.1. 敏感信息使用场景

敏感信息指用户的 身份证号、银行卡号、手机号 等身份信息。重要敏感信息的脱敏规范如下。

1.1.1. 敏感信息用于展示的场景

原则：敏感信息的展示请严格按照脱敏规范进行脱敏 说明：脱敏的逻辑必须在服务端完成，不能使用 Javascript 在客户端进行脱敏，包括代码注释、隐藏域、url 参数、cookies 等处的数据也必须脱敏。 说明：不能使用可逆的编码/加密方式，如 base64 编码等代替脱敏规范。 说明：若敏感信息明文展示在应用中，没有按照脱敏规范完成脱敏。支付宝开放平台将有权暂停敏感数据相关接口的开放。

1.1.2. 敏感信息用于身份校验的场景

原则：不要直接将敏感信息的明文信息在客户端与服务端之间传递 说明：可以将敏感信息在服务端关联到用户标识 ID，在客户端保存用户标识 ID 并提交到服务端，服务端根据 ID 取出对应信息后进行校验。 说明：如果服务端没有用户标识 ID 的机制，同时也必须在客户端与服务端之间传递敏感信息，请使用 AES128 对称加密算法进行加密后传输，并且不能将解密密钥传输给用户端。

1.2. HTML 页面渲染

原则：所有在页面渲染的敏感数据 (身份证、银行卡号、手机号) 必须进行脱敏

原则：禁止在 Cookie 中 明文写入 敏感数据

原则：禁止向 HTML 页面输出未经安全过滤或未正确转义的用户数据

原则：HTML 页面动态输出 JSON、JavaScript 必须对其中的字符串值做 XSS 防御处理

原则：默认设置 HTTP Header 中的 HttpOnly 属性为 true

原则：如果网站使用 HTTPS 协议，默认设置 HTTP Header 中的 secure 属性为 true

1.3. 接口调用操作

原则：AJAX 接口必须执行 CSRF 过滤

原则：AJAX 接口输出 JSON 字符串禁止通过字符串拼接构造，且输出的 JSON 需要经过安全过滤

原则：AJAX 接口返回头必须设置 Content-Type 为 application/json;charset=utf-8

1.4. 表单提交操作

原则：统一使用 POST 方式提交表单 说明：Get 请求可以通过构造 img 等标签发起，造成 CSRF

原则：Form 表单提交必须执行 CSRF 过滤

原则：用户输入的富文本浏览器展示之前必须由服务器端做安全过滤

1.5. 数据库操作

原则：用户密码存储须加盐存储，各用户盐值不同 原则：若涉及证件号等敏感信息的存储，须使用 AES-128 算法加密存储 原则：编写的 SQL 必须预编译，不允许通过字符串拼接的方式合成 说明：部分特殊场景，必须通过拼接合成，则拼接的变量必须经过处理，只允许 [a-zA-Z0-9_-.] + 字符。

1.6. URL 重定向

原则：URL 重定向的目标地址必须执行白名单过滤

1.7. 跨域操作

1.7.1. JSONP 跨域

原则：JSONP 接口 Callback 必须验证有效性 原则：JSONP 接口输出 JSON 字符串禁止通过字符串拼接构造，且输出的 JSON 需要经过安全过滤 说明：参考章节 2.1 跨站脚本（XSS）漏洞 原则：JSONP 接口必须对 REFERER 进行白名单校验，或执行 CSRF 检查 原则：JSONP 接口返回头必须正确设置 Content-Type 为 application/javascript;charset=utf-8

1.7.2. CORS 跨域

原则：支持 CORS 跨域的接口，返回头 Access-Control-Allow-Origin 必须使用白名单验证，禁止直接返回*

1.8. 文件上传与下载

原则：限制可下载文件所在的目录为预期范围，并通过指定文件编号的方式来定位待下载文件

原则：保存上传文件的目录不提供直接访问 原则：对上传文件的大小和类型进行校验，定义上传文件类型白名单

1.9. 加密与签名

不同场景使用的加密算法请参考下表。

场景	算法
加密场景	AES128
摘要场景	SHA256
签名场景	RSA2048