CYBER SECURITY POLICY

1. INTRODUCTION

The purpose of this Policy is to ensure appropriate use of the Company's information technology infrastructure. The Company's policy seeks to place security and privacy policy specifics in order to provide Members and associates with a trusted and secure computing environment, protecting and securing its assets, interests and data.

2. TITLE AND OBJECTIVE

2.1. This Policy shall be called as "Cyber Security Policy" (hereinafter to be referred to as "this Policy")

2.2. The obligations set out under this Policy are mandatory and shall be enforceable between the Company and its Member/s and Associate/s

2.3. Objective of this Policy

- 2.3.1. to prevent unauthorized disclosure of information
- 2.3.2. to prevent unauthorized alteration of information
- 2.3.3. to prevent unauthorized destruction or deletion of information and prevent practices which obstruct or degrade the usability of the information technology resources
- 2.3.4. to safeguard against situations wherein the Company could incur legal liabilities due to unacceptable actions of its Members or Associates
- 2.3.5. to comply with all applicable regulatory and legislative requirements
- 2.3.6. to safeguard HAPL associates having access to HAPL information assets from cyber threats

3. COMMENCEMENT, APPLICABILITY AND BREACH

3.1. This Policy is effective and getting reviewed time to time.

3.2. Applicability:

- 3.2.1. This Policy is applicable to all the Members and associates.
- 3.2.2. To the extent this Policy conflicts with Applicable Law, the Applicable Law shall prevail.

3.3. The obligations set out under this Policy are mandatory.

3.4. Breach of any of the obligations, by a Member or Associate shall invoke the penalty and indemnity clauses as contained in the Policy. In the event of any notice of non-compliance under this Policy, the burden of proof of compliance shall be that of the Member or Associate as case may be.

4. MODIFICATIONS TO THE POLICY

HAP reserves the right to modify this Policy from time to time. Any changes to this Policy shall be duly communicated to all Members and Associates through appropriate channels and would be effective and shall be binding on the Members and Associates.

5. GUIDELINES FOR PROVIDING SUGGESTIONS ON THIS POLICY

If any Member or Associate has any doubts about this Policy or wish to make any comments or suggestions regarding these guidelines, you can email us at info@HAP.com.

6. GENERAL RESTRICTION

6.1. Any Device which is provided by the Company including any personal Device (together with the Data), which is, or has been, engaged in any Communication with or without attachment(s) in respect of any Company information and / or Data; in course of employment or association with the Company will be deemed to be Company asset.

6.2. It is hereby clarified that any Communication through such Device whether such communication is made during office hours or otherwise and / or on a holiday or on working day will be deemed to be made for “official purpose”.

6.3. The Company shall have the right to access, copy, share, transfer, remove, and delete, all Information /Data on Device that is used by a Member or Associate for official purpose. The individual waives his right to privacy in respect of any personal data including photos/ files etc. stored on the Device.

7. RESPONSIBILITIES OF USERS

7.1. User should read, understand and comply with these Guidelines.

7.2. User may make a requisition for Company asset only by contacting System Helpdesk if such Company asset is required to carry out the

entrusted functions. The user should clearly mention the purpose for the usage of the Company asset. Such form needs to be approved by Manager and above of respective departments.

7.3. Laptop may be provided to a user in accordance with the Laptop Policy

7.4. Any deviation in the Laptop Policy shall require approval of Head-IT.

7.5. User should ensure that they are aware of, and understand, the security procedures for the specific Computer Systems they use.

7.6. User should take all reasonable precautions to protect Information Systems against unauthorized access, use, disclosure, modification, duplication or destruction of computer, Computer Network, Computer System, Device, Information System.

7.7. User should use Information Systems only as may be necessary for their job responsibilities.

7.8. User should use available mechanism and procedures to protect their own Data and Data under their control.

7.9. User should ensure that One Drive for Business is configured, and data stored locally is backed up regularly. Usage of external hard disk to store local data back-up is not acceptable. In case an exception is required, an approval along with duration for which access is required and business justification should be obtained from respective Head of Department and Cyber Security team.

7.10. User should use Information Systems in compliance with Applicable Laws relating to electronic activity, confidentiality, copyrights, licenses and contractual obligations.

7.11. User should report security problems/threats or issues to……

7.12. User should acknowledge on email (like machine and adaptor serial number) of temporarily issued laptops at the time of asset allocation.

7.13. The Users shall be solely responsible for the physical security of the devices provided by the company. In the event of loss of Computers other than due to the negligence of the Users, the Company shall provide a replacement.

7.14. User should ensure that the desktop/ laptop provided to user is handled with proper care. In the event of shifting of desk location, user should contact local helpdesk, who will co-ordinate with Admin Department for shifting of IT equipment.

7.15. IT assets allocated to associates are sole responsibility of their reporting supervisors (HAP FPR). Supervisor shall ensure contractual obligation regarding the same.

7.16. On separation from the services / association of / with HAP, a separation request should be raised by respective Line Manager or concerned Business HR.

7.17. On separation from the services / association of / with HAP, user should ensure that for any assets registered with him but in use by the associate, transfer of ownership request needs to be raised with info@HAP.com which should be approved by HOD of the department.

8. POLICY PERTAINING TO ELECTRONIC COMMUNICATION (EMAIL/ TEAMS/ ONEDRIVE/ SHAREPOINT)

8.1. Users shall be provided with access to communication resources through any device shared or for exclusive use depending upon the nature of work and level of the user in the Company.

8.2. Users shall be provided with official email address with permission to receive and send internal and external mail.

8.3. Mail and Mailbox size on mail server shall be decided by the IT department from time to time and communicated to the Users. Request for relaxation of mailbox size shall be considered by the IT department subject to approval by the HOD.

8.4. User should refrain from adding 'Auto-Forwarding' rules on their official email IDs.

8.5. User should ensure that important office emails are not deleted and are archived for any future use.

8.6. Google Meet and Workspace are official mediums of communication and collaboration.

8.7. All temporarily associated Users will be provided with email ids to send internal mail on request from HOD of relevant department. Permission

to send external mail will be given on recommendation by concerned department to IT.

8.8. The Company may monitor, inspect, disclose email or data of any User in the business interests; or required under any law or order of the Court or any Statutory authority(ies); or when there is reasonable ground to believe that Cyber Security Policy is being violated, or has been violated.

8.9. Any deviation to this Policy will require written or email authorization from such user's HOD and HR HOD.

9. ACCEPTABLE USE:

9.1. Email is permitted primarily for official purposes with limited personal use only. It is however advisable that personal email ids be used for unofficial mail.

9.2. Use of official email ids for subscription to newsgroups, interest groups, or any mode of communication through internet will be strictly as per provisions of this Policy. This does not include all sites given access byHAP. Official Email ids can also be used for receiving communications on topics related to official business. A common email ID shall be created and used for all official subscriptions which are to be used by multiple members of the team.

9.3. No Communication for official purposes shall be routed through any means other than through Company provided Devices, Computer Resources, Computer Networks, Email Addresses.

9.4. Accessing email on mobile devices via any Mobile device management (MDM) software as may be prescribed by the organisation.

10. UNACCEPTABLE USE:

10.1. Transmitting internal, confidential, proprietary communication without permission or authority.

10.2. Personal use which can interfere with the Company's computing resources or cause irritation, inconvenience to the recipients or other Users.

10.3. Mass mailers or chain initiation/forwarding i.e. sending or forwarding of any non-business email to more than 2 individual recipients or any group id outside the Company.

10.4. Use of another User's email account without express written permission.

10.5. Revealing password to any other person.

10.6. Sending messages or viewing content which is offensive, discriminatory, inflammatory or defamatory about individual, group or organization, race, gender, religion, national origin, attributes or sexual preferences using official email id or company resources.

10.7. Viewing / Sending messages containing any obscene, indecent or pornographic material.

10.8. Download/ Transfer/ Copy of data from official email, one drive, SharePoint on non-corporate managed machine is strictly prohibited.

11. POLICY FOR INTERNET USAGE

11.1. Company may impose reasonable restrictions in respect of timings, duration, sites etc. in the best interests of the Users and Company.

11.2. ACCEPTABLE USE

11.2.1. Browsing sites or search engines for business related work and furthering the knowledge in areas of expertise.

11.2.2. Limited personal use.

11.3. UNACCEPTABLE USE

11.3.1. Unauthorized access / entry into any third party or Company's Computer System.

11.3.2. Activity resulting in disruption to third party or Company operations

11.3.3. Playing online games, viewing or transmitting sexually explicit content, hacking, gambling or any such activity which is illegal and prohibited under applicable law(s)

11.3.4. Downloading software without permission of the IT department.

11.3.5. Posting unpublished sensitive information either of Company or any third party on social networking sites, groups, blogs etc.

11.3.6. Sending messages or viewing content which is offensive, fraudulent, discriminatory, inflammatory or defamatory about any person. This is in relation to race, religion, national origin, attributes or sexual preferences.

11.4. INTERNET PRIVACY

11.4.1. Usage of Internet via Company's Computer Network is not confidential

11.4.2. All accesses to internet will be logged. These logs will be viewed by authorized IT personnel. These can also be shared with the concerned HOD or HR. Logs can also be shared with law enforcement authorities when called upon to do so.

12. DIAL-IN-ACCESS ("VPN") POLICY

12.1. Users can use VPN connections to gain access to the Company's Computer Network from the outside.

12.2. User should ensure connecting to VPN at least once in a day when working from a remote location/ home.

12.3. It is the responsibility of User with VPN access privileges to ensure that a VPN connection is not used by any non-User to gain access to the Company's information system. A User who is granted VPN access privileges must remain constantly aware that VPN connection between his/her location and the Company is literal extension of the Company's computer network, and that they provide a potential path to the Company's information. User must take every reasonable measure to protect Company assets.

12.4. Dial in access account activity shall be monitored, and if a VPN account is not used for a period of six months the account will expire and no longer functional. If dial-in access is subsequently required, the User may request a new account in the manner prescribed.

12.5. ACCEPTABLE USE

12.5.1. Users shall keep domain password confidential.

12.5.2. Users shall have installed antivirus & its latest updates onto their Computer before using VPN.

12.5.3. Users shall be careful to log out from the Computer on completion of the work.

12.6. UNACCEPTABLE USE

12.6.1. Users shall not save passwords in the phone book of the dial-up adaptor.

12.6.2. Users shall not download/save/store any data on devices other than those that are Company provided.

12.6.3. Large data file transfers over official network

13. PROTECTION OF INFORMATION

13.1. Virus Protection

13.2. Company provided endpoint security platform shall be installed in all the computer systems to protect the system from Virus, Trojans, Malware or any such unwanted programs. A firewall installed at the perimeter of HO & all data centres connected via internet is used to protect internal network from hackers.

13.3. ACCEPTABLE USE:

13.3.1. Users shall ensure that his / her desktops or laptops are configured with the standard anti-virus or any other security software that is used within the Company.

13.3.2. Users shall report virus attacks if any, to the system administrator along with the necessary details like name of the virus, the action taken and the results thereon.

13.3.3. All software shall be installed with help of IT Helpdesk team only. After obtaining approval from reporting manager/ HOD, user should raise a request with info@HAP.com.

13.4. UNACCEPTABLE USE:

13.4.1. Users should not attempt to modify the configuration of the anti- virus installed on their desktops or laptops.

13.4.2. Users should not download or install any shareware or freeware on the Company's Computer systems.

13.4.3. Computer systems without latest updated Antivirus installed shall not be connected to Company's network.

13.5. Securing Data on Desktop/ Laptop Computers

13.5.1. One Drive for Business should be used to backup the data present in the desktop/ laptop.

13.5.2. It is the responsibility of the user to ensure that One Drive for business has been setup and data backup is configured. For any assistance, users shall contact IT Helpdesk team at info@HAP.com.

13.5.3. Data in folders Documents, Pictures and Desktop shall be backed up on Google drive/File server.

13.5.4. Microsoft Teams, Share

13.6. ACCEPTABLE USE:

13.6.1. Users should lock screen with passwords that activate after 3 minutes of inactivity. The screen should go blank after this period.

13.6.2. Users should take back up of all-important Data before travelling. If travel is for an extended duration i.e. for more than 10 days, it is advisable to take a complete backup of the Data

13.6.3. If User's laptop Computer is lost, User must immediately notify the nearest police station as well as the Company's Systems Manager, and give them specific information to identify their laptop Computer.

13.7. UNACCEPTABLE USE:

13.7.1. Users should not leave printouts of sensitive information unattended.

13.7.2. Users shall not share directories over the Computer Network without password protection and specific User-level access;

13.7.3. Users shall not tamper with or attempt to modify the registry on Windows based systems.

13.7.4. Users should not leave laptops unattended in public places.

13.8. Password Use

13.8.1. Passwords help in maintaining confidentiality of data and restricting access to authorized Users. Users are provided passwords to gain access to applications such as SAP, Email, Intranet and other applications.

13.9. ACCEPTABLE USE:

13.9.1. Users should use work group passwords solely within the users of the group.

13.9.2. Users should keep passwords confidential.

13.9.3. Users should select and change their own passwords.

13.9.4. Users should change all Computer System-level passwords (e.g. root, enable, NT admin, application administration accounts, etc.) as per the Company's enforced policy.

13.9.5. Users should change all User-level passwords (e.g., email, web, desktop computer, etc.) at least every 90 days.

13.9.6. Users should conform passwords implemented on server level to the following:

13.9.7. The passwords should be at least 8 characters in length.

13.9.8. Password must include alphabets, numbers and must contain a special character.

13.9.9. Passwords must not contain dictionary words.

13.10. UNACCEPTABLE USE:

13.10.1. Users shall not use obvious and easily guessable passwords.

13.10.2. Users shall not store passwords on computer system in an unprotected form / clear text.

13.10.3. Users shall not reveal passwords to others.

13.11. Safe Disposal of information storage devices

Users should adhere to the following:

(i) Be attentive when handling Device that will be disposed of.

(ii) For disposal of hard disk, pen drives, tablets, mobile phones, they must be formatted multiple times and low level formatting of hard disks must be ensured before disposal of personal devices containing official information.

(iii) CD ROM and DVDs must be broken before disposal. Manual destruction or shredders may be used for the same if available.

(iv) Users shall not dispose external disk drives without following proper process as provided by the Company.

(v) Protection from Phishing attacks and Identity Theft

(vi) Users shall report any suspicious Phishing email received in their mailbox to Cyber Security team by clicking on the button provisioned in their HAP mailbox.

(vii) If the user has fell victim to phishing email i.e. user has clicked on URL and entered credentials or downloaded any file/ attachment, user shall report the details to info@HAP.com for further investigation.

(viii) Protection of data theft via USB or peripheral devices

(ix) No CD-ROM or Pen drive or any other external device should be connected to the desktop/ laptop and all the USB ports should also be disabled.

(x) In case USB access is required for business purpose, exception shall be provided only after obtaining the HOD approval on case to case basis.

14. LAPTOP/DESKTOP USAGE POLICY

14.1. Users shall maintain the integrity and prohibit misuse of device, computers, peripherals and other related resources that may be provided by the Company.

14.2. Users shall ensure that the desktop/ laptop assigned to them is shut down and re-started at least once every week.

14.3. Assigned laptop is given for a period of 5 years post which replacement with New Laptop is done.

14.4. It is Member's responsibility to maintain the equipment and avoid the exposure to damage to the equipment once the device is assigned to the user.

14.5. ACCEPTABLE USE:

14.5.1. Users shall consider the Computer and its related peripherals (mouse/monitor/keyboard/external storage Devices etc.) assigned for official purpose and should not swap with any Computer within or outside their departments. The User should take good care of their assigned Devices.

14.5.2. Users shall maintain the identity of computers by not tampering with the asset ID and vendors Serial No.. User shall inform the IT department in the event of these labels not available on their machines.

14.5.3. It is recommended that temporary files on computers shall always be deleted on a regular basis as this utilizes a lot of disk space and can slow down the performance of the computer. Users must take help from IT support person for doing the same, if required.

14.5.4. User must lock his desktop/laptop (Ctrl+Alt+Del+Enter) while leaving the desk for extended periods of time.

14.5.5. Users are discouraged to share their folders as a normal practice. If at all it is required then the Users may share the folders in "READ only" mode and if required passwords protect them.

14.5.6. Guest Account on Computer Network must be disabled by default and Users shall not be enabling it under any circumstances.

14.5.7. Administrator account must be renamed and must have strong password as laid down by the password policies.

14.5.8. Screen savers with password shall be used to protect the machine from unauthorized access.

14.6. UNACCEPTABLE USE:

14.6.1. Users shall not change the basic input output settings as configured by IT dept. on their computers.

14.6.2. Users shall not use objectionable wallpaper on the device provided to them by the Company.

14.6.3. Users shall not under any circumstances change the hostname or IP address of their Computers.

14.6.4. Users shall not use the "administrator" User account for logging on to the Computer System.

14.6.5. Users should not tamper or dismantle their workstation, Desktops and Laptop Computer or any Devices attached with the computer systems.

14.6.6. Users should not attach any personal Devices with the computer like pen-drive, external HDD, CD writer, floppy drive or any other storage Device including iPods. In case User wants to do it for some business purpose then it should be approved in writing by HOD / Head - IT.

14.6.7. Users should not allow visitors / guest to connect their laptop / any Device with the Company's Computer Network i.e. LAN/Wifi without permission of IT. Connecting devices to projector is allowed. Users can connect only those Devices which are provided by the Company for official purpose

14.6.8. Users should not use the devices for bitcoin mining or any such purpose which is non organisation related.

15. SOFTWARE USAGE, MAINTENANCE AND MONITORING

15.1. Users shall ensure proper utilization of software used at the Company's Computer System and Computer Network and to control unapproved / unauthorized software usage.

15.2. User should ensure that for any purchase of a SaaS (Software as a Service), HAP's Cloud Security checklist should be used for performing the due diligence.

15.3. ACCEPTABLE USE:

15.3.1. Users shall request for installation of new software with an approval from his/her reporting manager. This software must have a valid license. If the license with not available, then user shall share Internal Order for new purchase of the required software.

15.3.2. Justification is required for installation of any particular software and IT may suggest alternate software in best interest of the Company.

15.3.3. Users shall not install software on devices provided by the Company (like music players, chatting messengers etc.) Devices are handled by IT support and they must be informed if any changes are required to be carried out.

15.3.4. Users must ensure that antivirus patches and windows updates are applied on a regular basis.

15.3.5. Users shall not override, disable or change configuration of Windows updates or antivirus updates.

15.3.6. Users shall disable the macros in case a file that is received contains macros that they are unsure about.

16. WIRELESS COMMUNICATION POLICY

16.1. REGISTER ACCESS POINTS AND CARDS

16.1.1. All wireless access points / base/ stations connected to the Company's Computer Network must be registered and approved by the IT department. These access points / base stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards used in corporate laptop or desktop computers must be registered with the IT department.

16.1.2. All wireless LAN access must use Company -approved vendor products and security configurations.

16.2. VPN ENCRYPTION AND AUTHENTICATION

16.2.1. All Computers with wireless LAN Devices must utilize a Company approved VPN configured appropriately to prevent unauthorized access into the Company's Computer Network. To comply with

this Policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong User authentication.

16.2.2. All gateways/routers acting as base stations/wireless hotspots should be configured to log all terminals connected to/through it and the logs should be stored for a minimum period of three months unless specified otherwise specified by any law for the time being in force.

16.2.3. Use of unsecured Wi-Fi such as those found in airports/ coffee shops is allowed only if used along with company provided VPN. This is because any hacker can eavesdrop and gain access to your computer.

17. WORK FROM HOME POLICY

17.1. Users shall be permitted to work from home in accordance with the terms of the Human Resources Department as and when required and intimated.

18. DUE DILIGENCE MEASURES

18.1. Users when using company device or using company resources shall not view, create, host, display, upload, modify, publish, transmit, update or share any information that —

18.1.1. belongs to another person and to which the User does not have any right;

18.1.2. is harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

18.1.3. harms minors in any way;

18.1.4. infringes any patent, trademark, copyright or other proprietary rights;

18.1.5. violates any Applicable Law for the time being in force;

18.1.6. deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

18.1.7. impersonates another person;

18.1.8. contains software viruses or any other Computer code, files or programs designed to interrupt, destroy or limit the functionality of any Computer Resource;

18.1.9. threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.

18.2. The Company shall remove any Information or Data specified in (IT Act 2000, Clause 2) above or Communication link to any such Information or Data within 36 (thirty-six) hours of such Information, Data or Communication link coming to the actual knowledge of the Company, without seeking any permission from the User;

18.3. The Company may preserve such information as is specified in clause 2 above and associated records for at least 90 (ninety) days for investigation purposes;

18.4. The Company may appoint and keep appointed at all times a Grievance Officer to provide information or any assistance to Government agencies who are lawfully authorised for investigative and protective cyber security activity, on a request in writing stating clearly the purpose of seeking such Information or any such assistance. As a part of the investigation, information may be shared with appointed third party without knowledge of the employee.

18.5. The Company shall at no time shall the Company knowingly deploy or install or modify the technical configuration of any Computer Resource or become party to any such act which may change or has the potential to change the normal course of operation of the Computer Resource than what it is supposed to perform, thereby circumventing any law for the time being in force, except where such technological means is developed, produced, distributed or employed for the sole purpose of performing the acts of securing the Computer Resource and Information contained therein.

18.6. The mechanism by which, Users or any victim who suffers as a result of access or usage of IT Devices by any person in violation of IT Act 2000, Clause 2 of these due diligence measures can notify their complaints against such access, may be made publicly available and published on the Company's corporate website.

19. INDEMNITY BY USERS

The User shall hereby indemnify and agree to keep indemnified HAP from or against any loss, damage, demand, claim, penalty, liability including but not limited to third party claims, that are lodged against the Company and that may arise statutorily or otherwise with regard to the breach, non-compliance, mal compliance, part compliance of the obligations of the User as stated in this Policy.

20. SEVERABILITY

If any provision of this Policy is or becomes illegal, invalid or unenforceable, such provision shall be severed and the remaining provisions shall continue unaffected.

21. AMENDMENT

This Policy can be amended by the Company at its discretion. The company may notify any draft amendments to the policy on the Company intranet inviting comments and suggestions. The Company may after considering the comments and suggestions may make suitable further amendments. Such further amendments, if any, shall come into force immediately with effect from the date of such notification of the amendment.