Custom-Code Standard Operating Procedure (SOP) v1.10

Table of Contents

Background

Thor (including Thor Industries, Inc. and its subsidiary companies) engages suppliers to create custom-code applications such as web sites and mobile apps. Thor has vulnerability management processes to test applications, but this testing is often done after the code is accepted and deployed. When post-deployment testing exposes issues, remediation occurs at the most expensive part of the development cycle. By this time the warranty period is often expired. In these cases, Thor is charged for time and materials to fix the application.

The intent of this this Standard Operating Procedure (SOP) is to communicate our minimum standards to suppliers, to ensure that suppliers deliver secure code. Suppliers will use industry-standard testing mechanisms and provide Thor with the results.

The scope of this SOP is all custom-code applications which will Process Personal Data. We use the EU's definition of Processing and Personal Data:

- Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

ISO Control	A.15.1.1	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
ISO Control	A.15.1.2	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Web Application Headers

ISO Control	A.18.1.4	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

Web Application Headers are used to define the communications between a web server and a web client. The following are the Web Application Headers that Thor considers mandatory for any application:

Web Application Header	**Example of an Appropriate Directive**
Content-Security-Policy	Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; style-src https://example.com/; script-src https://example.com/ ; object-src 'none'; form-action 'none'; report-to csp-endpoint;
Strict-Transport-Security	Strict-Transport-Security: max-age=31536000, includeSubDomains
X-Content-Type-Options	X-Content-Type-Options: nosniff
Cache-Control	Cache-Control: max-age=0, no-cache, no-store, must-revalidate
X-Frame-Options	X-Frame-Options: SAMEORIGIN
Set-Cookie	Set-Cookie: Secure
X-XSS-Protection	X-XSS-Protection: 1; mode=block
Referrer-Policy	No-referrer
Permissions-Policy	accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Server	Header reveals information that can be useful to an attacker. Do not use this unless necessary.
X-Powered-By	Header reveals information that can be useful to an attacker. Do not use this unless necessary.
X-AspNet-Version	Header reveals information that can be useful to an attacker. Do not use this unless necessary.

Note: for the Content-Security-Policy "Unsafe-eval" and Unsafe-inline" are not acceptable sources for the Content Security Policy.

Inline Javascript

The Mozilla project states the following on Inline Javascript:

https://wiki.mozilla.org/Security/Inline_Scripts_and_Styles

> "Cross-Site Scripting (XSS) and other content injections are a prevalent, yet very serious security issue for the web. But there is a way to make it less harmful: Content Security Policy (CSP). A content security policy is a list of allowed scripts, styles and other resources. Creating such a policy can disallow any kind of injected HTML to be harmful to the user. For CSP to understand which things are allowed and which are injected, everything has to live in its own document: An .html-file just for the HTML, a .css-file for stylesheets, a .js just for scripts and so on. This means, that there is quite a lot of code that requires to be rewritten."

To resolve this issue, move blocks of Inline JavaScript into their own JavaScript files. Use <script src="myscripts.js"></script> to render the JavaScript through the web page.

SSL Certificates

ISO Control	A.18.1.5	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

Elimination of Clear-Text sites

All Thor web sites will use HTTPS. Clear-text sites over HTTP are not acceptable.

- Search Engine Optimization: Google search rankings favor HTTPS over HTTP
- Brand Impression: most modern browsers tell the user when they are on an insecure site
- Performance: HTTP/2 is an improved protocol for faster web site performance. It only works with HTTPS.
- HTTP traffic can be intercepted (this includes reading and even modifying the contents)
- HTTP cannot be verified: attackers can impersonate Thor sites to attack dealers, end users, and products and services.

Requirements

Certificates will be purchased from a trusted Certificate Authority (CA). Thor will not accept the use of self-signed certificates.

TLS 1.2 is the minimum cryptographic protocol.

- Legacy versions of TLS will not be supported (TLSv1, TLSv1.1)
- Legacy versions of SSL will not be supported (SSLv1, SSLv2, SSLv3)

SHA-2 (256 bit) is the minimum hash.

- SHA-1 will not be supported.

Mobile Development

Mobile code will be developed in a manner that addresses the OWASP Top 10 Mobile Risks:
https://wiki.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

The issues we typically see are:

- Sensitive Data stored on the phone / stored in clear text
- Sensitive Data stored in backups
  - Android has an attribute called android:allowBackup. If this is set to True, sensitive data can be stored on the phone.
- Issues with transport security
  - IOS apps have a feature called Application Transport Security (ATS). This must be enabled.
- App is allowed to run on Jail-Broken or Rooted phones
- Applications lacked Certificate Pinning. This allowed manipulation of the authentication certificates.
- Certificates, pairing a device to a trailer, are not removed when the trailer is unpaired from the user's account

Vulnerability Testing

CIS Control	18.7	Apply Static and Dynamic Code Analysis Tools
ISO Control	A.14.2.9	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

Rating Vulnerabilities

Thor uses the Common Vulnerability Scoring Systems (CVSS) to assign qualitative ratings to vulnerabilities:

Rating	CVSS Score
None	0.0
Low	.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Testing

There are numerous tools for testing Code Security and Vulnerability scanning. Thor will not be proscriptive regarding the tools the supplier uses. The supplier must be able to do the following:

Code Security

Thor uses the Open Web Application Security Project (OWASP) Top Ten Project as its criteria for code testing. Suppliers will use static code testing against the OWASP Top 10 vulnerabilities.

- Thor will not accept code with Critical or High-severity findings.
- Supplier will remediate Medium-severity findings within 60 days of delivery, under the contract's Warranty terms.

Vulnerability Scanning

Thor expects that all suppliers will test their code in a DEV environment. Network vulnerability scanning will be done to ensure that there are no vulnerabilities introduced by the interaction of the code with the underlying infrastructure.

- Thor will not accept code with Critical or High-severity findings.
- Supplier will remediate Medium-severity findings within 60 days of delivery, under the contract's Warranty terms.

Web Content Accessibility Guidelines

Thor is committed to compliance with the Web Content Accessibility Guidelines. All custom-code web sites and applications must conform, at a minimum, to the WCAG 2.1 standard and all applicable laws and regulations. There are 3 levels of conformance to this standard:

- A – Minimum level of accessibility
- AA – General accessibility for most people
- AAA - Highest standard of accessibility

Thor expects that suppliers will test their code for WCAG 2.1 compliance.

Thor will not accept code without testing results that show an "**AA**" level of WCAG 2.1 conformance.

Acceptance Criteria

Supplier will provide **Code Security**, **Vulnerability Scanning, and Website Content Accessibility (including WCAG 2.1)** reports, which comply with the acceptance criteria, before delivery can be considered complete for final invoicing.

Representations and Warranties

Supplier, by entering into any agreement with a Thor company pursuant to which custom code may be provided by or through Supplier, represents, warrants, and covenants that Supplier and the custom code does and will comply with this Standard Operating Procedure.