



Harman International  
400 Atlantic Street, 15th Floor  
Stamford, CT 06901 USA

September 2020

## *Harman Third Party IT Security Management Policy*

### **1 TABLE OF CONTENTS**

1	Table of Contents .....	1
2	Purpose .....	2
3	Scope .....	2
4	Policy .....	2
4.1	Third-Party Security Requirements .....	2
4.2	Third-Party Access Control .....	2
4.3	Information Exchange .....	2
4.4	Third-Party Contracts .....	3
4.5	Personnel Security .....	3
4.6	Software Procurement .....	3
4.7	Assessment, Monitoring and Audits.....	3
4.8	Contingency Plans .....	4
5	Terms & Definitions .....	4
6	Violations.....	4

## 2 PURPOSE

This policy defines the requirements for the management of third-party services that handle sensitive information for Harman in any manner.

## 3 SCOPE

This policy applies to all employees, partners and third-parties with access to sensitive Harman information assets.

## 4 POLICY

### 4.1 Third-Party Security Requirements

**Third-Party Risk Assessment** – Third- Parties shall be reviewed whether they will get access to any Harman sensitive information. In case they do not, this policy does not apply. If they do, prior to commencing business relation with Harman, third-parties shall submit to a security related self-disclosure to evaluate risks. Risks must be identified in advance, mitigating controls must be established, and all contractor expectations must be incorporated into the contract for these services.

**Third-Party Information Security Responsibilities** - All Harman business partners, suppliers, customers, and other business associates must be made aware of their information security responsibilities through specific language appearing in contracts that define their relationship with Harman.

**Intellectual property rights** – Third-Parties shall implement appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements related to Intellectual Property Rights and use of proprietary software products.

### 4.2 Third-Party Access Control

**Third-Party Access To Internal Systems** - Third-party access to any Harman informational asset must be approved in advance by the Hiring Manager.

**Third-Party User IDs** - Before a user ID for access to any Harman informational assets is issued to a third party, the third party must agree in writing to prevent any unauthorized and improper use of Harman systems via the assigned IDs.

**Protection of records** – Third-Parties shall protect records from loss, destruction, falsification, unauthorized and unauthorized release, in accordance with legislative, regulatory, contractual, and business requirements.

### 4.3 Information Exchange

**Third-Party Sensitive Information Handling** - All disclosures of secret, confidential, or internal Harman information to third parties must be accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used.

**Third-Party Non-Disclosure Agreements** - Prior to sending any secret, confidential, or internal information to a third party for copying, printing, formatting, translating or other handling, the third party must sign a Harman non-disclosure agreement.

**Information Handling At Contract Termination** - If Harman terminates its contract with any third-party organization that is handling Harman sensitive information, the third-party organization must immediately thereafter destroy or return all of the Harman sensitive data in its possession.

**Third Party Information Disposal** - If the third-party destroys the information, Harman must receive notice that the data was disposed according to the procedures established or approved by Harman.

#### 4.4 Third-Party Contracts

**Service Level Agreements with Third Parties** - All agreements with third-parties, such as suppliers, service providers, and business partners, which could negatively impact the business processes of Harman must define service level agreements, privacy level agreements and require minimum standards of contingency planning and preparation on the part of these third parties. The SLA agreement should specify service provider's criteria related to type of service, the expected quality, the performance and the responsiveness. These characteristics must be measurable. SLAs are to be reported to and reviewed by Harman regularly. Any SLA breaches are to be investigated in order to prevent future occurrences of the same nature.

**Control Measures in Outsourcing Contracts** - All Information Technology outsourcing contracts must include specific words defining the control measures that will be provided and maintained. In addition, these contracts must specify a clear and expedient mechanism that Harman management can employ to immediately update these controls without bureaucratic delays, prolonged negotiations, or outsourcing firm management objections.

**Reporting Third-Party Security Violations** - All outsourcing contracts must stipulate that the third parties must notify Harman immediately of any security incident likely to impact sensitive Harman information under their control. Harman will retain the right to aid in the investigation of these incidents.

**Outsourcing Security Violations** - All third-party outsourcing contracts must stipulate that the contract may be terminated due to information security violations by the outsourcing partner.

**Outsourcing Firm Penalties** - All outsourcing firm contracts must include fiscal penalties for the outsourcing firm's failure to maintain information systems controls in a manner consistent with Harman's requirements.

**Sub-contractor Relationships** – Third parties shall have information security policies or procedures for its use of Contractors that impose requirements consistent with this security requirements.

#### 4.5 Personnel Security

**Right to Approve Personnel for Key Outsourced Positions** - Harman has the right to approve or reject any personnel provided by third-parties to perform duties on Harman premises or handle Harman sensitive data. This requirement must be included in any contracts with third parties performing Digital or security-related duties for Harman.

**Non-Employee Background Checks** - Temporaries, consultants, contractors, and other third-party organization staff must not be given access to sensitive information, or be allowed to access critical information systems, unless they have gone through a background check commensurate with the background checks given to regular employees.

#### 4.6 Software Procurement

**Software Integrity Statements** - If procurement of third-party software is being considered, management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise the software's security, and will not require the modification or abandonment of controls found in the affected operating system.

#### 4.7 Assessment, Monitoring and Audits

**Right to Audit** – Harman reserves the right to conduct audit or designate third party auditors to evaluate suppliers' compliance with information security policies & procedures.

**Independent Security Control Reports** - All agreements with third-party outsourcing organizations must stipulate that as per Harman's request, Harman will receive a report expressing an independent opinion about the adequacy of the controls in use at the outsourcing organization.

#### 4.8 Contingency Plans

**Service Provider Contingency Plans** - All contracts with web site hosting organizations, application service providers, managed systems security providers, and other information systems outsourcing organizations must include both a documented backup plan and a periodic third-party testing schedule.

**Outsourced Production Systems Back-Out Plans** - An effective and regularly-tested back-out plan, that permits Harman to revert to internal processing is in place.

**Contract Failure Remedies** - In addition, the contract language of these priority and Service Level Agreements (SLA) should specify remedies to Harman in compensation for losses incurred by failure to meet the specified priority or service level.

## 5 TERMS & DEFINITIONS

**Sensitive Information** – Any Harman information that is not publicly known, hence having a classification of internal, confidential or secret. This includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form.

**Information Asset** – Any Harman data in any form, and the equipment used to manage, process, or store Harman data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Password** – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**Service Level Agreement (SLA)** – A contract with a third party defining the measurable details of services to be provided.

**User** - Any Harman employee or partner who has been authorized to access any Harman electronic information resource.

## 6 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment or business relationship. Harman reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Harman does not consider conduct in violation of this policy to be within an employee's, supplier's, contractor's, or other 3<sup>rd</sup> party's (that may use Harman's technology) scope of employment or association with Harman, or the direct consequence of the discharge of the employee's, supplier's, contractor's, or other 3<sup>rd</sup> party's (that may use Harman's technology) duties. Accordingly, to the extent permitted by law, Harman reserves the right not to defend or pay any damages awarded against an employee, supplier, contractor, or other 3<sup>rd</sup> party that result from a violation of this policy.

Any employee, supplier, contractor, or other 3<sup>rd</sup> party who is requested to undertake an activity which he or she believes is in violation of this policy, should voice their concerns, either verbally or in writing, to any member of Harman management as soon as possible.