**北京沃丰时代数据科技有限公司**

**员工信息安全规范手册**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 员工信息安全规范手册 | | |
| **文档编号** | ISMS-L3-10 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 孟庆鑫、肖立鹏 | **编制日期** | 2018-11-29 |
| **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 | 新增 | 2018-11-29 | 孟庆鑫、肖立鹏 |
| V1.1 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 

# 总则

1. 信息安全是公司的一项重要工作，对信息安全的关注涉及到日常工作的方方面面。为了更好地维护公司的整体利益，实现信息安全目标，特制定本手册，作为公司信息安全策略和规章制度中员工行为准则相关内容的集合。
2. 本手册适用于公司全体员工，包括正式员工、临时人员以及短期工作人员。

# 职责分工

1. 人力资源部：
2. 负责制定、审核本手册，并负责在公司范围内监督管理本手册的实施情况。
3. 负责督促相关人员和部门落实本手册。
4. 其他各部门：
5. 负责根据本手册执行相应具体措施，落实相应的日常信息安全工作。
6. 不定期由部门负责人组织开展自查。

# 总体要求

1. 信息安全意识：
2. 员工应积极主动地提高自身的信息安全意识和知识水平，主动参与公司的信息安全保障工作。在日常工作中如发现可疑的异常情况，或在系统及服务中发现疑似的安全漏洞和技术薄弱点，应及时通知部门信息安全管理员，并依据相关制度具体要求及时上报。此外，禁止将未经证实的情况和信息随意扩散。
3. 信息保密职责：
4. 员工应自觉遵守公司规章制度和职业道德，维护公司利益，保护公司的敏感信息。
5. 公司的保密信息分为三个级别：机密、秘密、内部，公开信息不属于保密信息。
6. 公司的数据分类分级策略参照《数据分级分类标准规范》。
7. 资产使用职责：
8. 日常工作中，以各种形式存在的信息和用以生成、获取、处理、传递、存储信息的软、硬件设施，以及保障软硬件资产正常运行的各种辅助设备均属于公司的信息资产，员工在使用这些信息资产的过程中承担相应的保护信息资产的责任。
9. 遵守制度法规：
10. 员工在日常工作中应自觉遵守国家法律法规和公司信息安全相关的各项规章制度，包括但不限于与信息安全相关的管理规定、技术标准、行为准则和实施指南等，应确保自己的行为符合国家相关法律法规的要求，符合公司管理和信息安全管理的要求。
11. 知识产权保护：
12. 所有员工都应该根据知识产权保护相关法律法规以及公司制度，自觉保护公司自主知识产权和第三方的知识产权，既不能非授权泄露公司的自主知识产权保护信息，同时也不能非法侵犯第三方的自主知识产权。

# 管理规定

1. 桌面系统使用规范：
2. 公司全体员工须使用正版软件。正版软件由公司正常的采购流程获取。桌面系统的安装和初始设置应由公司相关部门的指定技术人员负责。
3. 操作系统硬盘应保证至少两个分区，即系统分区和工作分区。如无特殊需要，员工不应在办公桌面计算机上设置共享文件夹。如必须设置时，应设置保护口令、只读权限等安全措施，并在共享完成后及时取消共享设置。
4. 安全软件是指为保障桌面计算机系统的正常运行和使用而必须安装的桌面安全防护软件，包括桌面管理客户端软件和企业级防病毒客户端软件。安全软件由公司安排技术人员统一进行安装、升级和维护，严禁员工随意卸载。
5. 员工应确保自己的桌面计算机系统安装了公司指定的安全软件，一旦发现未安装或软件功能异常应及时联系相关部门。若员工由于长期出差在外等原因无法由技术人员帮助安装安全软件，则在自行安装时必须使用公司提供的指定安装介质或软件包，按照公司指定技术人员的指导意见进行安装。
6. 员工在日常工作中必须保证安全软件的正常运转，并确保安全软件及时升级和更新，若发现问题应及时联系相关部门。
7. 禁止员工以任何方法强制关闭常驻内存的安全软件进程。禁止员工以任何方式修改统一安装的安全软件客户端参数配置。禁止员工在未经相关管理人员同意的情况下，卸载删除统一安装的安全软件客户端程序，或是使用同类产品的其他版本覆盖统一安装的安全软件客户端。
8. 基础软件在通常情况下指桌面办公系统所必须使用的基础应用软件或工具软件，如办公软件、邮件客户端、压缩解压软件、汉字输入法等。员工使用的基础软件必须使用由相关部门统一提供的安装介质或软件包进行安装。
9. 严格禁止在桌面办公设备上安装或使用对公司信息安全造成威胁、非法获取公司或他人信息的、带有攻击性的各类软件。
10. 员工对于自己所使用的桌面办公系统的安全保护承担最终责任，除非有特殊情况并获得批准，否则不应授权他人使用自己的桌面办公系统。
11. 密码使用规范：
12. 员工在设定系统或网络登陆密码时，应根据密码策略的要求选择具有一定复杂度的字母和数字的组合。员工应避免办公系统或网络的密码与私人密码雷同，避免在多个系统中设置相同的密码，以防密码被非法获取后造成连锁影响。
13. 员工应妥善保管自己的密码。在输入密码时，应保持必要的警惕性，以防止被他人通过偷窥等手段非法获取自己所拥有的密码。
14. 禁止员工在使用终端系统时开启任何形式的“自动保存密码”功能，禁止员工在未经相关部门允许的情况下使用自动程序登录系统。相关部门在为终端用户安装终端之后，应关闭任何形式的“自动保存密码”功能。
15. 员工在使用新的或经密码重置过的系统或终端时，必须在第一时间对初始、默认或重置密码进行更改。员工必须严格按照所使用系统或终端的具体要求定期更改自己的密码，在没有明确规定的情况下应保证至少每3个月更换一次密码。
16. 员工更新的密码应保证至少和最近三次使用的密码不相同。员工更新的密码不应是上次所使用密码的简单更改，比如在上次所使用的密码后面增加一位数字等。
17. 员工不应在电子邮件、手机或电话、调查文件或表格中泄露密码信息，不应在任何人面前谈及自己设定的密码。
18. 员工应尽量避免将密码书写在纸面上或是存放在电子文档之中，禁止将记录有密码信息的载体任意放置在工作区域。一旦发现或怀疑自己的密码被人非法获取，应立即进行密码更新，并及时向部门信息安全管理员报告情况。
19. 病毒防护管理规范：
20. 员工桌面计算机系统必须安装和使用公司统一部署的企业级防病毒客户端软件，应保持桌面计算机上所安装的防病毒软件能够及时更新。
21. 未经相关技术管理人员同意，禁止卸载删除统一安装的防病毒软件客户端程序，或是使用同类防病毒产品的其他版本覆盖统一安装的防病毒软件客户端。禁止以任何方式强制关闭常驻内存的防病毒程序进程。禁止以任何方式修改统一安装的防病毒客户端程序的配置，包括通过注册表修改软件强制关闭防病毒软件的开机启动选项等。
22. 员工应经常关注公司内部发布的病毒警告通知或提示，并采取必要的预防措施。
23. 公司在所有桌面计算机上都配置了定期自动执行的病毒扫描功能，员工应尽可能保证自动查毒功能的顺利执行，在没有特殊原因的情况下不得中断或关闭自动查毒的进程。
24. 如果由于工作上受到影响而确实需要中止病毒扫描进程时（如在演示PPT，或需要紧急处理相关工作等），员工应在完成工作后及时手动开启防病毒软件进行查毒。
25. 当发现异常情况时，员工应立即断开网络连接，启动防病毒软件进行查毒。当防病毒软件提示发现病毒时，员工应根据防病毒软件的提示完成病毒清除的过程。
26. 若遇到无法独立完成病毒清除等特殊情况时，应及时向本部门的负责人或者信息安全管理员寻求技术支持。员工不应自行采取一些未经验证的处理方式，或是随意在公司内发出病毒警告，影响正常工作的开展。
27. 电子邮件使用规范：
28. 禁止员工利用公司的办公邮件或类似系统制作、复制、发布、传播含有下列内容的电子邮件或信息：
29. 违反我国宪法所规定的基本原则的；
30. 损害国家或公司声誉和利益的；
31. 煽动民族仇恨，民族歧视，破坏民族团结的；
32. 破坏国家宗教政策，宣扬邪教和封建迷信的；
33. 散布谣言，扰乱社会秩序，破坏社会稳定以及公司正常业务的；
34. 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
35. 侮辱或者诽谤他人，侵害他人合法权益的；
36. 含法律、行政法规禁止的其他内容的；
37. 其他公司制度所规定的不准在网上传播的信息。
38. 在下载邮件附件时，应对附件内容以及发件人进行判断。对于某些来源不明的邮件附件，特别是对带有后缀名EXE、COM类的可执行文件，应对其直接删除或与相关信息技术人员确认后再进行下载。
39. 员工若发现可疑邮件时不可盲目打开，应先向邮件发送人员进行确认，在无法确认的情况下，应及时联系相关信息技术人员。
40. 员工对办公邮件的使用必须是以工作为目的，同时在使用过程中应采取一切可能的措施以对邮件本身和公司的邮件系统进行保护。
41. 员工应定期接收邮件，并及时删除过时和无保留价值的邮件，珍惜公司的系统和网络资源。对于重要的电子邮件信息，员工可在自己使用的终端上创建本地备份文件夹进行保存。
42. 员工不得试图打开和偷看其他员工的办公邮箱，员工如果误收到发送给其他员工的电子邮件，应在第一时间内将发送错误的情况通知邮件发送者，并从邮箱中删除该邮件。
43. 员工的办公邮箱启动后应被严密保管在自己的办公计算机中，禁止以任何形式与他人共享。员工的办公邮箱账号一旦开通之后，应及时更新密码。
44. 员工所发送的电子邮件必须代表真实的邮件作者和发送者，禁止利用任何手段伪造电子邮件的发送者。
45. 员工在使用过程中如果发现邮件系统存在任何安全漏洞，应及时通知所在相关信息技术人员。
46. 对于含有保密信息的邮件应按本规定中“保密信息管理规范”中的要求进行处理。
47. 保密信息使用规范：
48. 在非必要的情况下，禁止在员工办公桌面上摆放带有保密信息的文件。员工日常工作中含有保密信息的文件应当妥善保存在各人的抽屉中，并加锁保护。
49. 敏感或重要信息经打印、复印、传真后应立即拿走。对于打印或者传真不成功的带有敏感信息的纸张要及时用碎纸机销毁。
50. 不得在公共、私下等非工作需要的场所谈论自己掌握或知晓的任何公司规定需要保密的消息和事件。不探听、保留自己职责外的保密信息。
51. 对以各种理由打来电话或到现场的任何人员，如果询问一些个人信息、客户信息、系统网络设置等，原则上应一律不做回答。
52. 对重要的信息数据（如手头的重要资料、重要分析报告文件、专用的程序等）要做好备份，防止因丢失造成不必要的损失。
53. 网络使用规范：
54. 当使用笔记本电脑或台式计算机在公司内部办公时，应严格遵守公司对于内部网络的统一配置和管理。未经相关部门批准，禁止私自变更办公计算机的IP地址，不得随意改动办公计算机网络硬件的配置。未经允许不得以任何方式向外部机构或人员提供内部网络结构、配置等重要信息。
55. 严禁员工利用公司提供的互联网访问途径从事任何违反国家法律、法规，损害国家利益和他人合法权益的活动。禁止员工利用公司提供的互联网访问途径从事可能占用公司网络资源、影响网络安全的活动。
56. 终端计算机在外网必须通过申请VPN接入访问公司内部资源，严禁使用其他内网穿透工具接入，同时应在使用完毕后及时断开网络连接，避免连接通道被他人盗用；严禁在终端计算机上安装和使用点到点（P2P）的远程控制软件和文件共享软件；公司范围内禁止从公司终端向个人终端上传输数据。员工应加强远程访问的安全意识，保护VPN账号密码，只限自己使用，严禁透露给他人。
57. 办公设备使用规范：
58. 员工应使用标准配置的桌面计算机设备，禁止员工在未经相关技术部门批准或授权的情况下私自改动办公设备硬件。员工不得随意改动或移动办公区域内的电源、空调、机柜、终端、服务器、收发器和布线系统等设备。当所使用的硬件设备发生故障时，员工应及时通知技术人员前来解决，不应擅自拆卸。
59. 下班离开办公场所之前，如不是工作必须则必须关闭办公电脑。
60. 硬件设备在外借、维修或报废（弃用）时，需对机内的保密数据信息作相应处理，防止泄密。
61. 无人值守设备的责任人应采取合理的安全措施保护该设备，以避免未授权使用和入侵。
62. 员工在离开座位时，应对终端屏幕及时锁屏。员工应根据情况设置进入屏幕保护的时间和密码，通常设定进入屏幕保护的等待时间不应超过5分钟。
63. 员工在外出旅行、酒店房间、顾客及客户场所、乘坐交通工具等公共场所时，不得使笔记本电脑处于无人看管状态；若物理锁定可用，则在不使用时锁定。
64. 员工在非工作场所使用的笔记本电脑等其它设备，不得存放有公司保密信息。特殊情况对工作必须的保密信息，必须得到授权批准并加密方可随机保存。
65. 员工在公共场所使用电脑的过程中需防止信息泄密，避免电脑屏幕被偷看或偷拍，离开座位时必须立即锁定电脑屏幕，防止他人未经授权使用。
66. 若员工笔记本电脑被盗，应确保立即报告当地执法机构及公司相关部门。
67. 除笔记本电脑外的其他离场设备（比如放置在公司的合作伙伴的设备等）也应进行妥善的保护，以保证公司设备、信息的安全性。
68. 工作环境安全规范：
69. 员工在日常工作时，应佩戴身份识别标志（徽章、工作牌、名卡）等，不得伪造或冒用他人的身份识别标志。
70. 员工必须妥善保管身份识别标志，以及所持有的特定办公区域的门卡和钥匙，禁止将自己的门卡、钥匙以及所佩带的识别标志转借他人。一旦遗失应立即向相关区域的安全保卫部门汇报。
71. 未经批准，员工不得带任何外部人员参观公司的内部工作区域。
72. 员工应明确自己所拥有的权限，不得采用任何手段随意出入自己无权进入的区域。如果确有需要，必须严格遵循相关的审批和登记手续，不得伪造虚假登记信息。
73. 禁止携带任何危险品、可燃品或其它可能影响人员和设备安全的物品进入办公场所，如有特殊需要必须得到相关管理人员的批准。
74. 员工在办公区域内发现陌生且未佩带身份识别标志的人时应主动上前询问，或通知行政部对此情况进行关注。
75. 对工作中所产生、收集、使用的有关商务活动信息，研究、开发工作所产生出的数据或资料均应进行保护，严禁在工作区域内随意放置保密资料，严禁在未经允许的情况下将其带出办公场地，更不允许擅自将其泄露给外来人员或单位。
76. 移动存储介质使用规范：
77. 移动存储介质包括：优盘、光盘、移动硬盘、笔记本电脑、智能手机、平板电脑等，在存放和保管移动存储介质时，要防止高温、潮湿、磁场、强光、辐射的影响；当其它设备正在向移动存储介质记录数据或从其上读取数据时，不应擅自移动存储介质。
78. 员工不应在办公电脑上使用任何可疑或来历不明的移动存储介质，未经同意，不得将存放有公司敏感信息、内部事项、涉密信息的移动存储介质转借给无权获悉此类信息的人员。
79. 当需要在公司以外的计算机上使用保存公司敏感信息的移动存储介质时（尤其是可读写的移动存储介质，如优盘、磁盘等，也包括加密优盘和加密硬盘），员工应在使用过程中采取必要的措施，保证移动介质中的信息不被非法访问、篡改或删除，保证移动存储介质不丢失。
80. 员工应及时将存有公司重要信息和工作文档的存储介质移交给专门的保管人员归档，在进行移交前应确保介质以及其存储信息的完整和可用。例如项目组开发的应用程序源代码等。
81. 移动存储介质的维修、更换、报废应由相关部门统一负责，确保上面所存储的重要信息或保密信息不会被复原或部分复原。
82. 信息安全事件报告规范：
83. 员工在发现系统异常、网络速度大幅下降、密码被篡改、出现影响业务、财产或声誉的事件或其它可疑情况时，应及时向信息安全部报告。
84. 所有的员工、合同方和第三方用户应关注并及时报告系统或服务中已发现或疑似的安全弱点或技术薄弱点。
85. 对于突发信息安全事件，员工应按相关应急预案的要求采取有效措施，尽可能防止事态扩大。
86. 运维部应当保证在辖区内公布正常工作时间、非正常工作时间的联络电话以及电子邮件地址等与信息安全事件相关的信息。
87. 员工应事先熟悉信息安全事件响应流程，了解自身在其中承担的角色，并在信息安全事件发生后自觉按要求履行应尽的职责。
88. 员工应当从信息安全事件中认真学习，汲取经验教训，防止信息安全事件的再次发生。

# 信息安全违规处罚

1. 若员工违反上述管理要求，按照《信息安全违规处罚管理规定》进行处罚。

# 附则

1. 本手册由公司研发部和人力资源部负责解释和修订。
2. 本手册自印发之日起施行。