

**昆山华恒工程技术中心有限公司**

**管理文档 内部资料**

**昆山华恒工程技术中心有限公司**

**外包人员管理办法**

软件部

2017.5.24

文档修订记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 修改时间 | 修改人 | 审核人 | 备注 |
| 1 | 2017.05.24 | 董永胜、郑博 | 王亮 |  |
| 2 |  |  |  |  |
|  |  |  |  |  |

目录

[1 目的 2](#_Toc483411434)

[2 适用范围 2](#_Toc483411435)

[3 相关定义 2](#_Toc483411436)

[4 在场外包员工信息安全管理 3](#_Toc483411437)

[4.1 责任人 3](#_Toc483411438)

[4.2 办公主机使用管理 3](#_Toc483411439)

[4.3 帐号和访问权限管理 4](#_Toc483411440)

[4.4 信息使用管理 4](#_Toc483411441)

[5 场外外包员工信息安全管理 5](#_Toc483411442)

[6 外包员工离场管理 5](#_Toc483411443)

# 目的

本管理规范专为昆山华恒工程技术中心有限公司（以下简称：“公司”）的外包员工设立，主要为了建立完善的外包员工的信息安全管理制度，明确外包员工在场和离场需遵守的规范，包括但不限于：机器使用规范、帐号使用规范、场外接入规范、离场规范等。

# 适用范围

本管理规范适用全公司范围内所有外包员工。

# 相关定义

公司将其非核心的业务外包出去，利用外部优秀专业团队承接业务，从而使其专注核心业务，达到降低成本、提高效率、增强企业核心竞争力和对环境应变能力的目的，这类服务外包及项目外包的员工统称为**外包员工**。

在场外包员工：外包员工在公司自有或租用办公环境内进行办公的称为在场外包员工。

场外外包员工：外包员工在公司自有或租用办公环境外进行办公的称为场外外包员工。

公司办公内网主要分为两类：办公网、开发网，使用原则为“专网专用、专机专用”，相关定义如下：

办公网：从事日常办公行为，如公文处理、访问内部系统、访问授信互联网网站、使用公司域收发邮件等。

开发网：从事软件开发、测试等研发行为，如访问SVN代码管理系统、使用开发环境编写代码、对代码进行测试、访问运维接入平台等。

# 在场外包员工信息安全管理

# 责任人

4.1.1外包员工在场办公必须使用公司提供的办公和开发主机。

4.1.2外包员工本人对所使用的办公、开发主机和外包帐号负直接责任，应尽到保全资产完整性以及合理使用帐号的义务。

4.1.3管理外包员工的员工对外包员工使用的办公、开发主机和外包帐号负管理责任。

# 办公主机使用管理

外包员工通过办公或开发机接入公司内部网络进行工作，须遵守公司相关管理规定。

4.2.1外包员工使用的办公或开发机必须满足以下要求，才允许接入内部办公或开发网：

1. 必须安装指定的标准化操作系统；
2. 安装公司指定办公安全接入软件；
3. 安装公司指定的防病毒软件和办公安全接入软件。

4.2.2严禁办公或开发机在接入内网的同时接入其他网络，包括但不限于：

1. 使用双网卡，在连接内网的同时连接其他网络；
2. 在连接内网的同时，使用GPRS或3G；
3. 在连接内网的同时，使用拨号或专线的方式连接到公司外部网络。

4.2.3 外包员工必须使用开发机接入开发网访问公司内部研发资料。

4.2.4禁止外包员工在办公和开发主机中安装任何类型的扫描、窃听或攻击性质的应用程序。

# 帐号和访问权限管理

4.3.1内网信息系统分级规定：

|  |  |
| --- | --- |
| **安全级别** | **信息系统** |
| **一级** | 邮件系统、互联网、OA系统、企业通内部沟通工具 |
| **二级** | 源代码管理系统、文档系统、项目管理系统、业务管理系统 |

4.3.2外包员工默认使用公司域办公帐号，不得私下使用自己账号。

4.3.3外包员工帐号须唯一对应一个外包员工，禁止外包员工共用帐号。

4.3.4外包员工帐号默认不具有内网信息系统访问权限，根据实际工作需要可申请一级和二级信息系统访问权限。

4.3.5禁止外包员工使用开发电脑访问互联网。

# 信息使用管理

4.4.1外包员工禁止以任何形式对公司敏感信息进行未授权访问和处理。

4.4.2禁止对敏感信息做如下处理：

1）非工作缘由将敏感信息携带出公司；

2）向非公司授权方公布敏感信息；

3）未授权浏览、篡改敏感信息。

4.4.3敏感信息包括：

1）源代码信息，包括但不限于：开发测试代码、已发布产品代码、已下架产品代码等；

2）未发布产品信息，包括但不限于：产品属性、界面UI、功能和使用说明等；

3）用户数据，包括但不限于：用户个人资料、产品使用记录等；

4）人事信息，包括但不限于：薪酬、组织架构、职级等。

# 场外外包员工信息安全管理

5.1 原则上要求所有外包工在公司提供的职场环境内办公，默认不开放外网接入公司内网系统进行办公的权限。如因实际工作需要，需从外网环境接入内网，必须经企业相关部门评审，并由公司总经理签字授权方可。

5.2 对场外办公的外包员工开放的内网系统，需与其它内网系统实施隔离措施，隔离方案由公司制定。

5.3 对场外办公的外包员工开放的内网系统，不得对外提供如下信息：

1）公司内部的开发测试代码。

2）公司内部服务器运维操作权限。

# 外包员工离场管理

6.1外包员工离场前须配合公司完成文档、代码下载检查和访问权限回收工作。

6.2外包员工离场流程、门禁使用等参照《外包员工入场离场管理规范》。

7.外包员工违规处罚

7.1在场外包员工须遵守公司相关规范《。。。。。》，若发现有违反本规范或触及高压线等行为者，停止此外包员工相关工作，退回到外包公司，由外包公司根据商务合同进行处理，并保留追究相关外包员工法律责任的权利。

7.2 管理外包员工的员工对外包员工的行为负管理责任。