**北京汇聚融达网络科技有限公司**

**——外部人员访问管理制度**

**文件编码：HJRD-3-02**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 外部人员访问管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-3-02 | | **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 | 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。

总 则

为加强对外部人员在北京汇聚融达网络科技有限公司（以下简称“公司”）的信息安全管理，防范外部人员带来的信息安全风险，规范外部人员在公司各项与信息系统相关的活动所要遵守的行为准则，特制定本办法。

本办法所述的外部人员是指非公司内部员工，包括软件开发商、产品供应商、系统集成商、设备维护商、服务提供商、业务合作单位、临时雇工、实习生等外来人员，外部人员分为临时外部人员和非临时外部人员。

* + 1. 临时外部人员指因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的外部人员；
    2. 非临时外部人员指因从事合作开发、参与项目工程、提供技术支持或顾问服务，必须在相关单位办公的外部人员。

本办法适用于公司。

外部人员风险识别

各部门在与第三方进行接触过程中，应防范外部人员对于公司可能带来的各类信息安全风险，这些风险包括但不限于如下内容：

* + 1. 外部人员的物理访问带来的设备、资料盗窃；
    2. 外部人员的误操作导致各种软硬件故障；
    3. 外部人员对资料、信息管理不当导致泄密；
    4. 外部人员对计算机系统的滥用和越权访问；
    5. 外部人员给计算机系统、软件留下后门；
    6. 外部人员对计算机系统的恶意攻击。

接待部门应对外部人员进出接待区域的物理和信息风险进行识别和防范；关键区域的进出应填写《联合伟业卫星定位监控平台信息咨询有限公司外部人员访问申请表》，经部门负责人签字确认后， 由内部人员的全程陪同，方可进入。

涉及公司业务合作的外部人员风险识别由各业务合作部门负责管理，各部门应正确、合理识别各类业务信息的关键程度和保密程度，根据外部人员或项目保密协议严格控制，依照“按需访问”的原则对公司信息进行安全管理。

基本安全管理

在未经公司相关部门负责人的审核审批的情况下，禁止外部人员了解和查阅公司的敏感、重要和商业秘密信息。

外部人员如因业务需要查阅公司敏感资料或访问公司网络和信息系统资源，必须经过相关部门负责人批准并详细登记，须与公司签署有效的《 联合伟业卫星定位监控平台信息咨询有限公司外部人员保密协议》。

未经相关部门负责人的许可，外部人员不得在办公区域、设备间、机房等关键区域摄影、拍照。

外部人员物理访问控制

外部人员进出公司时，遵守信息安全工作组相关管理规定《公司办公环境信息安全管理办法》， 接待人必须全程陪同临时外部人员，告知有关安全管理办法。

业务洽谈和技术交流应当在接待室、会议室或培训教室内进行，招标、谈判等正式洽谈和重大项目的会谈应当在专门的会议室进行，不得在办公区域内进行。

外部人员进入机房、设备间等重要区域时，应遵从《公司机房环境安全管理办法》等相关办法。

外部人员信息系统使用控制

未经允许，禁止外部人员携带的电脑接入公司网络，如因工作需要访问公司网络和信息系统资源，必须填写《联合伟业卫星定位监控平台信息咨询有限公司临时接入网络申请表》，由接待人负责向信息安全工作组申请，并使用指定的设备。

未经允许，禁止外部人员远程访问公司网络。如确因工作需要（例如维护、故障处理）需要远程访问，必须由远程接入业务的需求部门填写《联合伟业卫星定位监控平台信息咨询有限公司临时接入公司网络申请表》，经部门负责人审批，报信息安全工作组领导批准。

外部人员在机房内的所有操作，都必需说明该操作可能引起的安全风险，并由接待人认可后才能操作。接待人必须对外部人员的操作进行全程监控，参照《公司机房环境安全管理办法》中的相关附件，记录外部人员的操作内容并存档备案。

更换机器硬件的操作需向接待人指出硬件损坏的证据，由接待人员上报信息安全工作组批准，将机器上的应用切换到其它机器上后，方可进行更换，并参照《公司机房环境安全管理办法》中的附件记录并存档。

外部人员对机房附属设备（如空调、UPS等）的维护和保养，事先要由接待人员上报信息安全工作组领导批准后选择合适的时间进行，确保操作不影响公司系统的正常运行，并参照《公司机房环境安全管理办法》中的附件记录并存档。

未经信息安全工作组批准，禁止外部人员携带移动存储介质进入机房。

外部人员如因工作需要使用移动存储介质，必须在接待人的监控下使用，由此而产生的安全风险由接待人承担。

附则

本办法由公司信息安全工作组制定，并负责解释和修订。

本办法自发布之日起执行。