**北京汇聚融达网络科技有限公司**

**——信息安全工作管理制度**

**文件编码：HJRD-1-02**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 信息安全工作管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-1-02 | | **牵头部门** | 技术部 | |
| **分发范围** | 制度管控员工 | | | | |
| **版本修订** | | | | | |
| **生效日期** | **版本号** | **版本说明** | **制作** | **复审** | **批准** |
| 上半年工作日 | V1.0 | 第一版 | 刘陵镇 | CTO | CEO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：文档基本信息记录本文档提交时的当前有效的基本控制信息，当前版本文档注有效期将在新版本文档生效时自动结束。文档版本小于1.0 时，表示该版本文档为草案，仅可作为参照资料之目的。

# 目的

北京汇聚融达网络科技有限责任公司（以下简称：公司）信息安全方针的具体要求，作为信息安全工作和具体标准、程序、指引和制度等实施的指导方针和最重要的依据。

指导信息安全工作符合国际、国内的有关安全标准及我国相关法律和法规。

形成一个安全机制，有效地保障各项安全责任的落实；并且根据实际情况的变化，能够及时地、适宜地保障信息安全管理体系的维护和完善。

保护信息和信息系统的安全，使其保密性、完整性和可用性得到有效保障。

# 适用范围

公司所有业务活动、信息和信息系统，公司所有部门和全体员工以及第三方人员。

# 职责

信息安全领导小组负责对本程序的执行和管理。

# 安全策略内容

## 安全组织内容

1. 信息安全领导小组负责协调信息安全建设所需的人员、资金、设备、场地等资源，制定人员安全技能和安全意识培训的安全需求，对公司的信息安全建设工作提供方向性和原则性的指导、建议。
2. 信息安全领导小组的成员来自公司不同的部门，这些成员要保证安全活动的实施与安全策略一致，核准信息安全相关的方法和过程（如风险评估、信息分类等），评估安全控制措施实施的充分性和协调性，促进信息安全教育、培训和人员安全意识的提高，有效、合理协调公司信息安全建设的工作。
3. 信息安全领导小组的成员要明确并履行各自的安全职责，安全职责包括资产保护的责任、执行特定安全过程的责任以及授权级别，保证公司的安全责任能有效落实。
4. 保持与外部安全组织的适当联系（如国家计算机网络应急技术处理协调中心-CNCERT/CC、国家计算机病毒应急处理中心、公安机关网安部门、集团公司信息安全应急处理领导小组、第三方信息安全咨询公司等），了解信息安全的最新知识和政策，获取关于新技术、产品、威胁或脆弱性的信息，尽早接受到关于攻击和脆弱性的警告、建议和补丁，保证公司的安全问题能得到专家的有效指导和建议。
5. 定期（或出现重大安全变化时）对公司的信息安全方法和实施进行评审，确保管理信息安全方法的持续适宜性、充分性和有效性。评审的对象包括控制目标、控制措施、安全策略、程序文件和作业指导书。评审由信息安全领导小组来启动，评审的结果要记录成文件，并报告给信息安全工作小组。如果评审识别出信息安全方法和实施不符合当前的安全要求，信息安全领导小组必须及时考虑纠正措施。
6. 控制任何外部机构对公司信息处理设施的访问、对信息资产的处理以及与信息系统进行了通信，保证公司被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全，确保在引入外部产品和服务的同时，不降低信息处理设施和信息资产的安全。
7. 识别外部机构访问公司信息和信息处理设施的风险，包括被访问的信息处理设施、访问类型、被访问信息的重要性、不被访问信息需要的控制措施、外部访问的人员等，并在允许访问前实施适当的控制措施，确保外部机构的访问不影响信息和信息处理设施的安全。
8. 外部机构的人员在访问公司资产前必须明确相关的安全要求，包括对资产的保护要求、访问控制策略、信息安全事故和安全违规的报告、承担的责任和业务。通过签订协议来落实这些安全要求，保证外部机构人员不会对访问的资产造成破坏。
9. 在现有信息系统中新增产品或服务，以及对现有信息系统进行变更时，必须在相关的协议中，明确体现所有涉及的安全要求，主要包括资产保护要求、安全职责要求、访问控制要求以及变更管理要求等方面，并保证严格执行协议中规定的各项条款。

## 资产管理策略

1. 所有的资产要指定责任人，并对责任人赋予相应的职责，确保所有资产都可以核查。
2. 根据资产的重要性、业务价值、依赖程度，对所有资产进行分类、分级，编制资产的清单。对资产清单妥善保管，并在资产变更时及时更新清单，确保可以对资产进行有效的保护。
3. 指定负责所有资产的部门或责任人，责任部门或责任人对资产的安全承担责任，保证资产能得到有效保护。
4. 制定资产使用的规则，形成文件并加以实施。公司所有员工和外单位人员应遵守这些规则，对资产的使用负责，以保证对资产的合理使用。
5. 根据对公司的价值、法律要求、敏感性和关键性对公司的信息进行分类、分级保护，为每一个类别和级别指定相应的处理措施，并在处理信息时指明保护的需求、优先级和期望程度，确保信息受到适当级别的保护。

## 人力资源安全策略

1. 应根据员工职位说明书严格履行各自的安全角色和职责，主要包括保护资产免受未授权的访问、泄漏、修改、销毁或干扰，执行特定的安全过程或活动，报告安全事件或其他风险。安全角色和职责必须清晰的传达给所有员工，确保他们能清楚各自的安全责任。
2. 外单位人员在访问公司信息处理设施前必须签署保密协议，保密协议内容包括外单位人员访问信息资产的权利、承担的安全责任、违反职责要承担的后果等。要保证外单位人员了解保密协议的条款和内容，并同意协议规定的权利和责任。
3. 信息安全领导小组应该承担管理职责，保证所有员工和外单位人员能按照安全方针、策略和程序进行日常工作。管理职责包括使所有员工和外单位人员清晰了解各自的安全角色和安全职责、提高他们的安全意识和安全技能等。
4. 定期对所有员工和外单位人员进行安全培训，培训内容包括公司的安全方针、策略、程序、信息处理设施正确使用方法、安全意识等。根据人员的安全角色和职责制定不同的培训计划，保证所有员工和外单位人员能认识到信息安全问题和信息安全事件，并能安装各自的安全角色履行安全职责。
5. 制定正式的纪律处理过程，来严肃处理安全违规的员工，并威慑其他员工，防止他们违反安全策略、程序和其他安全违规。纪律处理要正确、公平，要根据违规的性质、重要性和对业务的影响等因素区别对待。
6. 当员工离职或调离其他岗位、外单位人员合同期满时，立即终止原来的安全角色和安全职责，并通知公司所有员工，使所有员工能及时清楚人员的变化。
7. 当员工离职或调离其他岗位、外单位人员合同期满时，及时回收他们使用的所有资产，如设备、软件、文件、访问卡、电子资料等，防止对资产的非授权使用。
8. 当员工离职或调离其他岗位、外单位人员合同期满时，及时删除他们对信息和信息处理设施的访问权限，访问权限包括物理和逻辑访问、密钥、身份卡、信息处理设备、签名等。对于他们知道的账户，应修改密码。所有与他们在工作上有联系的员工，不能再共享信息给他们。要保证撤销他们所有的访问权限，避免不满的人员可能故意破坏信息和信息处理设施，或可能为将来的使用而收集信息。

## 物理和环境安全策略

1. 公司的物理场所划分为安全区域、办公区域和公共区域，根据安全区域内资产的安全需求和风险评估结果，使用如围墙、门禁、监视设备、报警系统、访问控制手段等物理保护措施，来对安全区域边界提供物理保护，防止被未授权访问和恶意破坏。
2. 使用安全控制措施，对安全区域的入口进行控制，确保只有授权人员才可以访问安全区域。安全控制措施包括记录访问者进入和离开的时间，审计访问重要区域的行为，外单位人员需有专人陪同等。信息安全领导小组应要对安全区域的访问权限定期进行评审，必要时进行更新和废除。
3. 使用物理保护措施，对来自外部和环境的威胁提供安全防护，防止由于火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为灾难而引起的破坏。物理保护措施包括危险或易燃材料在离安全区域安全距离以外的地方存放，恢复设备和备份媒体的存放地点与主场地保持安全距离，在安全区域合适的地点提供灭火设备等。
4. 员工和外单位人员应严格遵守安全区域内的工作指南，避免由于误操作对安全区域造成的物理破坏并减少恶意活动。工作指南包括监督在安全区域内的工作行为，未使用的安全区域要上锁并定期进行检查，不允许非授权携带摄影、视频、声频或其他记录设备等内容。
5. 合理安置和保护设备，包括将设备安置到安全区域并尽量减少不必要的对安全区域的访问，把处理敏感数据的信息处理设施放在限制观测的位置，禁止在信息处理设施附近进食、喝饮和抽烟，监视温度、湿度等环境条件等，来减少由环境威胁造成的风险和避免对设备的非授权访问。
6. 提供足够的支持性设施，包括使用不间断电源（UPS），使用稳定足够的供水以支持空调、加湿设备和灭火系统，定期进行检查、测试以确保功能有效等，来减少由于他们的故障或失效带来的风险，并使设备避免由他们引起的电源故障和其他中断。
7. 对传输数据和支持信息服务的电源布缆、通信布缆进行有效防护，保证他们免受窃听和损坏。防护措施包括将电源和电信线路埋在地下，分开电源电缆和通信电缆以防止干扰，使用清晰的电缆识别标记以防止操作失误等。
8. 对设备进行正确维护，以确保其持续的可用性和完整性。要按照设备供应商建议的时间间隔和规范对设备进行维护，对设备的修理和服务必须是已授权的维护人员，要保存所有可疑的、实际的故障和所有预防、纠正维护的记录，设备进行维护前需删除其中的敏感信息。
9. 包含储存介质的设备，要删除或安全重写敏感信息和注册软件，确保敏感信息和注册软件已被安全处置，避免由于草率处理或重用而导致信息泄漏。
10. 设备、信息或软件在带出公司场所时，要进行授权、记录，设置设备移动的时间限制，在返还时执行一致性检查并作送回记录，以保证设备被带出公司场所时的安全。

## 通信和操作安全策略

1. 根据信息处理设施的管理、操作职责和程序，进行数据备份、设备维护、媒体处理和机房管理，确保能正确、安全的操作信息处理设施。
2. 严格控制信息处理设施和系统的变更，包括策划和测试变更、制定变更批准程序、向所有有关人员传递变更细节、制定变更反馈程序（即从不成功变更中退出和恢复的程序）等，避免对信息处理设施和系统的变更缺乏控制，降低系统故障和安全故障。
3. 业务系统的开发、测试和运行设施要分离并进行控制，控制措施包括敏感数据不能拷贝到测试系统环境中、禁止开发和测试人员访问运行系统及其信息等，以减少对运行设施及其信息的未授权访问和带来的潜在风险。
4. 定期根据外包服务协议中的安全要求，监视、评审由外单位提供的服务、报告和记录，监督协议规定的信息安全条款和条件的严格执行。监视、评审内容包括监视服务执行效率，评审服务报告，审查外包服务的安全事件、操作问题、故障、失误追踪和破坏的记录。
5. 规划新系统时，要对新系统的用户量、未来的能力需求等进行分析，评估出所需的系统性能，避免新系统出现过载等潜在的瓶颈。
6. 新业务系统或升级版本在正式上线前，要进行合适的测试，并根据验收要求和标准进行正式的验收，以证实全部验收准则完全被满足。
7. 在全网采取防病毒机制，来实现对病毒、木马、恶意代码、移动代码的预防、检测和查杀。
8. 制定详细的备份策略，使用足够的备份设施，定期对业务数据进行备份，确保业务数据在灾难或媒体故障后能及时进行恢复。
9. 在网络边界、安全域之间使用防火墙或VLAN进行逻辑隔离和访问控制，使用网络安全审计系统对网络访问行为进行记录、监视和回放，保证对网络进行充分的管理和控制，防止威胁的发生，维护业务系统和信息的安全。
10. 应对磁带、磁盘、U盘、可移动硬件驱动器、CD、DVD、打印媒体等进行有效的管理，防止非授权的使用和破坏。对可移动存储介质的管理包括所有介质应存储在符合制造商说明的安全、保密环境中，使用介质要进行授权、登记并追踪审计等。
11. 应对不再需要的介质进行安全处置，降低介质敏感信息泄漏给未授权人员的风险。
12. 依据信息处理和储存程序，对信息进行有效的分类、处理、存储，防止信息的未授权泄漏和不当使用。信息的处理和储存包括按照信息的分类级别来标记、处理信息，标识未授权人员的访问限制，维护已授权的信息使用者的正式记录，定期评审已授权使用者的使用记录等。
13. 依据信息交换控制程序，来保护通过使用各种类型通信设施的信息交换。
14. 严格遵照与外部单位之间交换信息和软件的协议，来保证信息传递的安全。交换协议应考虑发送方、接收方的管理职责，确保交换信息的可追溯性和不可抵赖性，信息安全事故中的职责和义务等。
15. 包含信息的介质在往外运送时，要采取一定的保护措施，以防止未授权的访问、不当使用和毁坏。采取的保护措施包括使用可靠的运输和人员，授权人员要经过领导的批准，包装要足以保护介质在运输期间可能出现的任何物理毁坏等。
16. 对在电子消息发送中的信息提供安全保护（如电子邮件），防止信息遭受未授权访问、修改或其他攻击。
17. 记录用户活动、异常和信息安全事件的日志信息，并保留一定的时间，以支持将来的调查和审计。记录的日志应包含用户名称，日期、时间和关键事件的细节，终端身份或位置等信息。
18. 使用审计系统，来对信息处理设施的使用进行审计和监视，记录审计和监视结果，并定期评审，使管理员能及时了解设施的状态，并确保用户只执行被明确授权的操作。
19. 记录日志的设施和日志信息应加以保护，防止被篡改和未授权访问。
20. 记录系统管理员和系统操作员的操作日志，并定期评审这些日志信息。系统管理员和系统操作员的日志应包括事件发生的时间，涉及的账号和管理员或操作员，事件或故障的信息内容等信息。
21. 记录信息处理设施报告的故障事件，并实施采取措施进行处理。定期评审故障日志和故障处理措施，确保故障已经被正确处理。
22. 正确设置系统时钟，公司所有相关信息处理设施的时钟应使用已设的精确时间源进行同步，以确保日志记录时间的准确。

## 访问控制策略

1. 按照正式的用户注册及注销的程序，对所有信息系统及服务的访问权限进行授予和注销。
2. 各部门必须向信息安全工作小组提交一份系统与互联网连接的列表。
3. 所有管理性的、特殊账户的用户必须有账户管理说明书、文件，必须获得授权。
4. 每一个使用管理性的、特殊账号的个人都必须避免滥用权力，并且必须在信息技术中心的指导下使用。
5. 共有的管理性的、特殊账号的口令在人员离职或发生变更时必须及时更改。
6. 在系统只有一名管理员的情况下，口令必须由另外的人来保管，以便在紧急情况下其他人可以访问系统。
7. 当因内外部审核、软件开发、软件安装或其他规定需求而需要特殊的访问账号时，账号必须被授权；创建的日期期限必须明确；工作结束时此账号必须删除。
8. 创建的所有账号都必须有适于系统或服务的要求。
9. 所有账号都必须使用分配的用户进行唯一性标识。
10. 用户账号长期不用（超过30天），建议将该账号锁定。
11. 所有新用户账号自创建之日起30天不登录，建议将该账号锁定。
12. 系统管理员或其他指定人员：负责删除个人账号；必须将修改用户账号相关信息的过程文件化；必须定期评审现有账号的有效性，并将此过程文件化；服从单独的审核评审；在管理者要求时，必须提供他们管理的系统账号的列表；必须与授权的管理者合作调查安全事故。
13. 所有口令，包括初始口令，都必须依据信息技术中心规定的下列规则建立和执行：必须定期更改；必须符合信息技术中心规定的最小长度（8位）；必须是字母和数字字符的组合；必须不能是可以轻易联想到的账号所有者的特性：用户名、绰号、亲属的姓名、生日等；必须不能用字典中的单词或首字母缩写；必须保存历史口令，以防止口令的重复使用。
14. 用户的账号口令必须不能泄露给任何人，信息技术中心不能询问用户的账户口令。
15. 如果怀疑口令的安全性，应立即进行更改。
16. 管理员不能为了使用信息资源规避口令。
17. 用户不能通过自动登录的方式绕过口令登录程序。
18. 计算机设备如果无人值守必须启动口令保护屏保或注销。
19. 所有网络连接设备必须按照主管部门批准的网络设备安全配置表进行合理配置。
20. 所有连接到网络的硬件必须服从主管部门的管理和监控标准。
21. 在没有主管部门批准的情况下，不能对活动的网络管理设备的配置进行更改。
22. 网络基础设施支持一系列合理定义的、被认可的网络协议，使用任何未经认可的协议都必须经过信息技术中心的批准。
23. 支持协议的网络地址由信息技术中心集中分配、注册和管理。
24. 网络基础设施与外部网络的所有连接都由信息技术中心负责。
25. 防火墙必须按照防火墙实施规范文件进行安装和配置。
26. 未经主管部门批准不可以安装路由器、交换机、集线器或者无线访问端口。
27. 在未经主管部门批准的情况下，用户不得安装网络硬件或软件提供网络服务。
28. 不允许用户以任何方式更换网络硬件。
29. 通过提供给用户唯一得识别码（用户ID）和选择一种适当的鉴别技术（密码手段、智能卡、令牌或生物手段）证实用户身份的方法，对访问操作系统的用户进行用户识别和鉴别。
30. 应严格控制对可能越过系统和应用程序控制的工具程序的使用，防止系统工具的滥用。
31. 在访问操作系统过程中，对于不活动的会话必须设定在一个不活动周期后关闭，以防止未授权人员访问和拒绝服务攻击。
32. 基于各个业务应用要求，应严格限制用户对信息和应用系统功能的访问权限，防止对信息系统的未授权访问。
33. 对关键的业务系统，必须建立隔离的运算环境，以防止对关键业务信息的未授权访问。
34. 只有被批准的笔记本电脑才能用来访问信息资源；
35. 笔记本电脑必须有口令保护；
36. 数据不应存储在笔记本电脑中。但是，在无可选择区域存储的情况下，可以存储，但必须使用被认可的加密技术进行加密；
37. 不使用笔记本电脑通过无线方式传输数据，除非使用经信息技术中心批准或认可的无线传输协议；
38. 需要连接互联网的计算机系统必须符合信息服务标准，并被信息技术中心书面批准；
39. 对无人看守的笔记本电脑必须实施物理保护，必须放在带锁的办公室、抽屉或文件柜里，或者锁在桌子或柜子上。

## 信息获取、开发与维护策略

1. 在新的信息系统或增强已有信息系统的业务需求陈述中，应该识别和明确对安全控制的相关需求。
2. 对于输入应用系统的数据，主要包括业务事务处理、常备数据和参数表，必须加以验证，以确保数据是正确且适当的。
3. 在设计和实施应用系统或业务系统的过程中，要求有控制措施，以检查系统运行的有效性和完整性，从而将系统运行失败的风险降到最低。
4. 在业务过程中，必须明确出所有需要完整性保护的信息，通过安全风险评估确认完整性保护需求，使用密码技术手段对完整性保护进行紧鉴别，从而保护信息的完整性。
5. 在需要通过网络通信方式进行业务，或通过网络来传输业务数据时，必须使用密码控制方法来实现通信安全或数据保护，主要包括密钥管理方法、密码策略实施的角色分配与安全职责等方面，以确保数据的保密性、完整性和不可否认性。
6. 在业务过程中，要求使用适当的密钥管理措施，主要包括分开密钥证书的生成、使用、变更、撤销、恢复、归档等操作，以防止使用的密码或密钥被修改、遗失和毁坏，从而防止通过密钥对信息的未授权访问。
7. 在操作系统上安装或升级软件时，必须按照既定流程来进行控制，使运行系统被损坏的风险减到最小。
8. 应该从下列几个方面考虑对系统测试数据的保护：访问控制程序是否适用测试应用系统、访问测试系统授权、测试后清除运行信息以及运行信息的拷贝和使用等。
9. 严格限制对程序源代码和相关事项（包括设计、规范、证明设计和确认设计）的访问，以防止带入一些非授权功能，避免对源代码的无意识的修改。
10. 在引进新的系统和对已有系统进行变更时，要按照既定的变更控制过程来进行，使信息系统的损坏减到最小。
11. 当操作系统发生变更后，应对一些关键业务应用系统进行审查和测试，以确保对业务操作或信息安全没有负面影响。
12. 相关负责部门必须管理和监视外包软件的开发，主要考虑以下方面：落实知识产权、代码质量和安全功能的合同要求以及发生故障时对外单位的要求。
13. 定期评估现有信息系统的技术脆弱性，并采取打补丁等控制措施来处理相关风险。

## 安全事件策略

1. 遵照信息安全事故报告机制，报告可能对公司的信息资产安全造成影响的不同种类的安全事故和弱点，并确保所有的员工、合同方和外单位人员都遵守执行这套报告程序。
2. 以信息安全工作小组为信息安全事故和弱点报告对象，确保所有的员工、合同方和外单位人员都知道这个报告对象，并尽可能快地向其报告信息安全事故和弱点。

根据事件危害程度，对安全事件进行相应的等级分类。

1. 一旦信息安全事故和弱点报告上来，要立即明确责任，按照程序进行有效处理，启动适当的事故管理活动，包括事故管理程序中规定的恢复活动，确保能对信息安全事故做出快速、有效和有序的反应。
2. 信息安全工作小组在报告问题的员工协助下，负责启动、完成并文件化事故调查过程。
3. 应及时对信息安全事故的类型、频率和影响等进行评估，并采取适当措施防止事故再次发生。
4. 在事故调查过程中，信息技术中心负责搜集和整理实物和电子证据，证据的存储和处理要符合相关司法程序中的要求。
5. 在不牵涉到法律强制的地方，信息安全工作小组可以向信息安全领导小组建议惩戒措施，在牵涉到法律强制的地方，信息安全工作小组组长负责与外部单位以及法规强制部门的协调沟通。

## 业务连续性策略

1. 为满足关键业务活动的连续性对信息安全的需求，要求公司各个相关部门执行和维护既定的业务连续性管理过程。这个过程包括资产识别、业务影响分析、控制措施、计划测试与更新等。
2. 在日常的业务活动中，应该识别设备故障、人为错误、盗窃、火灾、自然灾害和恐怖事件等能引起业务流程中断的事件，定期进行风险评估，确定这些中断发生的概率和影响、损坏程度和复原所需时间。
3. 必须根据关键业务活动的目标制定业务连续性计划，并且应该满足信息安全相关要求，以确保在关键业务过程中断或失败后能够在要求的水平和要求的时间内恢复信息的可用性。
4. 必须维持一个确定的业务连续性计划框架，应包含相关信息安全需求，并确保由此制定出的所有计划是一致的。每一个业务连续性计划都必须说明计划实施的可行方法，指定计划责任人，并确定优先次序以进行测试和维护。
5. 业务连续性计划要定期测试和更新，以确保其及时性和有效性。

## 符合性策略

1. 遵守所有与信息安全相关的法律法规、合同和安全要求，由综合部定期收集和整理，将这些内容形成文件并保持更新。
2. 现有或新增的信息处理系统，必须符合知识产权相关的法律法规和合同要求。
3. 各部门应按照相关法律法规要求，明确规定重要记录的保存期限并提供适当的保护，防止丢失、损坏和伪造。
4. 各部门应按照国家有关规定对个人信息进行妥善管理与保护，防止丢失或泄露个人秘密。
5. 公司的所有信息处理设备，只允许完成岗位相关的信息处理任务或工作。
6. 采用的加密技术必须符合国家相关法律的规定。
7. 每半年进行一次内审，以确保安全措施得到有效的实施和保持，符合已确定的信息安全要求。
8. 每半年进行一次技术符合性审查，确定信息系统是否符合安全实施标准，主要确定信息处理系统软硬件的控制措施得到实施，并保存审核的记录，对于不符合项必须给出纠正措施。
9. 严格按照制定的审核程序对信息系统进行审核，在审核前必须制定详细的计划，尽量减少对业务处理的影响。
10. 对审计工具需加以保护，在不使用审计工具时，应将工具和工具产生的审计数据从服务器彻底删除，将审计数据保存在特别保护的光盘中，防止任何可能利用工具及数据的滥用。

# 相关文件

无。