操作中的重要业务信息，定义其查阅方式及其所需的操作权限、级别等。

⑤ 特殊操作对诸如交易冲正、隔日冲帐、跨部门操作等特殊操作，如何进行控制。

⑥ 管理制度对于系统/软件面向的业务领域的一些其他安全控制措施、行业规范、业务管理制度以及规定等，如何体现在系统中。如在建设网上银行系统时，就必须考虑人民银行关于网上银行的安全规范、国家有关商用密码、CA 的

管理制度。

（3）技术安全需求

以安全的三个通用要素（机密性、完整性、可用性）为基础，从技术角度入手，描述系统应满足或实现的安全需求，如果系统中子系统或模块较多，则在每小节中按照子系统或模块分别提出安全需求。

① 机密性

机密性指保证只有被授权访问的人才可以获取信息。机密性要求信息免受非授权的披露。它涉及到对计算机数据和程序文件读取的控制，即谁能够访问那些数据。它和隐私、敏感性和秘密有关。机密性的要素包括：

用户鉴别方式用户鉴别是指如何验证用户的合法身份，有时也称身份验证或身份认证，用户鉴别的方式较多，可以根据系统的安全级别、成本投入等因素来确定验证方式。

常见的鉴别方式有固定密码、动态密码、数字证书、基于生物特征（如指纹识别）或它们的任意组合等。

授权方式授权方式是指如何进行具体操作的授权，也称为访问控制方式。要在此说明系统/软件是集中进行授权控制，还是分散地、逐级的方式进行授权控制。

对于操作员可以对进行那些操作的权限控制，目前使用较为普遍的方式是基于角色的访问控制（ Role Based Access Control），即先将各种操作权限授予预定义的角色，然后再指定用户属于那些角色（一个用户可以扮演多个角色），通过对用户所属角色的检查，就可以获得用户可以进

行那些操作。

如果选用基于角色的授权方式，要根据系统 /软件的实际情况划分角色，并定义角色所能完成的操作。

- 抗抵赖性

指出哪些重要的业务操作需要防止抵赖，如可能，指定抗抵赖的方式，如：记录操作日志（有据可查）、具有电子签名和时间戳（法律依据）

- 加密级别的选择按照数据的重要程度可以选择加密级别，加密级别有：
  - 秘密：普通加密/编码，可反向解密/解码
  - 机密：高级加密，需要大量计算资源及较长时间才能解密
  - 绝密：最高加密，使用非对称算法或 128 位密钥长度以上的对称算法，保证破解的可能性接近于 0
- 数据存储安全

对于系统/软件中要加工或处理的数据的物理存储，需要以何种方式保护，主要指数据库安全保护，尤其是对绕过系统/软件本身，直接对数据库的存取行为的控制要求。

- 数据传输安全

指定哪些数据，在通过哪些传输通道的时候，应进行安全保护。数据传输安全可以分为应用程序间的传输安全（SSL等）和网络间的传输安全（IPSec），前者适用外部或公用网络，后者适用于内部或专用网络。

➢ 隐私保护

遵照有关国家法律、行业规范及业务管理规定，定义哪些客户信息、资料等为隐私信息，并要实行哪些保护或隐藏措施，以免这些信息泄露给外部其他人或内部操作人员。

➢ 日志指定系统中记录日志的范围、详细程度等。

② 完整性

完整性的目标是保证信息和处理方法的准确与完整。完整性要求信息必须是正确和完全的，而且能够免受非授权、意料之外或无意的更改。完整性还要求计算机程序的更改要在特定的和授权的状态下进行。普遍认同的完整性目标有：

数据检查对哪些数据要做何种检查（数据格式、数据内容等），以防止由于用户输入特殊数据使得系统安全受到威胁。

➢ 数据校验

列举在系统/软件中那些数据需要额外的数据校验，以检验数据是否来自可信源，是否被篡改。

➢ 防止数据损坏

防止数据在存储或传输的过程中，是否采取额外的手段验证数据，以确保数据的正确性。

➢ 数据容错机制

对于稳定性要求比较高或数据非常重要的系统，有必要采用容错机制以防止由于硬盘损坏等事件导致数据丢失。容错机制普遍采用磁盘冗余阵列（RAID）不间断电源（UPS）等。

- 数据备份机制及周期
- 数据存取日志等

③ 可用性

可用性是保证经过授权的用户在需要时可以访问信息并使用相关信息资产。可用性要求信息在需要时能够及时获得以满足业务需求。它确保系统用户不受干扰地获得诸如数据、程序和设备之类的系统信息和资源。不同的应用有不同的可用性要求。

- 可用性指标（平均无故障时间）

平均无故障时间通常以可用时间百分比来表示，无故障时间计算公式为：无故障时间= 可用时间百分比 X 运行总时间。

- 业务持续性要求

如何防止单点失效后造成的业务中断，如采用双机热备措施等。

- 灾难恢复要求

为了在系统遭受攻击或意外灾难后能够快速恢复，应考虑的备份措施、工具等。

④ 其他安全相关因素

除以上内容外，还要对应用软件的其他与安全相关的要素进行分析说明，由于这些要素和安全要求相关，要根据系统的实际情况进行选择。

5、安全设计

在安全设计阶段，主要完成安全需求、安全技术在架构

及设计中具体体现，此阶段非常关键，它从很大程度了将确定最终的应用软件的安全性。

（1）通用设计原则

在进行应用软件的安全设计中，要遵守和贯彻以下一些通用原则：

① 整体安全

系统的整体安全程度受最薄弱环节的制约，因此考虑安全性时，应该将应用程序所有层的安全性都考虑在内，尤其是加强整个安全链条中较弱环节的保护。

② 纵深防御

在应用系统之间或应用软件的每一层或每个子系统中都要设置检查点，进行身份鉴别，授权检查，数据检查及校验等安全检查工作，确保只有经过身份鉴别和授权的用户能够访问下一层，而且确保数据的合法性。

③ 职责分离

职责分离通常是应用在职能与责任方面的一条安全原则。职责分离包含两个方面的内容：一是限制单个用户的能力，以免其做出欺诈行为或滥用其权限；二是在划分应用程序的组件时，设计人员应该尝试根据功能和权限来划分它们，不同功能应由不同的组件来处理，如订单处理与检查账户状态的组件应该区分开。

对于用户的职责分离来说，如果在一个安全模型中确定了用户或用户角色，而且他们各自具有不同级别或类型的信息资产访问权限，那么应进行用户职责分离。虽然由角色和

权限构成的矩阵是由客户来定义的，但是设计人员必须确保应用软件能够提供必要的支持功能来满足客户的这种需求。

对于组件的职责分离来说，可以按照各种不同的方式划分组件，如：

- 按照编程人员划分：各个编程人员应该编写不同的组件，尤其对大多数安全敏感型的组件来说，更应该这样；
- 按照管理员划分：各个系统管理员应该负责管理不同的组件；
- 按照网络层次划分：各个组件应该被分布部署到网络的各个层次中，因为各层面临的攻击程度不同；
- 按照功能划分：每一个组件中只包含必要的功能；

具有不同权限的组件大多是完全隔离的。考虑将展现层和应用层的功能划分开的这种情况，一般来说，展现层所包含代码的权限要比应用层代码的权限低。例如，展现层的代码通常不能直接访问数据库，而应用层的代码就可以。

④ 最小权限

对于系统中用户，应该只授予其完成必要功能的最小权限，避免其提升权限

对系统安全带来威胁。

对于执行代码的进程应当尽可能用权限最少的帐户运行，从而在危及进程安全时限制可能造成的破坏。一般情况下禁止以系统管理员的身份来执行应用程序。如果恶意用户设法将代码注入某个服务器进程，那么授予该进程的权限会在很大程度上决定该用户可执行的操作类型。应当将需要更

多信任（和更高权限）的代码分别隔离在不同的进程内。

⑤ 默认安全

开发人员往往仅仅为了使应用程序不受限制地运行而经常使用较高的系统权限，而且在应用程序内部采用宽松的安全控制措施。这可能会带来两方面的问题：在系统权限（如操作系统的文件访问控制）较为严格的情况下，应用程序的功能可能失效；在应用程序内部，较低权限的用户可能会不受限制地提升权限而执行一些权限要求较高的功能。以上两方面的影响都会对应用软件的正常运行带来较大的影响。

因此，应按普通用户（即非管理员）的身份来设计和测试应用程序，同时，在应用程序中，应采取严格的权限控制措施，对于未明确授予的权限，应予以拒绝。

⑥ 减小暴露界面

尽量减少应用软件的暴露界面，因为任何暴露界面都可能成为攻击者的目标，减少暴露界面即有助于降低被黑客攻击的可能性，也有助于把有限的资源更好地投入到所必需保护的信息资产上。

（2）安全技术的使用

针对所关注的安全主题，在安全技术使用上，要合理、恰当，推荐使用业界一些成熟的安全解决方案，如以公用密钥体系（PKI）为基础的各种应用。具体在各个安全控制环境，要有针对性的采用应用的安全控制措施。

⑦ 身份鉴别

对于用户的身份进行识别是每个系统进行安全保护的

第一道关口，在各种基础平台中已经提供了相当多的、可靠的身份鉴别技术，例如：

Web 服务器提供的明文验证、摘要式验证、集成验证、数字证书验证

操作系统提供的集成验证

数据库管理系统身份验证等如果由于某些限制而不能利用以上技术，可以使用一些类似的自定义的身份鉴别技术，如常见的用户名/密码的鉴别方式。

除了单要素身份鉴别方式外，可以使用多要素验证方式和一些安全性非常高的基于生物特征的身份鉴别技术，如指纹识别等，在成本可控的前提下，为应用软件提供最为安全的保护。

在提供身份鉴别机制的同时，也要注重提供相应的安全策略控制，在身份鉴别方面一般需要提供以下方面的策略控制：

- 密码复杂性要求

如对密码长度、字母或数字的组成等进行限制，以防止出现弱密码。

- 密码使用周期

密码存留期（即多长时间后强制更改密码）、是否记录密码历史。

- 登录策略

是否对用户的登录位置和时间进行限制，是否允许同一用户在多个位置同时登录等。

- 帐户锁定

经过指定阀值的失败登录尝试后，是否锁定登录的目标用户，锁定的时间、解锁的方式等，对于已登录用户，经过指定阀值的未操作时间后，是否锁定界面等。

- 注销

多长时间未操作将自动注销等。

⑧ 授权

授权主要是指对于登录进入系统的用户的操作权限进行合理设置，以使其完成所需工作。

在各种基础平台中已经都内置较为完备的授权机制，可以充分利用，如下列表所示：

- 操作系统的文件系统权限设置
- 应用基础平台中的授权框架，如.NET 中的角色与用户控制，Java 中的鉴别与授权服务（JAAS）等
- 数据库管理系统中的数据库角色、数据库对象权限设置

除了利用基础环境的访问机制外，可以在应用软件中设计实现自定义的访问控制，这种访问控制一般是采用基于角色的授权机制（ RBAC），RBAC 访问控制模型实现了用户与访权限的逻辑分离，减少了授权管理的复性，降低了管理开销，而且与日常信息统管理的架构类似，降低了管理复杂度。

要配置和设计实现授权体系时，要特别注意以下事项：

- 在进行授权体系的设计时，一定要完备，避免个别环境的控制措施缺失所带来的安全隐患；

- 严格执行最小权限原则，只给用户开放完成其功能所必须的权限；
- 在用户执行每个功能前，要首先对其权限进行检查；
- 要注意 Web 应用系统中所包含的URL 资源进行严格权限设置，这是一个最易受攻击的区域；
- 要利用数据库服务器集成的权限控制措施来控制用户的操作权限，要限制一些危险操作的进行，如删除数据表、更改数据库结构、执行危险的存储过程等。

⑨ 安全通讯

目前在操作系统和网络层次，已经提供了较为成熟的安全通讯技术，如果是利用已有的应用传输协议（如 HTTP、FTP 等），完全可以利用对应用安全套接字（SSL）的协议（如 HTTP、SFTP 等）。目前操作系统及相应的应用基础平台对这些安全协议支持十分完备，配置使用也十分简单。

如果不是利用已有应用传输协议，而是基于自定义的 TCP/IP Socket 通讯应用，基于操作系统、网络环境及系统效率的考虑，一般可以使用网络层的透明安全机制，即 IPSec 来保证数据传输的安全，IPSec 作为业界标准协议，在各主流操作系统上都有很好的支持。

如果由于部分环境的限制无法实现以上两种保护机制，要使用自定义的加密机制来对保护被传输的数据，即在数据传输加密前后分别进行加解密。

使用安全通讯机制，将对系统性能带来一定的影响，因此要合理评估其使用范围，但要注意的是在用户鉴别等传输敏感的环节一定要采用安全传输协议。

⑩ 日志

在应用系统中，要根据用户的需求、系统效率的考虑来实现合理的、完备的日志记录，以实现系统对于审计的支持。

日志中至少应包括如下信息：日志类别（一般信息、警告、错误）、日期与时间、日志内容、当前操作用户名、操作用户所在的机器名或地址（IP）以及处理结果（成功或失败）等。

通过利用以上日志信息结合基础平台（如操作系统、Web或应用服务器、数据库服务器等）内置集成的日志功能，能够最大限度地为审计提供数据支持。

在进行日志功能设计时，要考虑其可能对系统性能带来的影响。

⑪ 数据安全

除了保证数据库中存储数据安全，还要对数据库服务器以外的一些关键数据进行安全保护，这些数据包括 Web 服务器、应用服务器和客户端（浏览器）中与应用系统有关的配置信息（如数据库连接定义、后台系统连接定义等）、缓存数据、会话数据、临时数据以及 Cookie 等。

实现数据安全的主要机制是加密和完整性校验，在选取加密算法时，要根据不同场景采用足够安全但又不会影响系统效率的算法，数据加密方法及适用情况如下所示：

- 如果数据量较大，要求效率较高，一般采用对称加密算法，如 3DES、AES 等；
- 如果数据量较小但安全要求高，可以采用非对称加密算法，如 RSA 等；
- 如果数据量较大，要求效率较高，同时也要求具有很高的安全性，则可以使用非对称加密算法来完成密钥交换，然后再使用交换密钥和对称加密算法来加解密数据。
- 如果要对数据进行完整性校验，则一般可采用简单的循环冗余校验（CRC）算法或一些散列（哈希）算法，如 MD5、SHA1 等算法。

6、安全测试

安全测试工作是同应用软件的整体功能测试工作同时进行的，安全测试工作一般包括两部分：安全功能测试和穿透测试。在测试过程中，安全功能测试的工作是必须要完成的。

安全功能测试是一种白盒测试方法，其目的是验证安全控制机制是否存在，

是否满足要求。而穿透测试则是从攻击者角度进行的一种黑盒测试方法，其目的是检验安全控制措施是否完备和有效。一般情况下，穿透测试在安全功能测试之后进行，且应由不同的团队来分别完成。

安全功能测试的目标是基于安全需求分析和安全设计来进行的，确认安全需求分析中用户所要求的安全功能（如

身份鉴别、授权、数据机密性保护、日志与审核等）都已满足，确认安全设计中定义的功能和使用的技术是正确的、完整的。

对于穿透测试，没有指定的模式，任何能够突破系统安全控制的方法和技术都可以使用，其目标也包含应用软件的方方面面。

7、其他安全问题

（1）配置安全

要加强软件开发环境的安全性，即加强配置管理的安全性，防止与应用软件开发相关的核心技术、设计文档、源代码等内容的泄露，这不但可能造成知识产权的损害，而且可能会给攻击者分析应用软件的处理逻辑和漏洞从而发起攻击的可能性。

（2）部署安全

虽然应用软件的开发过程并不包含部署过程，但要为下一阶段具体的安全部署做好准备工作，这主要是通过提供完备安全部署文档来完成，即在系统安装/部署的文档中，提供专门的增强安全性的说明，如系统中提供的与安全相关的参数设置等，这里着重强调软件本身中所涉及的内容，操作系统、应用基础软件平台及数据库管理系统的安全性，参照通用其他通用规范或厂商提供文档。

在构建（Build）应用软件的最终可执行版本（即执行码）时，要采用一些必要的安全手段对其进行保护，以防止被篡改，且有助于安全部署。具体措施主要是对与应用程序

相关安装程序、可执行程序、控件（如 ActiveX 或 Java Applet）进行数字签名，以便让用户能够确认其来源和完整性。

8、附件

附 1：源代码变更发布授权审批记录

源代码变更发布授权审批记录

申请人		**申请部门/岗位**	
申请类别	☐代码变更　☐授权发布		
申请的系统名称			
申请陈述			
项目经理审批意见	申请 ☐批准☐拒绝 签字　　年月日		
主管审批意见	申请 ☐批准☐拒绝 签字：年月日		

第十四章　代码编写安全规范

1、通用编码原则

（1）不要信任外部的用户输入或系统。

应用程序应该彻底验证所有用户输入，然后再根据用户输入执行操作。验证可能包括筛选特殊字符。针对用户意外地错误使用和某些人通过在系统中注入恶意命令蓄意进行攻击的情况，这种预防性措施对应用程序起到了保护作用。常见的例子包括 SQL 注入攻击、脚本注入和缓冲区溢出。此外，对于任何非受控的外部系统，都不要假定其安全性。

（2）不要通过隐藏来保障安全。

尝试使用让人迷惑的变量名来隐藏机密信息或将它们存储在不常用的文件位置，这些方法都不能提供安全保障，最好使用平台功能或使用已被证实可行的技术来保护数据。

（3）以安全的方式处理失效

如果应用程序失效（如发生严重错误等），要恰当的进行处理，一定要保护好机密数据。同时，在向最终用户返回错误消息时，不要公开任何不需要公开的信息。也就是不要提供任何有助于攻击者发现应用程序漏洞的详细信息。

2、防范常见安全编码问题

在实现应用软件的编码阶段，也较容易因缺乏严谨思考或不好的编程习惯而引入安全问题，而且这些安全问题产生的危害作用非常大，因其产生的漏洞常常会造成应用程序中其他部分构筑的安全控制措施完全失效.目前存在的相当数量系统漏洞都是由编码问题造成的.因此要想保证应用软件

的安全性，必须在编码阶段继续高度贯彻安全性原则.

在编码阶段，避免安全问题的基本原则如下：

- 程序只实现指定的功能
- 永远不要信任用户输入，对用户输入数据做有效性检查
- 必须考虑意外情况并进行处理
- 不要试图在发现错误之后继续执行
- 尽可能使用安全函数进行编程
- 小心、认真、细致地编程

目前在各种应用软件中常见的安全漏洞如下所示，应对这些常见问题进行有针对性的防范。

（1）缓冲区溢出

如果对输入参数（字符串、整数等）处理时长度检查不严格，或对指针和数组越界访问不进行保护，就容易产生缓冲区溢出（Buffer Overflow）问题，这种问题主要出现在主要出现在C/C++ 语言编写的系统中，它造成的漏洞是当今绝大多数安全漏洞的主要根源。在Java / .NET 等利用虚拟机的(托管)平台上不会产生此问题。

要避免此问题，则必须对系统输入数据进行严格的长度检查，废弃或截断超长的越界数据，同时利用基础库函数中的一些更为安全的字符串处理函数来处理数据，也可以利用编译器或代码复查工具提供的检查功能来尽早发现可能会产生问题的程序。

（2）输入非法数据

恶意的攻击者会尝试在用户界面或接口中向系统输入恶意数据，以便期望绕过系统的安全限制，致使系统出甚至崩溃或其他非法目的，因此在编码时，须要对所有输入数据(包括用户在界面中输入的数据和其他应用系统通过接口传递的数据)进行严格的合法性检查。

（3）SQL 注入式攻击

SQL 注入式（SQL Injection）攻击是一种典型的，因对输入数据不当处理而产生的非常严重的安全漏洞。其原因是基于数据库的应用程序中经常会使用动态 SQL 语句，而且在程序又没有对输入数据严格检查，致使攻击者能在界面层或接口层注入非法的 SQL 语句，从而非法访问和破坏数据、反向工程、甚至对服务器本身造成威胁。对于攻击者来说，SQL 注入式攻击是一种简单有效的攻击方式，也是首选方式，尤其是在基于 Web 的应用程序中，因此开发人员必须重点关注此问题。

预防 SQL 注入式攻击的手段就是严格检查用户输入的数据，要使用基础系统提供的参数化查询接口，避免使用字符串来构造动态 SQL 查询。同时对于数

据库对象的访问权限进行严格限制，避免恶意 SQL 语句破坏数据或系统。

（4）拒绝服务攻击

拒绝服务攻击（Denial of Services -DoS）是指通过大量并发访问，使得服务器的有限特定资源（如网络、处理器、内存等）接近枯竭，使得服务器或系统失效的攻击行为。

DoS 攻击的一般方式有发送大量数据包造成网络阻塞、执行内存泄漏代码使得系统可用内存越来越少、执行大量消耗 CPU 处理能力的代码、通过客户端发送大量的 HTTP 请求造成巨量 Web 点击以及 SYN Flood 等。DoS 攻击虽然不会直接对服务器本身带来损坏，但它使得真正的合法用户无法访问系统，从而可能带来业务上的损失。除了 DoS 之外，攻击者还可能利用数量庞大的攻击源发起 DDoS（Distributed DoS，分布式拒绝服务）攻击，其破坏和危害作用更大。

在编码时要注意防范可能的 DoS 攻击，具体措施包括提高软件行为的可管理性、主动拒绝异常连接、自动锁定攻击源、提供实时监控界面，能够有效甄别攻击源、具有(异常)事件报警机制、具有审核日志等。通过这些主动或被动的防御手段，能够将 DoS/DDoS 攻击行为带来的破坏和危害降到较低水平。

（5）敏感信息泄露

攻击者可能会通过暴力攻击、侦听、截取中间数据、反向工程、社会工程学（Social Engineering）等手段，获取访问凭据或机密信息，危及数据的私有性/安全性或者暴露敏感的商业数据，如用户名/口令、加密密钥、数据库连接串、商业敏感信息等。

因此在处理这些数据时，必须利用以密码技术为主的安全技术来进行强有力的机密性保护。在使用密码技术时，一般要利用公开的、经过广泛验证的可靠加密算法，同时加强密钥的管理和保护。

第十五章　外包软件开发管理

1、总则

（1）目的

明确公司对于软件外包开发的过程控制方法，通过对外包软件过程的有效控制，使外包开发软件满足等级保护的规范和要求。

（2）范围

本管理办法适用于黄石大数据信息发展有限公司对于外包软件的开发管理。

（3）职责

① 安全运维部负责对软件开发方（外包方）的调查、评定和选择。

② 安全运维部提出外包要求，并组织对外包要求的审核，确定后将细节要求纳入外包开发合同。

③ 安全运维部实施对外包过程的控制，并组织在项目结束时对外包供方的评估。

2、管理细则

（1）外包项目过程控制

由安全运维部按照外包合同的规定，对外包项目过程进行控制。

（2）外包软件验收

① 由安全运维部组织专业服务商在软件安装之前检测软件包中可能存在的恶意代码，做代码级审计。

② 要求开发单位提供软件设计的相关文档和使用指南，

作为项目验收的标准之一。

③ 要求开发单位提供软件源代码，并聘请专业服务商审查软件中可能存在的后门。

④ 上述验收无误后，由安全运维部按照外包合同规定的接收准则和方法，参照开发需求检测软件质量，对外包软件进行验收。

（3）外包软件维护

① 在外包合同规定的维护期内，若要对外包软件进行维护，由安全运维部按外包合同规定的维护方法，向该软件开发供方提出维护要求。

② 由安全运维部按照外包合同规定的维护结果接收方法，对维护结果进行确认。

③ 将维护过程中产生的文档，按开发和维护过程配置管理要求，分别纳入配置控制。

3、附件

附 1：外包软件安全检测记录

外包软件安全检测记录

外包软件名称		供方单位名称			
软件可维护性					
检测项目	1	2	3	4	5
代码注释情况					
代码可读性					
模块化程度					
命名规范程度					
软件安全性					
评估项目	1	2	3	4	5
恶意代码检测					
后门检测					
软件文档质量					
评估项目	1	2	3	4	5
可阅读性					
规范程度					
详细程度					

注：若要对外包软件产品的每份文档分别评估，可增加附页。

第十六章　服务商安全管理

1、总则

（1）目的

为了规范黄石大数据信息发展有限公司信息系统建设和运行过程中服务商的选择，按照信息安全等级保护要求进行服务商管理，特制定本管理规范。

（2）范围

本办法适用于黄石大数据信息发展有限公司在信息化建设和运行过程中服务商选择的安全管理。

（3）职责

较小项目由安全运维部负责服务商选择，较大项目的服务商选择，可通过招标方式由招标小组进行选择，但须遵循本管理办法的要求。

2、管理细则

① 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三级集成资质，对于较为重要的系统应有更高级别的集成资质；

② 工商要求：

- 产品、系统或服务提供单位的营业执照和税务登记在合法期限内；
- 产品、系统或服务提供商的产品、系统或服务的提供资格；
- 连续无相关法律诉讼年限要求；
- 没有发生重大管理、技术人员变化和流动的期限要求；
- 没有发生主业变化期限要求。

③ 安全服务商资质：至少应具有国家一级安全服务资质，对于较为重要的系统应有更高级别的安全服务资质；

④ 人员资质要求：系统集成人员、安全服务人员以及相关管理人员应获得国家权威部门颁发的信息安全人员资质认证；

⑤ 其它要求：系统符合国家相关法律、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。

第十七章　系统安全管理制度

1、总则

（1）目的

为进一步强化黄石大数据信息发展有限公司应用系统运行维护管理工作，建立业务、技术支持相结合，规范、高效运转的综合运行维护管理体制，确保各类应用系统稳定、安全、高效运行，特制订本办法。

（2）范围

本办法适用于黄石大数据信息发展有限公司应用系统的运行维护。由于业务处理的特殊性，各应用系统的具体运维管理内容可根据本办法进一步细化。

（3）职责

安全运维部承担各类系统的技术运维工作，具体系统运维工作由安全运维部系统管理员负责。

2、管理细则

（1）运维组织

① 安全运维部经理统筹安排力量，建立以业务、技术支持为主体、以总体运维为依托、以基础运维为基础的高效、有序的应用系统运行维护管理体系。

② 对于各个应用系统，应确定其运维负责主管，各应用系统有关的业务处室还应设立联络人。

③ 重要应用系统，安全运维部确定两名以上技术人员担任系统管理员，实行AB岗制。

④ 对于综合性大型应用系统，由安全运维部指定多人成

立负责小组，负责组织、协调该应用系统的日常运维。

⑤ 安全运维部建立统一的应用系统运行维护管理平台（常规通过堡垒机实现），实现各类应用系统的日常运维管理、行为审核，并通过实现运维信息共享。

⑥ 日常运维人员、第三方维护人员必须通过堡垒机系统来实现运维管理。

（2）身份鉴别

① 应对登录操作系统和数据库系统的用户进行身份标识和鉴别，且口令强度需满足以下要求：密码长度不能少于8个字符；必须由数字、字母或特殊字符的任意组合构成；设置密码时应尽量避开有规律、易破译的数字或字符组合作为自己的密码。

② 密码要定期更换：核心应用系统服务器操作系统及数据库系统密码更换；

③ 服务器操作系统应设置带口令的屏幕保护功能。

④ 应在Windows、Linux、等操作系统中，对身份身份鉴别策略进行安全配置。

⑤ 在windows系列操作系统中，可以通过控制面板→管理工具→本地安全策略→计算机配置→Windows设置→ 账户策略，对其中“密码策略”和“账户锁定策略”进行配置。

⑥ 密码应符合复杂性要求：启用此安全设置后，在更改或创建密码时要求密码必须符合复杂性要求；

⑦ 密码长度最小值：可设置用户帐户密码包含的最少字符数；密码最长使用期限：确定系统要求用户更改密码之前

可以使用该密码的时间（单位为天）；

⑧ 密码最短使用期限：确定用户可以更改密码之前必须使用该密码的时间（单位为天），密码最短使用期限必须小于密码最长使用期限，除非密码最长使用期限设置为 0（表明密码永不过期）；

⑨ 强制密码历史：重新使用旧密码之前，确定与某个用户帐户相关的唯一新密码的数量，将确保旧密码不被连续重新使用来增强安全性；

⑩ 用可还原的加密来存储密码：确定操作系统是否使用可还原的加密来存储密码，此项设置将降低密码的安全性，除非应用程序必须，否则严禁启用。

⑪ 帐户锁定时间：确定锁定的帐户在自动解锁前保持锁定状态的分钟数；

⑫ 帐户锁定阈值：确定造成用户帐户被锁定的登录失败尝试的次数；

⑬ 在此后复位帐户锁定计数器：确定在登录尝试失败计数器被复位为 0 之前，尝试登录失败之后所需的分钟数。

⑭ Linux 系统的密码策略可以通过多种方式进行实现，比较常用的有：/etc/login.defs 文件控制、pam_cracklib 模块或 pam_passwdqc 模块。/etc/login.defs 文件中可以配置以下参数：

- PASS_MAX_DAYS：密码的最大使用天数；
- PASS_MIN_DAYS：密码的最小使用天数；
- PASS_MIN_LEN：密码的最小长度；

- PASS_WARN_AGE：密码失效前多少天通知用户修改密码。启用 pam_cracklib 模块须修改/etc/pam.d/system-auth 文件，实例如下：
- Passwordrequisepam_cracklib.sominlen=8ucred=-2lcred=-4dcred =-1ocred =-1;
- minlen：密码的最小长度；
- ucred 信息技术=N：大写字母个数；
- lcred 信息技术=N：小写字母个数；dcred 信息技术=N：数字个数；
- ocred 信息技术=N:其他字符个数,如键盘上的标点符号、特殊符号等。
- （N>=0：密码中最多有多少个数字；N<0 密码中最少有多少个数字）pam_passwdqc 模块与 pam_cracklib 模块不能同时启用，两种的参数配置比较类似。具体可参看相关帮助文档。Linux 系统中对于登录失败的设置，通常使用 pam_tally 模块。启用 pam_tally 模块也须修改/etc/pam.d/system-auth 文件，实例如下：
- authrequiredpam_tally.sodeny=3lock_time=5deny=n：在登录失败 n 次后拒绝用户登录；
- lock_time=n：在用户达到登录失败次数后，锁定用户 n 秒钟。

（3）系统配置调整流程

① 对于涉及应用系统日常运行的系统参数、初始化代码、业务参数、打印参数、批处理设置、工作流配置等系统配置

调整工作，适用本流程。

② 对于按照应用系统的岗责权限设置，对本部门业务参数具有前台设置权限的，可以直接使用设置功能进行操作。

③ 对于涉及全局性的系统参数、业务参数以及其它系统配置，按照《变更管理程序》规定执行。

（4）运维安全与用户权限管理

① 仅系统管理员掌握应用系统的特权账号，系统管理员需要填写《系统特权用户的授权记录》，该记录由安全运维部文档管理员保管留存。

② 为保证应用系统安全，保证权限管理的统一有序，除另有规定外，各应用系统的用户及其权限，由系统管理员负责进行设置。

③ 用户权限设置，按照确定的岗责体系以及各应用系统的权限规则进行。

④ 新增、删除或修改用户权限，应通过运维平台的用户权限调整流程来完成：

⑤ 应用系统系统管理员应加强对各类用户帐号与口令的管理，制定口令管理安全策略，加强对口令安全性的监督检查，强化系统的权限管理。

⑥ 应用系统用户的登录密码，不得使用默认密码或弱口令。应定期更换口令。用户不得将自己的登录名与口令转交他人使用。

⑦ 应定期至少每季度一次对应用系统进行漏洞扫描，生成扫描报告存档，并对扫描发现的问题及时进行处理。

⑧ 需要安装补丁时，必须做好数据备份工作之后才可进行补丁安装实施工作。

⑨ 加强系统运行日志和运维管理日志的记录分析工作，并定期至少每季度一次记录本阶段内的系统异常行为,记录结果填入《系统异常行为分析记录单》。

（5）故障与应急管理

① 应用系统在建设、部署过程中应充分考虑系统的高可用性和可靠性要求，采取合理有效的技术手段，尽可能消除单点故障。

② 应用系统系统管理员应协同其它技术岗位，制定应用系统的日常监控工作规程和技术应急预案，并做好应用系统的程序、数据、参数等的备份工作。

③ 各应用系统的经理（或牵头经理）业务部门应制定各应用系统的业务应急预案，明确在应用系统无法使用时手工办理相关业务的处理流程。

3、附则

附 1：系统特权用户的授权记录

系统特权用户授权记录

服务器类：

服务器IP	运行业务系统	账号名	权限角色	用户姓名	登记时间	备注

应用系统类：

应用系统名称	账号名	权限角色	用户姓名	登记时间	所属部门	备注

*此表主要登记业务系统用户权限，记录其姓名、及部门。

附 2：系统异常行为分析记录单

系统异常行为分析记录

违规行为详细记录（含违规时间）	处理措施	记录人	记录时间

第十八章　机房安全管理制度

1、总则

（1）目的

为规范黄石大数据信息发展有限公司机房管理、提高机房安全保障水平、确保机房安全，通过对黄石大数据信息发展有限公司机房出入、值班、设备进出等进行管理和控制，防止对黄石大数据信息发展有限公司机房内部设备的非受权访问和信息泄露。

（2）范围

本管理办法适用于公司主机房的日常管理，包括出入管理、环境管理和值班管理。

（3）职责

安全运维部负责主机房日常管理，消防器材检查维修、UPS 后备电源由相关设备厂商负责。

2、管理细则

（1）机房出入管理

① 安全运维部主任为机房的第一责任人，所有外来人员进入机房必须填写机房进入申请单，且经过安全运维部授权人书面审批后方可进入。

② 审批后的机房进入人员由当日的安全运维部值班人员陪同，并登记“机房出入管理登记簿”，记录出入机房时间、人员、操作内容和陪同人员。

③ 安全运维部人员无须审批可直接进入机房，但须使用自己的门禁卡刷卡，严禁借用别人门禁卡进入。

④ 机房工作人员严禁违章操作，严禁私自将外来软件带入机房使用。

⑤ 严禁在通电的情况下拆卸，移动计算机等设备和部件。

（2）机房环境管理

① 保持机房整齐清洁，各种机器设备按维护计划定期进行保养，保持清洁光亮，至少每月由安全运维部协调清洁人员，清洁一次灰尘。清洁期间当日值班人员必须全程陪同，防止清洁人员误操作。

② 定期（至少每季度一次）检查机房消防设备器材，并做好检查记录。

③ 计算机机房后备电源(UPS)由工程部统一管理，除了电池自动检测外，每年必须充放电一次到两次。

④ 安全运维部定期对空调系统运行的各项性能指标(如风量、温升、湿度、洁净度、温度上升率等)进行测试，并做好记录，通过实际测量各项参数发现问题及时解决，保证机房空调的正常运行。

⑤ 机房内禁止随意丢弃储蓄介质和有关业务保密数据资料，对废弃储蓄介质和业务保密资料要及时销毁(碎纸)，不得作为普通垃圾处理。严禁机房内的设备、储蓄介质、资料、工具等私自出借或带出。

⑥ 机房内严禁堆放与机房设备无关的杂物，避免造成安全隐患。

⑦ 机房内应保持清洁，严禁吸烟、喝水、吃东西、乱扔杂物、大声喧哗。

⑧ 机房禁止放置易燃、易爆、腐蚀、强磁性物品。

⑨ 禁止将机房内的电源引出挪做他用，确保机房安全。

⑩ 未经许可，机房内严禁摄影、摄像。

⑪ 机房内机柜、设备未经许可，不得任意改动；如果已获得许可，需详细记录改动后的情况。

⑫ 进入机房工作的人员有责任在工作完成后及时清理工作场地、清除垃圾、做好设备标签、关闭机柜柜门。

（3）机房值班管理

① 机房值班员由安全运维部安排技术人员负责。机房值班人员应具有高度责任心，做到不迟到、不早退、不擅离职守。

工作日值班时间：8：00-18：00

休息日安排备班人员

② 机房安装的监控设备，由保卫处专人监控，保卫处值班人员须及时对可疑情况排查、确认。

③ 机房值班人员应按要求及时监控交换机、服务器、网络工作站、供电 等设备的运行，发现问题妥善解决，并向相关岗位管理员报告。

④ 值班人员负责当日的机房管理、安全检查；初步处理网络、各类工作站的技术问题，并做好处理记录。

⑤ 值班人员需每日巡检机房至少一次，并填写《机房巡检记录单》。

3、附件

附 1：机房出入登记簿

机房出入登记簿

事由	进入时间	离开时间	进出人员	陪同人员	审批人	备注

附 2 ：机房巡检记录单

公司机房巡检记录单

时间	设备运行情况	温度	湿度	防水/防火	门/窗/锁	UPS/电源	线路情况	巡检人

注：设备检查包括：服务器、网络设备、存储、前置机、安全设备、空调。

第十九章　安全和监控中心管理

1、总则

（1）目的

云平台安全和监控中心管理制度的建立旨在实现黄石大数据信息发展有限公司以资产和风险为核心的安全风险监控管理，并将之规范化、常态化。

（2）范围

本规范适用于黄石大数据信息发展有限公司对于云平台信息系统的综合安全管理、风险监控管理，主要适用于安全运维部的日常综合管理。

（3）职责

结合现有信息安全管理现状，安全运维部负责整合现有的信息安全管理技术解决方案，初步建成黄石大数据信息发展有限公司的信息安全监控和管理中心。

2、管理细则

因公司目前还未部署安全监控和管理中心，需要通过管理手段弥补技术上的不足。各安全管理岗位人员需要统一协作，互相配合，手工整合现有各分散的安全管理子系统的日志后统一汇总后分析，达到安全监控和管理中心的目的。主要管理要求如下：

（1） 网络管理员定期分析检查各个系统日志数据，通过对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等监测和报警数据的分析形成分析结论。

（2） 系统管理员定期分析防病毒系统的日志数据，分

析恶意代码、补丁升级情况，形成分析结论。

（3） 安全管理员应定期分析堡垒机和数据库审计系统的审计日志，分析人员行为；定期进行全网漏洞扫描，分析全网脆弱性和威胁状况。

（4） 安全运维部安全管理员应组织网络管理员、系统管理员、数据库管理员定期对各自的上述分析结果进行汇总、评审，发现可疑行为，形成总体分析报告，并相应地采取必要的应对措施。

第二十章　主机运维操作规程

1、总则

（1）目的

为了加强对各类主机设备的安全管理，确保各类主机设备在安全可控的前提下实现对公司网络和系统的使用与维护，制定本规范。

（2）范围

本规定适用的主机指接入公司网络及信息系统范围内的所有主机设备（含计算机、个人笔记本、Ipad 等）。

本规定适用的人员包括使用或维护公司网络和系统的职工，但不包括使用自助业务主机设备(自助查询机、自助打印机等)的公司客户。

（3）职责

总体遵循“谁主管谁负责，谁运营、谁负责，谁使用谁负责，谁接入谁负责”的总原则。安全运维部作为公司信息安全管理和运维部门负有管理职能，负责制定全公司主机安全管理实施细则、推进并落实各项主机管理工作，并定期检查各部门对于本规定的执行情况。

2、管理细则

（4）个人使用规范

① 主机帐号口令：应依据《账号口令和权限管理》规范对主机进行帐号口令管理，设置开机登录口令。

② 软件部署：由安全运维部统一安装操作系统、办公软件和其它必要软件，个人不能随意安装操作系统和其他软

件。

③ 防病毒软件：主机必须统一安装防病毒软件,并开启病毒定义库自动更新机制。如发现未安装防病毒软件或防病毒软件工作不正常时应及时跟安全运维部联系要求处理。

④ 移动存储介质：主机不得私自连接、装配刻录光驱、磁带机、移动硬盘、闪存盘等移动存储设备，需要进行数据交换时必须使用公司专用移动存储介质，严禁使用个人移动存储介质，专用移动存储介质须由部门指定专人保管并确保信息安全。

⑤ 共享管理：主机不允许开放任何形式的共享（包括共享文件夹、FTP 等）。

⑥ 禁止双网卡连接：所有主机都不允许以双网卡（包括有线网卡和无线网卡）的方式连接相同或者不同的网络。

⑦ 信息保存：主机上不允许以任何形式保存与系统、应用、设备登录相关的帐号口令信息，不允许保留从系统中导出的客户信息。应采用文档加密、授权等技术手段保护各类主机上的与企业运营有关的各种内部敏感信息。

⑧ 主机使用者若需要较长时间离开主机时，必须关闭主机或将其设置进入屏保状态。

（5）安全运维部检查

安全运维部定期由专人进行主机安全的合规性检查，该检查人员不能同时具有主机维护或管理人员的身份。检查的主要内容如下：

主机安全配置的规范性

主机接入和访问控制的规范性

主机安全使用的规范性

主机设备维护管理的规范性

安全运维部的检查人员汇总各类信息进行分析，总结问题，并记录归档。必要时与其他单元的检查结果归并后进行全公司通报。

第二十一章　系统交付管理

1、总则

（1）目的

为规范公司系统建设管理过程中的系统交付管理，特制订本管理办法。

（2）范围

本规范适用于黄石大数据信息发展有限公司项目管理、工程管理过程中的系统交付管理，对项目管理和工程管理过程中的系统交付管理环节进行规范和约定。

（3）职责

安全运维部负责项目类系统交付管理

2、管理细则

系统建设完成后，项目承建方要依据项目合同的交付部分向安全运维部进行项目交付，交付的内容至少包括：

（1）制定详细的系统交付清单，对照系统交付清单，对交付的设备、软件和文档进行清点；

（2）制定项目培训计划，对系统运维人员进行技能培训，目标是经过培训的系统运维人员能胜任日常的运维工作；

（3）提供系统建设的各类过程文档，包括但不限于：实施方案、实施记录等；

（4）提供系统运行维护的帮助和操作手册；

（5）系统交付过程文档必须有项目承建方和安全运维部双方项目负责人进行签字确认；

（6）系统交付工作由安全运维部、系统交付商共同参与，双方签字后，交付物交由安全运维部管理。

（7）必须安照系统交付的要求完成交付工作。

3、附件

附 1：系统交付清单

系统交付清单

项目名称					
交付设备	交付软件	交付文档	其他	接收人	时间

附 2：成果转移培训记录单

成果转移培训记录单

项目名称			
培训时间		培训地点	
参加人员			
培训内容摘要			
参加人员签名			

第二十二章　信息系统应急预案管理

1、总则

（1）目的

为保证黄石大数据信息发展有限公司业务信息系统的连续性，必须有系统、有组织地作好应急预案的管理工作。尽量降低风险，减少损失，保证的正常业务处理，最大限度地降低信息系统故障给我公司工作人员及客户造成的影响，特制定本管理办法。

（2）范围

本管理办法适应用于全公司信息系统应急预案的管理和指导性意见，各业务部门可根据自身业务的特点制定本部门范围内的应急预案执行细则。

（3）职责

应急预案组长：公司总经理

应急预案小组组长批准预案的实施与撤消及向上级相关部门的报告

应急预案副组长：公司副总经理

负责全公司范围内人力、物力资源协调、组织、指导应急预案的实施。

成员：各职能部门负责人

负责各自部门内部人员的协调、在各自熟悉领域内统一接收组长的指令，完成应急预案的实施。

（4）定义

信息安全应急预案是在对各部门的全部业务处理功能

的严格调查基础上，针对每项关键业务流程，受信息系统可能发生不同程度突发事件的影响，准备和实施的一套信息安全应急预案，其基本价值在于：在信息系统突发事件出现之前就已经制定相应措施，做好一定准备；一旦信息系统安全事件发生，可以提供和实施这些替代方案，以最大限度地争取时间，减少损失。

2、统一应急预案框架

（1）信息系统应急预案故障分类

根据网络与信息安全突发事件可控性、严重程度和影响范围的不同，分为以下四级：

I 级（特别重大）：公司网络与信息系统发生全公司性瘫痪，对公司正常工作造成特别严重损害，且事态发展超出公司控制能力的安全事件；

II 级（重大）：公司网络与信息系统发生大规模瘫痪，对公司正常工作造成严重损害，事态发展超出公司单一部门自身控制能力，需公司各部门协同处置的安全事件；

III 级（较大）：公司某一区域的网络与信息系统瘫痪，对公司正常工作造成一定损害，但安全运维部可自行处理的安全事件；

IV 级（一般）：某一局部网络或信息系统受到一定程度损坏，对公司某些工作有一定影响，但不危及公司整体工作的安全事件。

（2）信息系统应急预案的启动

当各部门发现计算机访问数据库速度迟缓、不能进入相

应程序、不能保存数据、不能访问网络、应用程序非连续性工作时，要立即向安全运维部报告。安全运维部工作人员对各工作站提出的问题必须高度重视，做好记录，经核实后及时给各工作站反馈故障信息，同时召集有关人员及时进行讨论，如果故障原因明确，可以立刻恢复的，应尽快恢复工作；如故障原因不明、情况严重、不能在短期内排除的，应立即报告公司领导，在网络不能运转的情况下由公司领导协调全公司各部门工作，以保障全公司业务的正常运转。但是否启动应急预案需要参照以下描述执行：

① 机房主服务器发生不可抗拒因素（不可预知的突发故障）导致信息系统停止运行 15 分钟以上时。

② 突发供电系统大范围停电，供电系统不能及时修复，并且备用电源亦不能提供电源，造成全部电脑不能运行。

③ 遇地震、火灾、水灾等不可抗拒因素且对信息系统造成大面积影响，业务信息系统不能访问，或基础网络系统不能访问。

一旦发生上述情况之一，应迅速启动信息系统应急预案，但须遵守以下流程：安全运维部在第一时间汇报公司领导，如遇夜间或节假日有关使用部门立即上报总值班，总值班通知安全运维部人员，安全运维部人员到场后作出初步结论，汇报公司领导，由公司主管领导决定启动应急预案，并通知各个部门相关责任人。安全运维部开展相应的处理，如发生不能自行处理的因素，立即通知签约的服务商、其他部门派人员到场处理。

（3）安全运维部应急预案响应办法

① 应急预案故障响应基本原则

- IV 级故障由安全运维部完成应急响应工作；
- III 级故障由信息安全领导小组牵头下，依靠公司自身信息技术人员、供应商完成应急响应；
- I 级、II 级故障协调第三方服务机构、武汉网络安全应急响应中心等完成应急响应；

② III、IV 级故障的处置方法

- III、IV 级故障的处置要根据网络与信息安全事件分类采取不同应急处置方式。

1）网络攻击事件处置：

判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。根据具体情况选择以下处置方式：

a．病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

b．外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关

闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

c．内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

2）设备故障事件处置：

判断故障发生点和故障原因，迅速联系服务厂商尽快抢修故障设备，优先保证公司主干网络和主要应用系统的运转。

3）供电系统断电处置：

在行政部通知供电系统进行检修的同时，随时观察注意 UPS 不间断电源的运行情况，停电时间接近 4 小时，必须停止服务器的运行。待电源恢复后，再按正常操作步骤恢复系统运行。

4）灾害性事件处置：

根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

5）信息内容安全事件处置：

接到公司内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；对

公安机关要求我公司协查的外网不良信息事件，根据上网相关记录查找信息发布人。

6）其它不确定安全事件处置：

可根据总的安全原则，结合具体情况，做出相应处理。不能处理的及时咨询信息安全公司或顾问。

（4）信息系统应急预案的撤消与恢复

a．安全运维部确认公司信息系统恢复正常。

b．门办确认公司秩序恢复正常。

c．信息系统正常运行 10 分钟以上，安全运维部上报公司管理层，由主管领导批准撤消“信息系统应急预案”。

d．在“信息系统应急预案”撤消后 24 小时内，安全运维部整理有关故障经过，填报《信息系统应急响应报告》，上报信息安全领导小组和公司领导。

（5）信息系统应急预案的善后

信息系统恢复正常，信息系统应急预案撤销后，信息系统预案应急小组还需要开展以下善后工作：

a．查找事件发生原因，总结经验教训；

b．如事件由人为引起，追究相关人员责任，如触犯法律，可直接报告公安机关处理；

c．如事件因为管理疏忽引起，除追究当事人责任之外，还需要追究相关主管领导责任；

d．根据事件危害程度，在部门范围内或全公司范围内就信息安全事件处理情况进行通报；

e．如有必要，在相关部门或全公司范围内开展教育培训，

提高人员安全意识，杜绝类似事件发生。

3、应急预案演练

a．应定期对应急计划中各种安全事件的应急恢复方案进行演练和测试，确保应急恢复方案的可行性和可靠性，锻炼应急恢复人员的应急响应速度和熟练程度，每次应急恢复演练和测试均应当作详细的记录。

b．各部门负责组织编制应急预案演练指南，提出规范各类突发事件应急预案演练的组织与实施的方法，指导相关应急预案演练活动。

c．应急预案应每年至少演练一次，信息安全领导小组开展演练评估工作，总结分析应急预案存在的问题。

4、应急资源保障

a．资源保障是实现突发事件快速响应、高效处置的基础和先决条件，各部门应充分考虑日常与应急两个方面，范围包括人员、技术、联络协调、物资和资金保障等内容，涉及事前和事中环节。

b．各部门应建立应急人员保障机制，配备足够的应急保障人员，包括落实主备岗并定期进行互换，配备专职灾备管理人员等，并通过应急培训和演练，确保应急处置人员具备应急工作必要的技术资质，提高人员应急处置的熟练度。

c．安全运维部应建立有效的技术保障机制，提高监测预警与应急处置的技术水平，应与通信运营商、重要设备服务商、系统集成服务商以及其他外包服务商签订服务水平协议，确保相关厂商应急处置过程中能够及时提供有效的技术服

务支持。

d．各部门应建立应急物资和资金保障机制，储备一定数量应急设备或物资，建立应急响应专项资金预算，保证应急储备。

5、附则

a．在此统一应急预案框架下，各部门需要根据部门工作具体流程和特点制定本部门应急预案响应细则，并做好各方面储备。

b．各部门应建立应急预案培训机制，就此统一应急预案框架和部门内部应急预案响应细则进行培训，至少每年要对部门信息应用人员进行一次应急预案培训。

安全运维部对该统一应急预案框架应定期审查和根据实际情况更新，各部门对部门内部应急预案响应细则也应该根据业务信息系统变化定期进行审查和更新。

6、附件

附 1：应急预案演练记录

黄石大数据信息发展有限公司应急演练记录单

演练名称		演练时间	
组织人		演练地点	
记录内容： 记录人：			
参加部门			
演练结果			
发现的问题			
需要改进之处			

第二十三章　安全事件/故障应急响应处理流程

1、分类分级

本预案所指的各系统突发事件，是指各个项目或系统等软硬件设施突然遭受不可预知的破坏、毁损、攻击、故障，对大数据公司造成或者可能造成重大危害，影响各系统提供信息服务、影响数据安全的事件。

（1）事件分类

根据各系统突发事件的发生过程、性质和特征，可分为因自然灾害、事故灾难和人为破坏引起的系统软硬件的损坏，以及利用信息网络进行有组织的大规模的反动宣传、煽动和渗透等破坏活动。

① 自然灾害

是指地震、台风、雷电、火灾、洪水等引起的系统软硬件损坏。

② 事故灾难

是指电力中断、网络损坏或者是软件、硬件设备故障等引起的系统软硬件损坏。

③ 人为破坏

是指人为破坏网络线路、通信设施、黑客攻击、病毒攻击、恐怖袭击等事件引起的系统软硬件损坏。

（2）事件分级

根据安全突发事件的可控性、严重程度、影响范围和各系统的实际情况，分为两级：一级(特别重大)、二级(重大)、三级(较大)和四级(一般)。国家有关法律法规有明确规定

的，按国家有关规定执行。

本方案中，一级二级三级事件定义为重大事件，四级事件定义为普通事件，分别对应不同级别事件的应急响应流程。

事件分类	事件等级	危险等级	判断标准	解决时限
重大事件	一级	特别重大	1.造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于大数据公司是不可承受的； 2.极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。	30 分钟
	二级	重大	1.造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于大数据公司是可承受的； 2.引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益。	60 分钟
	三级	较大	1.造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于大数据公司是完全可以承受的； 2.可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。	120 分钟
普通事件	四级	一般	1.造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小； 2.对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。	210 分钟

2、应急工作小组

根据不同项目，设立不同项目应急工作小组，名单模板如下：

事件分类	角色	姓名	单位/	主要职责	联系电话
重大事件	主管单位		XXXX 局	使用单位（按该单位意见通知以下单位）	
			市政数局	信息化主管单位	
			市政府总值班室	引起社会影响	
			市网信办	网络舆情、黑客攻击、病毒破坏、数据泄露等	
			公安网监支队		
普通事件	小组组长		市大数据公司	应急事件指导和协调	
	组员 A				
	组员 B				
	应用商 A				
	应用商 B				
	主数据中心	曹树林	市移动公司	应急事件协调	15907239207
		万里鹏	华三公司	云平台故障排查	13789337198
	备数据中心	李瑶	市广电公司	应急事件协调	15907233367
		陈星星	群宇科技	云平台故障排查	15272055163

3、普通事件应急响应流程

（1）分级处置和应急响应

根据事件的重要程度，采取不同的解决手段：

① 四级事件发生时，由小组组长初步判断故障类型，分别通知应用商和云平台人员进行故障排查（特殊情况工程师到场解决），同时在公司联系群内做故障情况通报。综合判断故障后，告知业主方故障情况。后续跟进故障处理进度，定时通报，直至故障完全解决。

② 发生三级或者三级以上事件时，直接启动重大事件应急响应流程。

（2）分级上报

安全事件发生后，由小组组长将安全事件定级并分级上报，具体分级如下：

① 四级事件：由小组组长分配人员对安全事件进行处理，并定时通报。

② 三级或者三级以上事件：直接启动重大事件应急响应流程。

（3）事件升级

普通事件在处理时间超过 2 小时,且未能查明故障原因，未能明确后续处理办法的情况下，应及时启动事件升级流程，将普通事件升级为重大事件，启动重大事件应急响应流程。

（4）后期处置

突发事件应急处置完成后，大数据公司相关部门和人员对事件原因、故障情况、处理措施进行总结，针对故障原因提出改进意见，完善相关措施，避免同类事件再次发生。

总结后要在系统恢复正常运行 48 小时内，将事件分析总结，填写《大数据公司故障处理报告》（见附件 3），上报公司领导，按实际情况判断是否上报业务主管部门。

（5）监控和预警机制

各个业务系统服务商和各云平台运维人员需设立系统监控和预警机制，建立便捷的通信渠道（电话、群），要求在第一时间发现故障并通知小组组长。

4、重大事件应急响应流程

对于四级事件，由大数据公司组织，按普通事件应急响

应流程进行处置，没有特殊情况，不启动本预案所规定的应急措施。

（1）应急预案启动

发现或接收到系统风险事件报告后，由应急小组根据实际情况判断风险等级。如发生三级或者三级以上风险，应急小组成员立即报告应急小组组长，并通知支撑单位技术人员等，到达指定现场。

应急工作小组组长召集小组成员，分析故障等级，并报告应急领导小组组长。经应急领导小组组长同意后，宣布启动相应级别的应急处置程序。

（2）应急处置流程

① 异常事件发生后，按照系统故障处理流程如下：

a．发生三级及以上事件时，应急领导小组组长立刻召集应急小组成员到达指定地点，分析故障等级，并立即报告上级主管部门领导。应急领导小组组长宣布启动相应级别的应急处置程序。

b．应急领导小组组长根据突发事件情况，迅速决定处置方案。当安全事件级别达到一级时，立刻向上级主管部门领导报告故障情况以及拟采取的处置方案。

c．应急小组对故障原因进行排查。当故障原因确定后，应急小组根据情况提出恢复服务的申请。经应急领导小组组长批准后执行。同时根据实际情况决定是否需要发布事件公告。

d．异常情况消除后，相关人员加强系统监控，保障后续

系统服务的正常进行。同时对系统事件产生的原因及时进行详细分析和研究，出具相关报告。

e．当发生的安全事件大数据公司现有技术资源无法使系统恢复正常时，应协调外部单位进行技术支持。

② 应急处置的同时，应根据异常事件的风险级别以及事件的具体影响程度，采取以下一项或多项应急措施：

a．停止系统服务；

b．进行应急处置；

c．研究事件影响范围；

d．成立调查小组（包括安全巡检扫描、请网监机构协助等）；

e．发布公告（包括必要时发布澄清公告）；

f．其它措施（包括媒体沟通协调、安保措施，以及必要时提请网监机构协助控制影响范围等）。

（3）应急事件报告

当发生一、二、三级级事件时，在事件发生后48小时内填写《大数据公司安全事件处理报告》（见附件2），并向上级主管部门报告。

（4）信息发布

当发生重大突发事件后，大数据公司可通过政府网站等权威渠道及时发布相关公告，与此同时，通过服务电话做好外部咨询和解释工作。

（5）应急结束

当重大突发事件处理完毕，由应急处理小组组长决定是

否需要对外发布公告。系统恢复正常服务后，相关部门应按照正常业务流程履行相应的书面审批手续，应急小组工作结束。

5、应急保障

（1）技术保障

为及时、有效发现和控制外部攻击行为，采取必要的保护措施，采购必要的防护设备，保证系统的正常、有效运行。

系统管理员、网络管理员等岗位配备主备岗、并熟练掌握应急预案，确保能够有效应对应急安全事件。

为及时、有效应对重大突发事件，与软硬件产品供应商的合同中应有应急处理及服务保障条款。对条款的执行情况要进行定期检查和评估，确保服务保障措施落实到位，确保应急事件发生时能及时与相关单位取得联系，获得相关支持。

（2）物质保障

建立完善的设备储备管理制度，定期检查备份设备和通信系统，保证其安全可用，并做好相应的采购工作，确保应急期间各项设备可随时调用替换，减少处置时间。

（3）培训和演练

为使应急人员熟悉本预案，掌握应急内容和实施程序，对应急人员进行不定期的基本知识和技能培训。

为强化工作人员应急意识，提高应急反应和处置能力，不定期举行应急演练，并对演练的效果、取得的经验和存在问题进行总结和评价，及时改进和完善相应的应急措施和流

程。

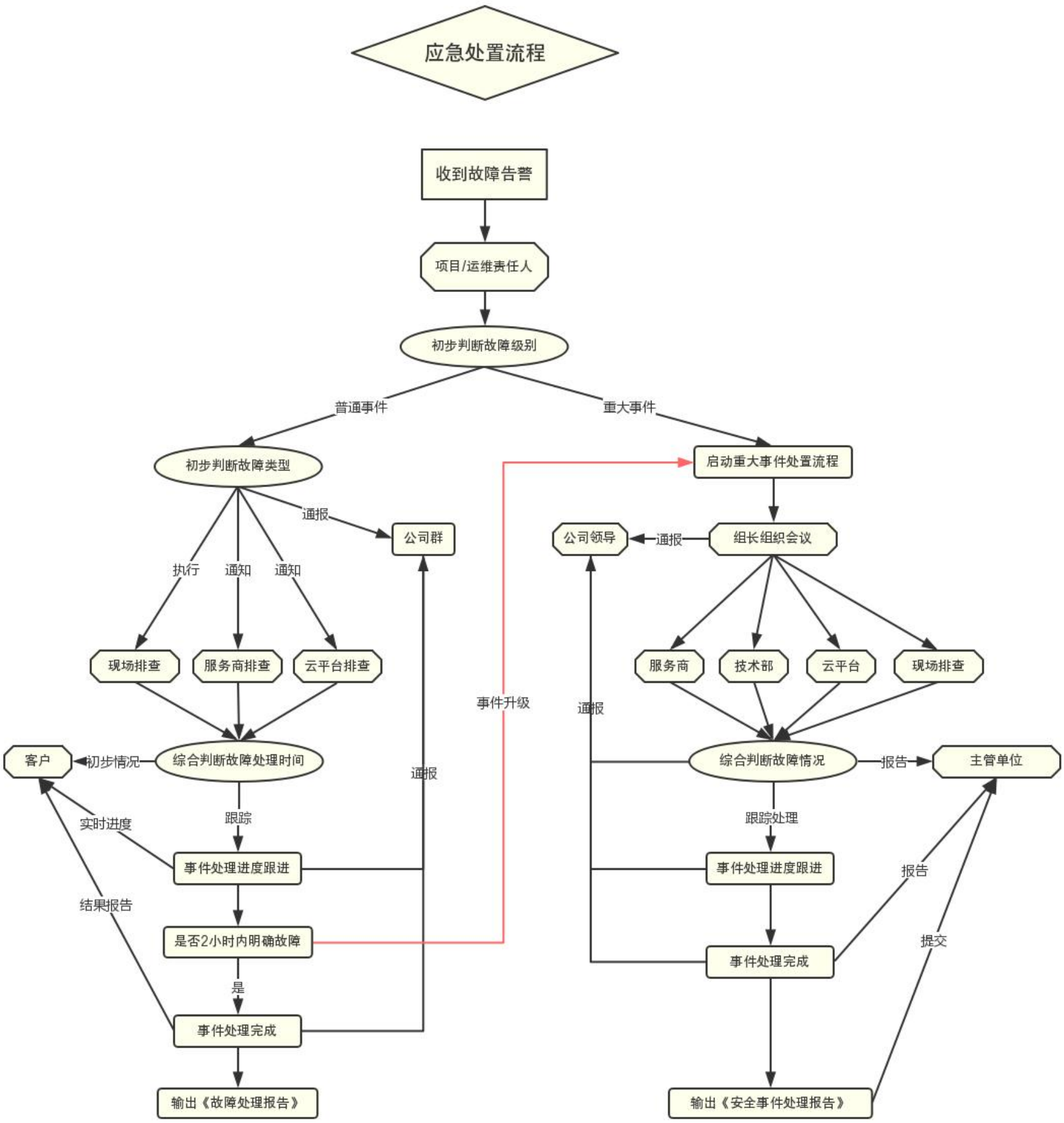
（4）敏感时期特别保障措施

在收到启动敏感时期报告的通知后，应根据要求每日以敏感时期信息安全报告的形式向上级主管部门上报信息系统运行情况。无异常情况的，要进行平安运行报告。

敏感时期技术部门负责人不能离岗，通报联络人要保持通信联络通畅。应增加对信息系统的巡检巡查频度。除非确有必要，原则上不应在敏感时期对重要信息系统进行改动或升级。

6、附件：

（1）应急处置流程图



（2）大数据公司故障处理报告

《大数据公司故障处理报告》

一、xxxx 年 xx 月 xx 日上午/下午 xx 点，具体情况描述.....

二、主要原因分析.....

三、解决办法及目前进展.....

四、附件（服务商故障报告）

大数据公司应急工作小组

xxxx 年 xx 月 xx 日

（3）大数据公司安全事件处理报告

《大数据公司安全事件处理报告》

一、xxxx 年 xx 月 xx 日上午/下午 xx 点，具体情况描述.....

二、主要原因分析.....

三、对社会和市民造成的损害.....

四、解决办法及目前进展.....

五、附件（服务商故障报告）

大数据公司应急工作小组

xxxx 年 xx 月 xx 日

第二十四章　信息安全责任制

1、总则

（1）第一条

为加强黄石市大数据信息发展有限公司（以下简称“大数据公司”）职工信息安全责任意识，界定职工信息安全违章行为，明确信息安全违章责任追究和处罚依据，特制定本管理办法。

（2）第二条

信息安全违章行为分为一般违章和严重违章。信息安全违章行为由安全运维部责组织调查和认定，并依据本办法进行责任追究。

（3）第三条

本管理办法中所称“计算机”包括桌面计算机、便携式计算机（含各类上网本），除特别说明，通指内网计算机和外网计算机。

（4）第四条

本管理办法适用于公司各部门全体人员。

① 组织机构与职责

② 违章行为界定

（1）第五条

凡具有下列行为之一均属违章行为：

① 违反国家信息安全有关法律和法规。

② 违反大数据公司信息安全管理规章制度。

③ 违反本单位信息安全管理规章制度。

（2）第六条

一般违章界定

① 计算机未设置操作系统登录口令；设置了操作系统登录口令，但口令长度低于8位且不是由字母、数字或符号组合构成；未启用屏幕保护和超时锁屏功能。

② 未按规定安装运行或自行卸载大数据公司统一的防病毒软件、补丁更新策略、桌面终端管理软件。

③ 未按要求使用安全移动存储介质进行内外网信息交换， 擅自删除或破坏已注册安全移动存储介质内的管理软件。

④ 擅自卸载（含格式化）本单位规定安装的操作系统和业务应用系统客户端。

⑤ 未使用大数据公司统一的外网邮件系统处理和发送与工作相关的电子邮件。

⑥ 计算机外委维修时未拆除硬盘导致与工作有关的信息外泄； 更换计算机和硬盘或在报废处理前，未对原硬盘进行信息不可恢复操作处理。

⑦ 在内网计算机上对未关闭互联网访问功能的手机和PDA 等设备进行充电或数据同步导致发生违规外联。

⑧ 开启文件共享且不设置共享密码或共享密码过于简单导致共享文件被非授权访问和破坏。

⑨ 移动存储介质丢失未向本单位信息化技术研究部和保密管理部门及时报告， 并说明移动存储介质中包含哪些与工作相关的文件、数据和程序。

⑩ 擅自将本人的门户及应用系统帐号和口令告诉他人由其长期代为进行业务操作。

⑪ 职工岗位异动后未及时向信息化技术研究部申请账号和权限的变更。

⑫ 违反大数据公司信息安全管理规定被认定为一般违章的其他行为。

（3）第七条

严重违章界定

① 未经大数据公司进行安全检测和许可，擅自将外来人员的计算机接入信息内网或信息外网。

② 擅自更改计算机网卡的 MAC 地址或 IP/MAC 地址绑定策略。

③ 在计算机上私自开启 WW、WFTP、VOD、代理、游戏、论坛等服务对网络访问造成干扰或信息资源被非授权访问。

④ 在内网计算机上利用电话线、电信运营商 ADSL、无线上网卡或具备上网功能的手机和 PDA 等设备访问互联网，以及任何具备有意识或故意性质使用内网计算机访问互联网。

⑤ 使用手机或 PDA 设备的无线WIFI 功能访问信息内网或信息外网。

⑥ 在计算机中存储和处理国家、大数据公司秘密信息，在外网计算机中存储涉及大数据公司重要敏感信息的电子文件。

⑦ 在同一台计算机（包括具备隔离卡和双硬盘的计算机） 上安装两个操作系统或双网卡分别接入信息内网和信息外网。

⑧ 安全移动介质损坏后私自丢弃未交信息化技术研究部处理并造成企业信息外泄。

⑨ 私自在网络中接入任何具备网络地址转换（NAT)、MAC 克隆等功能的网络交换机和路由器等有线设备和无线设备。

⑩ 擅自组建无线网络并接入信息内网。

⑪ 干扰他人正常工作行为，包括：发布不真实信息、垃圾信息；散布病毒及木马；未经授权或通过口令猜测和破解等手段使用他人设备、系统、邮箱等。

⑫ 擅自在计算机中安装黑客程序、 端口扫描或漏洞扫描软件并使用其进行网络扫描或攻击破坏。

⑬ 拒绝信息化技术研究部维护人员对计算机进行安全性检查和安装大数据公司统一要求的桌面终端管理软件、防病毒软件等。

⑭ 违反大数据公司和本单位信息安全管理规定被认定为严重违章的其他行为。

1、督察与检查

（1）第八条

对违章的查处采用专项督查、日常检查及应用工具软件检查相结合的方式进行。

（2）第九条

发生信息安全违章，按照管理权限，实行分级查处、分级追究。

① 各部门自查自纠发现的违章，参照本办法自行处理。

② 发展计划部组织的督查、日常检查及采用大数据公司统一部署工具软件检查发现的违章，按照本办法规定处理。

③ 大数据公司督查、日常工作检查及采用大数据公司统一部署工具软件检查发现的违章，按本规定处理并将处理情况报告大数据公司领导。

2、处罚规定

（1）第十条

在年度内第一次发生一般违章，对当事人给予诫勉谈话或通报批评；半年内同一当事人发生两次一般违章，对当事人给予200元的经济处罚并通报批评；一年内同一当事人发生三次一般违章，对当事人给予300元的经济处罚，并对当事人所属部门予以通报批评。

（2）第十一条

在年度内第一次发生严重违章，对当事人给予500元的经济处罚，并对当事人所属部门予以通报批评；半年内同一当事人发生两次严重违章，除对当事人给予1000元的经济处罚，通报批评当事人所属部门外，当事人必须自学信息安全。

信息安全基本知识并通过公司考核；一年内同一当事人发生三次严重违章，给予当事人降级的处罚，当事人申请并

经公司对其进行信息安全知识考核合格后方能正常晋升。

3、附 则

（1）第十二条

本管理办法由黄石大数据信息发展有限公司负责解释。

（2）第十三条

本管理办法自发布之日起执行。