INFORMATION TECHNOLOGY POLICY MANUAL

CONTENTS

1. General

Policy Management

These policies are created and intended to provide required level of protection of information with respect to confidentiality, integrity and availability. The policies development is a dynamic process and requires involvement of all members of organization in view of continuously changing threats, risks as well as statutory and regulatory compliance, simplicity and ease of use.

- In general, unless otherwise specified,
- Approval of the IT Security Policy is vested with the HOD IT of the organization.
- Advice and opinions on the Security Policy will be given by Management.
- Formulation and maintenance of the policy is the responsibility of the HOD, IT of organization.

Policy Implementation

Each user of Harman will be responsible for meeting the requirements of these policies. Information Security of each system will be the responsibility of its custodians who are responsible for the proper care and use of IT resources under their direct control. Harman IT shall ensure necessary technological interventions, monitoring and provide facilitation of these policies.

Custodians/Information Assets Owners

Harman IT will be the custodian of all central system platforms, security equipment, storage media, documentation and spares etc. Harman IT will also be custodian of the Data Center Individuals will be custodians of allocated equipment such as desktops, laptops, smart phones, tablets etc. under their control. HR will be custodian of personal records which may have information security related compliances such as non-disclosure agreements, release checklists etc.

Policy Documentation

It is intended that this IT Security Policy be publicly accessible in its entirety via the Intranet Site. There is the requirement that all users of Harman IT resources be familiar with relevant sections of this policy.

Policies Changes

The IT Security Policy document will be reviewed on regular basis and altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived risks etc. Major changes will be made in consultation with Harman IT, and with the approval of HOD IT.

2. PURPOSE

Harman Finochem Ltd. depends on its information systems, data, equipment and information processing capabilities. This policy details employees' responsibilities for information systems security and care of IT related assets. Every employee must be aware of these risks and act in a way to protect M/s Harman Finochem Limited.

3. SCOPE

The policy applies to all Harman Finochem Ltd. Group employees, contractors, and temporary workers, as well as anyone to whom Harman Finochem Ltd. gives access to its systems, hereinafter collectively referred to as "employees"
Uses of IT assets, data, systems and applications owned and operated by M/s Harman Finochem Limited

Policies defined in this document are applicable to Software Product, Version Management Tool, IT Network, IT Infrastructure, IT Assets, Information assets, IT resources, Users, Visitors, Employees, Work area, Physical storages, Cloud storage, Peripherals, Suppliers and other stake holders (as applicable).

4. POLICY

4.1 User identifications and passwords for application

User credential are an important aspect of information security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Harman's entire corporate network. As such, all Harman employees (including contractors and vendors with access to company's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Company information systems must only be accessed with a unique User identification (User ID).

4.2 Each site is having User Account Management Policy/SOP.

4.3 Basic Policy for User ID and password as follows:

4.3.1 User ID Creation

The user ID shall be unique for each individual with alphanumeric characters contain 3 alpha characters from initial letter of first name, initial letter of middle name and initial letter of last name with user Employee ID numeric digits. (E.g. User name: George Walker Bush, Employee code: 1234 User ID will be: GWB1234).

4.3.2 Password Policy

After logging in for the first time, each user shall change his password as generated at the time of user ID creation, in order to maintain the secrecy of his/ her password.

4.3.3 Each user shall be accountable and responsible for actions initiated under his/her password usage.

4.3.4 User names must never be used by more than one person.ie users must not share their username and password.

4.3.5 Passwords must not be revealed to any other persons.

4.3.6 User should ensure that his password is confidential and not known to anyone in order to maintain the authenticity, confidentiality and integrity of data generated under his password usage.

4.3.7 Users must never write down their username and password in an unsecure place.

4.3.8 Users must never save their passwords to the internet browsers
Each password shall be alphanumerical with special characters having at least 8 characters long, in order to avoid easy detection and

4.3.9 MUST contain at least uppercase letter.

4.3.10 MUST contain at least lowercase letter.

4.3.11 MUST contain at least number.

4.3.12 MUST contain at least special character (!"#$%&'()*+,-./:;<=>? ...)

4.3.13 Each user password shall have an expiry period of maximum 90 days, after which the user have to change his/her password, either on being prompted by the system or otherwise.

4.3.14 Users will be prohibited from re-using the last 10 previously used passwords.

4.3.15 User account shall be locked in case user tried 3 illegal attempts.

Note: All types request covered under this procedure are only applicable for Computer used for application software's.

Do not share company passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Harman information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to anyone.
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call Harman IT. Do not use the "Remember Password" feature of applications (e.g., Eudora, Netscape Messenger etc., unless it is integrated with AD by Harman IT). Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system (including Palm Pilots or similar devices) without encryption. Change passwords every month. If an account or password is suspected to have been compromised, report the incident to Harman IT and change all passwords.

5. DO'S AND DON'TS

5.1 Every employee is responsible for the protection of company assets and security, including all IT related equipment, systems and data.

5.2 Information systems resources and technology shall only be used for purposes related to Harman Finochem Ltd. business by Harman Finochem Ltd. employees.

5.3 Any user detecting an actual or a suspected security breach as defined in this policy is responsible for promptly reporting the event to IT Administrator.

5.4 Stealing or unlawfully copying software or data is subject to disciplinary action.

5.5 Storage, upload, download or use of illegal software and other digital material (e.g. music, movies, and pictures) on Harman Finochem Ltd. IT equipment is prohibited and could lead to disciplinary action.

5.6 Employees are not allowed to use their personal Software and hardware on the Harman Finochem Ltd. Network.

6. ACCESS TO EQUIPMENT

6.1 Only authorized persons whose work requires will be allowed access to information system resources:

6.2 Harman Finochem Ltd employees involved in processes requiring the use of information technology.

6.3 Consultants and temporary employees involved in processes requiring the use of information technology.

6.4 Vendors to the company who require access to information systems to provide IT support services. Categories specifically excluded.

6.4.1 Vendors of the company not requiring IS support services

6.4.2 Competitors

7. DATA

7.1 Implementation, maintenance and security of the M/s Harman Finochem Limited Network (M/s Harman Finochem Limited) is under the control of IT Administrator. Any change to M/s Harman Finochem Limited configuration must be authorized by IT Administrator. Necessary safeguards must be in place to ensure that unauthorized persons cannot unlawfully access M/s Harman Finochem Limited.

7.2 By default, external consultants have no access to generally shared M/s Harman Finochem Limited, and will only be granted access to specific data or specific systems after having appropriate non-disclosure or confidentiality provisions.

7.3 Respective department is responsible for compliance with local regulations including the relevant rules on the privacy of data.

7.4 Corporate data should not primarily reside on user's computers. These should be viewed as temporary data storage devices. Data must be transferred by user to departmental folder as soon as possible.

7.5 Every employee is expected, when required, to classify data in order to understand how data should or should not be exposed to other inside or outside of the company. IT Administrator may provide further guidance.

8. E-MAIL

8.1 The purpose of using the Harman Finochem Ltd. e-mail system is to conduct Harman Finochem Ltd. business.

8.2 The Harman Finochem Ltd. e-mail system is mandatory for sending e-mails containing any Harman Finochem Ltd. business related contact.

8.3 The Harman Finochem Ltd. e-mail system is mandatory to be used for all Harman Finochem Ltd.-related e-mail communication within Harman Finochem Ltd. and externally with third parties, vendors, customers, authorities etc.

8.4 E-mail messages created or sent using the company's e-mail systems may not contain illegal or otherwise considered offensive or disruptive content. Such content includes, but is not limited to: obscene or harassing language or images, racial, ethnic, sexual or gender specific comments or images or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, national origin or age.

8.5 Transfer via e-mail or the Internet of confidential information personal information or information which Harman Finochem Ltd. considers proprietary must be done with caution and in a manner designed to protect the confidentiality of such information. Any employee transfer Harman Finochem Ltd. such information is responsible for appropriately safeguarding it.

8.6 It is the responsibility of all employees to be aware of risks attached to email usage (e.g. phishing, virus and other malware attacks) caution must be exercised to avoid disruption or systems or unintended disclosure of company information.

8.7 It is prohibited to forward mails from Harman Finochem Ltd. into personal non-company related email accounts and vice versa. Personal email accounts are not to be used for Harman Finochem Ltd. business.

8.8 For the purposes of auditing compliance with this Policy and general system administration, and to the extent legally feasible, Harman Finochem Ltd. reserves the right to access and read e-mail messages created, sent or received using the company's e-mail systems.

8.9 Creation, deletion and disablement of email account of any Harman employee will be the responsibility of Harman IT upon approval by an appropriate authority.

8.10 Users have to download their emails from the Mail Server on daily basis or as required. In other case IT will have the right to block the email Id. This is applicable to the users who don't have the roaming permission.

8.11 In case of roaming users, email storage on servers will be restricted to 25 GB and in case of a user crossing this limit, account will be automatically blocked. Hence such users are expected to archive the emails frequently from the Mail Server based on the requirements and messages received.

8.12 To prevent tarnishing the public image of the organization. When email goes out from Harman, the general public will tend to view that message as an official policy statement from the organization. Attachments types and size of attachments are restricted by Harman IT for avoiding misuse of email services.

8.13 Following is strictly prohibited use of emails services:
Harman's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, email background, political beliefs, or national origin.

8.14 Employees who receive any emails with this content from any Harman employee should report the matter to their supervisor immediately.
Using a reasonable amount of organization's resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.

8.15 Sending chain letters or joke emails from any Harman email account is prohibited. Virus or other malware warnings and mass mailings from Harman shall have to be approved by the appropriate authority before sending. These restrictions also apply to the forwarding of mail received by an Harman employee.

8.16 The employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Harman IT may monitor messages without prior notice. However, Harman IT is not obliged to monitor email messages.

8.17 Email accounts are required to be sometimes disabled due to business reasons so that no email cannot be sent. Guidelines for disabling of accounts include:

8.18 When an employee is terminated or resigns, his or her department authority will have to intimate Harman IT for disabling/deleting his/her email account. As appropriate the Harman IT may, at his or her discretion, allow continuing use of the email account for organization's business and/or provide an automatic reply indicating that the account is no longer active. Forwarding information ordinarily will be included in the automatic reply upon request

8.19 Any account that is inactive for six months may be disabled by Harman IT.Any disabled account that has not received activity after it has been disabled or for which no valid requests for reactivation have been made with in a period of 3 months may be deleted

8.20 Spam, Junk Email, or Unsolicited Commercial Email (UCE) has also been observed many times to be linked with fraudulent business schemes, chain letters, and offensive and inappropriate messages. Harman IT cannot protect email users from receiving mail that may be offensive to them. However, Harman IT attempts to block as much spam as it can without hindering legitimate communications. Some things users can do about spam:

8.21 When any user receives spam mail, the same can be deleted/blocked.

8.22 Never click on any web links or open attachments associated with spam. If you are given the "option" to remove your address, do not do it unless you are certain the organization is reputable. More often, this is just a way to verify that your address is still actively used and therefore more valuable.

8.23 Never reply to spam. If a spammer does anything with a reply, it is to collect the removed addressed and put these on a list of known good addresses.

8.24 In most mail readers, such as Outlook, Eudora, or Netscape, you can create filters to automatically delete messages (or send them to specific folders for later deletion) with certain subject lines. Search for "spam" in the online help for your mail reader.

9. INTERNET USAGE

9.1 Internet access to Harman employees will be administered by Harman IT upon approval by an appropriate authority.

9.2 Harman IT, from time to time, will review the internet usage pattern and may restrict access to websites being visited by users or a particular user, if required.

9.3 When you surf the web at work, follow these security rules to be sure you use the Internet responsibly and securely, and primarily for business purposes.

9.4 Authorized users are allowing to access internet facility. The purpose of using the Internet via Harman Finochem Ltd.'s IT system is to conduct Harman Finochem Ltd. business.

9.5 It is not allowed, via Harman Finochem IT systems, to visit Internet sites that contain content that is illegal or content that may be considered offensive. Offensive content includes but is not limited to Armory, Explosive, Sexual or National.

9.6 Downloading of non-business related information from the Internet via Harman Finochem Ltd.'s IT systems is not permitted.

9.7 Report any misrepresentation of the company (e.g. phishing scams pretending to be Harman Finochem Ltd.) to IT Administrator.

9.8 For the purposes of auditing compliance with this Policy and general system administration, and to the extent legally feasible, Harman Finochem Ltd. reserves the right to monitor the usage of the Internet via Harman Finochem Ltd.'s IT systems.

9.9 Don't post sensitive company information or company-related comments on message boards, in chat rooms or anywhere else on the Internet.

9.10 Don't visit inappropriate Internet sites.

9.11 Some examples of inappropriate sites are pornographic, game and gambling sites or any disruptive, discriminative or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, religious beliefs and practice, political beliefs or national origin.

9.12 Be aware that in many companies, network-monitoring software keeps track of the websites that users visit. In many cases, access to inappropriate sites is blocked

9.13 In the case of certain rogue web sites, the very act of visiting the site could pose a virus hazard. This is an important reason to primarily limit your use of the Internet to conventional and business-related purposes.

9.14 Don't download non-business-related files to your company's network or to your company-issued computer.

9.15 Some examples of inappropriate downloads are screen savers, music files, audio files, graphic files, pornographic files, software and software utilities.

9.16 Downloads from the Internet are often virus hazards.

9.17 Downloading to a company network takes up precious storage space, decreasing the availability of an essential business resource.

9.18 Harman's network is protected by manageable Firewall whose policies are reviewed periodically based on the guidance of operations and attacks encountered. Harman's external Internet firewall policy is to deny all external Internet traffic to the Harman's network unless explicitly permitted. Access and service restrictions may be enforced by IP address and/or port number. Proxy services

10. PERSONNEL GADGETS

10.1 Personnel Gadget not allowed to use in office premises

10.2 If any employee wants to bring Personnel gadgets to office regular basis, need to take the approval from Department head and share the approval to IT Administrator.

10.3 If any gadget brings to office without department head approval, then it should be registered in security gate while brining to office.

10.4 Unregistered gadgets will be seized by security guards while checking the baggage's. That will be considered and used as Harman Finochem Property.

11. COMPUTERS AND IT DEVICES

11.1 Harman Finochem Ltd IT equipment and devices must enforce password protection. Password protection must be prompted automatically when device is left inactive.

11.2 Lost or stolen equipment must be reported immediately to IT Administrator / Admin in order to limit potential damage such events could cause to company data.

11.3 IT equipment should not be left unattended in public spaces.

When working outside the office (e.g. airport, train, café) exercise caution when entering passwords and working on confidential data. Someone could be looking over your shoulder.

11.4 Exercise caution when connecting to public internet outside the office. Always select the more secure option if prompted with a choice. Avoid performing financial transactions or working with confidential data while connected to unknown networks.

11.5 Do not connect unknown flash drives (e.g. USB-key, memory cards) to your computer or mobile device. Do not open unfamiliar files on your flash drive. These could contain malicious software.

12. PROCEDURES, STANDARDS AND SERVICES

Information Security Procedure

The Harman Finochem has the right and obligation to manage, secure and control access to its Information Technology resources, including electronic files and data. Employees are expected to use these resources while protecting the resource's security and appropriate level of access.

Property right

Harman Finochem has the right to protect all information, business and scientific applications, computer and network equipment. Harman Finochem considers as property, all records, software and software that are part of a program's information system. As Harman Finochem property it is to be used for business purposes only. A "record" includes any images, letters, photos, computer tapes, disc, or any other form.

Disclosure of Information

Employees are to access and use Harman Finochem information technology resources for business purposes only. Disclosure of Harman Finochem information or data to individuals or entities (whether employees or not) without a business need to have known such information is prohibited. Harman Finochem information or electronic data may not be transmitted over the Internet or via email except for business purposes to authorized recipients. Confidential client or employee information may not be transmitted to persons or entities that are not authorized to receive such confidential information

Reporting Suspicious Events

Any observations of suspicious activity must be reported to the IT Infrastructure team. Suspicious activity can include: signs of unauthorized IT systems usage during non-Department hours, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on network servers and abnormal activity recorded in log files.

Access Security
Appropriate safeguards must be in place to limit physical access as appropriate to network, computer or computer-related devices. The IT department is responsible for locating servers, networking equipment in an environment that protects them from unauthorized physical access.

Employees must protect their computers by logging off when unattended or by placing the computer in lock" mode by pressing Ctrl+Alt+Del then choosing "lock Workstation." Computer hard drives must not be shared with any other
Computer or person. Employees must also not leave unattended portable computing devices such as notebooks, laptops, and PDA's, unless the device has been physically secured. When traveling, these devices should remain with the employee's carry-on luggage.

Remote External Access
Remote external access to the Harman Finochem network requires approval from a departmental functional head or his designee. The IT infrastructure team will provide such access and authentication methods.

13. POLICY ENFORCEMENT

Execution against this policy and the supporting SOPs, standards and services are subject to regular audit by external agencies and Harman Finochem Ltd. appointed staff. Deviation from SOPs or absence thereof can lead to critical observations which may jeopardize Harman Finochem Ltd.

14. MALWARE/ANTI−VIRUS POLICY

To establish requirements which must be met by all computers connected to Harman networks to ensure effective virus detection and prevention.

This policy applies to all Harman computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to desktops, laptops, smart phones, tablets etc. and any PC/Server based lab equipment's.

Policy and Guidelines:
All Harman computer systems must have company's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Harman IT is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Harman's networks (e.g., viruses,

worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Harman IT should monitor the Antivirus Server daily for virus list/Antivirus engine updations. A log file should be maintained for reports generated by the antivirus server related to the client updation and virus infection. Internal users are informed about any warnings related to new virus/worm/Trojan by Harman IT to avoid hoaxes.

Recommended processes to prevent virus problems are given below:

1. New viruses are discovered almost every day. Follow the specific guidelines that are sent by Harman IT periodically to ensure system protection.
2. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
3. Always scan a floppy diskette from an unknown source for viruses before using it.
4. Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
5. Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
6. Delete spam, chain, and other junk email without forwarding, in line with organization's Acceptable Use Policy.
7. Never download files from unknown or suspicious or untrustworthy sources.
8. Backup-up critical data and system configurations on a regular basis and store the data in a safe place.

15. LAPTOP POLICY

Laptop computers provide important functionality for specific purposes, allowing staff to have computing resource at hand in meetings/trainings, enabling those who travel on business to be maximally functional and productive while away, and those who occasionally work at home to eliminate duplication of resources and efforts. Along with the privilege of using laptops, there comes an additional responsibility to safeguard them from potential theft or damage. If a laptop is stolen or lost there are additional security implications for any data that might have been stored on that laptop. This policy addresses actions that must be taken in order to minimize the risk of the theft of laptops and the associated costs. All employees should take extra care of laptop which are provided to them.

This policy applies to all the employees, managers, team leaders, directors, board members, consultants and third party vendor who are using company owned or personal laptop. Laptops owned by company should not be used for any person use.

Policy and Guidelines:

Following are the responsibilities and liabilities for Laptop User

- All users are personally responsible for the security and safety of their assigned laptop.
- All users are personally responsible for full repair or replacement cost if the laptop is damaged or made inoperable by gross misuse or negligence.
- Department or employee who has loaned the laptops from Information Technology Department for use will be liable for the replacement or full repairing cost of the unit in case laptop got stolen, lost, damaged or if it is not returned in legitimate time duration.
- Failure to follow this policy and these procedures may result in loss of computer or laptop privileges. The Information Technology Department provide support to fulfill needs and issues of laptop users when they are in office or out-stationed.

Physical and Data Protection

- Each user who is using laptop is responsible for the security of that laptop, regardless of whether the laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport. Users are expected to provide reasonable care and effort to protect the laptop.
- Laptop should not be transported or shipped in any condition using couriers.
- The Laptop may not be transported as checked in luggage on public transportation (airplanes, trains, and buses). The user will keep the equipment in their possession at all times while traveling.
- Carrying cases and laptops should be labeled accordingly with mobile numbers so that in the event of a loss the equipment might be returned.
- Special care should be taken with the security of the laptop. Laptop must not be left unattended in public areas. Do not leave your office unlocked, even for a brief time, if your laptop is not secured in the office.
- Do not store laptops in a locked car as there are cases when laptops are stolen by breaking window glass.
- User who is using laptop must scan with antivirus software which is installed on laptop on regular basis.

Inventory Tracking and Disposal

- Upon resignation, the laptop, all peripherals, and carrying case need to be returned either to the Information Technology Department on or before the last day of work.
  - Do not give the laptop to anyone else for use. Doing so will be considered misuse of the equipment.
  - Employees who are taking administrative leave must have prior approval from their immediate supervisor before taking a laptop while on leave.

- Information Technology Department must maintain basic records of laptop allocation (e.g., user name, type of laptop, Laptop issue date).
- If the laptop does not have a barcode, then the unique identifying number along with details of OEM should me identified by bar cord or with unique numbering patter.
- Identification of laptop should be visible and must contains logo or name of company, Asset number, OEM details etc. Identification should be clearly visible on.
- Information technology department should conduct inspection on regular basis to check health and identification of Laptop.
- When a laptop reaches the end of its useful life, it should be returned to the Information Technology department along with all the equipment and accessory which were provided at the time of issuing laptop.
- Information Technology Department will provide laptop with similar or higher configuration to uses who has return laptop which reaches to the end of its useful life.

Reporting Loss

- In an event laptop is theft or lost concern user should immediately report incident to Information Technology Department, Human Resource Department and respective manager or team leader and call Helpdesk. User must provide police report or FIR to HR department.

Following Laptop Security Tips may be considered:

- Back up all irreplaceable information daily. Maintain copies of important data somewhere other than the laptop. You might consider using an external portable storage device.
- Be sure to back up all data, and make use of encryption features when you do so.
- Exit out of programs prior to shutting down your laptop to avoid data loss and program corruption.
- Never handle or manipulate a drive while it is operating.
- Carry your laptop with you in a very non-descript carrying case, perhaps a backpack. Make sure your carrying case is sturdy, weatherproof, and padded. Keep it with you at all times, never place it on a seat beside you.
- Never leave your laptop in open view in your car. Lock it in your trunk.
- Save a copy of your purchase receipt. Copy the serial number and description of your laptop.
- Consideration required to use a disk drive lock to prevent unauthorized access and operation of the computer
- Protect the data and access of the computer with strong password and or a hardware key device. Hardware key products include fingerprint identification devices or other access control devices that plug into the USB port.
- Tape some ID, such as a nametag or business card, to the top of your laptop. This makes your laptop easy to recognize when you send it through airport X-ray, and makes it easier to return to you if it gets lost.

- When you travel or commute, guard against laptop thieves. The most valuable part of a stolen laptop is the data. Many groups have cash premiums out for particular information that can be resold for identity theft or competitive use.

    - If possible, carry your laptop in an inconspicuous bag that does not look like a laptop bag.
    - Never leave your laptop or laptop bag unattended.
    - Keep your arm (or leg, if you set down the bag) through the strap.
    - Never leave your laptop or laptop bag in a visible area of a car; it is best to take it with you out of the car whenever possible.
    - If you place your laptop in the trunk of your car, place it there before you leave for your destination, not after you are parked at your destination. Thieves watch for people who place items in the trunk and then walk away from their car.
    - In your hotel room, lock your laptop with a security cable if left unattended for short periods, and use a hotel safe to store your laptop when you are out of the room for longer periods.
- When traveling, never check your laptop as baggage.
- Never put your laptop on the airport security x-ray machine belt before you have a clear path to the end of the belt.
- Take extra care at times and places where you can be easily distracted, such as:

    - At an airline or rental car counter, when going through airport X-ray, while waiting for a flight
    - While speaking to someone, whether in person, on a mobile phone or on a pay phone
    - While on a train or bus
    - While loading luggage into a taxi - keep your laptop bag with you inside the taxi
    - When a stranger distracts you by asking for assistance or bumping into you - it could be a decoy.
- Report a missing laptop immediately to Harman IT, and to all the concerned people in the company who are responsible for physical and information security.

Following steps can be taken at the BIOS level to further protect your laptop from unauthorized access:

Configure the BIOS to boot from C: then A: Any internet source BIOS will allow user to configure the primary drive to boot from during startup. By selecting **C: then A:** over the default settings of **A: then C:,** one can prevent an attacker from forcibly booting the system from their own customized boot disk. In situations where you may need to startup from a boot disk, reverse the BIOS options to **A: then C:.** When you are finished, don't forget to reinstate the original BIOS boot option.

Enable BIOS passwords: To ensure that an attacker does not reconfigure the BIOS to allow them to boot from a disk drive, enable the BIOS password system to protect BIOS configuration. This will require a password to be input before the computer will boot.

16. BACKUP POLICY

Purpose:

Backup is a copy of files and programs made to facilitate recovery if necessary. The purpose of this document is to set process in which backups of servers, critical network equipment's which includes network switches, firewall, routers and Wi-Fi device backed up their configuration and business critical data which are residing in server/storage

Scope:

This control applies to all systems, people and processes that constitute Harman's information systems, including Harman IT as well as users of all levels such as senior management, employees, suppliers and other third parties who have access to the systems and generate business critical data which needs to be backed-up.

Policy and Guidelines:

Lack of proper backup procedures can result in unavailability of the critical information in case of a disaster or Information Security Continuity situation. Considering that the organization is highly dependent on IT, loss of data can have direct financial and non-financial implications in the event of a disaster or Information Security Continuity situation.

- Backup media should be labeled properly giving details such as;
    - Type of backup
    - Date of backup
    - Date for overwriting /expiry date
    - Name of the person responsible
    - Name of the application
- The backup procedures should be documented for each application.
- Log should be maintained for all the backup activities. Back-up media register is updated for receipt and issue of back-up CDs/Tape drives/Portable hard-disks.
- Once every six months at least 2 random Back-up devices (Tape Drives/Portable Hard-disks etc.) are tested for restoration test and records maintained
- Don't keep back-up CDs/Folders/Tape Drives/Portable Hard-disks without zipping and password protection or encryption

Following guidelines are required to be adhered for user level backup:

- The responsibility of user level back-up is individual PC User/information user.
- Harman IT has made provision of a Backup Server for individual users where only important files from my document except jpg can be stored.

- User needs to take the backup of their own document, not on my document files excel worksheets, email (PST) etc. on this sever.
- In case of a disaster, the user himself will be responsible for loss of data residing on his PC.

Following guidelines are applicable for mail server backup:

- The responsibility of mail server back-up is Harman IT.
- Every day the backup of E-Mail server is taken by Harman IT.

Following guidelines are applicable for database servers backup:

- The responsibility of individual application data servers is DBA/Project Leader.
- Database of individual applications will be backed up every day on the DAT which can be over-written only the subsequent week. This means that a day's backup will not be overwritten for a week. Also, weekly backups and a month-end backup will be taken on DAT and stored in a safe off-site location at a safe distance to ensure availability of data in case of a building wide disaster. Monthly backup tapes are maintained for current year. Yearly backups are stored permanently and will not be overwritten.

Following guidelines are applicable for source code backup

- The responsibility of source code back-up is individual application DBA/Project Leader.
- Source code of programs will be backed up on the CD once every month and is overwritten.
- The backup files are stored with Harman IT.

Backup of the company's data, information and configuration of critical devices are very crucial and needs to be protected against the loss of information. The data will be backed up daily through online parallel server backup utility. Backup application will be scheduled to take a daily and weekly backup of the data.

There will be a daily incremental backup (i.e., Monday – Friday) for the critical data of the company, a full weekly backup on every Saturday's both scheduled through Backup application and a full monthly backup may be schedule by Harman IT

The logs of the backup shall be maintained and will be monitored by the HOD IT.
Below mention details are reviewed by the Information Technology Department at least once per year based on risk of not having the back-up when required during an information security continuity event.

- Frequency of backups
- Types of backups
- Timing of backups
- What needs to be backed up

- How CD or external drives or tapes are used and managed
- Arrangements for offsite storage of back up media
- Back up media retention period
- What regular reports are produced
- How disaster recovery information is saved

Backups are performed to a set of backup media such as portable hard disk/LTO, webserver, back-up server, CDs/DVDs etc. Weekly backup media (tapes) are stored offsite.

In case of any backup failure, it must be escalated to the concern manager or team leader of Information Technology department. A full backup must be scheduled to run immediately if the daily incremental backup has failed after informing the same to the IT manager.

The backup must be restored periodically at least once in Six months with the most recent backup and logs will be maintained for the same.

In case of any errors in the restore, it has to be escalated to the IT Manager and an immediate action must be taken to find the Root Cause Analysis and must be resolved. Backup schedule is maintained to keep a track record of data which are backed up and restored on time-to-time basis.

Following guidelines are applicable for back-up restoration:

- If the current data contained in the computer is lost, the backup files will be used to restore the system. Any transactions that have occurred since the time of the last backup will be entered into the system to finish the complete restoration of the data files.
- Backup arrangements for individual systems are regularly tested to ensure that they meet the requirements of information security continuity plans.
- Restoration procedures are regularly checked and tested (at least once in Six months) to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
- Back-up media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.\
- Back-up logs generated out of back-up utility are maintained for a period of 3 months to ensuring all backups are current, secure and accessible.

17. REMOVABLE MEDIA POLICY

Purpose:

The purpose of this policy is to provide directions for use of removable media such as pen-drives, CD drives, portable hard disks, data cards etc.

Scope:
This policy is applicable to all users of removal devices based on the access provided

Policy and Guidelines:

- IT Services Management Team discourages the use of removable devices due to risks of data lost, virus injection etc. The access rights for such removable device e.g., pen-drives, CD drives, portable hard disks, data cards are provided only to limited members based on the justification and approvals by managers. These rights may be provided temporarily by taking precautions such as running an antivirus scan for the removable media
- While removing pen drives the safe removal option is to be used. While inserting or removing the pen-drives/CD etc. care to be taken to avoid physical/mechanical damage to media or ports.
- Users are required to keep safely the removable media such as pen-drives/hard disks/data cards to avoid loss and damage
- When the CDs/DVDs are no longer required, the same should be destroyed by shredding. When pen-drive/data cards are not working the same should be destroyed so as to avoid loss of information contained therein

18. MOBILE COMPUTING POLICY

Purpose:
The purpose of this policy is to set out the controls that must be in place when practicing mobile computing and using mobile devices away from office premises. It is intended to mitigate the risks against loss of theft of mobile device, sharing confidential information over mobile computing, infection of virus and malware and loss of reputation. It is important that the controls set out in this policy are observed at all times in the use and transport of mobile devices.

Scope:
This control applies to all systems, people and processes that constitute the information systems, including senior management, employees, suppliers and other third parties who have access to systems.

Policy and Guidelines:
Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows. However, as the capabilities increase so do the information security risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of an office building. Mobile devices include items such as:

- Laptop and notebook computers
- Tablet devices
- Smartphone

- PDAs

All the employees are advised to not to use their personal mobiles or above given personal mobile computing devices except the authorized users. The company mobile or desk phones should be used by the employees in the operation work areas. All employees are advised to keep their personal mobile computing devices out of operation area.

Following practices must be considered and appropriate controls must be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments. Such procedures should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. The authorized persons using the mobile computing are advised to follow the controls listed below for allowing them to use mobile computing without compromise of information security:

Physical Protection: The authorized users always keep their personal or company mobile computing devices in their physical custody means keep it safe in their cup board or in their pocket and never allowed to keep it in unattended conditions without any physical protection. Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

Access Controls: All such computing devices must be protected by password so that un-authorized person cannot use it.
Cryptographic Controls: If such computing device is used for sensitive information then cryptographic controls must be applied as per cryptographic control policy.

Backups: Back up of the information of such mobile computing devices is taken for the specified folders such as my documents by Harman IT, when the device is made available by custodian for taking the back-up.

Virus Protection: All the computing devices used for the company purpose needs to be protected for virus protection and necessary precautions are taken up. Procedures against malicious software should be in place and be kept up to date. Suitable protection should be given to the use of mobile facilities connected to networks.
Network Connection: The personal computing devices should not be connected in the network of Local Area Network. In a situation where person computing devices are required to connect then concern user are requested to get the help from Information Technology department as they are authorized to connect such devices in the network. No employees are authorized to connect the computing devices in the network and all precautions are taken that by WiFi or LAN connection no mobile computing devices can be connected. Remote access to business

information across public network using mobile computing facilities should only take place after successful identification and authentication and with suitable access control mechanisms in place.

19. ACCESS CONTROL POLICY

Purpose:

The purpose of this policy is to define the standard access control practices for network, servers, desktops, pen-drives, CD drives printers, operating systems, application software etc. The creation of new user accounts and the on-going management of system access are fundamental to the provision of effective information security. This policy provides directions as to how user accounts should be requested, approved, created, amended, reviewed and removed in a secure way which complies with business requirements. Unauthorized access can cause serious damage to the organization and pose information security risks. Dissatisfied employees can use lingering accesses to enter systems or office space. Hackers can use inactive accounts to enter systems unnoticed. Potential damage includes theft of funds, equipment or intellectual property, disclosure of confidential information and/or damage to property or personnel.

Scope:

The policy is applicable to all information assets of the organization whose usages needs to be controlled

Policy and Guidelines:

The access rights for network, various USB devices/CD drives and information systems is provided based on the business needs and the role of the individual. These access rights are controlled using following guidelines:

- This formal process must be followed for all user creations, including those of users within IT Department. The IT team maintains and supports a wide variety of IT systems and the level of access required by individuals to these systems in order to perform their job role will vary widely across the organization. Although the specifics of how users are created will also vary across systems, basic process should always be followed.
- A request for access to computer systems must first be submitted to the Help Desk of Information Technology Department for approval. Applications for access must only be submitted if approval has been obtained from the line manager.
- Access to IT systems should be requested via the IT Service Help Desk. Where online or electronic forms/Ticket systems are available the same should be used. In addition to system-specific details, the details of the business need of access request should always be given.
- Where possible, requests for access are pre-approved based on the role of the user and the basic access rights are provided based on the role.
- All requests for access to a specific desktop/laptop or network resources must be approved by the concern department head/Manager or team leader. This will normally be a manager within the organization with specific responsibility for the

security and use of that system. In some circumstances the system owner may delegate authority to approve requests to the employee's functional manager.

- Access rights are ensured to be commensurate with the tasks users are expected to perform
- A unique user name and password that is not shared with or disclosed to any other user is provided to all users as per the requirements
- It is a user's responsibility to prevent their user name and password being used to gain unauthorized access to organization's information systems by using a strong password, ensuring that the computers are not left unattended and are is locked or logged out
- Users are required to inform the IT Service Desk of any changes to their role and access rights requirements. Employees must only have the accesses their position requires. When roles change, supervisors must withdraw unneeded access rights
- When an employee leaves the organization, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the IT Service Desk.
- When an employee leaves the access rights must be immediately revoked. Harman IT should initiate the systematic removal of accesses based on information from HR.
- When an employee leaves, their supervisor must also ensure that access rights are removed. In case of resignation of employee user rights are taken back by IT and ensured that all passwords in system or remote passwords or e mail passwords given to the employee are changed as well as all his rights are deactivated.
- The IT helpdesk goes to great lengths to track and rescind accesses. However, it is possible to overlook the extent of a user's accesses. The typical user may have more than required access rights. In that case users need to inform to IT Helpdesk to remove unrequired access rights. IT Team also change the access settings periodically to ensure only relevant access rights are only available. It is also other user's responsibility to report any weaknesses related to access rights e.g., if a user notices a former employee in the network.
- User access rights are reviewed at regular intervals to ensure that the appropriate rights are allocated. Admin rights must only be provided to users that are required to perform system administration tasks.

20. INFORMATION SECURITY CONTINUITY POLICY

Purpose:

This Information Security Continuity Plan has been developed to provide guidelines for all Harman employees when an unexpected or undesirable event occurs that disrupts the normal office operations. The procedures and techniques are intended to reduce the probability of undesirable event occurrence, minimize the severity of the effects of an unpreventable disruption, provide a timely response to an emergency, and provide an effective and timely recovery.

The primary purpose of the Information Security Continuity Plan is to provide for the protection and restoration of IT facilities and capabilities, and to reduce the damaging consequences of any unexpected or undesirable event. Information Security Continuity Plan strategies and procedures apply to all operations in the office. It would be extremely difficult and poor management practice to isolate the automated activities and limit the Business Continuity Planning to those activities.

The loss of operational capability may be caused by many types of occurrences, including;

1. Disasters such as fires, floods, power failures, wind storms, tornadoes, and earthquake.
2. Sabotage.
3. Carelessness.
4. Strikes and other civil disorders.
5. Accidents.

A comprehensive Information Security Continuity Plan not only reduces the severity of the effects of undesirable occurrences, it also permits responding in a timely manner and eventual effective recovery.

Scope:

This policy is applicable to all the information security continuity situations identified by the Harman IT Team. This Information Security Continuity Plan applies to all activities and operations in Harman. The plan is intended to provide protection for all information resources, whether automated or manual.

Policy and Guidelines:

- Preparing the Harman Information Security Continuity Plan and maintaining and updating the plan is the responsibility of the Harman IT team. However, other senior management representatives will have specific responsibilities for the plan and will contribute to the overall effectiveness of organization wide Information Security Continuity Planning.
- Backup and recovery actions required for disaster recovery are managed based on Back-up policy. The files that are copied for backup purposes include all master data files, application program files, and system software files. All backup files are logged in and out of the backup storage facility when needed for disaster recovery as per Back-up policy.
- The recovery procedures for equipment, cabling and power are managed by network maintenance team with the help of external agencies and suppliers. If any of the IT equipment needs to be replaced because of an emergency or disaster condition, Harman IT will be notified immediately by user and in turn the Harman IT carryout necessary coordination with the management. Other office equipment that needs to be replaced will also be ordered immediately. On a temporary basis, some equipment may be borrowed from, or shared with, other offices.

- Harman IT shall maintain documents related to IT infrastructure layouts and network diagrams, copy of which will be with the IT Head. Any changes in the network infrastructure will be promptly updated in the document. In the event of a disaster, this document shall be referred to bring up the network in the minimum possible time.
- A hot site building with servers, workstations and network to start the essential services is maintained. The facility is being currently used for software development and can be accommodated to execute essential services.
- The list of key Harman IT employees along with their mobile no/residential no is available at prominent places and with key personals.
- The sensitive areas such as Data Center are equipped with fire alarms/smoke detectors and fire extinguishers. Necessary trainings are provided for operation of these fire extinguishers and the same are periodically checked for availability when required.
- For a reasonable period (half an hour) the UPS, Diesel Generator ensures availability of power. These Equipment are well maintained as well as fuel is ensured for DG set. We have a hot site at Building which has servers, workstations and network to start the essential services. The facility is being currently used for software development and can be accommodated to execute essential services.
- The proactive mechanisms for information security continuity events such as earthquakes proof construction, use of non-flammable material, good electrical cabling, use of reliable equipment/air-conditioners as well as practices of regular cleaning, maintenance and cable dressing shall be followed by the Harman IT Team.

21. SECURE SOFTWARE DEVELOPMENT/ACQUISITION POLICY

Purpose:

The purpose of this policy is to provide direction and guidance to ensure that the Software Development and Acquisition processes has inbuilt security features.

Scope:

This policy shall be applicable to all Software Applications developed or acquired by the organization

Policy and Guidelines:

During the requirements finalization, security features shall also be invariably included in addition to performance and other requirements

Following application development standards shall be adopted by various application developers:

The application should support authentication of individual users, not groups.

The databases should not store passwords in clear text or in any easily reversible form. Rather than encryption tools and techniques may be considered

The workflows should provide for role management, such that one user can take over the functions of another without having to know the other's password.

  - User identification and authentication requirements based on statutory and regulatory requirements, criticality of transactions etc. to be incorporated
  - The application should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
- The system architecture shall be reviewed in the context of good design engineering principles for technology, databases, interfaces and accessibility
- The criteria and test cases for acceptance of the developed or acquired systems need to include security test cases in additional to functional test cases
- The development networks and production networks shall be separate to avoid any information security risks
- The outsourced development parties shall also be required to adhere to the secure development practices by including such requirements in development agreements, source code ownership, privileged access to databases, test data provision etc.
- In the maintenance phase, the information technology team shall download and maintain all latest patches to one central location.
- The applicable patches shall be installed and tested on test desktop for testing and abnormal and any behavior of connectivity, compatibility or features will be reviewed before deciding the application of the patch for all relevant users/network.
- Information Technology team shall also obtain feedback from respective team leader or manager to check the systems and send confirmation. If any problems or abnormal response are faced then the installed patches shall be rolled back and system will be resorted in the working condition.

22. NETWORK MANAGEMENT POLICY

Purpose:

The purpose of this policy is to provide the direction and guidance for the information security during Network Management. The information residing on the Local Area Network/WAN is critical and therefore security measures are required to be implemented to protect the information on Local Area Network/WAN/Cloud.

Scope:

Policy and Guidelines:

- Network details are to be maintained as network diagram
- Network elements and information assets are ensured to be covered under maintenance program.
- Preventive maintenance is done by in-house/external agencies as per warranty/AMC terms and necessary records are maintained
- Use of Local Area Network must be authorized and monitored by the Information Technology Department
- The network is administered by qualified professionals IT Team Lead and assisted by competent technical personnel
- The outsourced network elements installation/cabling and maintenance services are done by competent service provides.

- Any network element is inspected for proper working, packing, physical damage, correct model number, identification and then taken up for installation and configuration. Based on the successful configuration and operation, the system is accepted and included in the asset register
- For any changes in the access rights/location of work station or any other IT support, the Harman IT needs to be requested after due approval from departmental Head.
- Network monitoring and security reports must be generated and reviewed on a daily basis
- The clock of servers are synchronized to the National or International Standard Time so that all the activities log on the network has a valid date and time stamp. The users of standalone PCs/PCs connected to instruments and laptops are also required to ensure the date/time is synchronized with the server date/time.
- When the date/time of the servers/network PCs needs to follow any other date/time standard the change is done only after approval of senior management.
- The desktops are provided to various users and are required to adhere to following guidelines:

    - IT team allocates the desktops to users based on authorization.
    - Use of desktop is permitted for official use only. Only official applications, utilities and programs are allowed to be loaded. In case of any changes required or a new program to be loaded, the same is only done by IT department after permission of managers
    - User should login to given desktop only as per suggested by the IT department
    - Avoid direct disk/folders/files sharing with read/write access unless there is absolutely a requirement to do so. A dedicated shared folder is available for information sharing between relevant departments.
    - In case of any malfunctioning of programs/slow response/hang ups or virus activity, please inform to IT Department.
    - Desktop should be set with password protected screensavers when there is no activity for ten minutes.
    - Users should not change or delete the data which have previously stored by other users in desktop without permission of IT Department.
- The IT Team encourages paperless office and hardcopies printing is to be avoided as much as possible. However, when there is business need the hardcopies are allowed and prints can be taken on network printers. Following precautions need to be adhered to when using a network or standalone printer:

    - Follow the steps to operate as shown by the signs on the printer.
    - On completion of the cartridge, the monitor of the computer where the printer is installed will show the message of its completion. It is the responsibility of the staff using the system at that moment to convey the message to the concerned authority/IT Department.

- On knowing that the printer is not working properly the user should promptly express the difficulty to the concerned authority/IT Department for its repair and for doing the needful.
- The pages will be borrowed as required from the concerned authority/Stores.
- The permission of using the printer by third party shall be granted only by the Heads/IT Department.
- The usage of pages should be done judiciously which is the moral responsibility of each individual towards community and environment and sufficient awareness and consciousness regarding the usage of paper is provided to all users by management.
- Proper type of paper shall be used (e.g., glossy, matte, plain etc.) as required for the purpose.
- Unidentified users shall not be allowed to use printers.
- No employee shall be allowed to use the printer for personal use unless granted permission by the concerned authority.
- The draft and rough print–outs printed on one side shall be filed and they shall be reused. Else they should be collected and shredded. No printouts to be left unattended.

- The capacity of the network with respect to bandwidth, nodes and any up-gradation of network elements with respect to features, speed and memory is planned in annual budget and provided accordingly.
- The IT Services Management team ensure to manage capacity demand by taking actions such as deletion of obsolete data (disk space), decommissioning of applications, systems, databases or environments, optimizing batch processes and schedules, optimizing application logic or database queries, denying or restricting bandwidth for resource-hungry services if these are not business critical etc.
- The inventory of assets is maintained with respect to Asset i.d. Date of Acquisition, Name of Asset, Category of Asset, Broad Specifications, Location, Custodian of the Asset and Remarks. The assets are provided with a unique i.d. which is also labelled/marked on the asset. The category of asset can be hardware, Software, support accessories etc. Any changes with respect to allocation, specifications, configurations or condition of the asset are included in the remarks. Whenever, the asset is required to be sent out for repairs/disposal, the same shall be done only after approval of HOD IT. Whenever, there is a need to send the asset for repair or for disposal, the same is done only after ensuring that the data cannot be retrieved by any unauthorized personnel, which may include requirement to destroy the memory board/devices before disposal as buy-back or electronic waste.

23. EXTERNAL PROVIDERS INFORMATION SECURITY POLICY

Purpose:

The purpose of this policy is to provide directions for ensuring information security during acquisition of third-party services. The use of an external contractor to manage information processing or communication facilities may introduce potential security exposures, such as the

possibility of compromise, damage or loss of data at the contractor's site. Prior to using external facilities, the risks must be identified and appropriate controls agreed with the contractor and incorporated into the contract.

Scope:

This policy is applicable to control of all third-party services with respect to information security aspects.

Policy and Guidelines:

Particular issues that should be addressed include:

- identifying sensitive or critical applications and ensuring that they are better retained in-house
- obtaining the approval of business application owners on such third-party contracts
- implications for information security continuity plans
- security standards to be specified in contracts/agreements and the process for measuring compliance
- allocation of specific responsibilities and procedures to effectively monitor all relevant security activities
- responsibilities and procedures for reporting and handling security incidents for third party contract

24. TELEWORKING POLICY

Purpose:

- The purpose of this policy is to provide directions and guidelines for information security controls during management of operations based on teleworking practices. A Teleworking arrangement is a voluntary agreement between the organization and the employee which usually involves the employee working from home in a separate area of their living accommodation, whether this is a house, apartment or other type of residence away from the workplace.

- The introduction of a Teleworking arrangement, if managed effectively, has the potential to benefit both the individual and the organization. The individual will gain greater flexibility in working arrangements and possibly avoid a lengthy commute to and from an office. The organization is able to retain skilled and experienced staff whose circumstances suit to teleworking and possibly save money on the rental, lease or purchase of office space.

- This policy sets out the key information security-related elements that must be considered in agreeing a Teleworking arrangement. It ensures that all of the necessary issues are addressed and that the organizations information assets are protected.

Scope:

- Though Harman do not requires its employees to work away from the premises, in general, the situation may arise during emergencies or business needs. This policy is documented to handle such situations.

- This policy does not address the human resources aspects of Teleworking such as health and safety, absence monitoring, job performance and contractual issues. These will be handled by the HR department and the same are in place before the Teleworking arrangement begins.

- Policy and Guidelines:
- Users shall ensure:
- suitable protection of the remote computing site against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities
- that the existing physical security of the remote computing site is acceptable, taking into account the physical security of the building and the local environment
- that the communications security requirements are good enough, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system
- that the threat of unauthorized access to information or resources from other people using the accommodation is addressed

Harman IT shall ensure:

- that remote computing is both authorized and controlled by management and that suitable arrangements are in place for this way of working
- that the provision of suitable equipment and storage furniture for the remote computing activities is in place
- the provision of suitable communication equipment, including methods for securing remote access, physical security, the provision of hardware and software support and maintenance, the procedures for back-up and business continuity, and audit and security monitoring

- Remote user's reporting In charges shall ensure that:
- a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the user is authorized to access are clearly articulated

25. Social Media Policy

We want to provide practical advice to prevent careless use of social media in our workplace. We address two types of social media uses: using personal social media at work and representing our company through social media.

Please understand that any content (either own or third party's) which is liked, shared or endorsed by the employee shall be considered as carrying his concurrence and consent in spirit. Caution is thus advised while forwarding, liking or sharing any content that is against the company policy or tries to damage the company's name, goodwill & image either directly or indirectly.

25.1 Using personal social media at work

You are not permitted to access your personal accounts at work. But, we expect you to act responsibly, according to our policies and ensure that you stay productive. Specifically, we ask you to:

- **Discipline yourself**. Avoid getting sidetracked by your social platforms.
- **Ensure others know that your personal account or statements don't represent our company.** For example, use a disclaimer such as "opinions are my own."
- **Avoid sharing intellectual property (e.g trademarks) or confidential information**. Ask your manager or PR or Management before you share company news that's not officially announced. Any unsolicited information related to work or business without proper authorisation may invite legal action not restricted to termination and monetary damages.
- **Avoid any defamatory, offensive or derogatory content.** You may violate our company's anti-harassment policy if you direct such content towards colleagues, clients or partners.

25.2 Representing our company through social media

If you handle our social media accounts or speak on our company's behalf, we expect you to protect our company's image and reputation. Specifically, you should:

- Be respectful, polite and patient.
- Avoid speaking on matters outside your field of expertise when possible.
- Avoid speaking on matters that have not been flagged by the company for the brief or divulgence of information as such
- Follow our confidentiality and data protection policies and observe laws governing copyrights, trademarks, plagiarism and fair use.
- Avoid deleting or ignoring comments for no reason.
  Correct or remove any misleading or false content as quickly as possible

26. BEST PRACTICES

IT divides its documented responsibilities into categories based on industry best practice, and where these are required to be documented in detail to support execution, formal SOPs are developed to support the quality system.

27. ABBREVIATION(S)

SOP : Standard Operating Procedure
IT : Information Technology
ID : Identification
IS : Information System
USB : Universal Serial Bus
HW : Hardware
SW : Software
MPLS : Multiprotocol Label Switching
ISP : Internet Service Provider
ID : Identification
PC : Personal computer
CD : Compact Disc
DVD : Digital versatile disc

28. REFRRANCES :

- ISO 27001 standard for Information Security Management System
- National Institute of Standards and Technology (NIST), An Introduction to Computer Security:The NIST Handbook Special Publication 800-12
- SOC2 Standard for Data Security, AICPA
- US FDA 21 CFR Part11 (Rule for Electronic Records and signatures), [Title 21, Volume 1][Revised as of April 1, 2012]
- EudraLex Volume 4 GMP, Annex-11 : Computerized Systems, 30 June 2012
- WHO – Guidance on Good Data Management, Sept, 2015
- PIC/s Guidance -GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS; July 2021

29. SIGNATURE

Department	Name	Designation	Signature and Date
Prepared By			
IT	**Ajit Chavan**	**System Admin.**	
Reviewed & Approved By			
IT	**Ranjit Desai**	**DGM IT**	