**北京沃丰时代数据科技有限公司**

**信息安全违规处罚管理规定**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 信息安全违规处罚管理规定 | | |
| **文档编号** | ISMS-L3-07 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 孟庆鑫 | **编制日期** | 2018-12-11 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **状态** | **修订内容说明** | **修订日期** | **编制人** |
| V1.0 | 新建 |  | 2018-12-11 | 孟庆鑫 |
| V1.1 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. 总则
2. 为对违反北京沃丰时代数据科技有限公司（以下简称“沃丰时代”或“公司”）信息安全管理体系文件要求、控制措施、法律法规、合同要求的员工实施违规惩戒，并作为对可能在其它情况下有意轻视信息安全程序的员工的威慑，强化全体员工的信息安全意识，有效防止信息安全事故的发生，明确信息安全违规行为处罚的操作原则，特制定本规定。
3. 本规定适用于公司全体员工。
4. 职责分工
5. 研发部负责对信息安全违规事件的跟踪处理，收集和保护相关证据，确定事件责任人，上报信息安全委员会、人力资源部。并记录附件一：《信息安全违规记录》。
6. 信息安全委员会负责参照本规定对信息安全违规事件、以及造成的信息安全事件或事故做出处罚决定。
7. 人力资源部根据信息安全委员会的处罚决定对事件责任人做出处罚。配合公安机关对违反法律法规的信息安全责任人追究法律责任。
8. 违规处罚程序
9. 违规事件、违规等级与处罚措施，如下表：

|  |  |  |
| --- | --- | --- |
| **违规事件** | **违规等级** | **处罚措施** |
| 窃取、故意泄露公司保密信息的，或故意违反信息安全管理规定，性质严重造成重大影响或风险 | 一级 | 1. 直接开除，永不录用； 2. 如违反法律法规由公司移送公安机关处理；如给公司造成相关损失，须赔偿公司损失； 3. 全公司范围通报处罚决定。 |
| 故意违反信息安全规定，性质严重；或者造成较大影响或较大风险 | 二级 | 1. 如给公司造成相关损失，须赔偿公司损失； 2. 担任公司管理岗的员工，进行降职或者降薪处理；非管理岗位人员进行降薪处理； 3. 全公司范围通报处罚决定。 |
| 过失违反信息安全管理规定，造成一定影响或风险的；或者故意违反信息安全管理规定，但性质不严重且没有造成严重影响或风险 | 三级 | 1. 记入员工KPI考核结果或罚款1000元； 2. 12个月内2次三级违规升级为1次二级违规； 3. 团队/部门内部通报处罚决定。 |
| 过失违反信息安全管理规定，性质较轻，造成轻微影响或风险 | 四级 | 1. 记入员工KPI考核结果或罚款500元； 2. 12个月内2次四级违规升级为1次三级违规； 3. 团队/部门内部通报处罚决定。 |

1. 认错态度较好、积极配合调查处理的，可以考虑从轻处罚；未发现违规违纪行为时，主动交代全部违规违纪事实并配合公司调查处理的，可以考虑从轻处罚。
2. 证据的收集和保存
3. 证据的收集
4. 当信息安全事件涉及到诉讼（民事的或刑事的），需要进一步对个人或组织进行起诉时，应收集、保留和呈递证据，以使证据符合相关诉讼管辖权。
5. 证据在收集时不得侵犯个人权益，应在不侵犯个人权益时对证据进行收拾并且证实证据是否可在法庭上使用。
6. 应保证证据的质量和完备性，防止未被授权的篡改和泄漏。
7. 证据获得的保证：应确保收集证据其信息系统符合任何公布的标准或实用规则来产生被容许的证据。
8. 证据的保存及提供
9. 提供证据的份量应符合任何适用的要求。对该证据的存储和处理的整个时期内，应进行过程控制保证证据的质量和完备性。
10. 对计算机介质上的信息：任何可移动介质的镜像或拷贝（依赖于适用的要求）、硬盘或内存中的信息都应确保其可用性；拷贝过程中所有的行为日志都应保存下来，且应有证据证明该过程；原始的介质和日志（如果这一点不可能的话，那么至少有一个镜像或拷贝）应安全保存且不能改变。
11. 任何法律取证工作应仅在证据材料的拷贝上进行。所有证据材料的完整性应得到保护。证据材料的拷贝必须在可信赖人员的监督下进行，什么时候在什么地方执行的拷贝过程，谁执行的拷贝活动，以及使用了哪种工具和程序，这些信息都应记录作为日志。
12. 附则
13. 本规定由研发部、行政部负责解释和修订。
14. 本规定自发布之日起施行。

**附件一 信息安全违规记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 违规场景描述 | 违规等级 | 惩罚措施 | 审批人 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |