Web-Hosting Standard Operating Procedure (SOP)

Various legislative mandates require that THOR ensure adequate security for Personal Data. This document is intended to describe THOR's Standard Operating Procedure for ensuring adequate security of THOR-Personal Data, hosted by 3rd Party Providers.

Contents

All suppliers providing (directly or indirectly) web hosting services shall ensure that the supplier, any party collecting or processing personal data on behalf of the supplier, and all services provided by or through the supplier comply with this Web-Hosting Standard Operating Procedure and all applicable laws and regulations (including those obligations imposed by GDPR and CCPA).

Web Architecture - Security Standard

Application

This standard applies to officers, directors, employees, agents and contractors of THOR Industries as well as third parties hosting Internet-facing applications, which process personal data on THOR's behalf or which otherwise access personal data which THOR may possess or control.

A supplier under this SOP is any supplier of web-hosting services directly to THOR; anyone the supplier engages to provide web-hosting services to THOR (for example, through a subcontractor), and anyone processing data on behalf of the supplier in connection with services provided to THOR.

All suppliers providing web-hosting services shall know the data security/data privacy laws and regulations applicable to the services suppliers provides to THOR and applicable to THOR's intended use of those services.

All suppliers providing web-hosting services to THOR shall also ensure that supplier and all services provided by or through the supplier comply with this Web Hosting Standard Operating Procedure and all applicable laws and regulations (including those obligations imposed by GDPR and CCPA).

The following are intended to be examples of best practice. They are not intended to be a checklist for compliance. We will look to guidance from enforcement authorities and Standards Organizations to inform our decisions regarding compliance. If elements of this architecture are missing, we will look at compensating controls. Based on this, we will use the language "should" instead of "must" as applicable. Note, however, that compliance with laws and regulations (including those mandating privacy policies and security measures) is always required.

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.

Standard

1. Policy

Any organization hosting Internet-facing applications, which processes THOR's personal data must maintain the following detailed documentation

a. **Network Security Policy**: Customer-facing policy stating how the organization protects customer data
b. **Data Privacy Policy**: Customer-facing policy stating how the organization processes personal data and ensures compliance with legislative mandates

2. Network Segmentation

A. Tiers

CIS Control	2.10	Physically or Logically Segregate High-Risk Applications
ISO Control	A.13.1.3	Groups of information services, users and information systems shall be segregated on networks.

Multi-Tier is an architectural deployment style that describes the separation of functionality into layers with each segment being a tier that can be located on physically/logically separated computers.

1. Web Architecture should have (as a minimum) a 2-tier physical architecture.
    a. Presentation (e.g. IIS, Apache, …) & Application (e.g. PHP, .NET, …) tiers located on one server
    b. Database (e.g. ORACLE, SQL Server, …) tier on physically/logically separate server. This tier is intended to isolate the database for both performance and security purposes.
2. In cases, where the physical separation between Presentation and Application layers is viable (e.g. Java, JBoss, IBM Websphere, …), **3 tier physical architecture should be**

considered - Presentation, Application and Database tiers are located on different physical servers:

a. Presentation – The topmost layer which houses all IIS and Apache web servers that are Internet and customer facing. Several security zones are recommended within this layer to account for the specific business requirements of the applications.
b. Application – This mid-tier layer allows traffic originating from Tier 1 to access application servers and services.
c. Database – The third layer permits traffic from Tier 2 to access databases.

B. Data Flow Control

CIS Control	12.9	Deploy Application Layer Filtering Proxy Server

In case of **2-tier architecture** the following data flow control should be implemented:

1. Internet traffic is permitted to talk inbound to the Application Delivery Controller (ADC) which functions as an Application Proxy
2. The ADC is permitted to talk inbound to Presentation & Application tiers
3. Presentation & Application servers are permitted to talk inbound to database servers

In case of **3-tier architecture** the following data flow control should be implemented:

1. Internet traffic is permitted to talk inbound to the Presentation servers in Tier 1
2. The Tier 1 web servers are permitted to talk inbound to applications in Tier 2
3. Tier 2 application servers are permitted to talk inbound to Tier 3 to database servers

C. Security Zones

CIS Control	2.10	Physically or Logically Segregate High-Risk Applications
ISO Control	A.13.1.3	Groups of information services, users and information systems shall be segregated on networks.
ISO Control	A.12.1.4	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

Security Zones should be created within each of the tiers to provide the segmentation of applications and services. Security Zones will prevent applications housed within the same tier from accessing each other, unless permitted. Isolation of the applications and the data is the purpose of implementing the zoning. The following is a list of some proposed Security Zones:

1. PCI, eCommerce: This is a requirement for limiting the scope of the Cardholder Data Environment (CDE). Thor Policy IT-14 governs all PCI environments for Thor.
2. Personal Data: Both GDPR and CCPA recommend segmentation as a strategy to isolate and protect applications which house personal data.
3. Development/Staging/QA: Separate zones must be created for dev/stage (QA) environment in each tier with stateful inspection access control firewall controlling the data flow between zones.
4. Shared Service: Supporting infrastructure, considered to be a 'trusted' source. Management, monitoring and backup traffic are example of services within this zone (e.g. DNS, SMTP, Log management etc.).

3. Architecture

There are a number of capabilities listed below. As technologies converge, there will be architectures where several capabilities are delivered by one device. This is acceptable, relative to this SOP.

A. Firewall

CIS Control	12.4	Deny Communication over Unauthorized Ports
ISO Control	A.13.1.1	Networks shall be managed and controlled to protect information in systems and applications.

Stateful-inspection firewall should control the access and data flow between the tiers and zones.

B. Application Delivery Controller

CIS Control	12.9	Deploy Application Layer Filtering Proxy Server

Application Delivery Controller (ADC) should be deployed on the public facing infrastructure after the traditional, stateful–inspection firewall. The ADC will support the following functions:

a) Load Balancer (where appropriate)
b) SSL Termination
   - SSL traffic must be terminated at ADC to allow the IDS/IPS, Web-Application Firewall (WAF) etc. to read un-encrypted traffic and make determinations about possible threats.
c) Application Proxy
   - Where it is not practically possible to separate the presentation and application tiers (e.g. using PHP or .NET languages), Application Delivery Controller will function as Application Proxy and provide extra level of protection.
d) Network-address translation (where appropriate)

C. Web Application Firewalls

CIS Control	18.10	Deploy Web Application Firewalls (WAFs)

Managed Web Application Firewalls (WAF) should be deployed and reside on the public facing infrastructure after the ADC/Load Balancer and traditional stateful–inspection firewall. WAF will provide additional Defense in Depth for web-based attacks, which cannot be discovered by traditional firewalls.

D. Intrusion Detection/Prevention Systems

CIS Control	12.7	Deploy Network-Based Intrusion Prevention Systems

IDS/IPS should be deployed between all tiers and zones (including tier for shared services) to provide the appropriate coverage along each network of the web architecture.

E. Encryption at Rest

CIS Control	14.8	Encrypt Sensitive Information at Rest
ISO Control	A.10.1.1	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

GDPR minimizes Notification requirements when breached data is encrypted. CCPA's section on fines is specifically written in terms of unencrypted records. All personal data written to file systems, databases, and backup media should be encrypted at rest.

F. Encryption in Transit

CIS Control	14.4	Encrypt all sensitive information in transit.
ISO Control	A.10.1.1	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

GDPR minimizes Notification requirements when breached data is encrypted. CCPA's section on fines is specifically written in terms of unencrypted records. All personal data being transmitted should be encrypted in transit. Use of deprecated protocols (such as SSL v3 or TLS v 1.0) violates this standard.

G. SSL Termination

CIS Control	12.10	Decrypt Network Traffic at Proxy
ISO Control	A.18.1.5	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

SSL termination should be performed on the Load Balancers or Application Delivery Controller (ADC). This will decrypt data communicating between the load balancer and the destination presentation web server within Tier 1. The purpose of this is to enable IDS/IPS and WAF sensors to view the data and take action.

H. File Integrity Monitoring

CIS Control	14.9	Enforce Detail Logging for Access or Changes to Sensitive Data

File Integrity Monitoring (FIM) should be used to validate the integrity of host Operating Systems and data files within each system. Changes to configurations, files and file attributes should be monitored and reported.

> Note: This is only required for Payment Card Industries (PCI) compliance. THOR Policy IT-14 (as amended) governs all PCI environments for THOR.

I. Security Incident and Event Management

CIS Control	6.3	Enable Detailed Logging
CIS Control	6.6	Deploy SIEM or Log Analytic tool
CIS Control	6.7	Regularly Review Logs
CIS Control	6.8	Regularly Tune SIEM
ISO Control	A.12.4.1	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A Security Incident and Event Management (SIEM) solution should be deployed to correlate logs from all infrastructure components provided by IAAS provider and have a 24x7x365 Security Operation Centre (SOC) monitoring and alerting on potential threats.

The SIEM solution should collect and store logs in a native format and be able to normalize the collected data. The SIEM solution should maintain logs for a minimum of 90 days or longer

depending on regulatory or policy requirements. The logs older than 90 days should be archived and kept up to 12 months. All retained logs must be available to THOR upon request.

The intent of this control is to ensure that the supplier can detect a breach if one occurs. The supplier will need to be able to describe the scope of the breach and what occurred (read, change, delete, exfiltrate, etc.).

J. Patch Management

CIS Control	3.4	Deploy Automated Operating System Patch Management Tools
CIS Control	3.5	Deploy Automated Software Patch Management Tools
ISO Control	A.12.6.2	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Supplier should have a program to ensure that IT assets maintain current patching levels.

K. Anti-Virus

CIS Control	8.1	Utilize Centrally Managed Anti-malware Software
CIS Control	8.2	Ensure Anti-Malware Software and Signatures are Updated
CIS Control	8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
CIS Control	8.4	Configure Anti-Malware Scanning of Removable Devices
ISO Control	A.12.2.1	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

As a minimum, all Windows Operating System based servers should use host Anti-Virus protection. Where available, all Linux based servers should use Anti-Virus protection as well.

4. Requirements for IaaS provider

A. Controls Effectiveness

CIS Control	20.2	Conduct Regular External and Internal Penetration Tests

Infrastructure-as-a-Service (IaaS) providers should provide an annual audit of effectiveness of internal controls for the Data Center providing Thor service. Audits must be performed by a reputable auditor, recognized within the industry for providing such services. Upon request the vendor will provide the written evidence of such audit:

a. SOC 1 engagements are based on the **SSAE 18** standard and report on the effectiveness of internal controls at a service organization that may be relevant to their client's internal control over financial reporting (ICFR).
b. A SOC 2 audit evaluates internal controls, policies, and procedures that directly relate to the security of a system at a service organization. The SOC 2 report was designed to determine if service organizations are compliant with the **Trust Services Principles**. These principles address internal controls unrelated to ICFR.

Note: Note there are two types of SOC 2 reports:

- SOC 2, **Type 1**: tests the documented controls to determine if they are adequately designed.
- SOC 2, **Type 2**: Same as Type 1, plus tests to ensure the controls are complete in coverage and operating effectively.

Type 1 reports are not sufficient for our purposes. THOR will require the SOC 2, Type 2.

B. Vulnerability Management

CIS Control	3.1	Run Automated Vulnerability Scanning Tools

IaaS provider will allow Thor to perform the vulnerability scanning of dedicated hardware and applications.

Representations and Warranties

Supplier, by entering into any agreement with a THOR company pursuant to which web hosting services may be provided by or through Supplier, represents, warrants, and covenants that Supplier and the web hosting services do and will comply with this Standard Operating Procedure.