|  |
| --- |
|  |
|  |
| 数据安全管理规定 |
|  |
|  |

1. 分发控制

|  |  |  |
| --- | --- | --- |
| 分发对象 | 文档权限 | 说明 |
| XXX内部员工 | 只读 |  |

1. 文件版本信息

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 拟稿和修改 | 说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. 文件版本信息说明

文件版本信息记录本文件提交时的当前有效的版本控制信息，当前版本文件有效期将在新版本文档生效时自动结束。文件版本小于1.0 时，表示该版本文件为草案，仅可作为参照资料之目的。

1. **总 则**
2. 为保证XXX信息系统核心数据安全，维护数据所有者权利，明确利益相关者的责任与义务，按照分类管理、分级保护、授权使用的原则，根据《XXX信息系统安全管理规定》及国家信息系统安全等级保护等有关要求，特制订本规定。
3. 本规定所管理的数据均为非涉密的数据，XXX系统已标识密级的文件或已声明密级的数据不纳入本规定管理范畴。
4. 本规定适用于全国XXX信息系统环境中的数据安全管理工作。XXX各单位、部门均应按本规定开展数据安全管理工作。
5. **术语定义**
6. 本规定所称数据所有者是指，对所管理业务领域内的信息或信息系统，有权获取、创建、维护和授权的业务主管。
7. 本规定所称利益相关者包括数据创建者、数据所有者、数据管理者、数据使用者及信息安全管理人员。
8. 本规定所管理的数据涵盖以纸质、电子等形式存在的文件和非文件形式的信息及其衍生物。其中，非文件形式的数据包括数据库及配置文件中的数据、配置信息等。
9. **职责定义**
10. 数据创建者负责针对其所创建数据的内容和价值提出分类分级建议，提交对应级别数据所有者确认。
11. 来自XXX信息系统以外的数据，数据承接者视同创建者行使提出分级分类建议的责任和义务。
12. 数据所有者具有确认数据类别和敏感级别、确认销毁、提出技术保障需求、审查自检和审计报告、做出安全事件处置决定等权利和义务。其中，XXX业务数据的所有者为XXX指定的相应业务部门。
13. 各类数据的责任部门是该类数据的管理者。数据管理者作为数据所有者的代理者，代理数据所有者从事数据管理工作，负责其所管辖范围内数据的安全管理工作。数据管理者的职责包括但不限于：数据类别和敏感级别的标识与声明，根据级别进行管理与保护，数据使用培训，执行销毁操作并声明，定期自查提交报告，配合数据安全违规调查等。
14. **分类与分级**
15. 数据按其内容和用途不同分为技术类数据、行政管理类数据、业务类数据以及安全运行类数据。
16. 数据分级应根据其价值、内容的敏感程度、影响及发放范围进行确定。
17. 数据管理者负责制定其分管领域内数据敏感等级的划分规则，并制定和发布本部门或本领域的数据敏感等级目录。
18. **标识与声明**
19. 数据的分类分级标识、声明是数据不可分割的一部分，自其标识、声明之日起，数据及其标识、声明不得分离，数据管理者和数据使用者均须按照标识、声明的类别和级别安全管理和使用数据。
20. 对于文件形式的数据，须由数据管理者在文件明显位置标识其类别、敏感级别、失效日期等，且文件和标识不能分开。标识应该醒目，标识格式应统一，标识方法应便于审计。对于非文件形式的高敏感级别数据，如无法标识，须进行声明。
21. 失效日期指数据敏感级别的有效性截止日期。到达失效日期后，应对数据进行重定级。
22. 对于敏感级别高的数据，须由管理者对数据名称、类别、敏感级别、失效日期等以声明文件的形式进行声明，声明文件须由数据所有者审批签字。声明文件须跟随数据一起保管和传递。（声明文件模版详见附件）
23. 多个不同敏感级别的数据合并在一起时，按最高敏感级别给混合数据进行标识和声明。
24. **保管与保护**
25. 数据管理者须按照数据的敏感级别实施对应的保管与保护措施，并确保满足数据所有者对数据的安全要求。
26. 数据管理者在日常管理中，须对数据按敏感级别分级防护，采取对应的存储、归档、设定保存期限等措施。
27. 敏感级别高的数据纸质文件须参照XXX秘密级文件安全管理规定进行保管和保护。敏感级别高的电子数据须采用必要的访问控制措施。
28. 数据管理工作应该首选技术手段加管理要求实现。必须加强针对数据管理工作的技术手段的研究、选型、部署、维护等。
29. 敏感级别高的数据自产生之日起，所有者提出的技术保障需求应同步到位。如技术上无法达到，技术部门应持续跟踪技术进展，逐步使技术手段能够满足各项管理要求；对于已成熟并可采纳的技术手段，技术部门应验证其功能可靠性，逐步引入，持续优化技术保障工作。
30. **数据使用**
31. 数据使用者在使用数据时，须注意识别数据的敏感级别，按照其敏感级规范数据操作使用行为；使用中发现问题及时反映，发现违规行为及时举报，并积极配合违规事件的调查；自觉遵守数据管理规定。
32. 数据使用者须保证其所使用数据来源的合法性，不私自拷贝、使用、传播、保存与自己工作无关的数据。
33. 数据使用者和数据管理者无权未经所有者批准向发布范围以外的单位或个人提供中心数据或其衍生物，否则视为违规；如因工作原因需要对外提供的，应经数据所有者确认，并记录、备案、备查。
34. XXX业务数据须按主管业务部门授权或管理规定要求对外提供，否则视为违规，并需做好数据提供记录，备案、备查。
35. 数据管理者要对数据使用情况进行掌控和审计，发现违规行为及时制止，并依本规定进行处置。
36. **数据销毁**
37. 数据管理者有按照数据所有者要求清理和销毁原始数据的义务。
38. 数据使用者应具有数据安全清理和销毁的意识，具有按照数据管理者的要求清理和销毁本地临时数据、中间文件、过程文件的责任和义务。
39. 数据管理者和数据使用者具有按照规定记录清理和销毁数据过程，并接受安全管理人员审计的义务。
40. 数据管理者和数据使用者在清除和销毁电子数据时，须保证清除和销毁的彻底性。
41. **安全检查与审计要求**
42. 数据管理者有义务监督数据的安全使用，负责所管理数据的自查工作。周期性地检查数据安全使用和管理情况，更新过期的标识或声明信息，向数据所有者汇报。
43. 信息安全领导机构根据信息安全组织授权，独立开展高敏感级别数据的第三方审计工作。检查和审计数据所有者、数据管理者数据管理要求的执行情况，向信息安全组织汇报。
44. **数据保护**
45. 数据保护应遵循适度保护、积极防范、突出重点、分级管理的原则，通过数据的分类分级进行区别保护、动态保护。
46. X系X统信息安全组织，应根据信息安全工作的实际需要，制定数据保护的具体技术和管理措施。
47. 在数据的采集、决策分析、共享发布、存储和废弃的生命周期各阶段，对数据的相应级别进行防护和处理。
48. 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输和存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
49. 数据在存储和传输过程中须根据数据的级别采用加密或其他手段确保其存储安全。
50. 数据在使用过程中，须根据数据的级别进行控制，严禁非授权访问、传输和修改。
51. 数据交换过程中如涉及交换对象为非海关系统，应确保对端保护力度不低于海关系统数据保护力度。
52. 数据的销毁须严格按照XXX系统相关标准、规范要求及国家的法律法规要求进行处理。
53. **附 则**
54. 对在数据安全管理工作中做出贡献和创造性地开展工作的部门与个人予以表彰和奖励；对违反本规定而引发事故的相关责任人，按照XXX违规违纪相关规定予以处罚。
55. 本规定由XXX科技发展司负责解释。
56. 本规定自发布之日起执行。

附件、声明文件模板

附件、声明文件模板

**分类分级说明**

|  |  |
| --- | --- |
| 数据名称： |  |
| 失效日期： |  年 月 日 |
| 发放范围： |  |
| 类 别： |    |
| 敏感级别： |    |
| 声明者签字： 年 月 日 | 数据所有者签字： 年 月 日 | 信息安全部门备案： 年 月 日 |
| 注：“数据名称”项填写：文件形式数据的文件名称，或非文件形式数据的数据内容简称；“失效日期”项填写：数据敏感级别的有效性截止日期；“声明者”为数据管理者。 |

**请将此文档复印件交备案部门备案**