吕梁市发展和改革委员会文件

吕发改信用发〔2020〕326号

吕梁市发展和改革委员会
关于印发《数据安全保护管理制度》
等信息安全和应对制度的通知

机关各科室，委属各单位:

为贯彻落实信息安全管理有关规定，保障信息系统安全运行，加强网站建设和数据安全保护工作，切实维护网络运行安全、净化网络宣传环境，现制定《吕梁市发展和改革委员会数据安全保护管理制度》、《网络与信息安全应急预案》、《信息安全日常运维操作与管理制度》等13项制度，请结合工作实际，认真抓好贯彻落实。

附件：1.数据安全保护管理制度

2.网络与信息安全应急预案

3.信息安全日常运维操作与管理制度

4.信息安全组织架构及职责

5.信息系统总体安全方针与政策

6.信息系统管理人员岗位责任制度

7.第三方外包管理规定

8.信息系统安全管理人员上岗及离岗制度

9.信息安全培训与考核管理规定

10.病毒检测和网络安全漏洞检测管理制度

11.密码安全管理制度

12.信息安全事件管理制度

13.网络应用平台个人隐私保护制度

吕梁市发展和改革委员会

2020年8月14日

（此文主动公开）

附件 1

吕梁市发展和改革委员会
数据安全保护管理制度

一、总则

1、为确保全国信用信息共享平台（山西吕梁）数据安全与保密，规范数据使用范围，特制定本制度；

2、本制度所指的数据是所有在全国信用信息共享平台（山西吕梁）中的各类数据；

3、本制度所指的数据管理包括对数据的修改、查询、存储、使用等工作。

二、数据的存储管理

1、数据库及备份文件均保存在各系统所属的磁盘中，访问权限需严格控制，未经管理人员的授权严禁擅自访问数据库及备份文件；

2、数据管理权限参见《信息安全组织架构及职责》。

三、数据的变更管理

1、系统管理人员不得擅自访问数据库增添、修改、删除原始数据；

2、业务部门需要修改数据时，提交书面申请，分管领导签字盖章后提交市发改委，由发改委统一安排对应修改工作；

3、修改数据时应充分论证可行性和安全性，确定修改方案后才可进行修改工作，确保数据修改后系统无误。

四、数据的查询与使用管理

1、系统管理人员无正当事由不得随意通过数据库查询基础数据，因工作需要查询数据时，要做好保密工作；

2、业务部门需要通过数据库取得数据时，应提交书面申请并由分管领导审批签字，再提交市发改委，由发改委统一安排查询、提取数据的工作，业务部门取得数据后，需在审批的范围内正当使用，不得转用、泄密。

附件2

吕梁市发展和改革委员会
网络与信息安全应急预案

一、总则

（一）编制目的

完善网络与信息安全应急响应机制，规范网络与信息安全应急响应工作内容和流程，科学应对网络与信息安全突发事件，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，保障信息系统的实体安全、运行安全和数据安全。

以防范为主，加强监控。开展安全教育和培训工作，提高信息安全防护意识和水平，积极做好日常安全工作，提高应对突发网络与信息安全事件的能力。建立完善的信息系统安全监控和管理机制，保证对网络与信息安全事件做到快速觉察、快速反应、及时处理、及时恢复。

（二）适用范围

发生的严重影响网络与信息系统正常运行，造成系统中断、系统破坏、数据破坏或者国家秘密信息被窃取、泄露等，对网络信息系统造成不良影响以及造成一定程度经济损失的重大网络与信息安全事件，适用本预案。

二、处置办法

（一）网站、网页出现非法言论时的处置流程

1、网站、网页由主办科室负责随时密切监视信息内容。

2、发现网上出现非法信息时，吕梁市发展和改革委员会办公室派专人处理，作好必要记录，清除非法信息，确认后，再重新启动网站。

3、服务器责任人妥善保存有关记录及日志。

4、信息安全员通过技术手段追查非法信息来源。

5、向上级领导汇报处理情况。

6、如果非法信息不能自行处理或属严重事件的，应保留记录资料并立即向公安部门报警。

(二)黑客攻击的紧急处置流程

1、当发现网页内容被篡改或通过入侵检测系统发现网络正被攻击时，应立即将被攻击的服务器等设备从网络中隔离出来，保护现场并立刻向领导通报情况。

2、进行被攻击、破坏系统的恢复、重建工作。

3、追查非法来源。

4、向上级领导汇报处理情况。

5、如果不能自行处理或属严重事件的，应保留记录资料并立即向公安部门报警。

(三)病毒安全紧急处置流程

1、当发现计算机被感染上病毒后，将该机从网络上隔离开来。

2、对该设备的硬盘进行数据备份。

3、启用杀病毒软件对该机器进行杀毒处理工作。

4、如果现行反病毒软件无法清除该病毒，在确认数据完全备份后，征求使用人同意重装系统。

(四)软件系统遭破坏性攻击的紧急处置流程

1、重要的软件平时做好备份，并存于异地存储服务器。

2、一旦软件遭到破坏性攻击，应及时采取相应措施减少或降低损害，并立刻向领导报告。

3、网络安全人员检查日志等资料，确定攻击来源。

4、向上级领导汇报处理情况。

5、事态严重，应保留记录资料并立即向公安部门报警。

(五)数据库安全紧急处置流程

1、主要数据库系统应做双机热备设置，至少准备两个以上数据库备份，并存于异地。

2、一旦数据库崩溃，应立即启动备用系统，并立刻向领导报告。

3、在备用系统运行的同时，应对主机系统进行修复工作。

4、如果两套系统均崩溃，信息安全小组人员应立即向软硬件提供商请求支援。

5、系统修复启动后，将数据库备份取出，按照要求将其恢复到主机系统中。

6、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。

（六）关键人员不在岗的紧急处置流程

1、关键岗位实行A、B角色。

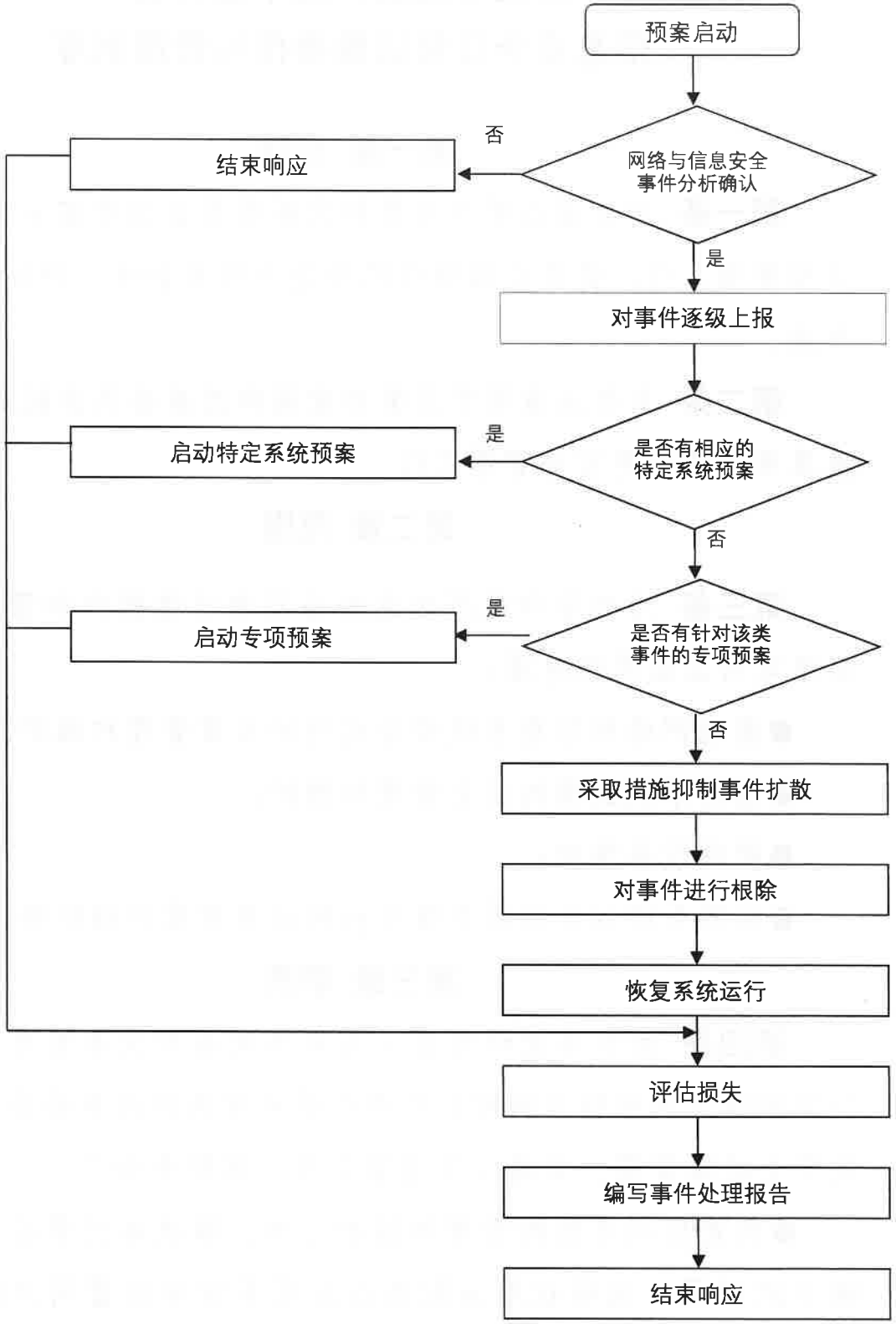
2、对于关键岗位平时应有人员储备，确保一项工作至少有两人能够操作。

魏二龙 电话： 13097589496

丁克斌 电话： 13379188386

附件： 网络与信息安全应急响应流程图

附件： 网络与信息安全应急响应流程图



附件 3

吕梁市发展和改革委员会
信息安全日常运维操作与管理制度

第一章 总则

第一条 为加强吕梁市发展和改革委员会信息安全日常运维管理工作，提高运维操作的规范性和安全性，特制定本办法。

第二条 本办法适用于吕梁市发展和改革委员会机关及直属单位的信息安全管理工作。

第二章 范围

第三条 为指导和规范信息安全日常运维操作和管理，本规定内容适用的范围：

●基础网络和信息系统安全运行的日常管理和维护；

●应用系统数据的安全管理和维护；

●硬件设备维护；

●应用系统以及应用支撑平台的日常管理和维护等。

第三章 职责

第四条 由信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）负责吕梁市发展和改革委员会机关安全运维管理、实施以及监督工作，其职责如下：

●负责应用系统的管理和维护工作，解决并记录应用系统中的问题，按照权限分配表在应用系统中设置用户的权限；

●负责服务器操作系统的管理和维护工作，对服务器中软件的安装及删除进行管理和记录；

●负责数据库的管理和维护工作，进行数据备份和恢复测试，并对备份的存放介质进行管理；

●负责网络的管理和维护工作；

●负责本单位内的信息安全管理工作；

●负责吕梁市发展和改革委员会机关机房的管理和维护工作；

●负责系统文档的安全管理工作等。

第四章 设备安全操作

第五条 在对信息化系统中的各类设备进行操作时，应严格按照具体应用需求进行。

第六条 在进行操作前，应书面填写操作申请单，列明操作所涉及的设备、对系统可能带来的影响以及相应的应对措施，在得到信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）审批后，方可进行操作。

第七条 在进行操作前，应对设备当前配置或者数据进行记录或者备份。

第八条 操作完成后，应对本次操作过程和操作结果进行记录并提交信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）存档。

第五章 终端日常使用管理

第九条 在网络中的用户终端应严格按照要求进行操作，遵守内外网分离的要求，不得擅自修改 IP 地址、擅自卸载

桌面管理系统、杀毒软件等。应按照要求按时进行病毒扫描和补丁升级。

第十条 移动介质安全管理：

1、移动介质不能在内、外网终端之间混用；

2、在移动介质接入终端后应立即进行病毒扫描；

3、使用移动介质拷贝重要数据完成后，应立即清除；

4、涉及信息化系统的技术资料、安装介质等应由专人进行妥善保管，借出使用时应登记并按要求准时归还。

第六章 应用系统运行安全管理

第十一条 对于各应用系统以及应用系统支撑平台的日常运行情况要定期进行记录、分析和汇报。各应用系统使用科室对于发现的异常情况要及时通报信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）以便及时解决。

第十二条 系统管理员负责应用系统的安装、维护和系统及数据备份；根据应用系统的安全策略，负责应用系统的用户权限设置以及系统安全配置。

第十三条 应用系统维护和应急处理记录要求：

1、设置“应用系统维护和应急处理记录”，系统管理员记录系统的运行情况；

2、对系统异常、系统故障的日期、现象、处理方法及结果等应急处理进行记录；

3、对应用系统的安装、设置更改、帐号变更、组变更、备份等系统维护工作进行记录，以备查阅；

4、对应用系统异常和系统故障的时间、现象、应急处理方法及结果作详细的记录。

第十四条 应用系统软件、资料以及许可证的管理：

1、必须对应用系统软件的介质、资料和许可证进行登记，并设专人负责保管；

2、登记的内容应包括软件的名称和版本、软件出版商、许可证类型和数量、介质的编号和数量、软件安装序列号、手册名称和数量、购买日期等；

3、应用系统软件和资料的借用，需要审批和借还登记手续；

4、对重要应用系统软件介质和资料要进行复制，借用时应提供复制品，以保护好原件及避免丢失。

第十五条 应用系统配置的备份的管理

1、系统管理员应对系统的配置参数及相关文件进行备份；

2、当配置发生变更时必须重新备份，以便系统故障时能尽快恢复系统配置。

第十六条 应用系统数据的备份的管理

1、备份权限，备份介质都必须加以妥善保管，防止非法访问；

2、如果开发数据库中导入了数据库的数据，要确保为生产数据库所指定的安全规则也用于开发数据库中；

3、制定备份策略，以高效备份与恢复为目标，与操作系统备份结合，物理备份与导出相结合。

第七章 系统数据的安全管理

第十七条 根据应用系统数据的生命周期和重要性，分别设置合理的在线、近线、离线数据的存储、备份策略。

第十八条 备份策略应形成书面材料由信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）审核后存档。

第十九条 当应用系统发生变化时，应及时评估其对数据备份要求的影响，制订新的备份策略，经审核后存档。

第二十条 备份的数据应定期检查，重要数据应在备份后随机抽取进行恢复测试以保证备份数据的可用性；超过时效的备份应在获得信息管理科室的书面同意后及时格式化或者销毁。

第八章 系统运行平台的安全管理

第二十一条 系统运行平台指的是支撑应用系统运行的主机、操作系统以及数据库、中间件等平台软硬件。

第二十二条 系统运行平台由信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）统一进行管理和维护，主要内容包括：系统平台配置，登录/操作审计、访问端口限制、补丁更新、日志分析、数据备份、口令管理等。

第九章 口令/密码/密钥安全管理要求

第二十三条 应用系统管理员在系统中为每个用户设立一个账户，其权限按照经单位负责人批准的《应用系统用户权限分配表》和《应用系统角色权限表》中的描述设定。应

用系统的所有账户应符合统一口令策略的要求设置和更新密码。

第二十四条 服务器的操作系统中没有未授权的登录账号，确需保留的系统账号应有明确的管理人员。操作系统中账户应符合吕梁市发展和改革委员会机关统一口令策略的要求设置和更新密码。

第二十五条 数据库中的所有账号应符合统一口令策略的要求设置和更新密码。

第二十六条 密码和密钥要求长度超过8位，要求信息管理科室管理员做好密钥的产生、保存、分配、使用、废除、归档和销毁工作。

第十章 系统文档的安全管理

第二十七条 信息化系统文档的管理由信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）统一进行。其职责包括：文档存档管理；文档更新管理；文档借阅管理；文档销毁管理。

第十一章 系统的安全监测

第二十八条 系统的安全监测由信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）统一进行。其职责包括：

1、依靠安全运维平台、网管软件、桌面管理系统等工具，每周对信息化系统进行监测，对于重点与核心部分内容则每天进行监测；

2、为每次监测填写监测记录；

3、分析监测记录，找出系统可能存在的隐患并及时处理等。

第十二章 备份和恢复管理

第二十九条 定期对信息系统的数据、软硬件的配置文件进行备份。

第三十条 根据应用系统数据的生命周期和重要性，分别设置合理的在线、近线、离线数据的存储、备份策略。备份策略应形成书面材料，交由吕梁市发展和改革委员会办公室存档。

第三十一条 网络服务器数据备份工作，系统备份每周做一次。系统管理员在每周最后一个工作日，将应用服务器的数据库文件做一次异机备份，数据保存一个季度。

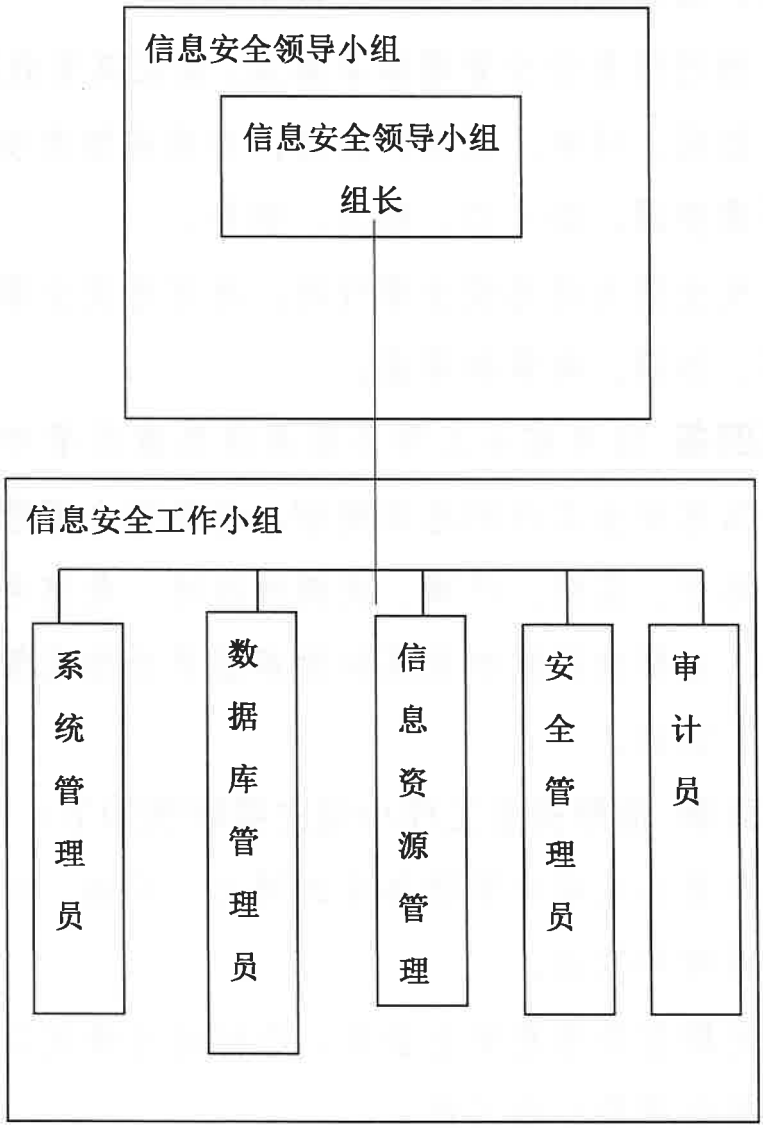
第三十二条 当应用系统发生变化时，应及时评估其对数据备份要求的影响，制订新的备份策略，经审核后存档。

第三十三条 备份的数据应定期检查，重要数据应在备份后随机抽取进行恢复测试以保证备份数据的可用性；超过时效的备份应在获得信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）分管领导书面同意后及时格式化或者销毁。

附件 4

吕梁市发展和改革委员会
信息安全组织架构及职责

第一条 信息安全组织架构。为了加强信息安全工作，明确安全目标，有效建立和管理信息安全体系，吕梁市发展和改革委员会信息安全组织架构如下图：



第二条 信息安全领导小组。信息安全领导小组是吕梁市发展和改革委员会信息安全工作的最高管理机构，信息安全领导小组组长由委主要领导担任，副组长由组长任命，领导小组成员由相关工作人员组成。

第三条 信息安全领导小组主要职责如下：

1.制定、评审、批准吕梁市发展和改革委员会的信息安全方针，为信息安全工作指引发展方向，并定期评审实施的有效性，确保信息安全目标得以识别。

2.推进信息安全管理体系落实，保证其有效建立、实施、运行、监视、评审、保持和改进，为实施信息安全管理体系提供所需资源，如人力、财力、物等。

3.发生重大信息安全事件时，对信息安全事件的处理进行指挥、协调、决策和审查。

第四条 信息安全工作小组具体负责吕梁市发展和改革委员会信息安全工作的总体规划，信息安全管理体系的建立、实施、运行、监视、评审、保持和改进，是信息安全工作执行机构。主要由吕梁市发展和改革委员会信息管理科室（即办公室）组成。

第五条 信息安全工作小组主要职责如下：

1.负责信息安全管理体系的建立、实施、运行、监视、评审、保持和改进。

2.定期召开信息安全会议，总结运行情况以及安全事件，向信息安全领导小组汇报。

3.负责信息安全事件的监控、处理、汇报、总结等。

4.定期对全国信用信息平台（山西吕梁）运行进行信息安全风险评估。

5.对全国信用信息平台（山西吕梁）使用人员及运维人员进行人员安全培训、应急演练等具体落实工作。

6.负责与第三方组织保持信息安全工作的沟通和交流，如安全厂商、行业主管部门等。

7.负责合规性检查工作的配合。

信息系统管理人员表

岗位名称	姓名	电话
信息安全领导小组	陈江平	8233062
系统管理员	魏二龙	8233062
安全管理员	丁克斌	13379188386
审计员	王瑞婧	18536158565
数据库管理员	冯文军	15935170223
信息资源管理员	杨彩霞	15135457625

附件 5

吕梁市发展和改革委员会
信息系统总体安全方针与政策

第一章　总则

第一条 为了保证吕梁市发展和改革委员会计算机信息系统的安全，规范计算机信息系统的安全管理，根据国家有关法律、法规和相关规定，并结合吕梁市发展和改革委员会信息系统建设的实际情况，特制定本制度。

第二条 本制度所指的计算机信息系统，是以计算机（包括相关配套设备）为终端设备，利用计算机、通信、网络等技术进行信息采集、处理、存储和传输的设备、技术、管理的组合。

计算机信息系统安全的含义是：通过各种计算机、网络、密码技术和信息安全技术，在实现网络系统安全的基础上，保护信息在传输、交换和存储过程中的保密性、完整性和真实性。

第三条 吕梁市发展和改革委员会计算机信息系统包括全国信用信息共享平台（山西吕梁），均应按照本制度进行管理，所有用户均应按照本规定执行。

第四条 吕梁市发展和改革委员会计算机信息系统的建设和应用要本着“预防为主、集中管理、分级负责、保障安全”的方针，按照“业务工作谁主管、安全工作谁负责”和“谁使用、谁负责”的原则进行管理。

第五条 吕梁市发展和改革委员会计算机信息系统安全管理的任务是根据计算机信息系统的性质，实事求是地确定基准威胁，按照基准威胁的需要，建立管理机构，配备管理人员，建立健全规章制度，加强安全教育和培训，适时进行安全检查和评估，落实各项人防、物防、技防措施，以保障单位信息的安全。充分体现技术与管理并重的原则，利用各种先进的技术手段加强管理。

第六条 吕梁市发展和改革委员会计算机信息系统按照《信息系统安全等级保护基本要求》进行等级保护和管理。

第二章 信息安全方针

第一条 本信息安全管理体系方针指明了吕梁市发展和改革委员会的信息安全目标和方向，并可以确保信息安全管理体系被充分理解和贯彻实施。本方针适用于吕梁市发展和改革委员会信息安全管理体系涉及的所有人员和过程。

第二条 信息安全的定义是：保证业务所依赖的信息和信息系统的保密性，完整性，可用性。

第三条 吕梁市发展和改革委员会信息安全的总体方针为：积极预防、及时发现、快速响应、确保安全，其目标是：满足已识别的信息安全要求，包括法律法规、业务要求，具体目标包括：

●秘密信息泄漏事故为零。

●保证重要信息系统可用性在98%以上。

●信息安全事件：如病毒感染、黑客攻击等事件在可控范围内、发生可能性较低、损失极小。

第四条 为了确保信息安全工作有一个明确的方向和获得可见的管理者支持，设立信息安全领导小组，负责：

●制定信息安全方针和目标；

●建立信息安全角色和职责；

●提供 ISMS（信息安全管理体系）所需要的资源；

●领导建立和实施 ISMS（信息安全管理体系）；

●监督和检查信息安全工作；

●制定和实施信息安全工作的奖惩政策。

第五条 信息安全管理人员要通过适当的标准和程序实施信息安全方针。所有职工必须按照相应的程序，维护此方针，所有职工有责任报告信息安全事件，以及识别信息安全风险。

重要原则和符合性要求所有职工应明确，在信息安全方面满足以下原则和符合以下要求是必须的：

●法律法规和合同要求的符合性；

●信息安全的安全意识；

●遵守单位所有信息安全策略和操作规程。

第六条 本文件需要定期或不定期根据需要进行评审，当信息安全管理体系发生重大变化时，也应评审，以维持其适用性。

附件 6

吕梁市发展和改革委员会
信息系统管理人员岗位责任制度

第一条 为保证吕梁市发展和改革委员会信息系统的安全运行和有效管理，进一步明确和完善吕梁市发展和改革委员会信息系统人员的组织管理，特制定本岗位责任制度。

第二条 本制度适用于担任吕梁市发展和改革委员会信息系统设计、建设、运行管理、技术支持和维护等工作的相关人员。

第三条 根据吕梁市发展和改革委员会信息系统的人员和管理情况，设立系统管理员、安全管理员、安全审计员、数据库管理员、信息资源管理员岗位。

第四条 上述岗位人员须首先履行吕梁市发展和改革委员会信息化安全工作日常执行机构的职责，系统主管还须履行吕梁市发展和改革委员会信息化安全工作领导小组的职责。

第五条 系统管理员职责：

（一）负责吕梁市发展和改革委员会信息系统建设规划设计方案的编写，并提交系统主管及吕梁市发展和改革委员会信息化工作领导小组审批；

（二）负责吕梁市发展和改革委员会信息系统的系统配置和管理；

（三）负责吕梁市发展和改革委员会信息系统主服务器

的系统软硬件管理及技术支持和维护工作，保证其正常运行；

（四）负责吕梁市发展和改革委员会信息系统主服务器上的用户管理并为用户分配相应的系统软硬件资源，包括用户的创建、删除、用户的环境设置、用户信息的修改等；

（五）负责定期维护服务器上的系统口令；

（六）负责吕梁市发展和改革委员会信息系统人员的系统管理培训；

（七）协助网络管理员进行网络的故障管理，如帮助定位服务器端的网络故障等；

（八）协助安全管理员进行系统的安全管理，包括系统的数据备份、系统审计日志的维护、系统的应急响应等。

第六条　安全管理员职责：

（一）负责吕梁市发展和改革委员会信息系统安全建设的设计方案编写，并提交系统管理员及吕梁市发展和改革委员会信息安全领导小组审批；

（二）负责吕梁市发展和改革委员会信息系统安全保密规章制度的编写、修订，并提交系统主管及吕梁市发展和改革委员会信息化安全工作领导小组审核；

（三）负责吕梁市发展和改革委员会信息系统安全建设方案的具体实施；

（四）负责安全规章制度的具体贯彻落实；

（五）负责对服务器、网络设备、数据库及应用系统进行安全管理，包括数据的备份与恢复、安全审计、应急响应、安全性能的监测等，并提交相应的报告（包括安全运行报告

和安全审计报告等）供系统主管及吕梁市发展和改革委员会信息化安全工作领导小组审批；

（六）负责吕梁市发展和改革委员会信息系统人员的安全培训；

（七）负责对吕梁市发展和改革委员会信息系统进行定期的自我安全检查与评估。

第七条　审计员职责：

（一）配合安全管理员完成相关的系统安全审计工作；

（二）对吕梁市发展和改革委员会内网每月进行一次漏洞检测，并提供相应的漏洞检测报告；

（三）提供合理的安全审计建议方案和技术路线；

（四）负责内网安全系统产品的审计，包括主机监控与审计系统、网络入侵检测系统、防火墙、防病毒系统、统一身份认证系统，并提交相应审计报告；

（五）提供应用系统安全审计的技术支持等。

第八条　数据库管理员职责：

（一）负责吕梁市发展和改革委员会信息化建设中数据库系统的需求调查分析，并提交报告供系统管理员及吕梁市发展和改革委员会信息安全领导小组审批；

（二）负责吕梁市发展和改革委员会信息化建设中数据库系统的配置、开发；

（三）建立和完善数据库系统的运行、维护规程，负责数据库的管理及技术支持和维护工作，保证其正常运行；

（四）负责创建、增加、删除数据库系统用户，并为用

户分配数据库系统中的资源；

（五）负责吕梁市发展和改革委员会信息系统中用户的数据库技术培训；

（六）分析并向管理层报告数据库应用系统的安全现状，参与调查数据库系统异常事件；

（七）协助安全管理员进行数据库系统的安全管理，包括数据库的备份与恢复、数据库审计日志的维护、系统应急响应等。

第九条　信息资源管理员职责：

（一）负责吕梁市发展和改革委员会信息系统中信息资源的需求调查分析，并提交报告供系统管理员及吕梁市发展和改革委员会信息安全领导小组审批；

（二）负责吕梁市发展和改革委员会信息系统中信息资源配置方案的编写，并提交报告供系统管理员及吕梁市发展和改革委员会信息安全领导小组审批；

（三）负责信息资源配置方案的具体实施；

（四）负责吕梁市发展和改革委员会信息系统中信息资源的管理及维护；

（五）协助安全管理员进行信息资源的安全管理，包括信息资源的密级界定、信息资源的安全审计等。

附件 7

吕梁市发展和改革委员会
第三方外包管理规定

第一条 为了保证吕梁市发展和改革委员会计算机信息系统的安全，规范外包开发软件的管理工作，防止部门信息资产和信息处理设施由于管理不当而面临第三方和外包的安全风险，特制定本制度。

第二条 本制度适用于吕梁市发展改革委员会各个科室对第三方外包软件系统开发的管理。

第三条 如果要将所有或部分信息系统进行外包，则必须要在签定的合同中体现出公司的安全要求，或签订保密协议。

第四条 外包服务公司资源申请需先向吕梁市发展和改革委员会提出申请，经相关科室领导审批后，按照“吕梁市政务云资源申请流程”向云平台申请资源。

第五条 外包服务公司资源访问申请需按照“吕梁市电子政务云平台服务手册”进行操作。

第六条 由外包服务公司负责云主机维护工作，提升系统性能及稳定性，保证系统 7X24 稳定运行主要内容包括应用部署、服务监控、故障处理。

第七条 外包服务公司需负责应用系统建设与运维工作；

第八条 外包服务公司需编制应急预案，定期进行演练，保证对突发事件的快速处理和恢复。

第九条 云主机出现漏洞，外包服务公司需及时修护和管理。

第十条 由外包服务公司负责对用户定期进行安全培训。

附件 8

吕梁市发展和改革委员会
信息系统安全管理人员上岗及离岗制度

第一条 在信息系统安全管理人员上岗前，要对其政治历史、身份、专业资格以及业务能力进行人事审查和核实；

第二条 有过刑事犯罪记录的人员不能上岗；

第三条 不符合要求的人员应及时调离岗位；

第四条 应根据人事审查结果、工作需要和国家相安全保密规定，具体确定每个涉密人员的岗位和职责，建立岗位责任制度；

第五条 每年进行一次政治思想、遵守安全管理制度等方面的考核，对于不合格者进行批评教育、处罚或调离岗位；

第六条 要与系统中的长期或临时工作人员签定保密协议，明确其应承担的安全保密责任和应遵守的保密规定；

第七条 对于系统中的工作人员，在岗位上岗前，要进行安全教育培训；在工作过程中，应每年组织一次安全知识培训；

第八条 应重点对系统主管领导和安全管理人员进行安全法规、国家标准和专业知识的培训，增强安全能力；

第九条 对于员工与外部的交流和信息交换的过程，要求认真落实安全责任；

第十条 对于遵守安全规定的先进人员予以适当奖励，对于违反安全规定的人员，要进行批评教育，行政处分甚至

依法追究刑事责任；

第十一条 对于离岗员工，必须严格规范人员离岗过程，及时终止即将离职员工的所有访问权限。

第十二条 工作人员离岗离职时，应该把自身掌握的全部工作资料完整移交宜宾市发展和改革委员会系统管理科室，包括：服务器，交换机，路由器的用户名和密码口令；网络系统集成的文档，如路由器、交换机和服务器参数、网络拓扑图、网络布线图、虚网划分、IP 地址分配等网络机密资料；随机赠送的服务器、网络通信设备携带的说明书、各种文字资料等网络系统的重要资料；其它重要资料。

第十三条 对于离岗员工，必须及时取回离职员工的各种有关证件、有关笔记、钥匙、徽章等以及机构提供的软硬件设备，并办理严格的调离手续。

第十四条 对于离岗员工离岗后应该严格执行《劳动合同》及《劳动合同补充协议》所约定的保密条款。

附件 9

吕梁市发展和改革委员会
信息安全培训与考核管理规定

第一章 总则

第一条 为加强吕梁市发展和改革委员会信息安全培训与考核工作，特制定本办法。

第二条 本办法适用吕梁市发展和改革委员会信息安全培训与考核工作。

第二章 目的和范围

第三条 培训的目的：为提高单位职工普遍的安全意识，使单位职工充分了解信息化安全策略，掌握基本的安全防范方法，确保信息化系统的安全稳定运行。

第四条 培训的人员范围：

全吕梁市发展和改革委员会职工：

●信息安全意识培训；

●安全策略、安全制度培训；

●信息化安全相关的法律法规培训；

●防病毒知识培训等。

●信息化技术员工：

●计算机病毒及防治知识培训；

●安全攻防知识培训；

●操作系统的安全培训；

●安全运维、安全监控；

●主流安全设备的使用；

●安全管理培训等。

第三章 培训与考核的管理

第五条 信息安全培训工作（包括培训需求收集、实施和记录等）由信息管理科室（吕梁市发展和改革委员会办公室和应用系统相关科室）负责；信息管理科室定期向各科室单位收集培训需求，组织培训并做好培训记录。

第六条 针对信息化技术员工，提供脱岗培训方式。邀请信息化安全专业机构或者取得一定资质的主流安全设备供应商对信息化技术员工进行脱岗培训，以提高其自身水平。针对非信息化技术人员，提供在岗培训方式。定期或不定期由办公室组织进行安全培训，从而提高安全意识和自我安全防护能力。

第四章 培训内容

第七条 计算机网络安全知识培训的内容包括但不仅限于：网络的基本安全对策、常见的信息网络安全问题、网络安全隐患、信息系统安全风险管理的方法、计算机信息系统安全事故的查处和管理、计算机犯罪的防范等计算机网络安全保护的相关知识。另外其它方面：

●计算机的安全使用知识；

●信息安全策略、制度；

●信息化安全的相关法律、法规；

●计算机病毒及防治知识；

●安全攻防知识；

●主流安全设备使用和管理知识等。

第五章 培训考核办法

第八条 为提高培训效率，量化衡量培训质量，在每次培训后都要对参与培训的人员进行考核。考核分为书面考核和应用考核方式。考核成绩不合格者，应限制其使用信息化平台，直至考核合格。

第九条 培训记录的保存，为每一位职工建立培训记录表，主要记录以下内容：

●参与了哪些培训；

●培训的时长；

●培训的考核结果；

培训记录表由人事处统一管理，作为绩效考核的一部分以及职位晋升的参考依据。

第十条 由信息管理科室负责培训效果的评估，不仅在培训结束时，在培训结束后一段时间内都要进行培训效果的综合评估，评估的内容包括：

●了解职工对培训课程的主观感受；

●了解职工对于培训内容的掌握情况；

●了解职工的工作行为方式发生了多大程度的改变；

●将人为信息化安全事件与培训内容结合评估。

第六章附则

第十一条 本办法由吕梁市发展和改革委员会负责解释。

第十二条 本办法自颁布之日起执行。

附件 10

吕梁市发展和改革委员会
病毒检测和网络安全漏洞检测管理制度

第一条 所有业务服务器都必须统一由吕梁市军民融合研究院安装服务器版防病毒软件、漏洞扫描，并接受集中管理。

第二条 防病毒软件的安装、升级、更新和策略设置由吕梁市军民融合研究院负责。

第三条 吕梁市军民融合研究院每周检查是否新的病毒并进行升级，同时发现问题会及时通知业务部门负责人。

第四条 吕梁市军民融合研究院每周会进行漏洞扫描，每月提供一次报告给业务负部门责人。

第五条 业务部门负责人需要积极配合吕梁市军民融合研究院并且及时整改。

附件 11

吕梁市发展和改革委员会
密码安全管理制度

第一条 本制度所指密码包括计算机终端设备启动、登录密码、全国信用信息共享平台（山西吕梁）等应用系统登录密码，主机房网络设备、服务器登录管理密码。

第二条 新应用系统上线运行或工作人员调入需要开设帐户，必须填写帐号开设申请表，注明使用者部门/单位/科室、工作内容和所需操作权限，由所在部门/单位/科室领导签字，然后由该系统管理部门/单位/科室审核，审核通过后可添加帐户并分配权限和初始密码。

第三条 每个应用系统的使用者每人只可以申请一个帐号，使用者必须使用自己的帐号进行操作。使用者应当及时修改账号初始密码，并注意不得泄露。

第四条 密码必须具有一定复杂程度，定期变换修改，密码必须由英文字母数字混合组成，并且长度不得小于 8 个字符。

第五条 使用者的部门变更或岗位变更，应当办理变更手续。使用人应当填写应用系统帐号变更申请表，由部门领导签字或盖章，报分管领导审核，然后由该系统管理科室执行。

第六条 当有工作人员调离、退休或辞退等不再在本岗位上工作时，应及时填写应用系统、终端帐号注销申请表或

持人事科开具的离职文件，通知该系统管理科室清除该员工的所有权限并停用此帐号。

第七条 应用系统使用人员的帐号和密码由本人保管，禁止把本人帐号借给其他人使用。使用人员应当定期修改密码，保证个人帐户的安全，并对通过个人帐户所做的一切数据操作承担相应的责任。

第八条 密码设备及放置密码设备的保密机柜、保险柜等，必须由密钥管理员设置口令保护，口令长度不得低于6位，不允许采用设备和系统默认的管理口令。密码设备的口令严禁告知其他无关人员。

第九条 用户帐号领取及口令初始化工作只能由使用人本人联系该系统管理科室系统管理人员办理，口令初始化时需出示相关证明。

第十条 不得对加密设备、密钥等进行拍照、录像。

第十一条 发现密码设备通信系统工作异常、有失泄密情况或隐患时，管理人员要立即停止使用，及时报告，并迅速查明原因，采取补救措施。

附件 12

吕梁市发展和改革委员会
重大信息安全事件管理制度

第一条 吕梁市发展和改革委员会办公室以及应用系统相关科室负责信息化系统重大信息安全事件管理工作，其主要职责包括有：

●针对各类安全事件建立安全应急预案；

●针对各类安全事件根据应急预案做出安全响应；

●查明信息安全事件发生的起因，经过和带来的危害结果；

●分析事件的起因；

●提出防范此类事件再次发生的有效措施；

●编写事件调查报告和处理建议。

第二条 日常信息安全工作中应建立应急预案，包括但不仅限于以下内容：

●针对各种可能发生的安全事件进行分类；

●针对各类安全事件进行风险评估；

●针对各类安全事件建立应急预案；

●对已建立的应急响应预案进行预演。

第三条 在发生重大信息安全事件后，应当做好以下工作：

●在迅速进行应急处理或者请求其他力量支援进行应急

处理的同时，应当立即报告，并请示按照预案进行处理响应或根据实际情况应急处理，尽可能保存好原始证据，保护好现场；如涉及违法犯罪的，还应当同时依法报告公安、安全等部门，处理完毕及时汇报情况，编写报告上报领导。

●发生秘密信息被窃取或者泄露事件的，应当在发现后立即报告并在二十四小时内书面报告，并采取有效措施防止相关秘密信息的进一步扩散；

●积极配合事件调查组开展工作，如实介绍情况，提供客观证据和相关服务保障；

●在应急处理过程中，应当采取手工记录、截屏、文件备份和影像设备记录等多种手段，对应急处理的步骤和结果进行详细记录。

第四条 重大信息安全事件的调查处理应当在接到事件报告后30天内完成工作，特殊情况不得超过180天。事件调查处理结束后，应当将调查处理结果以适当的方式予以通报。

附件13

吕梁市发展和改革委员会
网络应用平台个人隐私保护制度

第一章 总 则

第一条 为了保护吕梁市发展改革委员会各网络应用平台用户的合法权益，维护网络信息安全，依据《中华人民共和国电信条例》《电信和互联网用户个人信息保护规定》，制订本制度。

第二条 吕梁市发展和改革委员会提供网络信息服务过程中，全国信用信息共享平台（山西吕梁）收集、使用用户个人信息，适用于本制度。

第三条 本制度所称用户个人信息，是指全国信用信息共享平台（山西吕梁）在提供服务以及与各有关部门进行数据对接过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息，以及用户使用服务的时间、地点等信息。

第四条 全国信用信息共享平台（山西吕梁）在提供信息服务过程中，收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第五条 全国信用信息共享平台（山西吕梁）对收集、使用的用户个人信息的安全负责，应明确和落实相关人员安全管理责任，对工作人员实行权限管理，对批量导出、复制、

销毁信息实行审查，并采取防泄密措施。

第六条 全国信用信息共享平台（山西吕梁）收集、使用用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供，不得与他人谈论用户个人信息内容。

第七条 吕梁市发展改革委员会网络安全和信息化工作领导小组对用户个人信息保护工作实施监督管理，全国信用信息共享平台（山西吕梁）保管的用户个人信息发生泄露、毁损或者丢失，造成或者可能造成严重后果的，应及时通报领导小组办公室进行调查和应急处置。

第八条 全国信用信息共享平台（山西吕梁）保管的用户个人信息因泄露、篡改、毁损或者丢失，对吕梁市发展改革委员会工作带来不利影响的，参照《信息系统管理人员岗位责任制度》办理。

第九条 全国信用信息共享平台（山西吕梁）应积极接受公民、法人和其他社会组织的批评、意见和建议，建立异议申诉机制，明确异议申诉流程。

第十条 本制度由吕梁市发展改革委员会负责解释。

第十一条 本制度自颁布之日起施行。

吕梁市发展和改革委员会办公室　　2020年8月14日印发