|  |
| --- |
| 上海中远资讯科技有限公司 |
| **中远海运集运开放服务平台** |
| **合作伙伴应用安全规范** |
| v0.1 |
|  |

|  |  |  |
| --- | --- | --- |
| F:\资料\材料\COSCOSHIPPING01.png | 上海中远资讯科技有限公司  未经公司允许，该文档不得外传 |  |

目录

[1 目的和范围 4](#_Toc20436691)

[1.1 目的 4](#_Toc20436692)

[1.2 适用范围 4](#_Toc20436693)

[2 术语和定义 4](#_Toc20436694)

[3 规范性引用文件 5](#_Toc20436695)

[4 概述 5](#_Toc20436696)

[5 应用的安全功能开发 5](#_Toc20436697)

[5.1 账号、认证和权限 5](#_Toc20436698)

[5.2 日志审计 6](#_Toc20436699)

[5.3 数据保护 7](#_Toc20436700)

[5.3.1 数据传输 7](#_Toc20436701)

[5.3.2 数据使用 7](#_Toc20436702)

[6 用户使用的安全风险告知 8](#_Toc20436703)

[6.1 系统提示 8](#_Toc20436704)

[7 开发者运营的安全管理保障 9](#_Toc20436705)

[7.1 开发管理 9](#_Toc20436706)

[7.2 漏洞管理 9](#_Toc20436707)

[7.3 运维保障 10](#_Toc20436708)

文档信息

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 开放服务平台合作伙伴应用安全规范 | **文档版本** | v0.1 |
| **适用范围** | 上海中远资讯科技有限公司 | **发布日期** |  |
| **负责部门** | 运营管理部 |  |  |

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修改日期** | **内容说明** | **修订者** |
| v0.1 | 2018/12-27 | 初稿 | 陈吉鹏 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

相关文档

|  |  |  |  |
| --- | --- | --- | --- |
| **文档编号** | **文档名称** | **文档类型** | **修订者** |
|  | 中远资讯API管理和规划 | 规划 | 陈吉鹏 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 目的和范围

## 目的

为营造规范、有序、安全的中远海运集运开放平台环境，提升中远海运集运开放平台合作伙伴(以下简称“开发者”或“您”)提供的应用安全性，从而保障开发者及用户的合法权益，依据《中远海运集运开放平台服务协议》、《中远海运集运开放平台运营规则》、《中远海运集运开放平台合作伙伴开发协议》等内容，特制定此规范。

## 适用范围

本规范规定了对开发者所提供的应用在开发、部署、运营、维护和管理等方面的安全准则要求，适用于所有的开发者和相关应用的运营者。

# 术语和定义

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 电子商务 | 以电子形式进行的商务活动。它在供应商、消费者、政府机构和其他业务伙伴之间通过任一电子方式实现标准化的非结构化或结构化的业务信息的共享，以管理和执行商业、行政和消费活动中的交易。 |
| 中远海运集运开放平台 | Cosco Shipping Lines Open-api Platform，简称“COP”或“开放平台”，指基于中远海运集运各类航运物流业务的开放，由中远海运集运提供一些软件和支持材料，开发者通过这些软件和支持材料开发应用以便服务于自身或服务于中远海运集运平台其他用户。开发者可以通过开放平台应用编程接口调用指定的功能服务，访问由中远海运集运提供的或用户授权的与用户相关的数据和/或来自其他中远海运集运应用程序的数据信息，或者由开发者应用向中远海运集运提供、回流数据。开放平台可能包括但不限于一个或多个API、编程工具和文档。 |
| 开发者 | 指通过有效申请并通过验证的可以基于开放平台进行应用开发的单位或者个人，在开放平台开发者也可称为“COP合作伙伴”。 |
| 应用 | 指开发者基于开放平台所开发的软件或服务，包括自用型应用和他用型应用两种类型。 |
| ApiKey、  SecretKey | 指开发者在申请开发新应用时获得的由中远海运集运授予的应用程序接入账户和密钥。Apikey是应用的唯一标识，中远海运集运通过Apikey来识别应用开发者的身份。Secretkey是中远海运集运给应用分配的密钥，该密钥在一定技术条件下可保证应用来源的可靠性。 |
| 信息安全 | 保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。 |
| 安全策略 | 用于治理组织及其系统内在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、指导和实践，特别是那些对系统安全及相关元素具有影响的资产。 |
| 用户 | 使用中远海运集运合作伙伴所提供应用的机构或自然人，以注册的ID与用户信息为判断依据。 |
| 加密 | 加密是将明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码（通常称为"密文"）。 |
| 安全事件 | 特指电子商务安全事件，不仅包括网络上攻击或入侵行为造成的安全事件，也包括电子商务业务应用中出现的欺诈、盗号、违禁等恶意行为。 |
| 信息安全风险 | 人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。 |
| Webshell | Webshell常常被称为匿名用户(入侵者)通过WEB服务端口对WEB服务器有某种程度上操作的权限,由于其大多是以网页脚本的形式出现，也有人称之为网站后门工具。 |

# 规范性引用文件

* 《中华人民共和国网络安全法》，2016年11月7日；
* 《信息系统安全等级保护基本要求》，国标GB/T22239–2008，2008年6月；
* 《移动智能终端安全能力技术要求》，工信部，YD/T2407-2013，2013年4月；
* 《信息系统通用安全技术要求》，GBT20271-2006，2006年5月；
* 《电子商务基本术语》，GB/T18811；
* 《信息安全技术术语》，GB/T25069-2010；
* 《信息技术安全技术信息安全事件管理指南》，GB/Z20985-2007；
* 《信息安全技术信息安全事件分类分级指南》，GB/Z20986-2007；
* 《信息技术系统安全工程能力成熟度模型》，GBT20261-2006；

# 概述

开发者所开发的应用为电商平台上的商户提供支撑和服务，必须具备保证其参与电子商务活动中的数据安全的能力。本规范对开发者所开发的应用所提出的安全要求包括但不限于应用的安全功能开发、用户使用的安全风险告知和开发者运营的安全保障管理等方面的要求。

# 应用的安全功能开发

本部分是对开发者应用应开发实现的安全功能所提出的安全要求，包括：账号管理、身份认证、权限管理和安全审计。

## 账号、认证和权限

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 账号唯一 | 应用应为不同的用户分配不同的账号，确保一个用户一个账号，应禁止多人使用同一个账号。 |
| 账号有效期 | 应用应对用户账号和应用管理员的账号设置有效期。 |
| 无用账号删除 | 应用应及时删除或禁止多余的、过期的用户账号，避免共享账号的存在。 |
| 账号权限回收 | 应用应及时清理和回收应用相关的开发账号、测试账号和后台管理账号及权限，如：相关账号使用者离职或转岗时。 |
| 初始口令 | 应用管理员账号的初始口令应为系统随机产生的满足口令强度要求的口令。 |
| 口令更换 | 应用应定期（每半年）提醒用户对口令进行修改，建议口令至少每六个月更换一次。 |
| 口令重置 | 应用应提供给用户口令重置功能，口令重置的功能需要经过开发者客服人工确认或者经过“组合鉴别”通过才能生效，且重置后的口令必须通过短信、邮件等用户绑定的可信任的渠道告知用户。 |
| 重新验证 | 当会话空闲超过30分钟，应用应要求用户重新验证或重新激活会话。 |
| 登录控制 | 应用应对登录应用的用户进行身份标识和鉴别。 |
| 组合鉴别 | a)应用应支持对同一用户采用两种或两种以上组合的鉴别技术（口令验证、邮箱验证、短信验证等）实现用户身份鉴别； |
| b)在执行敏感操作（口令修改或重置）或账号行为异常的情况下，应用应采用两种或两种以上的组合鉴别方式。 |
| **说明：** |
| 短信、邮箱验证可以通过发送验证信息到用户绑定的可信手机号或邮箱中，并且需要对验证信息设置过期时间，建议10分钟。 |

## 日志审计

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 审计所有用户的行为和操作 | 应用应提供覆盖到每个用户的安全审计功能，对应用重要安全事件进行审计；审计内容应包括重要用户行为（包括：所有的登录访问、RDS的调用、TOP的调用、来自用户端的访问和订单的传递等）以及系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。 |
| 日志存储保护 | 应用应保护所存储的日志审计记录的完整性，避免其受到未预期的删除、修改或覆盖等。 |
| 日志保存期限 | 应用应保存日志至少六个月。 |
| 服务器端登录日志 | a)应用应记录应用所有的登录日志，包括且不限于：  1）用户登录应用的日志；  2）应用管理员登录管理后台的登录日志；  3）主机端进行的系统登录。  b)日志的内容应包括：时间、用户在开发者的自有账号、应用标识（AppKey）、应用名称、源IP和登录结果（成功或失败）等 |
| 服务器端调用COP日志 | a)应用记录服务器端调用COP的日志；  b)日志的内容应包括：源IP、时间、用户在开发者的自有账号、应用标识（AppKey）、应用名称和用户调用COPAPI的URL等。 |
|  |  |
|  |  |
|  |  |
|  |  |

## 数据保护

### 数据传输

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 传输加密 | a)应用中涉及敏感数据（比如订单数据等）的传输必须进行加密传输，实现系统管理数据、鉴别信息和重要业务数据的传输保密性；  b)加密算法应使用AES-128位或以上强度。 |

### 数据使用

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 数据处理 | 应用在对其敏感数据（比如订单、费用数据等）进行后台的处理或计算时，其相关功能的组件和模块应部署应符合《信息系统安全等级保护基本要求》。 |
| 数据展示 | 应用应对涉及敏感数据（比如电话号码、邮箱等）的展示，进行脱敏处理（模糊化、匿名处理等）。  建议的脱敏方案：  a)【手机号】显示\*+后4位。如：\*\*\*\*\*\*1050；  b)【固定号码】显示区号和后三位，如0571-\*\*\*\*\*123；  c)【邮箱】@前面的字符如果大于或等于3个字符，@前面的字符只显示其前3位且再增加2个\*,并且@后面显示其第1个字符、‘.’分隔符及其后面的字符，但其中间其他字符都统一替换成2个\*，例如：con\*\*@1\*\*.com；如果少于三位，@前面的字符全部显示且再增加2个\*，并且@后面显示其第1个字符、‘.’分隔符及其后面的字符，但其中间其他字符都统一替换成2个\*，例如tt@163.com则显示为tt\*\*@1\*\*.com；  d)【客户名称】显示首/尾各2位，中间加\*例如：Ki\*ny； |

# 用户使用的安全风险告知

本部分是对开发者应用在被使用的过程中，用户应知晓和注意的相关安全风险所提出的安全要求，包括：通过用户手册和系统提示的途径告知用户如何有效地使用应用的安全功能，以及用户应注意和避免的不良使用行为。

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 安全功能介绍 | 对于应用的商家用户，开发者应提供详尽全面的操作指导文档（如帮助文件和纸质文档），便于用户查询，用于指导用户使用或配置开发者提供的应用的安全功能。在文档中应写明应用中所提供的安全功能介绍，对于用户影响系统安全性的操作（如修改口令、配置权限等），在操作时应明确提示相关的风险；对于会影响应用正常运行的关键配置项和操作，文档中也应用警告标志标示，并明示其可能的影响。 |
| 应用间的数据交互 | a)开发者应告知用户对口令进行安全保护，包括：检验口令强度并提示用户设置强口令、设定口令修改默认时期，到期提示修改口令、口令不得存储在本地；  b)开发者应告知用户终端的安全使用需要注意的不安全的日常使用行为和基本安全建议：包括：屏保的安全设置、操作系统的及时升级、防病毒软件的有效安装、主机防火墙的正确配置、应用软件的下载与安装；  c)开发者应告知用户移动终端的安全使用，包括：设置屏幕解锁口令或图案、防病毒软件的有效安装等；  d)开发者应告知用户移动介质的安全管理，包括：U盾、U盘、移动硬盘的安全存放，设置用户口令等；  e)开发者应告知用户互联网的安全访问的注意事项，包括：无线上网、浏览上网、电子邮件、社交网络、即时通信、网上交易等方面；  f)开发者应告知用户防止基于社会工程的欺诈，包括：   * 基于人：物理的非授权访问呢； * 基于电话：呼叫者电话的欺骗； * 基于电子邮件：钓鱼攻击、Email地址欺骗； * 基于即时通信软件：通过QQ、微信等的欺骗； |

## 系统提示

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 使用风险提示 | 应用应在合适的界面提示用户使用应用时的安全风险及学习安全指南的建议，至少应包括：不开启云盾的风险、口令被盗的风险、使用默认账号的风险、使用共享账号的风险。 |
| 终端风险提示 | 应用应在合适的界面提示用户终端安全方面的风险及学习安全指南的建议，至少应包括：病毒感染的风险、不及时安装补丁的风险、使用访客账号的风险、使用默认账号的风险、不进行口令保护的风险、不设置屏幕保护的风险。 |

# 开发者运营的安全管理保障

本部分是对开发者在开发者应用的开发和运营中应进行的安全管理所提出的安全要求，包括：应用开发过程的安全管理，相关的安全漏洞管理以及日常运维中的安全保障。

## 开发管理

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 使用风险提示 | 应用应在合适的界面提示用户使用应用时的安全风险及学习安全指南的建议，至少应包括：不开启云盾的风险、口令被盗的风险、使用默认账号的风险、使用共享账号的风险。 |
| 终端风险提示 | 应用应在合适的界面提示用户终端安全方面的风险及学习安全指南的建议，至少应包括：病毒感染的风险、不及时安装补丁的风险、使用访客账号的风险、使用默认账号的风险、不进行口令保护的风险、不设置屏幕保护的风险。 |

## 漏洞管理

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 漏洞扫描 | 在应用上线运行前，开发者应对前后台系统执行漏洞扫描，保证上线应用不存在漏洞，并将扫描结果提交给中远海运集运。 |
| 漏洞修复 | 开发者应对漏洞进行跟踪管理，要求高危漏洞24小时内修复，中危漏洞3天修复，低危漏洞7天修复。 |
| 渗透测试 | 开发者应提供给中远海运集运渗透测试报告，所评测应用应通过中远海运集运开放平台上线审核安全测试/渗透测试。上线应用不可存在如下漏洞：命令执行漏洞、用户信息泄露、代码执行漏洞、上传漏洞、SQL注入、权限漏洞、跨站脚本漏洞、CSRF漏洞、URL跳转漏洞。该测试需由中远海运集运或中远海运集运授权的独立第三方独立进行。针对BS架构及有WEB服务的CS架构，中远海运集运安全工程师可以帮助进行针对系统的渗透测试。 |
| 漏洞信息通报 | a)开发者发现中远海运集运平台存在缺陷时，应及时向中远海运集运通报。任何情况下，均不应隐瞒或恶意利用；  b)开发者发现自研应用、操作系统及所用到的相关第三方应用程序/代码组件中存在安全漏洞时，应及时向中远海运集运通报。任何情况下，均不应在生产环境下尝试验证弱点。 |

## 运维保障

|  |  |
| --- | --- |
| 安全项 | 具体要求 |
| 安全职责明确 | 开发者应将相关人员（开发、测试、运维、管理等）的安全职责向中远海运集运进行报备。 |
| 安全专职负责人 | 开发者应指定专职的安全负责人作为与中远海运集运安全团队的安全接口人，并且在御城河平台上设置安全负责人，定期保持安全联络和沟通。 |
| 安全意识教育 | 开发者应对相关人员（开发、测试、运维、管理等）每年进行至少一次的安全意识教育，并对对安全教育和培训的情况和结果进行记录并归档保存。 |
| 安全制度学习 | 开发者应建立和文档化其必要的安全制度和操作流程，并要求相关人员（开发、测试、运维、管理等）每年至少一次确认自己已经阅读并了解公司的安全要求和制度流程。 |
| 安全责任书 | 开发者的相关人员（开发、测试、运维、管理等）应签订数据安全责任书。 |
| 安全自查 | 开发者应至少每年执行一次安全自查，并在环境发生重大变更时（例如收购、合并、迁址等）不定期地对线上应用执行安全评估，根据安全评估执行相应操作（如补丁管理、软件升级、系统加固等），并将该安全评估结果和安全整改情况通报给中远海运集运相关的接口人。 |
| 风险处置 | a)开发者应及时、有效地配合中远海运集运日常的服务排查，不应做出屏蔽中远海运集运IP等恶意行为；  b)由安全扫描和渗透测试发现的各类安全风险，应在其规定的时间内完成处置，包括：高危风险的处置应在24小时内完成，中危风险的处置应在3天内完成，低危风险的处置应在7内完成。 |
| 服务和端口开放 | 应用（含前后台）应附有详细的列表，列明应用所必须使用的系统服务和通信端口，且应仅开放应用运行所必须的系统服务和通信端口。 |
| 变更管理 | a)开发者应识别应用开发和运维中的主要变更需求，并制定相关的变更方案；  b)开发者应建立相关的变更流程和审批机制；  c)当相关系统变更时，开发者应向所有相关人员（开发、测试、运维、管理等）通告；实施变更时，必须进行记录且应妥善保存这些记录。 |
| 应急响应 | a)开发者应制定安全事件报告和处置管理制度，明确安全事件的现场处理、事件报告和后期恢复的角色职能及处理流程；  b)开发者应建立负责线上应急响应的团队，明确安全事件响应的角色和责任人员/组织；  c)开发者应制定有7X24应急响应计划（突发安全事件预案），并定期演练；  d)开发者应监控相关软件程序的安全漏洞和威胁情报，及时修复应用及相关支撑系统的安全漏洞；  e)开发者应记录和保存所有报告中的安全弱点和可疑事件，分析事件原因，监督事态发展，并采取措施避免安全事件发生; |