版本号：V1.0

网络安全与数据安全管理制度

北京东华万兴软件有限公司

2024 年 1 月

目　录

信息系统安全总体方针

第一章 总则

第一条 为加强和规范北京东华万兴软件有限公司数据安全工作，提高数据安全整体防护水平，实现信息系统的安全管控，依据国家有关法律、法规的要求，制定本方针。

第二条 本方针为北京东华万兴软件有限公司数据安全管理提供一个总体性架构文件，指导北京东华万兴软件有限公司数据安全管理体系建设，以实现统一的安全策略管理，提高整体的网络与数据安全水平，保障网络畅通和信息系统的正常运行。

第三条 本方针适用于北京东华万兴软件有限公司信息系统资产和数据安全人员的安全管理，适用于指导北京东华万兴软件有限公司数据安全策略的制定、安全方案的规划、安全建设的实施和安全管理措施的选择。

第二章 组织机构与职责

第四条 北京东华万兴软件有限公司信息化建设领导小组为北京东华万兴软件有限公司数据安全工作领导机构，领导小组下设办公室，由运维部负责数据安全具体工作。北京东华万兴软件有限公司其他部门主要负责人是落实数据安全管理制度的第一责任人。

第五条 北京东华万兴软件有限公司信息化建设领导小组负责统筹领导北京东华万兴软件有限公司数据安全工作，指导运维部负责的重大的数据安全工作。

第三章 数据安全体系框架和目标

第六条 北京东华万兴软件有限公司数据安全体系框架的组成是安全组织、安全策略、安全技术和安全运作，四大组成部分协同构建、完成和实现北京东华万兴软件有限公司数据安全工作和目标。

第七条

（一）数据安全组织工作目标是建立健全的安全组织，加强人员的安全管理，为数据安全工作提供组织保障。

（二）数据安全策略工作目标是制定完善的数据安全管理制度和技术规范，并确保其有效发布、执行和更新，规范北京东华万兴软件有限公司数据安全管理工作。

（三）数据安全技术目标是采用适当的技术手段，加强业务和支撑系统的安全防护，为数据安全工作提供技术工具支撑。

（四）数据安全运作目标是加强安全工作的运作管理，维护业务和支撑系统的安全运行，及时处理安全问题，为数据安全工作提供运行保障。

第四章 数据安全建设原则和目标

第八条 北京东华万兴软件有限公司数据安全工作的原则是：满足和推动服务业务发展，信息系统安全架构完整、统一，数据集中、信息共享，控制成本、提高工作效率，利用国家标准规范北京东华万兴软件有限公司管理。

第九条 北京东华万兴软件有限公司数据安全工作的目标是：通过建立和完善数据安全的策略体系、组织体系、技术体系和运作体系，保障日常工作的开展和各信息系统的连续正常稳定运行，维护信息系统的数据安全，促进北京东华万兴软件有限公司信息化工作健康发展。

信息系统安全管理策略

第一章 总则

第一条 本策略为北京东华万兴软件有限公司各项数据安全工作提供依据和指导。

第二条 北京东华万兴软件有限公司数据安全工作由信息化建设领导小组牵头，运维部具体组织，各部门分块负责，全员参与，专人管理。

第三条 北京东华万兴软件有限公司数据安全工作以风险管理为基础，在安全、效率和成本之间始终坚持“安全第一”的原则。

第二章 数据安全组织及职责

第四条 北京东华万兴软件有限公司信息化建设领导小组

（一）统筹领导北京东华万兴软件有限公司数据安全工作，指导运维部负责的重大的数据安全工作；

（二）审查和核准数据安全策略及制度；

（三）审核批准重大的数据安全活动；

（四）审核批准对数据安全事故的处置意见。

第五条 运维部

（一）负责组织北京东华万兴软件有限公司数据安全工作；

（二）负责制定北京东华万兴软件有限公司数据安全管理制度、技术规定、应急预案等，并督促执行；

（三）负责对北京东华万兴软件有限公司内各系统安全的检查和防护，及时处置安全风险；

（四）负责对计算机病毒感染的预防、检测和清除，定期维护计算机软件和数据、对重要信息定期进行检查和备份；

（五）负责数据安全事故的处置；

（六）负责组织数据安全培训和宣传。

第六条 数据安全责任

北京东华万兴软件有限公司其他部门主要负责人是数据安全第一责任人，负责本部门所有与数据安全相关的活动。其他部门数据安全联络员负责配合数据安全相关的检查、管理、上报及其他需协调的工作。

第七条 运维部必须与接触北京东华万兴软件有限公司敏感信息和核心技术资料的第三方签署保密协议，并与在北京东华万兴软件有限公司工作的第三方人员签署个人保密协议。

第三章 安全风险管理

第八条 定期对操作系统、数据库系统、网络系统、应用系统等进行漏洞识别与分析，对系统中所存在的高风险漏洞按照流程进行处置。

第九条 每年至少进行一次全面的风险评估，以确定是否存在新的威胁或薄弱点，并分析是否需要增加新的安全控制措施。

第十条 当发生以下情况时需及时进行风险评估工作:

（一）当发生重大数据安全事件时；

（二）当信息系统发生重大变更时；

（三）信息化建设领导小组确定必要时。

第十一条 针对风险评估结果制定风险控制措施及实施计划。风险整改后，应再次进行评估，以确保风险得到正确规避。

第四章 资产安全管理

第十二条 信息资产是指有业务价值的实物或者虚拟的事物。

第十三条 各部门应识别与信息生命周期有关的资产，形成资产清单，及时更新，并指定资产所有人，资产所有人负责资产的维护与安全，对资产进行安全等级划分。

第十四条 资产管理

（一）对所管理的资产必须明确说明使用、发布、复制、存储、传输、销毁的过程并记录；

（二）资产所有人负责信息的授权，资产只能授权给工作必须的人员；

（三）信息的获取应该遵照工作需要原则、受控审批的原则，严禁未经批准的私下获取行为；在对外提供任何可能涉及北京东华万兴软件有限公司信息的资料、数据、信息之前，不管提供的对象是上级管理部门，还是第三方，都必须事先经过资产所有人的审批许可；

（四）未经批准，严禁泄露信息系统的安全控制机制。对外公布的信息必须经过审批，不得在公开媒体上发布、谈论和传播北京东华万兴软件有限公司的数据和信息；

（五）必须采用北京东华万兴软件有限公司批准的销毁方式销毁信息。

第五章 人员安全管理

第十五条 聘用条款和保密协议

（一）运维部聘用人员的聘用条款应明确数据安全责任；

（二）所有数据安全相关人员需与北京东华万兴软件有限公司签订保密协议及岗位责任协议，明确各岗位安全职责。

第十六条 人员审查

（一）对相关信息化供应商以及工作人员应按照相关法律法规和对应的业务要求进行安全资格审查；

（二）必须对进入关键岗位的职工进行资格审查和技能考核。

第十七条 定期组织干部职工以及相关第三方人员学习数据安全知识，进行安全意识、安全态势培训。

第十八条 人员离职时应及时收回所有涉及北京东华万兴软件有限公司业务内容的资料、数据、信息，立即取消所有访问信息系统的权限。

第十九条 人员调离其他单位，需提交调离申请，经相关领导审批后进行工作交接，并对北京东华万兴软件有限公司有关所有信息进行保密，如若发现泄密，需承担相关的法律责任。

第六章 物理和环境安全

第二十条 场地安全

（一）运维部应根据国家相关标准以及工作性质划分相应的安全级别，并建立相应的准入控制措施；

（二）所有受控区域必须指定数据安全管理责任人。

（三）应建立外来人员访问机制，确保只有授权人员才允许进入受控区域。

（四）应建立受控区域安全操作规程，需要避免在受控区域进行不受监督的工作。

第二十一条 设备安全

（一）将设备放置到相应级别控制区域；

（二）建立防盗、报警、环境监控等保护措施；

（三）应保护设备使其免于支持性设施（电、温湿度、通信）失效而引起设备故障。

（四）采用专业技术人员对设备进行维护，确保其持续的可用性和完整性。

（五）设备、信息或软件在授权之前不宜带出受控区域。

第二十二条 环境安全

（一）办公室环境需满足正常的保密要求。

（二）办公室照明需满足目视及摄像头观测照度清晰要求。

第七章 网络通信安全管理

第二十三条 通过物理分离、防火墙、上网行为控制设备、VLAN 划分进行内外网的物理和逻

辑划分，建立网络安全区域，明确安全边界，并进行网络访问行为限制和监控。

第二十四条 网络设备

（一）网络设备的安装、配置、变更、撤销等操作必须经过运维部相关领导审批；

（二）网络的拓扑结构、IP 地址等信息未经授权，严禁泄露；

（三）网络设备的远程登录操作应限定在指定网段范围内。

第二十五条 所有与北京东华万兴软件有限公司的网络进行连接都需要经过信息化建设领导小组的批准；所有与北京东华万兴软件有限公司外部网络相连的出入口处必须设立防火墙；通过接入服务器接入北京东华万兴软件有限公司内部网络时，必须经过认证。与北京东华万兴软件有限公司外部网络相连接的系统必须有专人负责管理。

第八章 操作安全管理

第二十六条 运作流程

（一）必须明确并遵循信息系统运作的变更流程；

（二）必须明确并遵循安全问题处理流程；

（三）信息系统的生产环境和开发测试环境需要分离；

（四）系统的超级管理权限应采取双人控制，互相制衡。

第二十七条 恶意软件的防护

（一）实施恶意软件的监测、预防和恢复的控制措施；

（二）北京东华万兴软件有限公司的计算机系统都必须安装、运行单位统一部署的防病毒软件，并及时升级。未经批准，不能安装其它的防病毒软件；

（三）接收和发布信息时须进行病毒检测；

（四）服务器必须实时运行防病毒软件；

（五）定期对北京东华万兴软件有限公司的联网办公设备进行扫描，及时发现漏洞并修复。

第二十八条 信息系统管理

（一）建立备份策略，按照策略的要求，定期备份和测试信息、软件及系统。

（二）对系统操作人员的活动进行日志记录；

（三）定期检查和处理系统日志；

（四）对一些重要的信息系统进行实时监控；

（五）对组织内部的办公设施进行时钟同步；

（六）非正版软件不能安装。

第九章 访问控制

第二十九条 用户访问管理

（一）帐户开户

1.根据工作相关性原则并经过审批后为个人分配权限；

2.建立帐户开户和销户的闭环流程，控制用户对系统的访问权限；

3.含有保密信息的系统禁止建立公用帐户；

4.用户的岗位或职责发生变化时，应立即变更或取消相应的访问权限；

5.对分配的权限必须记录和进行维护。

（二）口令管理

1.口令的管理责任人为账户的使用者；

2.口令的设置要遵循北京东华万兴软件有限公司有关规定。

（三）对用户访问权限进行定期检查；

（四）用户责任

1.用户应采取方式保证口令安全；

2.不得共享个人的口令；

3.定期更改口令。

第三十条 操作系统访问控制

（一）严格控制操作系统管理员对系统文件和业务数据的操作权限；

（二）根据工作相关性原则授予用户相应权限；

（三）系统建立的日志必须满足审计要求，系统日志必须安全存放，防止被非授权的访问；

（四）必须及时安装系统安全补丁；

（五）关闭所有系统不需要的系统服务；

（六）服务器的密码文件须加密存放；

（七）定期修改用户口令。

第三十一条 应用系统访问控制

（一）根据业务访问控制策略对用户严格授权；

（二）严格限制业务人员越过应用程序对后台数据库或操作系统直接访问；

（三）建立和维护应用系统的用户权限表；

（四）删除所有系统上不使用的帐号。

第十章 运行维护安全管理

第三十二条 建立日常维护相关操作规程和规范手册，规范介质管理、账号口令管理、补丁管理、防病毒管理、服务器运行管理等日常运行维护操作。

第十一章 系统开发

第三十三条 确保安全贯穿系统整个生命周期的各个阶段。

第三十四条 系统的规划设计阶段必须做安全需求分析、总体安全设计、安全建设规划。

第三十五条 系统开发策略

（一）建立并遵循安全开发标准；

（二）、进行风险分析和风险管理，确定系统安全控制机制；

（三）操作人员只保留可执行代码；

（四）程序源代码尽可能不要保留在运行系统上；

（五）在系统发布前，应进行安全测试。

第三十六条 加密策略

（一）加密算法必须是经过政府批准的或符合业界标准；

（二）密匙必须有明确的管理人员。

（三）加密的数据和口令须分开传递；

（四）使用加密保护敏感数据，明确密钥管理员的职责；

（五）密钥产生、分发、存储的相关信息必须防止泄露给未授权的人员，当这些信息不再需要时，必须采用规定的方式予以销毁。

第十二章 数据安全事件管理

第三十七条 各部门应了解数据安全事件管理目标，熟悉数据安全应急响应流程，确保能快速、有效和有序地响应数据安全事件。

第三十八条 各部门相关人员应尽可能早的将数据安全事件通告给部门负责人，运维部根据安全事件的类型和级别定义判断安全事件，根据安全事件处理流程进行处理和汇报。

第三十九条 运维部根据数据安全事件预案向信息化建设领导小组提出应急恢复流程的启动申请，经批准后，按照应急恢复流程处理。

第十三章 应急响应管理

第四十条 建立统一的应急预案框架，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。

第四十一条 从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。

第四十二条 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期。

第十四章 数据安全通报机制

第四十三条 北京东华万兴软件有限公司运维部负责组织数据安全信息通报工作，必要时，向北京东华万兴软件有限公司各部门通报数据安全工作情况以及安全预警和病毒攻击等信息。

第四十四条 各部门数据安全联络员负责收集和反馈本部门数据安全信息，并向运维部报送。

第四十五条 将数据安全通报作为数据安全工作的重要环节。不能出现瞒报、缓报、谎报数据安全事件和推诿责任的行为。

网络与数据安全管理岗位职责说明

第一章 总则

第一条 目的

为规范数据安全管理系统中各安全岗位的人员职责，特制订本规范。

第二条 范围

本规范适用于北京东华万兴软件有限公司各网络与数据安全管理岗位和人员。

第三条 职责

网络与数据安全领导小组负责分配、协调各网络与数据安全管理岗位的人员角色和日常工作，各岗位人员负责本岗位的日常数据安全管理。

第二章 各安全管理岗位职责说明

第四条 数据安全各管理岗由网络与数据安全领导小组授权或指定，是北京东华万兴软件有限公司数据安全管理体系的具体执行者，设有安全管理员、系统管理员、网络管理员、数据库管理员、审计管理员等。各岗位的人员组成及各岗位职责描述如下：

1、安全主管职责：

领导各管理员进行工作，根据需要适时召开安全工作小组会议，研究落实计算机系统隐患整改事宜及事故处理决定，讨论有关规定及工作制度，布置有关工作，传达学习有关规定。

2、安全管理员职责：

负责制定和实施网络数据安全管理制度，以技术手段隔离不良信息，及时发布预知通告，发布计算机病毒、网络病毒的危害程度、防杀措施、及补救办法。教育计算机用户和网络用户树立安全意识，主动防范病毒、黑客的侵扰，抵制不良信息；建立网络数据安全监管日志。负责信息化建设相关文件资料的收集、归类与整理，做好资料收集、编目、建档工作。负责运维部设备、材料、软件介质等的建档、编号与借用管理。

3、系统管理员职责：

负责服务器系统的设计、安装、配置、管理和维护工作，为服务器的安全运行做技术保障。维持服务器系统的稳定、正常运转，及时解决服务器系统故障。做好服务器配置、安装和改动记录。如果服务器发生故障，必须记录故障发生的时间、故障情况、处理方法，及预防措施等。定期对硬盘进行整理，清除缓存或垃圾文件。定期保存系统日志。做好系统的硬件维护，对设备定期检查，定期清洁、除尘，保持设备正常运行。负责定期对系统运行日志进行审计，形成审计分析报告。

4、网络管理员职责：

负责网络系统的设计、安装、配置、管理和维护工作，为网络的安全运行做技术保障。维持网络的稳定、正常运转，及时解决网络故障。做好网络设备配置、安装和改动记录。如果网络发生故障，必须记录故障发生的时间、故障情况、处理方法，及预防措施等。做好系统的硬件维护，对设备定期检查，定期清洁、除尘，保持设备正常运行。

5、数据库管理员职责：

负责数据库系统的运行管理，实施系统安全策略。管理数据库用户权限，使单位信息系统安全运行。记录系统安全事项，及时向安全管理员报告安全事件。对重要数据定期进行备份及执行备份恢复工作。监督对系统进行操作的其他人员。

6、审计管理员职责：

负责定期对主机系统、网络产品、应用系统的日志文件进行分析审计，发现问题及时上报；负责对数据安全保障管理活动进行独立的监督，提供内部独立的审计和评估工作，并根据需要可以协同外部审计评估机构进行评估和认证，为决策领导提供信息系统和数据安全保障执

行状况的客观评价。

7、人员配备

岗位	姓名
安全主管	曹金国
安全管理员	孟令楠
系统管理员	罗昌华
网络管理员	王迦玮
数据库管理员	赵京鹏
审计管理员	石月

授权和审批管理办法

第一章 总则

第一条 为规范单位数据安全管理各环节的审批流程和审批责任人，特制订本规范。

第二条 本管理制度适用于信息系统相关的所有授权和审批事项，明确各相关管理环节授权和审批的部门和责任人。

第三条 运维部负责制订该规范并报网络与数据安全领导小组审批通过后，由单位相关部门和相关人员参照执行。

第二章 管理细则

第四条 内部人员授权管理办法：

一、内部授权程序：

（1）根据网络与数据安全领导小组的主要职责，数据安全主管由网络与数据安全领导小组授权后生效。数据安全工作小组直接对网络与数据安全领导小组负责。

（2）根据数据安全工作小组的主要职责，数据安全各安全岗位的负责人员由数据安全工作小组授权后生效。各数据安全岗位管理人员对数据安全工作小组负责。

（3）根据数据安全工作小组的主要职责，各业务信息系统的经办人员由各业务单元的相关部门提名产生，最终由数据安全工作小组授权后生效，各业务经办人员对数据安全工作小组负责。

二、变更审批办法：

1、变更分类与审批的一般原则：

（1）信息系统变更主要分两大类别：功能优化类变更和系统完善类（bug 修订，补丁修复）变更。

（2）功能优化类变更的发起人为各部门业务经办人员。

（3）系统完善类变更的发起人为各部门业务经办人员、系统管理人员。

（4）两类变更的审批办法和流程基本一致，原则是需要有效识别各类系统变更的风险，并严格按照审批程序有效规避风险、落实相关责任方。

2、变更审批流程：

（1）变更由上述变更发起人发起，根据变更的具体内容填写相关的变更管理表单。

（2）功能优化类变更审批的第一级部门是业务经办部门，因为不直接牵涉到信息系统的变更，该部分变更由业务经办部门审批，最后一个审批人须是业务经办部门的部门领导或者更高一级的主管领导，具体由业务经办部门自行决定。

（3）功能优化类变更审批的第二级审批部门是运维部，由运维部安排专人评估变更的风险和可行性，评估结果可行后，有运维部负责人审批，运维部负责人审批后交由系统实施人员具体实施，完成系统变更。

（4）系统完善类变更可能会涉及到系统的内核，影响系统运行的稳定性。此类变更一般由系统管理员发起，要求系统管理员在发起变更的同时需要就本次变更的潜在风险和风险规避措施进行描述后报请运维部负责人进行审批，运维部负责人审批后由系统管理员进行具体实施，完成系统变更。

三、其他审批办法：

（1）物理访问、系统接入等其他对信息系统（包括 业务网、主机房、各业务信息系统）的访问和修改操作，均由运维部负责人或运维部负责人授权的运维部其他人员负责审批并监督后续的访问过程。

（2）重要操作，如业务系统功能上的重大调整、重大升级变更、网络架构大的调整，均需

要由运维部负责人召集相关人员论证后初审，初审的结果报网络与数据安全领导小组做最后审批后进行。

第三章 附则

第五条 本管理规范牵涉多个部门和人员，必须在每年的年中和年末由运维部发起评审，进行评审修订，及时更新需授权和审批的项目、审批部门和审批人等信息。

第六条 遇单位组织机构调整等其他影响原定审批制度情况，可由运维部适时发起对于本规定的评审修订工作，适时修订各变动项目。

第七条 每次评审修订由文档专员在本制度的‘制度修订一览表’中如实记载评审修订内容，并更改制度版本号。

数据安全检查管理办法

第一章 总则

第八条 为了加强和规范北京东华万兴软件有限公司数据安全检查工作，保障相关信息系统安全运行，特制定本管理办法。

第九条 数据安全检查依据国家有关法律法规、行业有关规章制度，单位数据安全相关规章制度。

第十条 数据安全检查对象为北京东华万兴软件有限公司的信息系统。

第十一条 信息技术工作检查可采取日常检查、组织自查、专项检查、年度检查等方式。年度检查对象包括所有相关部门，且每年不少于二次。

第二章 组织机构与职责

第十二条 运维部负责数据安全检查工作，根据当前现状明确检查重点，制定检查标准。

第十三条 运维部成立数据安全检查小组，具体负责数据安全检查工作的实施。

第三章 数据安全检查分类

第十四条 各部门及相关人员要配合各项数据安全检查工作，并按要求完成检查中发现问题项的整改工作。

第十五条 北京东华万兴软件有限公司的数据安全检查包括数据安全主管部门对北京东华万兴软件有限公司进行的专项数据安全检查、数据安全认证机构对北京东华万兴软件有限公司的数据安全外部审核、风险监管部门主导的数据安全内部审核和内部数据安全技术检查等。

第四章 数据安全检查内容

第十六条 计算机安全检查

1.计算机应安装杀毒、防护等软件，及时更新系统，修复漏洞。

2.非涉密计算机不得存储涉密文件、敏感信息。

3.涉密计算机和安装了“三合一系统”的计算机必须按照相关规定严格管理，严禁违规外联。

第十七条 系统安全与设备管理的检查

1.服务器

（1）服务器应具有充分的可靠性和充足的容量。

（2）服务器应具有一定的容错特性，宜采用镜像、阵列、双机、群集等容错技术。

（3）服务器有安全可靠的备份措施。

2.工作站

（1）工作站应具有良好的性能及可靠性。

（2）除计算机机房外，一律使用无软驱或光驱等可卸存储装置的网络工作站。

（3）重要工作站应有冗余备份。

第十八条 安全管理情况的检查

1.建立由安全策略、管理制度、操作规程等构成的全面数据安全管理制度体系。

2.严格按管理制度规定进行管理，按操作规程进行操作，并进行记录。

第五章 数据安全检查实施

第十九条 实施检查前，检查小组根据检查目的和被检查部门情况，确定检查范围、检查重点，制定检查工作计划，编制相应检查表格。

第二十条 组织进行自查时，被检查部门应如实填写自查表，对存在的问题隐瞒不报的，将追究相关部门和个人责任。

第二十一条 进行现场检查时，检查小组应提前通知被检查部门，可根据需要要求被检查部门进行自查，以提高现场检查工作效率。每次检查前，检查小组应核查上次检查提出的整改

意见是否落实，整改措施是否有效。

第二十二条 被检查部门应积极配合检查工作，按检查人员要求提供与检查工作相关的资料，并对所提供资料的真实性、完整性负责。

第二十三条 检查过程中应切实防范检查操作风险，不得对在线运行系统进行检查测试和网络扫描检测。因检查需要需使用辅助检测工具时，应经运维部负责人审批同意后方可使用。

第二十四条 检查过程中发现问题和安全隐患时，检查小组应及时与被检查部门沟通确认后，拟定整改建议。对于随时可能引发事故的问题和安全隐患，应要求立即整改。

第六章 数据安全检查报告

第二十五条 检查工作结束后，检查小组应及时撰写检查报告上报信息化建设领导小组，根据批示意见对检查结果进行通报，对存在问题和安全隐患的部门下发整改意见书，要求限期完成整改工作。

第二十六条 检查小组应跟踪整改工作的落实情况，必要时可对整改工作落实情况进行确认检查。

数据安全违章行为责任追究办法

第一章 总则

第一条 为加强北京东华万兴软件有限公司工作人员的数据安全责任意识，界定工作人员数据安全违章行为，明确数据安全违章责任追究和处罚依据，特制定本管理办法。

第二条 数据安全违章行为分为一般违章和严重违章。数据安全违章行为由运维部负责组织调查和认定，并依据本办法进行责任追究。

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。

第四条 本管理办法适用于所有与信息系统相关的人员。

第二章 违章行为界定

第五条 凡具有下列行为之一均属违章行为：

1. 违反国家数据安全有关法律和法规。
2. 违反北京东华万兴软件有限公司数据安全管理规章制度。

第六条 一般违章界定

（一）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。

（二）未按规定安装运行或自行卸载单位统一的防病毒软件、补丁更新策略、桌面终端管理软件。

（三）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。

（四）擅自卸载（含格式化）北京东华万兴软件有限公司规定安装的操作系统和业务应用系统客户端。

（五）未使用单位统一的外网邮件系统处理和发送与工作相关的电子邮件。

（六）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（如低级格式化等）。

（七）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。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。

（八）移动存储介质丢失未向北京东华万兴软件有限公司运维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。

（九）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。

（十）工作人员岗位异动后未及时向运维部申请账号和权限的变更。

（十一）违反单位数据安全管理规定被认定为一般违章的其他行为。

第七条 严重违章界定

（一）未经运维部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。

（二）擅自更改计算机网卡的 MAC 地址或 IP/MAC 地址绑定策略。

（三）在计算机上私自开启 DHCP、WWW、FTP、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。

（四）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。

（五）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。

（六）在计算机中存储和处理国家、单位秘密信息，在外网计算机中存储涉及单位重要敏感

信息的电子文件。
（七）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。
（八）安全移动介质损坏后私自丢弃未交运维部处理并造成单位重要信息外泄。
（九）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。
（十）擅自组建无线网络并接入信息内网。
（十一）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。
（十二）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。
（十三）拒绝运维部维护人员对计算机进行安全性检查和安装单位统一要求的桌面终端管理软件、防病毒软件等。
（十四）违反北京东华万兴软件有限公司数据安全管理规定被认定为严重违章的其他行为。

第三章 督察与检查

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。

第九条 发生数据安全违章，按照管理权限，实行分级查处、分级追究。
（一）北京东华万兴软件有限公司各部门自查自纠发现的违章，参照本办法自行处理。
（二）运维部组织的督查、日常检查及采用单位统一部署工具软件检查发现的违章，按照本办法规定处理。
（三）单位督查、日常工作检查及采用单位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单位领导。

第四章 处罚规定

第十条 在年度内第一次发生一般违章或严重违章，对当事人给予诫勉谈话；半年内同一当事人发生两次一般违章或严重违章，对当事人给予通报批评；一年内同一当事人发生三次一般违章或严重违章，对当事人给予写检讨并通报批评，并对当事人所属部门予以通报批评。

安全教育和培训管理办法

第一章 总则

第一条 为规范北京东华万兴软件有限公司数据安全培训及教育工作，对干部职工进行有关数据安全管理的理论培训、安全管理制度教育、安全防范意识宣传和专门安全技术训练，确保北京东华万兴软件有限公司数据安全策略、规章制度和技术规范的顺利执行，特制定本管理规定。

第二章 数据安全培训要求

第二条 数据安全培训工作需要分层次、分阶段、循序渐进地进行，而且必须是能够覆盖全员的培训。

第三条 应制定完善的《培训计划》，计划应包含培训方式、培训类别、培训内容、培训费用等信息，并且需要相关领导对培训计划进行审批。

第四条 分层次培训是指对不同层次的人员，如对管理层、数据安全管理人员，数据安全联络员和普通干部开展有针对性和不同侧重点的培训。

第五条 分阶段是指在数据安全管理体系的建立、实施和保持的不同阶段，培训工作要有计划地分步实施；数据安全培训要采用内部和外部结合的方式进行。

第六条 管理层培训

（一） 管理层培训目标是明确建立数据安全体系的重要性，获得管理层的支持和承诺。

（二） 管理层培训方式可以采用聘请外部数据安全培训、专业技术专家和咨询顾问以专题讲座、研讨会等形式。

第七条 数据安全管理人员培训

（一） 数据安全管理人员培训目标是理解及掌握数据安全原理和相关技术、强化数据安全意识、支撑数据安全体系的建立、实施和保持。

（二） 数据安全管理人员培训方式可以采用聘请外部数据安全专业资格授证培训、参加数据安全专业培训、自学数据安全管理理论及技术和内部学习研讨的方式。

第八条 数据安全联络员培训

（一） 数据安全联络员培训目标是掌握各系统相关专业安全技术，协助维护和保障系统正常、安全运行。

（二） 数据安全联络员培训方式可以采用外部和内部相结合的培训以及自学的方式。

第九条 普通干部培训

(一) 普通干部培训目标是了解相关数据安全制度和技术规范，并安全、高效地使用信息系统。

(二) 普通干部培训方式应主要采取内部培训的方式。

第三章 数据安全培训内容

第十条 各级领导及职工应明确了解数据安全体系，并明确各自的安全职责，明确自身对维护保障系统正常、安全运行所需承担的相关责任和义务。

第十一条 针对业务需求进行相应安全意识培训，提高员工的安全意识和防范能力。

第十二条 针对系统的维护人员和管理员应定期开展安全技术教育培训（每年至少一次），明确如何安全使用有关业务系统及普通计算机周边硬件设备。

第四章 数据安全培训管理

第十三条 数据安全培训发起：

（一） 数据安全培训教育，纳入北京东华万兴软件有限公司的整体培训计划中。

（二） 具体操作过程遵守北京东华万兴软件有限公司的相关培训管理制度。

第十四条 数据安全培训实施：

（一） 数据安全培训的实施，主要由运维部负责组织和考核。

（二） 对专业性很强的安全培训，由运维部负责聘请外部专家进行安全培训。

（三） 具体操作过程遵守相关培训管理制度。

第十五条 数据安全培训过程中，要做好《培训签到表》，并将参与培训人员整理、备案。

外来人员安全访问管理办法

第一章 总则

第一条 为了规范第三方用户访问北京东华万兴软件有限公司内部信息系统时的行为，保护北京东华万兴软件有限公司网络与信息系统安全，特制定本管理办法。

第二章 来访人员出入管理

第二条 第三方人员进入北京东华万兴软件有限公司所属单位及其建筑物，应遵守北京东华万兴软件有限公司相关安保制度。

第三条 未经北京东华万兴软件有限公司特别许可，第三方人员不得在公司院内摄影、拍照。

第四条 北京东华万兴软件有限公司干部职工要遵守相关安全保密规定，禁止与第三方人员谈论与其工作无关的内容。

第三章 机房出入管理

第五条 除以下情况外，不得引领和允许第三方人员访问机房等重要区域：

(一) 北京东华万兴软件有限公司领导批准的参观活动；

(二) 必要的仪器设备现场安装、维修、调测；

(三) 第三方因业务需要进入上述区域的其它情形。

第四章 网络访问管理

第六条 北京东华万兴软件有限公司数据安全管理人员有义务向第三方人员说明网络接入安全要求。

第七条 第三方人员不允许私自连接公司网络。如果必要，必须提出申请，征得运维部允许后方可接入。第三方人员连接网络要进行相应登记备案，并签订网络使用安全协议。

第八条 长期使用内部网络的第三方人员的计算机必须接受北京东华万兴软件有限公司的统一客户端管理，包括客户端管理软件的安装、安全策略的配置等。

第九条 第三方人员如果需要访问网络资源，须提前明确申请要访问资源的类型、范围和方式，以便管理员进行审批，并提供相应的访问权限和访问方法。

第十条 第三方人员操作服务器或网络设备，必须使用临时帐号，使用之后由相应的管理人员及时清除；对于长期在北京东华万兴软件有限公司工作的技术支持、顾问、服务人员，如果需要长期操作服务器或网络设备，管理人员应该为第三方人员创建单独的帐号。

第十一条 北京东华万兴软件有限公司有权对第三方人员在公司内部网络的活动进行检查、审计和监控。

第十二条 第三方人员的计算机要求安装有防病毒软件，不得携带有木马、病毒等破坏性程序。

第十三条 第三方人员不准使用北京东华万兴软件有限公司网络从事同工作无关的网络活动。

第十四条 第三方人员不准在北京东华万兴软件有限公司网络内部通过拨号或其它手段直接建立到其它网络的物理链路。

机房运行管理办法

第一章 总则

第一条 为了加强北京东华万兴软件有限公司机房管理规范，保护重要服务器、网络设备、安全设备、应用系统等系统安全，特制定本规定。

第二章 职责及权限

第二条 北京东华万兴软件有限公司运维部是机房管理的主要部门，负责机房的日常检查、维护和管理、应急处置工作。

第三章 机房出入管理

第三条 非机房管理人员，一般情况下禁止进入机房，特殊情况需进入机房时须由机房管理人员全程陪同，并填写《机房出入登记表》后方可进入；

第四条 机房管理人员经授权获得门禁访问权限后，凭机房门禁卡出入机房，并由门禁系统和视频监视系统记录其在机房的行为；

第五条 未经许可，进入机房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，不准携带任何磁带（盘）、磁介质和资料进入机房。经特许携带的，必须填写《机房进出登记表》中相关项后方可进入；

第六条 未经许可不允许使用摄影、录像或其它音像记录设备等机房内各类设备、器材须经运维部机房维护人员批准，方可进出机房。对于需要经常出入机房的设备，需在设备上张贴专用的标记。

第四章 机房安全管理

第七条 机房维护人员随时监控中心设备运行状况，发现异常情况应立即按照预案规程进行操作，并及时上报和详细记录；

第八条 非机房维护人员未经许可不得擅自上机操作和对运行设备及各种配置进行更改；

第九条 严格执行密码管理，对操作密码定期更改，超级用户密码由系统管理员掌握；

第十条 机房维护人员应恪守保密制度，不得擅自泄露机房各种信息资料与数据；

第十一条 机房维护人员应对机房内设置的消防器材、监控设备进行检查，以保证其有效性。

第五章 机房环境管理

第十二条 机房管理人员对机房环境每天进行一次检查，对发现的问题要及时解决，填写《机房巡检记录表》;

第十三条 机房内要保持设备无尘、布线整齐、物品就位、资料齐全，应保持机房整洁；定期进行清扫，进行清扫时禁止使用带水的洁具。每年至少应聘请一次外部专业机房清洁单位对机房环境进行清扫；

第十四条 机房内严禁堆放与工作无关的其它物品及纸质物品。做好消防灭火设备检查工作；

第十五条 机房内禁止饮食、吸烟、打闹、大声喧哗，机房内不得会客、闲谈；

第十六条 机房内要保证足够的照明度，备有紧急照明设备，并有专人负责，定期检修；

第十七条 机房内需对温度和湿度进行监控，温度保持在 18℃-25℃，湿度保持在 40%-60%；

第十八条 UPS 必须定期年检，并填写检查报告。

第十九条 机房接地系统要符合相应的技术标准，各个设备交流工作电源应有工作接地，机柜应有效接地。

第二十条 机房配电柜要有防雷设施，进出机房的电缆应有防雷措施。

第二十一条 机房用电要使用独立的电线，专用变压器、电源稳压器等。

第二十二条　机房的环境应达到机房建设的设计要求。

第六章 机房操作管理

第二十三条　应指定专人负责机房的操作管理。

第二十四条　机房值班人员必须密切监视机房设备运行状况以及各端口运行情况，确保安全、高效运行。

第二十五条　严格按规章制度要求做好各种数据、文件的备份工作。重要的服务器数据库要定期进行备份，并严格实行专人保管。所有重要文档定期整理装订，专人保管，以备后查。

第二十六条　各类软件系统的维护、增删、配置的更改，各类硬件设备的添加、更换必需执行变更管理流程；必须按规定进行详细登记和记录，对各类软件、现场资料、档案整理存档。

第二十七条　网络与数据安全领导小组应对制度的执行情况进行检查，督促各项制度的落实，并作为人员考核之依据。

第七章 机房设备管理

第二十八条　机房要有完整的网络拓扑图并定期进行更新。

第二十九条　机房内的所有设备应贴有设备标签，并注明设备的主要参数。

第三十条　主机系统和网络设备的各类接线的两端应设置标签，网络接口侧应注明连接的设备。

第三十一条　对主要网络设备如核心路由器、交换机、防火墙、IDS 等设备的配置文件定期进行一次评审。

第三十二条　对机房的主机设备及核心网络交换装置应严格管理，做好应急准备，制定周密的故障应急措施。

第三十三条　严禁擅自在运行的业务系统服务器、交换机、路由器等设备上进行开发、调试或学习培训等工作。

第三十四条　进入机房的服务器应遵守机房规定，安装最完整系统补丁、防病毒软件、管理员责任明确，各设备需贴有资产标识，并在标识上明确该资产责任人，责任人发生变更时应及时更新资产标识。

信息分类与标识管理办法

第一章 总则

第一条 为有利于北京东华万兴软件有限公司信息系统相关信息的识别、保护和利用，加强北京东华万兴软件有限公司信息系统相关信息的安全管理，特制订本管理办法。

第二条 本管理办法适用于北京东华万兴软件有限公司信息系统相关信息的管理。

第二章 信息分类的定义

第三条 北京东华万兴软件有限公司信息系统相关信息的分类和标识的目的：

（一）通过对北京东华万兴软件有限公司信息系统相关信息按无形性质（非财务）进行分类和标识，促进信息的增值利用，提高信息的利用率；

（二）促进信息分布的合理化、促进非结构化信息向结构化数字信息的转换，降低信息管理成本；

（三）掌握北京东华万兴软件有限公司信息系统相关信息的状态，明确信息的使用方法、保存方式、放置位置、安全分类和责任人等，加强信息的管理，为信息系统的日常与应急工作提供基本资料；

第四条 根据各种信息的敏感度和重要性的不同，制定对信息各种相应的分类保护措施，对各类信息实施适当程度的保护。信息指北京东华万兴软件有限公司在生产、经营和管理过程中，所需要的以及所产生的，用以支持（或指导、或影响）北京东华万兴软件有限公司生产、经营和管理的一切有用的数据和资料等非财务的无形信息，其范围包括如下现在的和历史的信息：

（一）北京东华万兴软件有限公司的域名、网络拓扑结构、网络 IP 地址及分配规则；

（二）系统配置数据、系统授权信息、口令文件、密钥及算法文件、系统说明文档、用户手册等系统基础数据；

（三）各类专业系统的应用数据库及数据文件、业务报表等系统业务数据；

（四）各类专业系统的运行方案、运行记录、变更记录等系统运行数据以及应急计划；

（五）各类专业的规划、方案与策略、业务流程、业务规范、操作规程等管理数据；

（六）技术图纸、技术文档、工程资料等项目数据；

（七）其他纸介质的重要办公文件（信件）、图象、影象、录音和照片等非结构化办公资料；

（八）单个员工拥有的专家技能和经验等隐性数据。

第五条 北京东华万兴软件有限公司信息的安全分类：信息按信息的敏感度分类为机密信息、秘密信息、对内公开信息、对外公开信息。

第六条 信息的存放介质分别为电子介质、纸介质以及其他介质，对于存储介质同时有电子介质或纸介质两种情况的信息，其最终目标应该是信息存储在电子介质。

第三章 信息的管理与使用

第七条 信息的存放应立足于管理和安全的考虑，为了便于保管、提取、查询，信息应尽量以电子介质的形式存储，因此，对于存储在纸介质等其他非结构化的信息，如果技术上允许并且有必要的话，应及时进行适当的处理，转换为结构化的电子信息，并以电子介质的形式存储。

第八条 信息的存储介质存放的地点要求如下：

（一）对于对外公开信息，存放地点没有要求；

（二）对于对内公开信息，如果是结构化的电子信息，应存放在内部服务网络中的文件服务器等；如果是非结构化的其他信息，应存放在室内文件柜中，并有明显的分类标识；

（三）对于秘密信息，如果是结构化的电子信息，应存放在有严格管理制度、具有足够的安

全防护措施的机房环境中的相关服务器和存储设备上；如果是非结构化的其他信息，应存放在室内具有较强防盗窃能力的文件柜中，并造册登记，分项存放；

（四）对于机密信息，如果是联机存储的结构化电子信息，应存放在有严格管理制度、具有高强度的安全防护措施的机房环境中的相关服务器和存储设备上； 如果是脱机存储的结构化电子信息，以及非结构化的其他信息，应存放在具有严格保安措施的、专门的保管环境中（如机要室等），并造册登记，分项存放。

第九条 信息的存储介质使用控制要求如下：

（一）对于对外公开信息，介质使用没有限制要求，任何人在任何场合均可以使用；

（二）对于对内公开信息，对于存储在电子介质上的信息，必须通过内部网络，以注册的合法身份，登录访问和下载使用；对于非结构化的其他信息，经介质保存部门同意，可以提取存储信息的介质使用，使用完毕放回原处；

（三）对于秘密信息，对于存储在电子介质上的信息，原则上要求联机使用，信息只能通过应用系统专用界面使用，使用者必须具有足够的使用权限；秘密信息的脱机提取或抄录，必须有相关领导的书面批准意见，其提取或抄录的相关细节必须记录在案，使用者必须对其提取或抄录秘密信息的安全保密负责；对于非结构化信息的使用，必须符合秘密级文件的相关使用规定，信息的提取或抄录必须有相关领导的书面批准意见，其相关细节必须记录在案，使用者必须对其提取或抄录秘密信息的安全保密负责；

（四）对于机密信息，对于存储在电子介质上的信息，必须联机使用，信息只能通过应用系统专用界面使用，使用者必须具有足够的使用权限；机密信息绝对禁止的脱机提取，特殊信息的抄录，必须有相关领导及保密人员的书面批准意见，抄录的过程及内容必须有保密人员现场监督检查，抄录的相关细节必须记录在案，使用者必须对其抄录的机密信息的安全保密负责；对于非结构化信息的使用，必须符合机密级文件的相关使用规定，特殊信息的抄录必须有相关领导及保密人员的书面批准意见，其相关细节必须记录在案，使用者必须对其提取或抄录秘密信息的安全保密负责。

信息系统资产管理办法

第一章 总则

第一条 为加强北京东华万兴软件有限公司信息系统资产管理，保证信息系统资产的安全完整，提高其使用效率，根据北京东华万兴软件有限公司实际情况，特制定本管理办法。

第二条 信息系统资产包括硬件资产和软件资产，硬件资产包括服务器、网络设备、安全设备、计算机设备、数据库等，软件资产包括应用软件、系统软件、开发工具和实用程序等。

第三条 本管理办法适用于运维部。

第二章 组织机构与职责

第四条 北京东华万兴软件有限公司信息系统资产管理实行二级管理原则。

一级管理：运维部负责北京东华万兴软件有限公司的信息系统相关的硬件资产和软件资产的管理，是其责任部门；

二级管理：在运维部监督、指导下，个人使用的计算机设备由本人负责管理，对所使用的计算机设备的安全完整负责，是其责任人。

第三章 信息系统资产的验收、登记及领用

第五条 北京东华万兴软件有限公司的信息系统相关资产购进后，按规定程序办理验收、登记、领用手续。

验收。按归口原则由运维部组织专人办理验收手续。验收内容主要包括：核对发票所列项目、数量、价格与实物是否一致，实物是否完好无损。

登记。验收合格后，运维部的资产管理员对资产进行分类编号，明细登记（编号、录入）每项信息系统资产的资料（包括台账编号、实物编号、资产名称、购置时间、数量、购置价格、存放地点、供应商、保修期、购置人、验收人、使用部门、使用人等）。

领用。办理验收、登记后，由北京东华万兴软件有限公司总体资产管理部门安排信息系统资产的领用，并办理有关领用手续。

第四章 信息系统资产的使用、维护

第六条 运维部应定期对信息系统资产进行维护保养，以保证信息系统资产处于良好状态，充分发挥其效能。信息系统资产使用期间发生故障或损坏时，运维人员应立即通知运维部负责人，及时组织维修。重要或大宗信息系统资产由运维部安排维保单位定期进行修理。

第七条 所有信息系统资产因公用或维修搬出办公楼必须进行出库登记。

第五章 信息系统资产的实物台账管理

第八条 运维部负责建立健全信息系统资产实物台账。信息系统资产管理员具体负责对资产入库、处置、清查盘点、报废等的台账记录和管理。

第九条 实物台账登记的基本要求：

（一） 按信息系统资产类别和编号进行明细登记。

（二）信息系统资产购建后，按规定程序办理验收入库、登记领用手续，同时进行分类登记。

（三）信息系统资产责任人变动，资产管理员必须及时进行台账登记。

介质安全管理办法

第一章 总则

第一条 为加强和规范数据备份及存储介质的安全管理，确保各类数据的完整性、保密性和可用性，特制定本管理办法。

第二条 本管理办法所指的备份存储介质是指用于备份数据的存储载体，包括磁带、磁盘（U盘、移动硬盘）、光盘等。

第三条 本管理办法适用于北京东华万兴软件有限公司备份存储介质在使用、保存和传送过程中的管理。

第二章 介质的检查和维护

第四条 存储介质的管理部门，对介质应有详细的文档记录，记录信息应包括：介质的编号、存储的内容、存储数据的记录时间、转存日期、保留期限、维护人员等。

第五条 应定期检查各备份存储介质的状态和容量，并定期进行数据恢复测试。

第六条 备份存储介质在保存前，应仔细阅读介质的说明书，将介质存放在适合的地方。远离电磁干扰和灰尘，尽量通风，使用适合的容器、柜子、储存室以防止非法访问。

第三章 介质的传送

第七条 存储介质在传送途中需采用牢固、可靠的包装方式，以使其避免碰撞、受热、受潮。

第八条 备份存储介质在传送途中需根据其存储数据的敏感程度，采用有效的包装方式，以使其避免被非授权获取。

第九条 备份存储介质无论使用何种传送形式，都必须有可追溯的明确标识。

第十条 备份存储介质在单位内部传送过程中，同样需要采取以上的安全措施。

第四章 介质的备份

第十一条 对于特地为传送而制作的备份存储介质，原则上要求在传送前为该存储介质制作至少一个备份，用于存储介质在传送过程中被损坏或丢失后的快速重新传送和对丢失数据的评估。

第五章 介质的使用

第十二条 磁带和磁盘（U盘、移动硬盘）允许重复使用，光盘不允许重复使用。

第十三条 任何涉密介质和非涉密介质严禁交叉使用。

第六章 介质的数据清理

第十四条 数据清理应根据信息存储介质特性、运行成本和业务部门对数据使用、清理周期、清理内容等的要求进行实施。

第十五条 数据清理前必须对数据进行备份，在确认备份正确后方可进行清理操作。

第十六条 需要长期保存的数据要在介质有效期内进行转存，防止存储介质过期失效。

第十七条 借用数据介质时必须严格遵守数据介质借用登记、审批、交接和归还的流程，并保证备份数据完好无缺。

第十八条 外单位人员对存放数据的设备进行维修、维护时，必须由北京东华万兴软件有限公司设备管理人员现场全程监督。有关设备或介质需送交外单位维修、维护前，设备使用人员应确认设备或介质内的重要数据已经清除。

第七章 介质的销毁

第十九条 存储介质在销毁前必须登记备案。

第二十条 存储介质在销毁过程必须由两个或两个以上的专人进行监督和核对。

第二十一条 备份磁带、磁盘和光学贮存介质必须在处置前进行物理销毁，并由两个或两个以上的专人进行监督和核对。

第二十二条　销毁磁盘，需使用专用的消磁设备进行消磁后，再使用工具物理破坏磁盘，然后丢弃。

设备安全管理办法

第一章 总则

第一条 为促进北京东华万兴软件有限公司信息化设备管理规范化，提高工作效率，特制定本管理办法。

第二条 本管理办法中的信息处理设备包括计算机及打印机、刻录机、扫描仪等所有附属设备。

第三条 运维部是信息化设备的归口管理部门，负责相关设备的计划、运维、日常管理等。

第二章 组织机构与职责

第四条 运维部负责信息化设备的年度预算、选型、采购计划、验收、报废等事项的管理。

第五条 办公室负责信息化设备的采购。

第三章 设备选型和采购

第六条 运维部根据下年度项目建设计划和各单位的设备现状与需求，与各单位对接的基础上，编制出设备需求计划。

第七条 设备的选型。桌面计算机等低端设备要选用性价比高、售后服务好的品牌产品。所选设备需配备软件的必须安装正版软件。

第八条 设备采购过程中，由运维部人员负责做好硬件验机及软件测试工作，确保设备的可行性。

第四章 设备发放和领用

第九条 信息化设备管理部门为运维部，责任部门为各使用部门，责任人为所有设备使用人员。

第十条 未经运维部允许，任何部门与个人不得随意调用信息处理设备，如需调用，需由运维部审核。

第五章 设备维护及报修

第十一条 运维部负责信息处理设备的使用维护。

第十二条 设备发生故障时，使用者作简易处理后仍不能排除故障的，应立即报告运维部相关人员。

第十三条 如运维部人员经过修理后仍不能排除故障，则联系设备生产厂家或相关外部维修人员上门进行修理，运维部安排人员全程监督其修理过程。

第六章 设备报废

第十四条 报废条件。满足下列条件之一的设备，可申请报废：

（一）超出正常使用年限，且故障频发；

（二）发生不可修复的故障；

（三）故障的维修费用超过该设备的剩余使用价值；

（四）设备严重老化且其性能满足不了工作需要。

第十五条 报废手续。由使用部门提出设备报废申请，运维部进行技术鉴定，符合报废条件的，报办公室等相关部门审核，北京东华万兴软件有限公司相关领导审批同意后执行报废。

第十六条 报废处理。同意报废的设备统一交回运维部，办理实物资产核销，报废处理前运维部要对设备的报废进行台账登记。

网络安全管理办法

第一章 总则

第一条 为保证北京东华万兴软件有限公司网络系统安全、持续和稳健运行，根据国家相关法律以及相关文件要求，特制定本管理办法。

第二章 组织机构与职责

第二条 运维部是网络建设和管理的执行机构。其职责是：为网络建设和发展制订整体规划；负责组织实施已经批准施行的网络建设计划；负责网络的运行维护管理；负责网络的运行畅通、设备的运行维护、信息数据的安全保密工作；负责对网络安全事件进行风险识别、评估、监测和出具相关报告材料。

第三章 网络结构管理

第三条 各子网内的服务器、终端之间不允许跨网访问，各子网内的终端严禁混用及跨网访问，以提高网络管理平台数据的安全。

第四章 网络安全管理

第四条 针对服务器应建立相应的日志服务器，历史记录保持时间不得低于 6 个月；重要服务器日志应建立日志备份机制。

第五条 任何人不得利用各种软件技术从事用户帐户及口令的侦听、盗用活动，不得使用任何非法手段获取他人信息。

第六条 服务器发生破坏案件，或遭到黑客攻击，如该案件影响到公司信息系统的正常运行，运维部负责突发事件应急处置工作并及时向上级汇报。

第七条 网络管理员定期对配置文件进行离线备份，在配置变更前、变更后分别对网络设备的配置文件进行备份。

第五章 互联网上网管理

第八条 互联网出口必须部署防火墙等安全防护设备，接入互联网的电脑必须经过许可，并且安装防病毒、防火墙等安全防护软件。

第九条 接入互联网电脑严禁接入到办公网及通过移动介质拷贝文件至办公电脑和业务终端；

第十条 接入互联网电脑不得存储涉密文件和敏感信息。

第十一条 任何人不得在上班时间玩网络游戏、聊天、浏览非法网站和下载软件、音乐、电影等。上网应当遵守有关法律、法规的规定，加强自律，开展文明、健康的上网活动。严禁利用单位网络传播病毒，危害网络安全；制作、下载、复制、查阅、发布、传播或以其他方式使用反动、淫秽色情等有害信息。

第六章 安全加固及补丁管理

第十二条 供应商和集成商需在服务期内及时为设备和系统安装操作系统、数据库、中间件等第三方软件的安全补丁，保证系统不出现 CVE 高风险漏洞。

第十三条 供应商和集成商需在安全补丁安装前完成与设备或系统的兼容性测试。如果出现不能兼容的情况，供应商和集成商必须免费对现有程序、应用进行修改和升级，或者免费提供额外的安全措施，以保证安全性。

第十四条 供应商和集成商在系统验收前，必须对系统进行安全加固，并提交加固报告。集成商必须保证提供的系统上不存在任何 CVE 高风险漏洞。如在验收后发现 CVE 高风险漏洞，集成商和厂商应立即免费进行升级和加固。

第七章 日志审计管理

第十五条 网络管理员应定期对运行日志、网络监控记录的日常维护和报警信息进行分析和处理。

第八章 漏洞扫描管理

第十六条 每季度至少进行一次漏洞扫描，对漏洞风险持续跟踪，在经过充分的验证测试后对必要的漏洞开展修补工作。

第十七条 实施漏洞扫描或漏洞修补前，应对可能的风险进行评估和充分准备,如选择恰当时间，并做好数据备份和回退方案。

第十八条 漏洞扫描或漏洞修补后应进行验证测试，以保证网络系统的正常运行。

信息系统安全管理办法

第一章 总则

第一条 为规范北京东华万兴软件有限公司信息系统的技术管理和维护工作，确保系统安全运转和系统运行管理的及时、高效，规范系统操作，加强内部控制，最大程度地防范技术操作风险，特制定本管理办法。

第二条 本管理办法适用于运维部对信息系统的安全管理。

第二章 系统安全管理

第三条 禁用不必要的服务，尽量将系统中不用的服务、尤其是一些暂时不用的网络服务关闭，从而使系统遭受攻击的可能性降至最低。

第四条 系统遵循最小权限原则，系统只能授予应用程序和用户必要的权限，而不能授予额外的权限。

第五条 服务器需安装软件防火墙，由运维部统一部署，病毒库统一升级。

第六条 对于重要的数据进行加密。

第七条 安全性能评估，对于安全产品应选用经过国内、国外权威第三方认证的安全产品，系统管理员应随时保持警惕以预防攻击事件的发生或者将攻击的危害降至最低。

第八条 对系统漏洞情况每季度至少进行一次扫描，对漏洞风险持续跟踪，在经过充分的验证测试后对必要的漏洞开展修补工作，实施漏洞扫描或漏洞修补前，对可能的风险进行评估和充分准备,选择恰当时间，并做好数据备份和回退方案，漏洞扫描或漏洞修补后应进行验证测试，以保证系统的正常运行，扫描后记录扫描情况，填写《系统安全扫描情况记录表》（附件 1）。

第九条 持续跟踪厂商提供的系统升级更新情况，应在经过充分的测试评估后对必要的补丁进行及时更新，填写《系统与网络设备补丁分析评估表》（附件 2），在安装系统补丁前对现有的重要文件进行备份，并对备份情况和系统升级情况进行记录，填写《系统及网络设备升级记录表》（附件 3）。

第十条 至少每月对运行日志和审计数据进行分析。

第三章 系统访问控制要求

第十一条 用户或者应用程序访问系统资源时要求系统管理员通过设置必要的选项完成以下功能：

（一）提供适当的身份验证方法。

（二）识别和验证身份。

（三）记录成功和失败的系统访问（日志信息）。

（四）据情况限制用户连接时间。

第十二条 登录程序应最大限度地减少公开的信息，以避免非法用户使用。登录程序应：

（一）在登录过程未成功之前禁止显示系统或应用的标识。

（二）显示一般性注意事项。提醒用户只有合法用户才能访问计算机。

（三）登录期间禁止提供帮助消息。

（四）只有所有输入数据完成后才能验证登录信息。

（五）应限制允许登录的失败次数为 3 次。

（六）限制登录程序允许的时间上限和下限。如果超过限制，则系统必须终止登录过程。

（七）成功登录后，宜显示以下信息：

1、以前成功登录的日期和时间。

2、上次成功登录以来登录失败的详细情况。

第十三条 登录超时要求

（一）当系统超时未激活时，应能够自动锁住系统，防止非法访问，但不宜关闭应用或网络会话。

（二）超时的时间设置取决于连接系统的重要程度、终端风险暴露程度以及终端上信息的业务价值。

第四章 用户账号安全

第十四条 用户身份识别和验证

（一）信息系统所有用户都应拥有个人专用的唯一标识符（用户 ID）以便操作能够追溯到具体责任人。但是在认证和授权体系没有建立之前，特定操作系统内所有的用户必须有一个唯一的 ID，并且该 ID 名称不能让人猜测到该用户的权限级别，如管理员、主管等。

（二）对于每一个申请使用系统的用户，应要求填写《系统账号申请表》（附件 4），并在表格中包含北京东华万兴软件有限公司的密码安全政策规范，明确违反该规范的后果和责任，同时要求用户签名以产生法律效力，并在《系统账户登记表》进行登记。

（三）对于用户身份的验证，宜采用多种身份验证程序来加以证实。口令是一种很常见的身份识别和验证方法。采用加密方法和身份验证协议也可达到同样的效果。也可使用用户的内存标记或智能卡等进行身份识别和验证。也可使用基于个人唯一特点或特性的生物统计学身份验证技术来验证用户身份。将安全技术和安全机制结合起来可进行更为严格的身份验证。

第十五条 用户账号过期

（一）设置用户账号的有效有效期为一年。

（二）当某一个用户账号过期时，系统维修检查确认该用户账号所对应的员工是否还留在北京东华万兴软件有限公司，如果不是则将该账号自动删除，否则继续激活该用户账号。

（三）如果用户账号过期了但是用户无法联系到，先将其用户账号锁住，等用户回来以后按需要激活。

第十六条 Guest 账号

（一）应禁止长期保留 Guest 账号。

（二）当系统安装完成后必须视情况禁用 Guest 账号，
当用户确实需要 Guest 账号进行临时的访问时，才可将 Guest 账号激活。

（三）应确保 Guest 账号的口令安全。

第十七条 所有操作系统应禁止使用无口令的用户账号。

第十八条 除非有特殊的要求，不应有多个用户共享一个用户 ID 和口令，而应使用用户组的概念来代替。

第十九条 用户账号安全其它事项

（一）用户账号重命名，也就是对默认的账号重命名。包括 administrator、Guest 以及其它一些在安装统计时（如 ISS）自动建立的账号。

（二）建立伪管理员账号，如在系统中建立用户名为“administrator”的用户，并设定一个难以推测的口令，但是不赋予其真正的管理员权限。

第五章 文件系统安全

第二十条 文件系统的安全是指系统中所有文件的安全，包括所有操作系统管理的设备资源的安全问题，例如打印机。文件系统的安全是系统安全的最后防线，主要通过两种方式实现文件系统安全。

（一）通过文件系统权限控制文件被恶意地址访问或者在任何未经适当授权的情况下被访问。

（二）通过对文件进行适当地加密实现。

第二十一条

附件 1：系统安全扫描情况记录表

系统安全扫描情况汇总表

提交人		扫描日期	
扫描情况概述			

设备名称	多开端口	漏洞情况				主要隐患说明
		紧急风险	高风险	中风险	低风险	
加固建议						

附件 2：系统与网络设备补丁分析评估表

系统和网络设备补丁分析评估表

填表人:　　日期:

补丁描述及可能影响				
测试服务列表	补丁分析	补丁安装测试	跟踪测试情况	补丁安装计划
	□紧急 □危险 □不危险 □不适用 说明:	○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常 ○ 回退测试		
	□紧急 □危险 □不危险 □不适用 说明:	○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常 ○ 回退测试		
	□紧急 □危险 □不危险 □不适用 说明:	○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常 ○ 回退测试		
领导审批意见: 签字:				

附件 3：系统及网络设备升级记录表

系统及网络设备升级记录表

填表人: 日期:

审 批编号				补丁完整性、安全性校验		
设 备列表	数据备份	具 体 升级时间	验证检查	操作员	复核	跟踪监控 (签字并注明时间)
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			
	○ 已备份		○ 机器重启正常 ○ 漏洞已修改 ○ 业务系统正常			

附件 4：系统账号申请表

系统帐号申请表

申请人		所属北京东华万兴软件有限公司/部门	
联系电话		工号	

申请时间（年月日）	
申请人职位描述	
帐号申请目的	
帐号所属业务网名称	
变更类型	创建☐　　变更☐　　撤销☐
帐号使用期限　　到期日:　　年　　月　　日	
帐号名及需要权限描述:	
申请人主管意见及签字:	
系统主管意见及签字:	
系统维护管理员帐号权限生成完毕签字并备案: 日期: _____年_____月_____日	
备注: 被授权人的签字将被认为已阅读并知晓《帐号口令管理办法》并愿意接受帐号口令管理制度的约束。。	

备注: 表格名和编号由负责表格存档的部门负责填写。

恶意代码防范管理办法

第一章 总则

第一条 为了加强对恶意代码的预防和治理，确保北京东华万兴软件有限公司信息系统的网络和数据信息免遭计算机病毒的入侵和破坏，保障系统的安全、可靠运行，特制定本管理办法。

第二条 本管理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，并能自我复制和传播的一组计算机指令或者程序代码。计算机病毒疫情，是指某种计算机病毒爆发、流行的时间、范围、破坏特点、破坏后果等情况的报告或者预报。

第二章 恶意代码防范管理措施

第三条 各部门在从互联网上下载软件、程序、数据和购置、维修、借入计算机设备时，必须先对其进行计算机病毒检测，经确认无毒后方可使用。

第四条 运维部定期进行计算机病毒检查；并进行计算机病毒检测，确认无毒后方可使用。

第五条 运维部应采取加强访问控制机制，关闭不必要的共享服务与应用端口等措施，堵住漏洞，切断计算机病毒的感染与传播途径，防范计算机病毒入侵。

第六条 各部门必须安装正版防病毒软件，及时发现和清除计算机病毒，避免或尽可能减轻计算机病毒造成的危害或损失。

第七条 运维部计算机病毒防治人员必须定期升级计算机防病毒服务端软件，及时更新有关病毒库，并对病毒库的升级情况进行记录。

第八条 各部门在使用介质以及其他相关单位提供的信息介质前，必须先进行严格的计算机病毒检测，确认无毒后方可使用。

第九条 运维部对联入互联网的计算机和服务器，应当采取严格的计算机防病毒措施，认真审批入网资格及传输内容，限定访问使用权限，以防止计算机病毒与黑客的侵袭。

第三章 计算机病毒疫情监控、上报与分析处理

第十条 计算机使用人员严禁擅自任意修改查杀策略，删除防病毒软件。在每日病毒库升级过程中，严禁擅自中止系统升级；系统定时扫描时，严禁用户擅自中止系统扫描。

第十一条 计算机使用人员每日必须及时查看计算机病毒查杀情况。发现计算机感染了病毒，要立即停止使用疫情计算机，切断网络，隔离一切涉嫌感染病毒的存储介质和设备，同时报告运维部。运维部接到疫情报告后，应立即对疫情进行调查，查明病毒来源查明病毒来源并及时清除病毒，避免病毒进一步传播。

附件 1： 计算机病毒疫情报告表

计算机病毒疫情报告表

填表人: 日期:

病毒名称		发作时间	

影响范围			
现象及问题描述			
处理措施			
部门负责人		上报人	
上报单位意见及签章: 年　月　日			
运维部安全管理员意见			
运维部负责人意见			
备注			

信息系统变更管理办法

第一章 总则

第一条 为了对信息系统业务需求和优化请求做出快速响应，同时有效控制变更风险，尽可能减少突发事件和变更失效，特制定本管理办法。

第二条 变更管理的基本要求:

（一）变更申请必须经过评估，确保变更的合理性;

（二）变更必须经过周密的计划，确保变更实施和恢复方案的完整性和准确性;

（三）保证变更的透明性和各岗位间的有效沟通;

（四）确保变更有明确、完整的记录;

（五）变更实施后值班人员应加强观察和监控，确保变更达到预期目的。

第三条 本管理办法适用于运维部对信息系统所作的变更。

第二章 组织机构与职责

第四条 为确保北京东华万兴软件有限公司重要信息系统投产及变更工作的顺利开展，北京东华万兴软件有限公司建立重要信息系统变更领导小组,负责统筹管理北京东华万兴软件有限公司重要信息系统的建设,听取重大项目变更的风险评估报告和内容的评审、审批,并对风险控制过程进行监督。由北京东华万兴软件有限公司最高领导任组长，由运维部分管领导任副组长，并下设技术组、业务组、评审组、保障组等小组，指定运维部相关人员为组员。

（一）技术组职责为:

1、对重要信息系统变更业务影响情况进行分析和评估;

2、负责重要信息系统变更的具体技术实施工作。

（二）业务组职责为:

1、负责组织制定重要信息系统变更测试方案和业务应急处置方案;

2、组织北京东华万兴软件有限公司各业务部门在重要信息系统变更实施过程中进行业务测试和业务应急处置。

（三）评审组职责为:

1、对重要信息系统变更方案进行评审;

2、负责对整个实施过程进行监督和审计。

（四）保障组职责为:

1、提供重要信息系统变更所需人力、财力和物力等资源保障;

2、做好对受影响客户的解释和安抚工作;

3、组织对外发布公告，同时负责对相关第三方单位做好函告工作;

4、负责做好电力、通讯、公安和消防等相关外部机构的应急协调机制和应急联动机制。

第三章 变更分类

第五条 结合变更要求的迫切程度以及变更操作的规范性考虑，分为三类变更：紧急变更、一般变更和标准变更。

第六条 根据不同的变更类型共分为以下四种变更：硬件变更、系统变更、网络变更、测试变更。

第七条 紧急变更，是需要立即实施的变更，否则可能对大量用户、关键系统的服务质量或可用性产生重大影响。

第八条 是否为紧急变更由运维部负责人或指定的专人共同确定；必要时，运维部负责人可以召集相关人员紧急商议。

第九条 标准变更，适用于以下两种情况的任一种:

(一)　属于日常维护性质的低风险操作。
(二)　已经执行过的且确认无影响的变更操作，并且在操
作手册中具有经过验证的完整操作步骤（不符合定义或者不符合条件的操作，不能按照标准变更执行）。
第十条　标准变更的管理流程可参考一般变更管理流程，但变更计划评审部分可以省略。
第十一条　一般变更：除紧急变更、标准变更以外的变更，均属于一般变更。
第四章 变更通知
第十二条　如变更对现有的业务系统和业务操作产生影响，在变更执行前 5 日应通知有关部门。以便于各业务部门做好业务调整，避免变更冲突，减少对业务的影响。
第五章 风险评估
第十三条　运维部应从技术层面对重要信息系统变更风险进行识别、分析和评估，具体包括系统功能缺陷、客户信息泄露、业务中断、交易缓慢或其他因素可能造成的风险，并形成初步风险评估报告；网络与数据安全领导小组应对运维部重要信息系统变更的初步风险评估报告进行确认，并组织相关管理部门对重要信息系统变更实施过程可能产生的操作风险、法律风险和声誉风险进行评估，并形成最终的风险评估报告。
第十四条　重要信息系统变更风险评估流程
（一）运维部在重要信息系统变更实施之前，需进行风险识别和初步分析并出具技术层面的风险分析评估报告；
（二）运维部织相关管理部门对重要信息系统变更风险进行整体风险分析和评估，并出具风险分析和评估结果和评判重要信息系统变更是否实际实施；
（三）如有必要，运维部可委托外部专家或具备相应资质的外部专业机构进行重要信息系统变更的风险评估工作
第十五条　重要信息系统变更风险评估报告
（一）运维部从技术层面对重要信息系统变更风险进行分析和评估，并出具风险评估报告；
（二）网络与数据安全领导小组组织相关管理部门对重要信息系统变更实施过程可能产生的操作风险、法律风险和声誉风险进行评估，并形成最终的风险评估报告。
（三）运维部负责向分管领导提交重大项目的风险评估报告，并取得审核结果。
第十六条　针对风险评估中发现的薄弱环节应制定整改方案,明确整改时间。不具备整改条件的应采取风险缓释措施。
第六章 变更控制
第十七条　一般变更管理流程划分为变更描述、变更评估、变更测试、变更实施、变更跟踪五个主要阶段，风险较大的变更必须制定详细应急和回退方案。
第十八条　由运维部统一组织协调信息系统变更工作,每年年初制定并发布本年度重要信息系统变更规则，在变更前应制定实施计划和实施方案,确定实施策略和步骤,明确岗位职责,确保关键岗位职责分离。
第十九条　运维部负责建立重要信息系统变更内容评审和审批、授权机制。
第二十条　网络与数据安全领导小组对信息系统变更过程中所提交的有关文档资料进行审阅，了解是否具有相应的控制措施，指出存在的风险并提出评价和建议。
第二十一条　为保障信息系统稳定运行，运维部应按照对业务影响最小原则,采取与风险程度相适应的重要信息系统变更策略。
第二十二条　运维部应合理避开业务高峰期和敏感时段安排重要信息系统上线。
第二十三条　运维部应建立充分、完整的测试体系,测试结果应经过运维部和相关业务部门确认,并形成测试和验收报告,确保系统上线后的正常稳定运行以及系统功能与业务目标的一致性。

第二十四条 运维部应建立与生产环境相隔离的测试环境,测试环境应模拟生产环境的真实情况。

第二十五条 运维部应建立完善的版本管理制度,制定严格的审批、控制和操作流程,保存完整的日志记录。拟变更的重要信息系统应保证版本完整、准确、有效,遵从系统开发和运行管理制度规范。

第二十六条 运维部应加强重要信息系统变更过程中的数据管理与质量控制;测试环境中使用的敏感生产数据应进行脱敏、变形处理;需要历史数据迁移的,应制定详细的数据迁移计划,并提前进行数据迁移测试和数据有效性、兼容性验证,确保迁移后数据的完整性、安全性和可用性。

第二十七条 运维部和相关业务管理部门应制定重要信息系统变更应急预案,并根据变更回退时间跨度要求制定相应的系统回退和应急处置计划和流程,必要时应实施演练,并在重要信息系统变更实施后及时更新各项相关应急预案。

第二十八条 信息系统变更过程中,运维部应严格执行上线实施方案,加强监督与复核,避免操作失误和非法操作。

第二十九条 运维部应加强信息系统变更过程的风险监控和预警,各相关部门协同做好应急准备。

第三十条 运维部应制定并落实系统运行管理规程、制度,业务部门应制定和完善相关业务管理办法、操作规程,明确业务及运行管理职责,组织必要的培训,确保变更实施后业务顺利开展。

第三十一条 运维部应对重要信息系统变更过程产生的各类文档资料进行管理,确保文档资料的完整性、及时性和有效性,并满足独立审计要求。

第三十二条 一般信息系统变更由运维部统筹管理,应建立事前审批、事中控制、事后评估的管理流程和实施细则;重要信息系统变更由重要信息系统变更领导小组统筹管理,相关管理流程详见附件一。

第三十三条 为减少变更对信息系统稳定运行的负面影响,运维部应按照对业务影响最小原则,规定合理的变更时间窗口,严格控制变更次数。对于重要信息系统的变更,原则上每个重要信息系统每年不超过一次,全年累计重要信息系统的变更对业务持续性影响不超过四次。

第三十四条 每次变更前,应制定终止变更并从失败变更中恢复的流程,确保对系统的最小化影响。

第七章 变更报告

第三十五条 重要信息系统变更前至少 30 个工作日,由运维部向网络与数据安全领导小组提出申请,并由网络与数据安全领导小组组织进行评审,重要信息系统变更前至少 10 个工作日,须提交的评审材料包括但不限于:

(一)总体说明:投产及变更目的、内容、计划起止时间、业务影响范围、联系人及联系方式等。

(二)重要信息系统基本信息,包括:系统名称、业务功能、操作系统、数据库、中间件情况,应用架构、技术架构、数据架构,生产主机备份方案、数据备份方案,运行管理等相关职能部门,是否纳入灾难恢复计划等。

(三)重要信息系统数据安全策略和措施,包括对账户、交易和客户敏感信息的安全控制措施等。

(四)涉及基础设施的,需提供基础设施基本信息,包括机房和网络方案。机房方案包括等级标准、地址、供配电系统、消防、空调、弱电系统、机房加固、机房空间规划,以及机房验收报告等;网络方案包括网络架构分区、核心网络备份情况,以及区域间、外联网、互联网边界安全措施与网络监控措施等。

(五)投产及变更方案,包括投产及变更的组织结构与实施计划、操作步骤等。

(六)风险评估报告,应包括业务影响分析,技术风险分析与评估,控制措施的有效性,以及剩余风险等。
(七)应急预案,包括应急处置组织结构,应急场景,应急处置流程、步骤,应急联系方式与报告路线等,实施演练提交演练总结报告。
第三十六条 运维部应在重要信息系统投产及变更实施后 20 天内完成重要信息系统变更事后总结报告材料，内容包括但不限于：变更方案执行情况、效果，问题发现和处理情况，后续改进措施等，如变更失败，应详细说明失败原因，并进行报告。

第三十七条
附件 1：变更记录表
系统变更记录表

<table>
<tr><td>变更提交人</td><td colspan="2"></td><td>提交日期</td><td></td></tr>
<tr><td>变更类型</td><td colspan="4">☐硬件变更 ☐系统变更 ☐网络变更 ☐测试变更</td></tr>
<tr><td>补丁版本</td><td colspan="4"></td></tr>
<tr><td>变更名称及目的</td><td colspan="4"></td></tr>
<tr><td>变更操作流程</td><td colspan="4"></td></tr>
<tr><td>检验办法</td><td colspan="4"></td></tr>
<tr><td>应急和回退办法</td><td colspan="4"></td></tr>
<tr><td rowspan="5">变更评审流程及结果</td><td colspan="4">变更类别：☐紧急变更 ☐标准变更 ☐一般变更</td></tr>
<tr><td colspan="4">变更风险及通知范围：</td></tr>
<tr><td colspan="2">变更流程：☐合理 ☐不合理</td><td colspan="2">应急办法：☐合理 ☐不合理</td></tr>
<tr><td colspan="2">变更检验：☐合理 ☐不合理</td><td colspan="2">确定实施变更日期：</td></tr>
<tr><td colspan="4">变更评审主要参与人签字：</td></tr>
<tr><td>变更准备</td><td colspan="2">变更通知 ☐ 完成</td><td colspan="2">备份确认 ☐ 完成</td></tr>
<tr><td>变更操作记录</td><td colspan="4"></td></tr>
<tr><td>变更检验记录及结果</td><td colspan="4"></td></tr>
<tr><td>应急和回退情况</td><td colspan="4"></td></tr>
<tr><td>变更人、复核人签字</td><td colspan="4"></td></tr>
</table>

变更跟踪记录	
配置、操作文档更新	

数据备份与恢复管理办法

第一章 总则

第一条 为加强北京东华万兴软件有限公司信息系统数据的备份与管理，避免信息系统数据的丢失，确保生产、经营、管理等应用系统的安全稳定运行和历史数据的有效保存，特制定本管理办法。

第二条 数据备份与管理应遵循“统一领导、统一规划、统一标准、统一建设、分级管理”的原则。

第三条 本管理办法适用于北京东华万兴软件有限公司所有数据备份和恢复操作。

第二章 组织机构与职责

第四条 运维部负责北京东华万兴软件有限公司信息系统的数据备份、运行维护与管理。

第五条 运维部是数据备份的归口管理部门，负责北京东华万兴软件有限公司信息系统的数据备份、运行维护与管理工作。

第六条 运维部设立数据备份岗位，并实行主、副岗制度，具体负责北京东华万兴软件有限公司数据备份工作的日常管理，包括检查、监督、考核和统计等工作。

第七条 数据备份技术及相关人员上岗前要进行培训，具备必要的技能。设备或技术更新，或者备份策略和恢复预案发生变化后，要及时进行培训。

第三章 数据备份

第八条 数据备份应根据系统情况和备份内容，采用不同的备份方式:

（一）完全备份：对备份的内容进行整体备份。

（二）增量备份：仅备份相对于上一次备份后新增加和
修改过的数据。

（三）差分备份: 仅备份相对于上一次完全备份之后新
增加和修改过的数据。

（四）按需备份：仅备份应用系统需要的部分数据。

具体所采取的备份方式，应能确保真实重现被备份系统的运行环境和数据。

第九条 在规划设计以及新建信息系统时应充分考虑系统的备份需求，填写《数据备份需求登记表》（附件 1,）在系统投运前完成备份策略和恢复预案的制定并在系统投运后同时开始执行；已投运的信息系统备份需求发生变化时，要及时调整数据备份策略和恢复预案。备份策略和恢复预案的制定与调整需报主管领导批准。

第十条 运维部在对计算机和设备进行软件安装、系统升级改造或更改配置时，应进行系统、数据和设备参数的完全备份；系统更新后，应实现数据的迁移或转换，确保历史数据的完整性，并对原系统及其数据进行完全备份。

第十一条 数据备份系统的建设应统一纳入信息化发展规划并按分层分级组织实施。

第十二条 数据备份系统及介质的选型要满足各系统的备份策略及保存要求，包括安全可靠性、性能和服务质量、冗余等，确保通过数据备份能及时恢复各种故障情况下造成的数据丢失。

第十三条 运维部应制定相关运行和维护管理制度，加强对数据备份系统的运行和维护管理，确保数据备份系统可靠运行。

第十四条 应对数据备份操作进行记录，填写《数据备份记录表》（附件 2），操作可能影响到信息系统正常运行的，要报主管领导批准。

第十五条 数据备份工作人员要认真做好数据备份的文档工作，完整地记录备份系统的配置和备份数据源的系统配置；做好备份工作的运行日志和维护日志；建立备份文件档案及档案

库，详细记录备份数据的信息。要做好数据备份的文卷管理，所有备份应有明确标识，包括卷名、运行环境、备份人。卷名按统一的规则来命名，即由“系统名称－（数据类型+备份方式+存储介质）－备份时间－序号”组成。

系统名称	数据类型	备份方式	存储介质	备份时间	序号
ABC	0 操作系统	0 完全备份		YYYY.MM.DD	XXX
	1 应用软件	1 增量备份	1 光盘		
	2 应用数据	2 差分备份	2 硬盘		
	3 其他	3 按需备份	3 其他		
		4 其他			

如某备份资料文卷管理中记录的信息为：
卷名：OA 系统－221－20240628－001（表示所备份的资料是：OA 系统的应用数据，以差分备份方式备份在光盘上，备份时间为 2024 年 6 月 28 日，序号 001）。
运行环境：操作系统名称、版本号，数据库名称、版本号等。
其所在处室及备份人：（部署处室名称和备份人姓名）。

第十六条 重要信息系统数据备份应保留两份拷贝，一份在现使用场所保存，以保证数据的正常快速恢复和数据查询，另一份异地保存，避免发生灾难事件后数据无法恢复。

第十七条 保留周期在一年以内的数据完全备份拷贝由运维部自行保管，保留周期超过一年的数据完全备份拷贝，应按照有关规定移交至北京东华万兴软件有限公司档案管理部门统一保管。

第十八条 加强对存储介质的管理，建立介质的管理制度和废弃介质的处理制度，并符合有关保密管理规定。存储介质应存放在适于保存的安全环境（如防盗、防潮、防鼠害、磁性介质远离磁场、辐射性物质等），并有严格的存取控制。运维部对备份了数据的存储介质要进行定期检查，确认所备份数据的完整性、正确性和有效性。

第四章 数据恢复

第十九条 当出现故障而导致系统或数据损坏并无法修复时，运维部应根据恢复预案和实际情况编制详细的恢复实施方案，报信息系统业务主管部门审查，并经主管领导批准后，方可对系统进行恢复操作。恢复操作不得影响对故障原因的追查和故障的处理。

第二十条 恢复操作前，运维部须通知所有相关信息系统的管理员到场，并经其同意后，方可进行操作。操作时，应先备份现场系统、数据和运行环境，再按照恢复方案的要求进行恢复操作。

第二十一条 系统恢复后，应由相关信息系统的管理员进行测试，同时再进行一次备份，恢复的情况应报告运维部及相关信息系统的业务主管部门。

第二十二条 对于重要业务系统，每年应至少进行一次备份数据的恢复演练。

第五章 备份系统巡检

第二十三条 巡检员每周一对备份系统进行巡检。

第二十四条 巡检员必须对巡检结果进行记录，特别要详细记录出现的问题和故障，并通

知相关人员进行处理。

第二十五条　巡检内容主要是检查备份日志，查看备份介质池，是否存在备份异常等情况。备份数据有效性检测：

（一）每年按 2%的比例对离线备份介质抽查检测，发现

备份介质有问题时，继续按 2%的比例抽查检测。检测方法：

检验备份介质是否可正常读取，包括检查 readme.txt 是否可正常打开，压缩文件能否正常解压，并填写《离线备份介质抽检登记表》

（二）备份数据还原至测试系统中进行恢复验证，并填写《业务数据导入测试环境操作记录表》。

（三）根据介质使用期限及时迁移数据，并填写《离线备份介质迁移登记表》。

第六章 统计和考核

第二十六条　运维部应加强对数据备份工作的管理和考核，建立相应的管理和考核制度。如因未严格遵守本规定造成备份系统等发生故障，或数据丢失、泄密，或导致信息系统无法正常运行的，应核实造成的损失，查明事故原因和责任人，按照有关管理制度和考核办法进行处理。

第二十七条　运维部将北京东华万兴软件有限公司每月的数据备份工作情况写入信息化工作简报。

附件 1：数据备份需求登记表

数据备份需求登记表

申请单位		申请人	
备份介质类型		介质编号	
备份介质 名称/型号		备份介质 容量大小	
备份数据日期		备份数据时间	
备份周期		备份有效期限	
备份内容			
备份数据大小			

涉及系统	
备份操作	
相关部门意见	
备注	

附件 2：数据备份记录表

数据备份记录表

系统名称:		执行人:	
备份日期:			
备份内容			

执行情况	备份正常（ ） 备份不正常（ ）
备注	

数据安全事件报告管理办法

第一章 总则

第一条 为提高处置数据安全事件能力，加强网络与数据安全保障工作，最大限度地减轻网络与数据安全突发事件的危害，特制定本管理办法。

第二条 本管理办法适用于北京东华万兴软件有限公司各部门。

第二章 安全事件分类与分级

第三条 事件分类：根据网络与数据安全突发事件的发生过程、性质和特征，网络与数据安全突发事件可划分为网络安全突发事件和数据安全突发事件。网络安全突发事件是指自然灾害，安全事件灾难和人为破坏引起的网络与信息系统的损坏；数据安全突发事件是指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。

2.安全事件灾难是指电力中断、网络损坏或者是软件、硬件设备故障等。

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。

第四条 计算机安全事件具体包括：

1.信息系统软硬件故障；

2.网络通信系统故障；

3.供电系统故障；

4.系统感染计算机病毒；

5.数据处理中心遭水灾、火灾、雷击；

6.网络遭遇入侵或攻击；

7.信息系统敏感数据泄露；

8.信息系统数据失窃；

9.数据处理设备失窃。

第五条 事件分级：根据网络与数据安全突发公共事件的可控性、严重程度和影响范围，将网络与数据安全突发公共事件分为四级：Ⅰ级(特别重大)、Ⅱ级(重大)、Ⅲ级(较大)、Ⅳ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。

（一）Ⅰ级(特别重大)：网络与信息系统发生全局性大规模瘫痪，事态发展超出自己的控制能力，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件。

（二）Ⅱ级(重大)：网络与信息系统造成全局性瘫痪，对国家安全、社会秩序、经济建设和公共利益造成严重损害需要跨部门协同处置的突发公共事件。

（三）Ⅲ级(较大)：某一部分的网络与信息系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但不需要跨部门、跨地区协同处置的突发公共事件。

（四）Ⅳ级(一般)：网络与信息系统受到一定程度的损坏，对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益的突发公共事件。

第三章 安全事件处理

第六条 安全事件处理流程包括安全事件获取、安全事件判定、安全事件报告、安全事件调查和分析、安全事件解决和服务恢复、安全事件记录和关闭六个过程。处理过程应做到判定过程迅速，得出结论准确，报告上级及时。

第七条 安全事件获取：第一发现人是安全事件获取的责任人，安全事件发生后，第一发现人应提供安全事件发生时间、发现时间、安全事件现象等信息，向运维部值班人员汇报情况。

第八条 安全事件判定：运维部值班人员需尽快根据安全事件现象评估安全事件对业务正常运行的影响，并立即通知运维部负责人，由运维部负责人判断安全事件的级别。安全事件级

别难于界定的，按高级别安全事件判定。

第九条 安全事件报告：在事发 24 小时内，向相关负责人提交数据安全事故报告，计算机安全事件必须及时上报，报告内容应当要素齐全，客观准确。

数据安全事故报告包括以下内容：

1.计算机安全事件发生的时间、地点、单位、单位负责人和联系方式；

2.计算机安全事件的类别、涉及软硬件系统的情况和事件发生的过程；

3.计算机安全事件造成的后果和影响范围；

4.计算机安全事件发生的原因；

5.责任人或涉案人员；

6.计算机安全事件发生后采取的应急措施。

第十条 对造成系统中断和造成信息泄密的重大安全事件，第一时间应向衡阳市教育局报告，让其提供技术支持并追踪溯源。

第十一条 安全事件调查和分析：由运维部负责人召集各专业岗位人员进行安全事件调查和故障定位，制定安全事件处理方案。

第十二条 安全事件解决和恢复服务：若属于存在应急方案的安全事件，严格按照应急方案执行；没有存在应急方案的安全事件由运维部负责人召集各专业岗位人员制定临时处理方案。

第十三条 安全事件记录和关闭：所有安全事件事后必须详细记录，应包括安全事件时间、现象、处理流程、处理结果、原因、改进措施等。

第四章 事后培训和教育

第十四条 安全事件处理完后应把事件处理情况向全单位进行通报，分析事件发生的原因，总结经验教训，防止安全事件再次发生。

数据安全突发事件应急预案

第一章 总则

第一条 目的：为提高北京东华万兴软件有限公司信息系统处理突发信息网络事件的能力，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减少网络与数据安全突发公共事件的危害，保护公众利益，特制定本预案。

第二条 适用范围：本预案适用于北京东华万兴软件有限公司信息系统发生和可能发生的网络与数据安全突发事件。

第三条 工作原则：

⑴ 预防为主。立足安全防护，加强预警，重点保护基础信息网络和重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，采取多种措施，共同构筑网络与数据安全保障体系。

⑵ 快速反应。在网络与数据安全突发公共事件发生时，按照快速反应机制，及时获取充分而准确的信息，迅速处置，最大程度地减少危害和影响。

⑶ 以人为本。把保障公共利益以及公民、法人和其他组织的合法权益的安全作为首要任务，及时采取措施，最大限度地避免公民财产遭受损失。

⑷ 分级负责。按照“谁主管谁负责、谁使用谁负责”以及“条块结合”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强协调与配合，形成合力，共同履行应急处置工作的管理职责。

第四条 编制依据：根据《中华人民共和国突发事件应对法》、《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》。

第二章 组织机构及职责

第五条 组织机构：

成立北京东华万兴软件有限公司突发信息网络事件应急领导小组（以下简称信息网络事件应急领导小组）。

组　长：公司领导

副组长：运维部主管领导

成　员：运维部全体工作人员

第六条 信息网络事件应急领导小组职责

⑴ 负责编制、修订所辖范围内突发信息网络事件应急预案。

⑵ 通过本系统局域网络中心及国内外安全网络信息组织交流等手段获取安全预警信息，周期性或即时性地向局域网和用户网络管理部门发布；对异常流量来源进行监控，并妥善处理各种异常情况。

⑶ 及时组织专业技术人员对所辖范围内突发信息网络事件进行应急处置；负责调查和处置突发信息网络事件，及时上报并按照相关规定作好善后工作。

⑷ 负责组建信息网络安全应急救援队伍并组织培训和演练。

第三章 预防及预警机制

第七条 突发信息网络事件安全预防措施包括分析安全风险，准备应急处置措施，建立网络和信息系统的监测体系，控制有害信息的传播，预先制定数据安全重大事件的通报机制。

第八条 突发信息网络事件分类：关键设备或系统的故障；自然灾害（水、火、电等）造成的物理破坏；人为失误造成的安全事件；电脑病毒等恶意代码危害；人为的恶意攻击等。

第九条 应急准备：运维部和各单位信息系统管理员明确职责和管理范围，根据实际情况，

安排应急值班，确保到岗到人，联络畅通，处理及时准确。

第十条 具体措施:

⑴ 建立安全、可靠、稳定运行的机房环境，防火、防盗、防雷电、防水、防静电、防尘；建立备份电源系统；加强所有人员防火、防盗等基本技能培训。

⑵ 实行实时监视和监测，采用认证方式避免非法接入和虚假路由信息。

⑶ 重要系统采用可靠、稳定硬件，落实数据备份机制，遵守安全操作规范；安装有效的防病毒软件，及时更新升级扫描引擎；加强对局域网内所有用户和信息系统管理员的安全技术培训。

⑷ 安装反入侵检测系统，监测恶意攻击、病毒等非法侵入技术的发展，控制有害信息经过网络的传播，建立网关控制、内容过滤等控制手段。

第四章 有关应急预案

第十一条 通信网络故障应急预案

⑴ 发生通信线路中断、路由故障、流量异常、域名系统故障后，操作员应及时通知北京东华万兴软件有限公司信息系统管理员，经初步判断后及时上报信息网络事件应急领导小组和运维部。

⑵ 运维部接报告后，应及时查清通信网络故障位置，隔离故障区域，并将事态及时报告信息网络事件应急领导小组，通知相关通信网络运营商查清原因；同时及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

⑶ 事态或后果严重的，信息网络事件应急领导小组应及时报告应急领导小组。必要时，及时上报应急指挥部办公室和相关业务部门。

⑷ 应急处置结束后，运维部和事发单位应将故障分析报告，在调查结束后一日内书面报告信息网络事件应急领导小组。

第十二条 不良信息和网络病毒事件应急预案

⑴ 发现不良信息或网络病毒时，信息系统管理员应立即断开网线，终止不良信息或网络病毒传播，并报告信息网络事件应急领导小组和运维部。

⑵ 运维部应根据信息网络事件应急领导小组指令，采取隔离网络等措施，及时杀毒或清除不良信息，并追查不良信息来源。

⑶ 事态或后果严重的，信息网络事件应急领导小组应及时报告应急领导小组。如有必要，及时上报应急指挥部办公室和相关业务部门。

⑷处置结束后，运维部和事发单位应将事发经过、造成影响、处置结果在调查工作结束后一日内书面报告信息网络事件应急领导小组。

第十三条 服务器软件系统故障应急预案

⑴ 发生服务器软件系统故障后，运维部负责人应立即组织启动备份服务器系统，由备份服务器接管业务应用，并及时报告信息网络事件应急领导小组；同时安排相关责任人将故障服务器脱离网络，保存系统状态不变，取出系统镜像备份磁盘，保持原始数据。

⑵ 运维部应根据信息网络事件应急领导小组指令，在确认安全的情况下，重新启动故障服务器系统；重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商和上级单位，请求技术支援，作好技术处理。

⑶ 事态或后果严重的，及时报告应急领导小组。如有必要，及时上报应急指挥部办公室和相关业务部门。

⑷ 处置结束后，运维部应将事发经过、处置结果等在调查工作结束后一日内报告信息网络事件应急领导小组。

第十四条 黑客攻击事件应急预案

⑴ 当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删

除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告信息网络事件应急领导小组。
⑵ 接报告后，信息网络事件应急领导小组应立即指令运维部核实情况，关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。
⑶ 运维部应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应上报应急领导小组，并请求支援。必要时，及时上报应急指挥部办公室和相关业务部门。
⑷ 处置结束后，运维部应将事发经过、处置结果等在调查工作结束后一日内报告信息网络事件应急领导小组。
第十五条 核心设备硬件故障应急预案
⑴ 发生核心设备硬件故障后，运维部应及时报告信息网络事件应急领导小组，并组织查找、确定故障设备及故障原因，进行先期处置。
⑵ 若故障设备在短时间内无法修复，运维部应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。
⑶ 运维部应在故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商， 认真填写设备故障报告单备查。
⑷ 事态或后果严重的，及时报告应急领导小组。如有必要，及时上报应急指挥部办公室和相关业务部门。
第十六条 业务数据损坏应急预案
⑴ 发生业务数据损坏时，运维部应及时报告信息网络事件应急领导小组，检查、备份业务系统当前数据。
⑵ 运维部负责调用备份服务器备份数据，若备份数据损坏，则调用磁带机中历史备份数据，若磁带机数据仍不可用，则调用异地备份数据。
⑶ 业务数据损坏事件超过 2 小时后，运维部应及时报告信息网络事件应急领导小组，及时通知业务部门以手工方式开展业务。
⑷ 运维部应待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统业务员补录数据；重新备份数据，并写出故障分析报告，在调查工作结束后一日内报告信息网络事件应急领导小组。
第十七条 雷击事故应急预案
⑴ 遇雷暴天气或接上级部门雷暴气象预警，运维部应及时报告信息网络事件应急领导小组，经请示同意后关闭所有服务器，切断电源，暂停内部计算机网络工作。
⑵ 雷暴天气结束后，运维部报经信息网络事件应急领导小组同意，及时开通服务器，恢复内部计算机网络工作，并通知各部及时恢复设备正常工作，对设备和数据进行检查。出现故障的，事发单位应将故障情况及时报告运维部。
⑶因雷击造成损失的，运维部应汇同财务部门等相关部门进行核实、报损，并在调查工作结束后一日内书面报告信息网络事件应急领导小组。必要时，报告应急领导小组。
第五章 应急处置
第十八条 发生信息网络突发事件后，相关人员应在 5 分钟内向信息网络事件应急领导小组报告，信息网络事件应急领导小组组织人员采取有效措施开展先期处置，恢复信息网络正常状态。
第十九条 发生重大事故（事件），无法迅速消除或恢复系统，影响较大时实施紧急关闭，并立即向应急领导小组报告。如有必要，及时上报应急指挥部办公室和相关业务部门。
第六章 善后处置
第二十条 应急处置工作结束后，信息网络事件应急领导小组组织有关人员和技术专家组成

事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，根据应急处置中暴露出的管理、协调和技术问题，改进和完善预案，实施针对性演练，总结经验教训，整改存在隐患，组织恢复正常工作秩序。

第七章 应急保障

第二十一条 通信保障

运维部负责收集、建立突发信息网络事件应急处置工作小组内部及其他相关部门的应急联络信息。信息网络事件应急领导小组应在重要部位醒目位置公布报警电话，信息网络事件应急领导小组全体人员保证全天 24 小时通讯畅通。

第二十二条 数据保障

重要信息系统均建立备份系统，保证重要数据在受到破坏后可紧急恢复。

第二十三条 队伍保障

建立符合要求的网络与数据安全保障技术支持力量，对网络接入单位的网络与数据安全保障工作人员提供技术支持和培训服务。

第八章 监督管理

第二十四条 宣传教育和培训

将突发信息网络事件的应急管理、工作流程等列为培训内容，增强应急处置能力。加强对突发信息网络事件的技术准备培训，提高技术人员的防范意识及技能。信息网络事件应急领导小组每年至少开展一次信息网络安全教育，提高数据安全防范意识和能力。

第二十五条 预案演练

信息网络事件应急领导小组每年至少安排一次演练，建立应急预案定期演练制度。通过演练，发现和解决应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

第二十六条 责任与奖惩

信息网络事件应急领导小组不定期组织对各项制度、计划、方案、人员及物资等进行检查，对在突发信息网络事件应急处置中做出突出贡献的集体和个人，提出表彰奖励建议；对玩忽职守，造成不良影响或严重后果的，依法依规提出处理意见，追究其责任。

第九章 附则

第二十七条 预案更新

每年须对应急预案进行评审，结合信息网络快速发展和经济社会发展状况，配合相关法律法规的制定、修改和完善，适时修订本预案。

第二十八条 预案实施

本预案由北京东华万兴软件有限公司批准后实施。