Information Security Policy

Version	4.7
Date	04-Jun-2018
Status	Approved
Document ID	ITSCPL
Owner	S. Manjunath
Approved	Vijay Shinde

Version History:

Version Number	Approval Date	Type of Change	PCR ID	Author	Reviewed By
V.0.1	03-Oct-06	First draft		Vijay Shinde	Vijaya Shanker
V.1.0	17-Nov-07	Version approved		Vijay Shinde	Vijaya Shanker
V.1.1	10-Jan-08	Reviewed and converted to new template		Vijay Shinde	Vijaya Shanker
V2.0	28-Jan-10	Reviewed and no changes are required	168	Vijay Shinde	Vijaya Shanker
V 3.0	6-May-11	Document Reviewed Changes made to template	219	Vijay Shinde	Vijaya Shanker
V 4.0	6-April-12	Document Reviewed, Changes made to scope	287	Vijay Shinde	Vijaya Shanker
V 4.1	29-Jan-13	Template changed to HCSHarman Connected Services Template	437	Vijay Shinde	Luigi Sanna
V 4.2	23-Jan-14	Document reviewed and Hyperlink are modified. Infosec director and Head of IT are changed	436	Vijay Shinde	Luigi Sanna
V 4.3	13-May-15	Policy statement and objectives updated	523	Vijay Shinde	Luigi Sanna
V 4.4	29-Feb-2016	Migration to HCS , by changing the logo & name of Symphony telecal to HARMAN Connected Services (HCS) and its template Informaiton Security Objectives updated, Added abbreviations	598	Manjunath.S	Vijay Shinde
V 4.5	01-Mar-2017	Reviewed and updated template	699	Manjunath.S	Vijay Shinde
V 4.6	28-Aug-2017	Removal of availabiltiy of hardcopies of ISM documents, Addition of Russian Federal laws / legal act	753	Manjunath.S	Vijay Shinde

V 4.7	4-June-2018	Migrated to Harman's new template	822	Manjunath.S	Vijay Shinde

Table of Contents

1.0 Introduction

The purpose of this policy document is to provide management direction and support for information security so as to protect the organization's information assets from all threats, whether internal or external, deliberate or accidental.

Harman Connected Services will initiate and implement an organizational information security policy and undertake periodic reviews to ensure that its core and supporting business operations continue to operate with minimal disruptions. HCS will ensure that all information that are disbursed or produced by HCS have absolute integrity. HCS will guarantee that all relevant information are managed and stored with appropriate confidentiality procedures

2.0 Scope

Information Security Policy is applicable to all users of Harman Connected Services and its subsidiaries.

3.0 Information Security Policy Statement

The Information Security policy statement for Harman Connected Services is as follows:

"We commit to establish, implement, maintain, and continually improve risk based information security management systems by ensuring Confidentiality, Integrity and Availability of information assets of Harman Connected Services, Our customers, Partners and Suppliers."

We commit ourselves to:

1. To meet our stakeholders expectations on information security, while complying with the legal, statutory and regulatory requirements applicable to our activities, the contractual obligations and the requirements of ISO 27001:2013 standard.
2. Protect our information assets from all threats, both internal and external, prevent occurrence of any information security incident and ensure the confidentiality, integrity and availability of our information assets.
3. Maintain acceptable levels of risk.
4. Counteract interruptions to information continuity activities and ensure availability of information.
5. Provide all employees with regular information security awareness training.

4.0 Information Security Objectives

Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. The company has no greater responsibility than protecting its people, workplaces, communities and the continuity of its business. HCS shall implement rigorous and comprehensive information security policies that systematically address security measures for preventing relevant risks, threats and potential damage to its business.

Information Security Policy of the organization shall ensure that:

Information should be made available with minimal disruption to staff and the public as required by the business process[1];

The integrity of this information will be maintained[2];

Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured[3;]

Regulatory and legislative requirements will be met[4];

A Business Continuity Management Framework shall be made available and Business Continuity plans will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans should be maintained and tested[5]; the form of these security measures will vary according to the nature of business and the particular risks that it must address.

HCS shall communicate the information security policy to all users in a form relevant, accessible and understandable to the recipient.

Information security education, awareness and training will be made available to staff[6];

All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response[7];

Policies, Procedures and Guidelines of Information Security Management will be made available in softcopy format in online through an intranet system to support the ISMS Policy.

Internal Audit Unit has direct responsibility for maintaining the ISMS Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.

All managers are directly responsible for implementing the ISMS Policy within their units, and for adherence by their staff.

It is the responsibility of each member of staff to adhere to the ISMS Policy.

---

[1] This will ensure that information and vital services are available to users as and when they need them

[2] Safeguarding the accuracy and completeness of information by protecting against unauthorized modification

[3] The protection of valuable or sensitive information from unauthorized disclosure or unavoidable disruptions

[4] This will ensure that the organization remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations such as the Indian Copyright Act, Indian Evidence Act and Information Technology Act, Russian Federal laws / legal acts

[5] Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster

[6] Ensure that relevant and effective training is provided to all staff

[7] Ensure that the staff understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready

Information security is managed through HCS Risk Management framework. The framework outlines the basic security requirements and controls that must be in place.

HCS shall review this policy at planned intervals or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness.

- Users shall ensure that they do not send advertisement of sale of assets, invitations, wishes, etc to large groups without prior approval or unless they are authorized.
- Users of HCS systems shall be aware that their information systems and information are not private and the company reserves the right to monitor and audit these from time to time.
- Users will not download or have a copy of client data, documents, files etc. on the local desktop or laptop unless approved by the client.

5.0 ISO 27001:2013 Standards Applicable Controls

Sl No.	ISO 27001:2013 Clause / Control no.	Description
1	5.2	Policy

6.0 Process/Policy References

ISMS Policy Manual

7.0 Definition of Terms

Sl No.	Term/Abbreviation	Definition / Expansion
1	IT	Information Technology
2	HCS	Harman Connected Services

8.0 Administrative Information

Head – IT will be the final authority to handle all exceptions or conflicts in this policy. This policy will be reviewed on need basis and at fixed interval of once in year.