

Life Insurance  
***Beneficiary Nomination Form***

Plan Name :-  
 Policy No :-  
 Emp. No :-

### Beneficiary Details

Name of the Beneficiary*	Age/Date of Birth	Proof Of Identity**	Relationship to the life Assured	% share of benefit	Bank Details***	Communication Address
Dhivagar C	07/04/2003	254461818794	Brother	100	canara	133/5-w, North street, Gokilapuram, uthamapalayam (Tk), Theni(Dt) - 625526

\* If minor, the details of the guardian with proof of identity required

\*\* Original Certificate required

\*\*\* Bank Details required are;

Bank Name :-  
 Bank Branch Name/Code no :-  
 Account No :-  
 Account Type :-

**Employee Signature**

Thamotharan Chandran

(1) Name: ..... Signature: ..... Date:.....

For (Policy Holder) HR use only	
Date of receipt of the form	
Received by	
Signature	



Emp No. :

Full Name. : Thamotharan Chandran

**Nomination Form**

	Sr. No	Nominee	Relationship with the Employee	Date of Birth
<b>F &amp; F</b>	A	Dhivagar C	Brother	07/04/2003

<b>Personal Accident</b>	A	Dhivagar C	Brother	07/04/2003
--------------------------	---	------------	---------	------------

Signature of the Employee

Date :

Dear Employee,

Sub: Data Protection;

The Company's Data Privacy Notice, summarises how we protect your data, our usage of that data and other relevant information. For example, we set out in the attached Data Privacy Notice how we as an organisation collect, use, store, transfer and secure personal data.

When processing data, we have determined that consent is not a necessary basis for the processing of personal data for our day-to-day management of the employment relationship between the company and its employees. Hexaware Technologies will rely on the following grounds to process the personal data: -

**1. Where we need to perform the contract we have entered into with you.**

For example, Hexaware needs to have the freedom to perform the Company's obligations under the employment contract as will be common for any employer for processing personal data. In any case, the Company's employment relationship with its employees (or other types of contracts, e.g. consultancy contracts with our contractors) are governed by the terms and conditions of those contracts. Many of the other general rules of our organisation are covered in part in handbooks and policies to which employees are subject by virtue of the contractual obligation in their contracts. e.g. in respect of health and safety at work and I.T. Policies.

Non-exhaustive examples where this ground, is in our determination appropriate, include providing, controlling and processing:

- Home address details for communication
- Bank details to pay salary or fees under the relevant contract
- Next of kin for life assurance and other relevant benefits
- Details of previous employer for reference purposes
- Personal details to arrange directors' and officers' insurance for a director.

**2. Where we need to comply with a legal obligation.**

Under this ground, Hexaware's processing is necessary for compliance with legal obligations in the countries to which we, as an employer, might be subject to. In the employment context, this could be relevant to pre-employment vetting, performance of the employment contract (overlapping with the above ground), and compliance with legal obligations owed by Hexaware to a third party. Examples might include:

- Pre-employment vetting of the right to work in the countries of our business interests to comply with the relevant regulations and immigration laws to prevent illegal working and to carry out right to work checks on all prospective employees. Dealing with local tax authorities and other relevant authorities
- Pre-employment vetting for example in the financial services industry

**3. Where it is necessary for our legitimate interests (or those of a third party).**

Examples are set out in the attached Data Privacy Notice but include: -

- The usual and expected processing of personal data to maintain the employment relationship
- To protect Hexaware's proprietary and commercially sensitive information and to comply with its confidentiality obligations to its clients
- Processing for direct marketing purposes or preventing fraud
- Transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note: international transfer requirements will still apply)
- Processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems
- Reporting possible criminal acts or threats to public security to a competent authority
- sharing of personal information when required for the business needs with our business partners associates, customers and suppliers

We may also use your personal information in the following situations:

**4. Where we need to protect your interests (or someone else's interests).**

**5. Where it is needed in the public interest or for official purposes.**

If you have any further questions on this matter, please contact the HR Team in the first instance.

Thank you for your assistance.

Yours sincerely,

Contents

1. About this Policy ..... 2

2. Information Processing Asset Security: ..... 2

3. Logical Access..... 3

4. Password Management ..... 3

5. Physical Access ..... 4

6. Software Licensing ..... 5

7. Malware Protection ..... 6

8. Email Use..... 6

9. Internet Use ..... 7

10. Artificial Intelligence and Machine Learning..... 8

11. Social Media Usage: ..... 9

12. Use of Privileged Access..... 9

13. Intellectual Property Rights & Ownership ..... 9

14. Confidentiality..... 9

15. Customer assets ..... 10

16. Onsite deputation ..... 10

17. Awareness..... 10

18. Disciplinary action ..... 10

19. MONITORING ..... 11

20. PROHIBITED USE OF OUR SYSTEMS ..... 11

21. Employee/Contractor/Retainer Declaration..... 12

The Acceptable usage policies along with the user security responsibilities are detailed below.

## **1. About this Policy**

- Our Acceptable usage and User Security responsibility Policies are intended to promote effective Usage of Environment& IT assets and working practices within our organization. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.
- This policy covers all employees, Consultants, contractors, Retainers and anyone who has access to our IT and communication systems.
- Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.
- This policy does not form part of any employee's contract of employment and we may amend it at any time

## **2. Information Processing Asset Security:**

- The information created and used by Hexaware Technologies Limited including all its subsidiaries, affiliates, and / or any other group companies ("we, our") (or) received from our Customers is one of our most valuable assets. Damage or loss of these assets could severely impact our relationships with customers, violate laws and regulations and negatively affect the reputation of the company.
- Given the competitive nature of our business, Hexaware's and Customer's provided information assets must be protected always during and after your employment with Hexaware.
- Users are expected to access only information, information systems and facilities that are needed for performing the responsibilities assigned to them.
- Any information exchanged using Hexaware information assets is not private and may be reviewed, monitored and copied by authorized representatives at any time, with or without notice to employees/contractors/retainers and other users
- All Hexaware employees/contractors/retainers, consultants, trainees ("User") must take the necessary steps to ensure that Hexaware's and Customer's specific assets are properly protected from threats that exist
- Asset maintenance:
  - a. User shall be responsible for the assets, once purchased and handed over
  - b. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting [the IT Department OR [POSITION OR DEPARTMENT]].
  - c. If you have been issued with a laptop, tablet computer, BlackBerry, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords

must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

- d. The user should not abuse the product and cause any physical damage.
- e. In case of any doubts user shall contact the IT Helpdesk instead of experimenting on your own.
- f. The IT team shall be responsible for allotting asset numbers and physical numbering for all assets
- g. In case of loss of equipment or theft, the matter must be reported to the IT helpdesk and Corporate Security Team as early as possible (Within 4 Hours from the time of Loss)

### **3. Logical Access**

- Users must be responsible for all actions taken under their sign-on
- When leaving a workstation, the user is expected to properly log out of all application's and networks or lock the laptop or desktop.
- You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorized in the proper performance of your duties.
- You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our [Privacy Standard OR Data Protection Policy].
- You should use passwords on all IT equipment, particularly items that you take out of the office. You must not use another person's username and password or make available or allow anyone else to log on using your username and password.
- All workstations must have the password protected screen saver activated for unauthorized access to privileged information
- User level and System level passwords must remain confidential and not shared, posted or otherwise divulged in any manner
- You must not attach any device or equipment to our systems without prior approval from your function /supervisor. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.

### **4. Password Management**

- Strong passwords must be used at all levels and have the following characteristics:

- a. Contain both upper and lower-case characters (e.g., a-z, A-Z)
- b. Have digits and special characters as well as letters e.g., 0-9, !@#\$%^&\*()\_+|~-=\`{}[]:~<>?,./)
- c. Requires minimum 12 characters.
- d. Must include at least a digit, special character as well as letters.
- e. Are not a word in any language, slang, dialect, jargon, etc.
- f. Are not based on personal information, names of family, etc.
- g. Passwords should never be written down or stored on-line
- All user passwords must be changed once in 45 days and a password history of previous 6 passwords are maintained.
- Users password will be disabled after 5 consecutive failed logs in attempts.
- Users shall change the password immediately after first logon.
- Unacceptable Password Use:
  - a. Revealing your password over the phone to ANYONE, Through Email Message and to your Manager
  - b. Talking about your password in front of others
  - c. Hinting at the format of your password (e.g., "my family name")
  - d. Revealing your password on questionnaires or security forms
  - e. Sharing your password with family members
  - f. Revealing your password to co-workers while on vacation
- If someone demands your password, refer them to this document or Inform IT helpdesk and Infosec Governance
- Do not use the "Remember Password" feature of applications/systems
- Passwords shall not be written down and stored anywhere in the office. Do not store passwords in a file on ANY computer system
- If your account or password is suspected to have been compromised, report the incident to IT Helpdesk and change all your passwords

## 5. Physical Access

- Access cards shall be used for entry and exit into Hexaware facilities
- Employees, retainers, contractors shall cooperate with security checks carried out by corporate security department
- Employees, retainers, contractors or any other third party shall never access areas which are restricted to them
- Access cards and/or keys must not be shared or loaned to others.



- Access cards and/or keys that are no longer required must be returned to the HR /Admin Department.
- Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to Corporate Security Department. Appropriate action must be taken for revocation, response and escalation.
- All critical facilities that allow access to visitors, third parties, and employees/contractor/retainer without access to the respective facility will track access with a register which shall record sign in/out and other details
- Do not take visitors into the office premises without proper authorization
- Visitors must be escorted in card access-controlled areas including the IT Room.
- Issue of laptop or any other devices to staff/vendors is appropriately recorded and signatures taken
- Employees/Contractors/Retainers are expected to be cognizant of equipment located within their immediate offices and to immediately report missing equipment to IT Helpdesk, Corporate Security Department and Security Guard on duty
- Employees/Contractors/Retainers must not tailgate, and any suspected violations must be promptly reported
- Employees/Contractors/Retainers are expected to report any unauthorized access, entry or suspicious activity to Infosec Governance, Corporate Security Department and Security Guard on duty.
- All members of the staff, third party users as well as all customers of Hexaware, have the responsibility to report suspected violations. Investigation of suspected violations of security regulations will follow established procedures

## **6. Software Licensing**

- Systems Technology Group is responsible for ensuring that the software running on all computers operated or managed by employees/contractor/retainer is appropriately licensed
- All employees/contractors/retainers are advised not to download, install, or use any unlicensed software including free and opensource software
- Employee/Contractor/Retainer shall not use a completely written or partial code available on any opensource forums without appropriate reviews to license conditions and other legal requirements. This shall be done after an approval from STG, IG Team and Legal Team
- All software requests are to be raised in Genie+, and the IT team shall review the request along with Infosec Governance team and shall install the same with proper approvals
- Updates to software must be carried out by IT Team

## **7. Malware Protection**

- Organization approved Anti-Virus must be installed in all endpoints and systems
- Anti-Virus software is configured in such a way that the updates are automatically pushed to the systems. Employee/Contractor/Retainer shall ensure that their Anti-Virus is updated and in the event of any error or issues with updating, they shall report the same to the helpdesk

## **8. Email Use**

- User is expected to exercise due care in accessing the email facility
- Each user is responsible for the contents of his/her e-mail
- Individuals accessing the e-mail services of Hexaware must not use or access an e-mail account assigned to another individual to either send or receive messages
- The user must use only company approved applications as the e-mail customer. Use of any other customer is not permitted
- The following factors are to be considered before accessing and downloading an attachment
  - a. To prevent computer viruses, users must not open attachments that are from an unknown or untrusted source
  - b. In case of any doubt users must be advised to contact IT Helpdesk before taking any action on their own
- Users must not send files with extensions such as .exe, .bat , plug ins...
- All messages sent by users by the company e-mail account are company records. At any time and without prior notice, the management reserves the right to examine e-mail, personal file Directories, and other information stored on Hexaware's Systems. E-mail messages may be monitored for any of the following reasons:
  - a. Ensuring internal policy compliance,
  - b. To support internal investigations for suspected criminal activity and,
  - c. Any other reason which requires the email to be monitored
  - d. Hexaware reserves right to disclose e-mail messages sent or received to law enforcement officials without prior notice to the users who may have sent or received such messages. Users must restrict their communications to business matters in recognition of this electronic monitoring
- Users must not send confidential/sensitive information via e-mail, unless the information is password protected using a company approved technique. In general examples of confidential/sensitive information include:
  - a. Customer Information
  - b. Passwords
  - c. Research and development as well as business strategy information
  - d. Any other confidential information such as PI, PHI, SPII, PCI data etc.

- Users must not automatically forward their e-mails to any address outside the group/company networks, unless approved
- E-mail systems must be used primarily for business purposes only
- Alternatively, users are not allowed to use their personal e-mail accounts for sending official mail. All official e-mail communication must take place via the official e-mail account only.
- Incidental personal use is permissible as long as:
  - a. It does not interfere with normal business activities or hamper user productivity,
  - b. It does not consume more than trivial amount of resources,
  - c. It does not involve solicitation,
  - d. It is not associated with any outside business activity for personal gain,
  - e. It does not potentially embarrass the Company and its management.
- Blanket forwarding of e-mail messages is prohibited as this may use excessive network resource
- Users must not create their own, or forward externally provided e-mail messages which may considered to be harassment, or which may create a hostile work environment.
- Hence, users must not use profanity, obscenities, or derogatory remarks in e-mail messages discussing employees/contractors/retainers, customers, or competitors. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Among other things, a hostile work environment may also be created when derogatory comments about a certain sex, race, religion, political beliefs or disability are circulated
- Except as authorized in the proper performance of your duties, you should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time
- Users shall communicate with the originator of the offensive e-mails, asking him/her to stop sending such messages, and report such offensive e-mails directly to their respective HR BP's and the Infosec Governance Team
- Users shall not use or register their official email ID for any non-business activities like subscribing to a mailing list, creating a social media account, without appropriate approvals

## **9. Internet Use**

- Internet access is provided to all the employees/contractors/retainers and it shall be used for business purposes with due care
- The use or attempt to initiate such activities using companies computing facilities or equipment which could lead to abusive, unethical or "inappropriate" use of the Internet is considered grounds for disciplinary, legal and/or punitive actions, including termination

- . Examples of prohibited employee/contractor/retainer Internet use include, but are not limited to, the following:
  - a. Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company's network or systems, using Internet.
  - b. Conduct illegal activities, including gambling, access or download pornographic/illegal material.
  - c. Enter into contractual agreements via the Internet, e.g. enter into binding contracts on behalf of Hexaware over the Internet, unless you are authorized to do so by the management
  - d. Solicit for any purpose which is not expressly approved by the Hexaware management
  - e. Use Hexaware logos or materials in any web page or Internet posting unless Hexaware Corporate Marketing team and HR team has approved it, in advance.
  - f. Reveal or publicize proprietary or confidential information
  - g. Represent personal opinions as those of the company
  - h. Use software files, images, or other information downloaded from the Internet that has not been released for free public use for official/personal purposes using Hexaware computing system
  - i. Upload or download commercial software in violation of its copyright. Approval must be sort from STG by users before they download any software from the internet.
  - j. Make or post indecent remarks directed at someone or similar written attacks
  - k. Attempt to gain illegal access to remote systems on the Internet.
  - l. Attempt to inappropriately Telnet to or port scan remote systems on the Internet.
  - m. Establish Internet or other external network connections that could allow non-Hexaware users to gain access into Hexaware's systems and information assets

## **10. Artificial Intelligence and Machine Learning**

### **10.1 Usage of Generative AI**

- Hexaware employees shall not use generative artificial intelligence platforms in conjunction with client engagements / deliverables without the explicit approval for the use of these tools in customer agreements or MSAs.
- Hexaware employees shall not use generative artificial intelligence with any internal Hexaware intellectual property without written approval from the CxO levels.
- All use of generative AI platforms must be conducted in compliance with the platform's terms and policies.
- All Hexaware work products created by or adapted in conjunction with generative AI must clearly and appropriately attribute the use of the platform consistent with sharing, licensing, and sharing terms of the platform.
- Any approved use of generative AI platforms to create software, configuration, or data in conjunction with the Hexaware SDLC shall be subjected to the same review process as manually created assets

such as static code analysis, secure code analysis, peer review, and other processes as currently defined.

- Never share details of Hexaware customers, any data related to their projects and products.
- Be aware of intellectual property rights and the impacts of its violations.
- Be aware of plagiarism and its impact on existing and future business.
- Be aware of Brand Impact in case of any password or credential or URL or code / data sharing which could be directly or indirectly associated with Hexaware, its customers and business partners.
- Be aware that all access coordinates, visits, and interactions could be traced back and associated with related social networking and internet content for ever.

## **11. Social Media Usage:**

Refer Social Media Policy :

[http://sp.hexaware.com/sites/Hex/QMS/QMSBackEnd/QMS/Support%20Functions/Human%20Resources/i\\_Social%20Media%20Policy.pdf](http://sp.hexaware.com/sites/Hex/QMS/QMSBackEnd/QMS/Support%20Functions/Human%20Resources/i_Social%20Media%20Policy.pdf)

## **12. Use of Privileged Access**

- Privileged Access is not provided by default to employees/contractors/retainers
- Those needing privileged access shall raise a request with appropriate business justification
- The Access shall be provided only after approval by corresponding stakeholders
- The privileged access shall not be provided indefinitely. The access shall be provided only for a period of 3 months after which it has to be renewed
- Privileged Access shall be carried out with due care and the user shall be liable and responsible for any issues arising because of the privileged access
- Privileged access shall be monitored on a regular basis

## **13. Intellectual Property Rights & Ownership**

- All intellectual property created in the course of employment belongs to Hexaware. All computer equipment, software and facilities used by you are also proprietary of Hexaware, including all documents, materials and Email created.
- Hexaware reserves the right to withdraw any of the facilities provided if it considers that your use of it is in any way unacceptable.

## **14. Confidentiality**

- Handle Hexaware's and Customer's Confidential Information in strict confidence

- Do not disclose confidential Information to any third parties
- Protect confidential information from unauthorized use and disclosure.
- Refer Code of conduct document confidentiality section for more details  
<https://stationh.hexaware.com/NewStationH/Content/Index#/index/webapps>

## **15. Customer assets**

- Ensure Customer provided information assets (Login IDs / Passwords, Secure IDs, Confidential information) are appropriately protected
- Ensure only authorized information (Web sites, Applications) is accessed
- You will be accountable for any misuse of Customer provided information assets

## **16. Onsite deputation**

- Ensure you understand and adhere to the customer security requirements/ guidelines at customer's premises
- Information received from the Customer is to be used only for the Business purpose and protect confidential information from unauthorized use and disclosure.
- You will be accountable for any misuse of Customer provided information assets (Login IDs / Passwords, Secure IDs, Physical access cards, Confidential information) during your assignment at onsite
- Do not misuse email and internet facilities provided at onsite.
- Adhere to Information Security Policy and guidelines of the Customer.

## **17. Awareness**

- Refer to the Information Security Policy and other relevant documents available in the Intranet IG Portal in "StationH".
- Ensure that you attend the awareness training on Information Security that is held periodically and complete the corresponding online assessment within the stipulated time.
- For Mexico Location: Ensure that you attend the awareness training on Information Security that is held during NHT

## **18. Disciplinary action**

- If you ignore the rules and guidance indicated above or misuse and/or abuse the system, its facilities or any property belonging to Hexaware, you will be liable to disciplinary action, which may also lead to dismissal from service. Hexaware will take any breach of these rules very seriously and, your conduct and/or action(s) may be unlawful or illegal and you will be personally liable for such acts.

## **19. MONITORING**

- Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.
- A CCTV system monitors the exterior of the office premises 24 hours a day. This data is recorded
- We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):
  - a. To monitor whether use of the email system or the internet is legitimate and in accordance with this policy.
  - b. To find lost messages or to retrieve messages lost due to computer failure.
  - c. To assist in the investigation of alleged wrongdoing.
  - d. To comply with any legal obligation.

## **20. PROHIBITED USE OF OUR SYSTEMS**

- Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):
  - a. Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).
  - b. Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our customers.
  - c. false and defamatory statement about any person or organization.
  - d. Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy).
  - e. Confidential information about us, our business, or any of our staff, customers (except as authorized in the proper performance of your duties).
  - f. Unauthorized software.
  - g. Any other statement which is likely to create any criminal or civil liability (for you or us).

h. Music or video files or other material in breach of copyright.

- Any such action will be treated very seriously and is likely to result in summary dismissal.
- Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

## **21. Employee/Contractor/Retainer Declaration**

I have understood the specific Acceptable usage policies and use security responsibilities of my job and agree to abide by them.

<b>Employee/Contractor/Retainer Name:</b> Thamocharan Chandran
<b>Employee/Contractor/Retainer ID:</b>
<b>Employee/Contractor/Retainer Signature:</b>
<b>Date:</b>



**AGREEMENT FOR ASSIGNMENT OF INVENTIONS, COVENANT  
AGAINST DISCLOSURE AND AGREEMENT NOT TO COMPETE**

On clicking on the accept icon below I , hereby declare to abide by the below terms and conditions of this AGREEMENT FOR ASSIGNMENT OF INVENTIONS, COVENANT AGAINST DISCLOSURE AND AGREEMENT NOT TO COMPETE:-

**Property rights:** During and after my employment/engagement with Hexaware, I will not disclose or misuse any knowledge or information of an unpublished, confidential, proprietary, or trade secret nature generated or otherwise acquired by me from Hexaware or its customers. I agree that all concepts, designs, inventions, or improvements which I may conceive, make, invent, or suggest during my employment by Hexaware relating generally to any matter of thing, including computer programs, systems, designs, manuals, documentation, products, processes, or methods which may be connected in any way with Hexaware work or with work or tests carried on by Hexaware, shall become the absolute property of Hexaware.

**Obligations:** During and after my employment with Hexaware, I will keep all such knowledge and information confidential.

**\*Disclosure:** I agree to disclose promptly to my immediate supervisor all such concepts, designs, inventions, improvements, and any developments, I have made during my tenure with Hexaware.

**Return of Documents:** At the conclusion of my employment/engagement with Hexaware, or on demand at any time during my employment / engagement, I will immediately return to Hexaware any drawings, writing, prints, documents, computer media, samples, prototypes, parts, or anything else containing, embodying, or disclosing any of Hexaware's or its customer's unpublished, confidential, proprietary, or trade secret information that are in my possession or subjects to my control. I understand that all such materials, whether generated by me or by others, shall at all times remain property of Hexaware or its customers.

**Personal Information:** During the course of my engagement with Hexaware, I shall handle personal information of the employees, contractors and Customer's customers as part of the business. I agree to use this sensitive information only for Hexaware business purpose and not for any other means and also agree to secure these information all the time and comply with legal and regulatory requirements of Data Protection.

**\*Compliance Not Contingent Upon Additional Consideration:** I have not been promised, and I shall not claim, any additional or special payment or compensation for such assignments and for compliance with the other covenants and agreements herein contained.

**\*Prior Inventions:** If, prior to the date of execution of this Agreement, I have made or conceived any unpatented inventions, improvements, concepts, designs, or developments, whether patentable or unpatentable, which I desire to have excluded from this Agreement, I have attached to this Agreement a complete list and brief description thereof

**\*Covenant Against Disclosure:** In addition to all other obligations with respect to the observance of the security laws and regulations, I understand that it may be desirable or necessary for the Hexaware or any

of its suppliers, licensors, or customers to disclose to me information relating to the technology, systems methods of operations, products, persons and business data of Hexaware or its suppliers, licensors, or customers and, I therefore agree as follows:

(a) To accept and retain such data and information in complete confidence and, at all times during or after the termination of my employment, not to disclose or reveal such data or information to others and refrain from using such data for purposes other than those purposes authorised by Hexaware.

(b) Not to directly or indirectly publish, communicate, divulge, or describe to any unauthorized person nor use, claim, patent, or copyright any such data or information during the term of my employment or at any time subsequent thereto without the prior written consent of the Hexaware.

(d) To keep the contractual relationship of the Hexaware with its suppliers, licensors, or customers confidential. I further agree not to disclose any supplier, licensor, or customer relationships to any third party.

**\*Agreement Not to Compete:** Since I am employed in a position in which I may have intimate and complete knowledge of the operations, products, persons, services, systems, methods and trade secrets of Hexaware, which are unique, patented, and specially developed by Hexaware and allow Hexaware to effectively compete in its business, I hereby agree that during my term of employment with Hexaware, I will not directly or indirectly, either as principal, agent, employee, representative, consultant, or in any other capacity, contact, communicate with, or have any other business dealings with any customer of Hexaware, as defined in this section below, with whom I have had any contact, communications, or business dealings with during my terms of employment with Hexaware, except as specifically authorized by Hexaware.

I also agree that for a period of two years after my termination of employment with Hexaware, I will not contact, communicate, or have any business dealings with, either directly or indirectly, any customer of Hexaware. "Customer" includes those who are customers of Hexaware on the date of termination of my service contract as well as those who were customers of Hexaware at any time two years prior to the termination of my service contract. For avoidance of doubts, I understand that my obligation of "not to compete" as mentioned in this agreement will apply to all customers of Hexaware or Customers of customers on whose projects I am deputed or assigned whilst being in the employment of Hexaware.

I further agree that during my term of employment with Hexaware, I shall devote my skills and best efforts to the service of Hexaware and not perform any other activities for any competitor of Hexaware.

**Reasonable Scope:** I understand that unauthorized disclosure or use of Hexaware's or its customer's, unpublished confidential, proprietary, or trade secret information is likely to cause irreparable harm to Hexaware or its customers. I agree that Hexaware or its customers shall be entitled to, individually or jointly, an injunction restraining such unauthorized use of disclosure without (i) proof of irreparable harm caused or (ii) posting an injunction bond and in addition to the above would be entitled to any other equitable relief as available in law.

**Governing Law and Jurisdiction.** This Agreement will be governed by and construed under the laws of India, without giving effect to the conflicts of laws provision thereof.

\* In the event that any provision of this paragraph is deemed to be overly broad and unenforceable, the parties hereto stipulate and agree that any court of competent jurisdiction shall have the right to so limit, amend, or construe said provision so that the same shall be enforceable and hereby request the court to so act.

\* **Severability:** Each paragraph and provision of this Agreement is severable from the contract and if one provision or part thereof is declared invalid, the remaining provisions shall nevertheless remain in full force and effect.

\***Entire Agreement:** This Agreement shall inure to the benefit of and be binding upon my heirs, executors, administrators, and assigns and the successors and assigns of Hexaware.

The Failure of Hexaware to exercise its rights under or insist upon strict performance of the provision of the Agreement shall not operate as a waiver thereof or preclude Hexaware from exercising its rights.

**I AGREE TO ABIDE BY THE ABOVE TERMS AND CONDITIONS OF THIS AGREEMENT  
BY CLICKING ON THE ACCEPT ICON AND NON COMPLIANCE OF THE SAME SHALL  
AMOUNT IN SEVERE DISCIPLINARY AND LEGAL PROCEEDINGS AGAINST ME**

## Joining Report

---

To,

Hexaware Technologies Ltd.,

Dear Sir,

This has reference to your appointment order dated 27/05/2024 and I  
hereby join duties on 27-May-24

Thanking you.

(Name & Signature)

**Joining Report****CONFIDENTIALITY AGREEMENT**

I, Thamotharan Chandran currently residing at Sri Lakshmi ganapathi Hostel, Poomagal  
Chennai - 600032, with permanent residence at 4th street, Ekkatuthangal  
133/5-W, North street, Gokilapuram  
Uthamapalayam-tk, Theni(Dt) - 625526, this 27 day of  
05 (month), 2024 (year), having been employed/retained by Hexaware  
 Technologies Ltd., (hereinafter referred to as Hexaware) having its registered office at 152  
 Millennium Business Park, TTC Industrial Area, Sector -3, A Block, Mahape, Navi Mumbai  
 400701, from 27-May-24 (date of joining /retaining), agree to the following terms:

During and after my employment/engagement with Hexaware, I will not disclose or use any knowledge or information of an unpublished, confidential, proprietary, or trade secret nature generated or otherwise acquired by me from Hexaware or its customers. During and after my employment with Hexaware, I will keep all such knowledge and information confidential.

At the conclusion of my employment / engagement with Hexaware or on demand at any time during my employment / engagement, I will immediately return to Hexaware any drawings, writings, prints, documents, computer media, samples, prototypes, parts, or anything else containing, embodying, or disclosing any of Hexaware's or its customer's unpublished, confidential, proprietary, or trade secret information that are in my possession or subject to my control. I understand that all such materials, whether generated by me or by others, shall at all times remain property of Hexaware or its customers.

I understand that unauthorized disclosure or use of Hexaware's or its customer's unpublished confidential, proprietary, or trade secret information is likely to cause irreparable harm to Hexaware or its customers. I agree that Hexaware or its customers shall be entitled to, individually or jointly, an injunction restraining such unauthorized use of disclosure without (i) proof of irreparable harm or (ii) posting an injunction bond.

The failure of Hexaware to exercise its rights under or insist upon strict performance of the provision of the Agreement shall not operate as a waiver thereof or preclude Hexaware from exercising its rights.

Signature:

Print Name: Thamotharan Chandran

Date:

Place:

**Witness (1):**

**Witness (2):**

Signature:

Signature:

Name:

Name:

Address: Hexaware Technologies Ltd.,

Address:

Date:

Date:



Hex 5551-A

## Privacy Notice for Employees

---

# Privacy Notice for Employees for Non-EU Employees



## Privacy Notice for Employees

---

This is a privacy notice for employees that complies with the applicable data protection regulations. Hexaware Technologies Limited and its subsidiaries part of Hexaware relies on this notice to notify employees about the personal data that Hexaware Technologies Limited and its subsidiaries holds relating to them, how they can expect their personal data to be used and for what purpose.

### WHAT IS THE PURPOSE OF THIS DOCUMENT?

Hexaware Technologies Limited and its subsidiaries is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the applicable Data Protection Regulations and

applicable to all employees.

Hexaware Technologies Limited and its subsidiaries is the “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

### DATA PROTECTION PRINCIPLES

We will comply with the data protection laws. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way
2. Collected only for valid purpose that we have clearly explained to you and not used in any way that is incompatible with that purpose
3. Relevant to the purpose we have told you about and limited only to that purpose
4. Accurate and kept up to date
5. Kept only as long as necessary for the purpose we have told you about
6. Kept securely

## Privacy Notice for Employees

---

### THE OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Personal details of your dependants for the purposes of emergency contact information and management of insurance policies (e.g. health and medical insurance which will also require us to retain personal and special categories of data of your dependants for this purpose)
- Date of birth
- Gender
- Passport and /or National Identity card information
- Gender for equal opportunities monitoring purposes and compliance with legal requirements if any Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Employment start date
- Location of employment or workplace
- Copy of driving licence
- Recruitment information (including copies of right to work documentation, references and other information included in the CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipe card records
- Information about your use of our information and communications systems
- Photographs

We may also collect, store and use the following “special categories” of more sensitive personal information:



## Privacy Notice for Employees

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Information about your health, including any medical condition, health and sickness records and that of your dependants as explained in the section above
- Genetic information and biometric data
- Information about criminal convictions and offences

### HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency and/or background check provider and/or partner recruitment agencies and public platforms including, without limitation, LinkedIn, Job Portals, references from current and former employees, organisational websites & Portals. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information during job-related activities throughout the period of you working for us.

### HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you
2. Where we need to comply with a legal obligation
3. Where it is necessary for our legitimate interests (or those of a third party), and your interests and fundamental rights do not override those interests

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests)
2. Where it is needed in the public interest or for official purpose

### Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to administer our contract with you [\*] and to enable us to comply with legal obligations [\*\*]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties [\*\*\*], provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. We have indicated by asterisks the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of data are involved.

- Making a decision about your recruitment or appointment. \*\* and/or \*\*\*
- Determining the terms on which you work for us. \*\* and/or \*\*\*
- Checking you are legally entitled to work in the countries of our business intrestes <<country name>> and/or

## Privacy Notice for Employees

\*\* and/or \*\*\*

- Paying you and, if you are an employee, deducting tax and National Insurance contributions. \* and/or \*\* and/or \*\*\*
- Providing the following benefits to you: access to a pension scheme, health insurance, medical insurance and dental insurance and such other benefits as might be provided from time-to-time in future \* and/or \*\* and/or \*\*\*
- Liaising with your pension provider. \* and/or \*\* and/or \*\*\*
- Administering the contract, we have entered into with you. \* and/or \*\* and/or \*\*\*
- Business management and planning, including accounting and auditing. \* and/or \*\* and/or \*\*\*
- Conducting performance reviews, managing performance and determining performance requirements. \* and/or \*\* and/or \*\*\*
- Making decisions about salary reviews and compensation. \* and/or \*\* and/or \*\*\*
- Assessing qualifications for a particular job or task, including decisions about promotions. \* and/or \*\* and/or \*\*\*
- Gathering evidence for possible grievance or disciplinary hearings. \*\* and/or \*\*\*
- Making decisions about your continued employment or engagement. \* and/or \*\* and/or \*\*\*
- Making arrangements for the termination of our working relationship. \* and/or \*\* and/or \*\*\*
- Education, training and development requirements. \* and/or \*\* and/or \*\*\*
- Dealing with legal disputes involving you, or other employees, including accidents at work. \* and/or \*\* and/or \*\*\*
- Ascertaining your fitness to work. \* and/or \*\* and/or \*\*\*
- Managing sickness absence. \* and/or \*\* and/or \*\*\*
- Complying with health and safety obligations. \* and/or \*\* and/or \*\*\*
- To prevent fraud. \* and/or \*\* and/or \*\*\*
- To monitor your use of our information and communication systems to ensure compliance with our IT policies. \* and/or \*\* and/or \*\*\*
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. \* and/or \*\* and/or \*\*\*
- To conduct data analytics studies to review and better understand employee retention and attrition rates. \* and/or \*\* and/or \*\*\*
- Equal opportunities monitoring. \* and/or \*\* and/or \*\*\*
  - Pre-employment vetting of the right to work in the countries of our business interests to comply with the relevant regulations and immigration laws to prevent illegal working and to carry out right to work checks on all prospective employees. \*\* and/or \*\*\*
  - Dealing with local tax authorities and other relevant authorities\* and/or \*\* and/or \*\*\*
  - Pre-employment vetting for example in the financial services industry. \*\* and/or \*\*\*
  - Details of previous employer for reference purposes. \* and/or \*\* and/or \*\*\*
  - Personal details to arrange directors' and officers' insurance for a director. \* and/or \*\* and/or \*\*\*

## Privacy Notice for Employees

---

- Any other usual and expected processing of personal data to maintain our employment relationship. \* and/or \*\* and/or \*\*\*
- to protect Hexaware Technologies Limited and its subsidiaries proprietary and commercially sensitive information and to comply with its confidentiality obligations to its clients. \* and/or \*\*\*
- processing for direct marketing purposes or preventing fraud; \* and/or \*\* and/or \*\*\*
- transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note international transfer requirements will still apply) \* and/or \*\*\*
- processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems; \*\*\*
- reporting possible criminal acts or threats to public security to a competent authority. \*\* and/or \*\*\*
- sharing of personal information when required for the business needs with our business partners associates, customers and suppliers

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

### If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

### Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

### HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy and/or other relevant policies].

## Privacy Notice for Employees

3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme], and in line with our data protection policy and /or other relevant policies.

4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

### Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting
- We will use trade union membership information to pay trade union premiums (if relevant), register the status of a protected employee and to comply with employment law obligations
- We will share your data with the Government, Law enforcement and or Regulators as per statutory requirements

### Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

### INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with the provisions of data privacy regulations as relevant to the country as applicable.

Less commonly, and in accordance with applicable data privacy regulations of the countries as relevant, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

## Privacy Notice for Employees

---

We envisage that we will or may have to hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

### **AUTOMATED DECISION-MAKING**

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

### **DATA SHARING**

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the country in accordance with the provisions of the in-country laws and regulations. <<country Name>>.

If we do, you can expect a similar degree of protection in respect of your personal information.

### **Why might you share my personal information with third parties?**

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.



## Privacy Notice for Employees

---

### Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services, legal and accounting professionals, management consultants, data efficiency and monitoring consultants.

### How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, for accounting, taxation, human resources, recruitment, marketing and legal support.

### What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business or business requirements/developments. We may also need to share your personal information with a regulator or to otherwise comply with the law.

### Transferring information outside the country

We will transfer the personal information we collect about you to the following countries : - India, USA, Mexico, Australia, Europe, Singapore and other countries where Hexaware Technologies Limited and its subsidiaries is operational in order to perform our contract with you. If There is not an adequacy decision by the countries of interest.. This means that the countries to which we transfer your data are not deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the laws and regulations of the countries in accordance with the provisions of the in-country laws and regulations ; Data Protection Agreements which incorporate the appropriate Contractual Clauses. If you require further information about these protective measures, you can request it from Hexaware Technologies Limited and its subsidiaries data protection team by email at [Privacy@hexaware.com](mailto:Privacy@hexaware.com)

### DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat

## Privacy Notice for Employees

the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

### DATA RETENTION

#### How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations or our data retention policy.

### RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

#### Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

#### Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.



## Privacy Notice for Employees

---

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our data protection team in writing or by email at [privacy@hexaware.com](mailto:privacy@hexaware.com)

### No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

### What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our data protection team by email at [privacy@hexaware.com](mailto:privacy@hexaware.com). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

### DATA PROTECTION OFFICER

We have appointed a data protection officer (DPO) as part of our data protection team to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the our data protection team by email at [privacy@hexaware.com](mailto:privacy@hexaware.com). You have the right to make a complaint at any time to the appropriate data protection regulatory for data protection issues.

### CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.



**GLOBAL CODE OF CONDUCT**

---

**Hex 5733**

**Global Code of Conduct**



GLOBAL CODE OF CONDUCT

Date	Version No.	Prepared By	Reviewed By	Approved By	Summary of Changes
11-Dec-23	4.5	Vishnu Kumar Prasad A	Rajashree L	Nita Nambiar (Chief People Officer)	Updated the StationH links

GLOBAL CODE OF CONDUCT

Table of Contents

1. INTRODUCTION .....5

2. SCOPE.....5

3. PURPOSE .....5

4. COMPLIANCE TO REQUIREMENTS & FAIR COMPETITION .....6

4.1. COMPLIANCE WITH LAWS, REGULATIONS, POLICIES AND PROCEDURES .....6

4.2. FAIR DEALING.....6

5. LEGAL & ETHICAL CONDUCT .....6

5.1. INTEGRITY .....6

5.2. CONFLICTS OF DUTY OR INTEREST.....7

5.3. ANTI-BRIBERY & ANTI-CORRUPTION COMPLIANCE .....7

5.4. ANTI-MONEY LAUNDERING PRACTICES .....10

6. INSIDER TRADING.....11

7. BOOKS & RECORDS .....11

8. BUILDING A GREAT HEXAWARE .....12

8.1. DIVERSITY EQUITY INCLUSION- DEI .....12

8.2. MODERN SLAVERY .....12

8.3. CHILD LABOUR .....13

8.4. ANTI-BULLYING & PREVENTION OF SEXUAL HARASSMENT .....13

8.5. ABUSE OF MANAGERIAL AUTHORITY .....13

8.6. HEALTHY & SAFE ENVIRONMENT .....13

8.7. ABUSE FREE WORKPLACE .....14

8.8. FREEDOM TO EXPRESS & SOCIAL DIALOGUE .....14

9. ENVIRONMENT, SOCIAL & GOVERNANCE (ESG) MANAGEMENT .....14

10. CONFIDENTIALITY.....14

11. INTELLECTUAL PROPERTY RIGHTS & OWNERSHIP .....17

12. NON-SOLICITATION OF EMPLOYEES .....17

13. INFORMATION SECURITY, DATA PRIVACY & DATA PROTECTION.....18

14. REPORTING OF UNLAWFUL AND UNETHICAL BEHAVIOUR, WHISTLE BLOWER POLICY .....20



GLOBAL CODE OF CONDUCT

15. ORGANIZATION DISCIPLINE & DECORUM.....21

16. TRAINING & CERTIFICATION .....24

17. REVIEW OF THE CODE .....25

18. ADMINISTRATION OF THE POLICY .....25

19. ANNEXURE 1- STATEMENT OF COMPLIANCE .....25

20. FREQUENTLY ASKED QUESTIONS (FAQ).....27

## **GLOBAL CODE OF CONDUCT**

---

### **1. Introduction**

The code of conduct for employees defines standards for conduct in all business, legal, and ethical matters carried out in daily business, and is meant as a tool and a guide for dealings with employees, customers, suppliers, and partners; interaction with competitors; as well as in financial areas. It is part of Hexaware's business policy to carry out all company activities in accordance with the letter and spirit of applicable legal requirements and therefore keep high standards of business ethics.

Our commitment to ethical and lawful business conduct is a fundamental value of our employees and is critical to the company's success. We will strive to uphold ethical and legal standards vigorously even as we pursue our financial objectives. We will not compromise honesty and integrity anywhere at any time even while continuously striving to build value for customers through the innovative use of technology and talent. This code of conduct reiterates our commitment to the above principles.

### **2. Scope**

This code of conduct applies to

- i) all Hexaware employees (permanent and retainer roles) and is in addition to their legal and contractual obligations with Hexaware (which expression shall mean and include all its affiliates, subsidiaries, parent companies, successors & assignees)
- ii) board of directors of the company

Employees should address their immediate superior when questions or problems arise. The employee's manager is responsible for ensuring that conflicts of interests are resolved as quickly as possible.

Note:

- Any reference to "Hexaware" in this code of conduct means Hexaware Technologies Limited. (Which expression shall mean and include all its affiliates, subsidiaries, parent companies, successors & assignees)
- Any reference to "employee" in this code of conduct means and includes all Hexaware employees directly employed by Hexaware.

### **3. Purpose**

This code of conduct is intended to:

- Set high standards of honesty, integrity, ethical and law-abiding behavior expected of Hexaware's employees.
- Encourage the observance of those standards to protect and promote the interests of shareholders and other stakeholders.

## GLOBAL CODE OF CONDUCT

---

- Guide employees on their acts and actions necessary to maintain integrity; and
- Set out the responsibility and accountability of Hexaware's employees to report and investigate any reported violations of this code or unethical or unlawful behavior.

### 4. Compliance to requirements & fair competition

#### 4.1. Compliance with laws, regulations, policies and procedures

Employees must:

- comply with all applicable law, rule or regulation, in letter and spirit
- comply with the protocols, policies and procedures of Hexaware; and
- encourage other employees to do the same.

#### 4.2. Fair dealing

Hexaware expects each Employee to:

- ✓ Deal fairly with any executive, employee, shareholder, customer, supplier, competitor, auditor, lawyer or other adviser of Hexaware; and
- ✓ Encourage other employees to do the same.
- i. Employees must not take unfair advantage of any employee, customer, supplier, auditor, lawyer, other adviser of Hexaware through unethical or illegal conduct, manipulation, undue influence, concealment, abuse of confidential information, misrepresentation of material facts, or any other unfair-dealing practice.
- ii. Hexaware is committed to free and open competition in the marketplace. Directors and consultants should avoid actions that could reasonably be construed as being anticompetitive, monopolistic, or otherwise contrary to laws governing competitive practices in the marketplace, including antitrust laws. Such actions include misappropriation and / or misuse of a competitor's confidential information or making false statements about the competitor's business and business practices.

### 5. Legal & ethical conduct

#### 5.1. Integrity

Hexaware conducts its business with integrity. It has zero tolerance towards unethical activities like bribery & corruption. Every employee is expected to act professionally & with integrity in their work.

Employee shall,

- i. Work in the best interest of the company

**GLOBAL CODE OF CONDUCT**

- ii. Act honestly, fairly, ethically, with integrity and loyalty
- iii. Act in good faith, with responsibility, due care, competence, diligence and independence
- iv. Conduct themselves in a professional, courteous and respectful manner
- v. Treat their colleagues with respect & dignity and shall not harass any of them in any manner

**5.2. Conflicts of duty or interest**

- Employees must be aware of potential conflicts between (directly or indirectly):
  - o on the one hand:
 

The interests of Hexaware; or their duties to Hexaware.
  - o on the other hand:
 

Their personal or external business interests; or their duties to any third party.
- Employees must avoid placing themselves in a position that may lead to:
  - o An actual or a potential conflict of interest or duty; or
  - o A reasonable perception of an actual or potential conflict of interest or duty.
- Employees must:
  - o Fully and frankly inform Hexaware's senior management and Human Resources department of any personal or external business interest that may lead to:
 

An actual or potential conflict of interest or duty; or

A reasonable perception of an actual or a potential conflict of interest of duty; and
  - o Obtain and follow independent legal advice to avoid or resolve any actual, potential or perceived conflict of interest or duty.
- Employees must devote themselves exclusively to the business of the company and shall not accept any other work or assignment for remuneration (full time or part-time).
- Employees must affirm compliance with this code of conduct in the format given below in Annexure I.
- For more details, refer to the company's Hex 5878 Conflict of interest Policy which is available on the company's intranet portal.

**5.3. Anti-bribery & Anti-corruption compliance**

- a) Hexaware does not give or receive bribes, including facilitation payments.
  - Hexaware is committed to conducting business holding the highest standards of integrity and adhering to the letter and spirit of all the applicable laws and regulations of the locations where the Company operates.
  - Management of the Company including members of Board of Directors have adopted a 'zero

**GLOBAL CODE OF CONDUCT**

tolerance' approach to/from any form of Corruption within the Company by setting personal example of ethical attitude and ensuring compliance with applicable Anti Bribery and Corruption legislation and internal policies implemented by the Company, while executing their duties.

- Hexaware prohibits direct or indirect payment/acceptance of bribe or any form of corrupt payment to any party for furtherance of business or to gain any Undue Advantage. Further, Employees are not permitted to pay any form of bribe indirectly on behalf of the Company or authorize any Third Party representing Hexaware to pay bribe on the behalf of the Company.
- Bribery may not always be in the form of cash payments and may take many other forms, including gifts, hospitality, entertainment, political contributions, charitable donations, lobbying payments, sponsorships, employment opportunities among others.
- Facilitation Payments are also prohibited and must not be incurred by Employees or Third Parties either directly or indirectly on behalf of Hexaware.
- For more details, refer to Hexaware's Hex 5865 Anti-Bribery and Anti-Corruption Policy which is available on the company's intranet portal.

b) Giving or receiving Gifts, Hospitality and Entertainment ('GHE') should be reasonable, and in certain cases prohibited.

- Gifts, Hospitality and Entertainment given to or received from any Third Party who have a business relationship with the company are generally acceptable, if the GHE is modest in value, appropriate to the business relationship, and does not create an appearance of impropriety. No cash or cash equivalent payments should be given or received.
- In the case of Public Officials, giving gifts is prohibited except for gifts during festive seasons such as Diwali and Christmas. Hospitality provided to Public Officials should be reasonable and should not influence or appear to influence any business decision. Further, any form of entertainment for Public Officials is not permissible.
- Prior to offering a permissible gifts, hospitality or entertainment to any Third Party including Public Officials, Employee should be in compliance with respect to the approval guidelines and value limits set by the Company.
- For detailed guidance, refer to Hex 5861 Hexaware's Gifts, Hospitality and Entertainment Policy available on the Company's intranet portal.

c) Donation and Sponsorship to political parties, individual candidates and Public Officials is prohibited.

- Hexaware does not offer donations or provide sponsorship to Public Officials.
- Hexaware is politically neutral, i.e., not directly or indirectly affiliated with any political party and does not provide services linked to any political messages. Hexaware does not associate itself with any political party or independent candidate, and does not campaign for, support and offer donation to political parties to influence any decision or gain business advantage. Accordingly, Hexaware does



## GLOBAL CODE OF CONDUCT

---

not make political contributions, donations and sponsorships of any kind to political parties and individual candidates.

- For detailed guidance, refer to Hex5863 Hexaware's Donations and Sponsorships Policy available on the Company's intranet portal.

### d) Third party Management

- Anti-Bribery and corruption laws impose liability on companies that become involved in the direct or indirect acts of Bribery. The company may therefore incur criminal and/or civil liability where Third Parties indulge in any act of Bribery in the course of their work on the Company's behalf, or otherwise for the Company's benefit. This exposure can arise even where the Company Employees ensure to take preventive steps that improper payments or advantages are not offered or accepted on behalf of the Company by the Third Party or their representatives.
- In order to maintain the highest standards of integrity, with respect to any dealings with a Third Party, the Company will ensure that:
  - All the Third-Party contracts include Anti-Bribery and Anti-Corruption compliance clauses to ensure compliance with the terms of this Policy.
  - Include appropriate wording/clauses in the Third-Party contracts to make it possible to withdraw from the relationship and take the appropriate disciplinary action, on the Third Parties who fail to abide by this Policy.
  - At the time of onboarding a Third Party and later on Annual basis, the Company must obtain an Anti-Bribery and Anti-Corruption undertaking or declaration from every Third Party to this effect.
- Every Third Party appointed for representing Hexaware or carrying out any activity for Hexaware must be hired/appointed in accordance with the guidelines, protocols and procedures around Third-Party identification, due diligence, on-boarding and approvals as set forth in Hex 5869 Third Party Management Policy which is available on the Company's intranet.

### e) Dealing with Government (Including government customers)

#### ➤ Interactions with Government Officials

Interactions with Public Officials pose a higher risk on account of their role in the government and capability to influence business decisions of Hexaware. Hence, Hexaware expects its Employees and Third Parties representing the Company to maintain the highest professional and ethical standards while interacting with the Government and resultant relationship with Public Officials. Any interactions with Public Officials must be carried out in a clear, open and transparent manner and only for legitimate business purposes.

**GLOBAL CODE OF CONDUCT**➤ Government as Customer

Governments (including government authorities, agencies, quasi government agencies, public section undertakings among others) are unique customers for Hexaware. They often have unique bidding, pricing, disclosure, and certification requirements. When dealing with government customers, make sure to partner with the legal department when bidding for business, and contact the Compliance Officer with questions relating to compliance requirements.

➤ Hiring Government Employees

Laws often limit the duties and types of services that former government, military, or other public sector employees may perform as employees or consultants of Hexaware, especially regarding matters they were involved in while with the government. Employment negotiations with government employees may be subject to legal restrictions and disclosure requirements, particularly if the government employee is involved in a matter involving Hexaware's interests. Contact Compliance Officer before entering such negotiations. You may never hire any individual in exchange for securing or retaining business or securing an improper advantage. We also prohibit hiring preference being given to anyone in return for special treatment.

Refer Hex 5868 Interactions with Public Officials Policy available on the company's intranet portal.

**5.4. Anti-money laundering practices**

- Money laundering occurs when individuals or organizations try to conceal illicit funds or make those funds look legitimate. Money laundering is illegal and strictly prohibited by Hexaware.
- Hexaware is strongly committed to prevent the use of its operations for money laundering, financing of terrorism, or any other criminal activities, and will take appropriate actions to comply with all the applicable anti-money laundering and anti-terrorism laws throughout the world.
- Hexaware conducts business only with reputable customers involved in legitimate business activities, with funds derived from legitimate sources. Jurisdictions in which Hexaware operates may publish lists of individuals and organizations that any company is prohibited from accepting funds from or distributing funds to, under applicable Anti-Money Laundering laws. Employees are expected to use reasonable care to verify that counterparties are not owned or controlled by, or acting on behalf of, sanctioned governments, groups, individuals, organizations and other entities.
- If an employee deals directly with customers or Third Parties, the following examples may signal potential money laundering:
  - Attempts to make large payments in cash.
  - Payments by or to someone who is not a party to the contract.
  - Requests to pay more than the amount as agreed in the contract.
  - Payments made in currencies other than those specified in the contract.
  - Payments from an unusual and/or non-business account.

## GLOBAL CODE OF CONDUCT

---

- Transactions forming an unusual pattern such as bulk purchases of products or gift cards or repetitive cash payments.

For detailed guidance, refer to Hex 5858 Anti-Money Laundering and Sanctions Policy available on the Company's intranet.

### 6. Insider trading

- Employees while performing their duties for the Company, may have access to or become aware of material non-public information or unpublished price sensitive information (collectively referred as "Information") either about the Company or any of its customers or any other business partners which are publicly traded entities.
- Employees are prohibited from using this Information to gain a financial advantage for themselves or others, either by way of making a trade for themselves, "tipping" others on the Information (i.e., disclosing the information to others such as family, friends, acquaintances or any other person), or otherwise. Doing so is not only a violation of the code that may result in immediate termination for cause but is also a serious violation of applicable securities laws and will expose any individuals involved to potential civil and criminal prosecution.
- Employees must maintain the confidentiality of all such Information accessible to them during employment with Hexaware.

For detailed guidance, refer to Hexaware's Insider Trading Policy available on the Company's intranet.

### 7. Books & records

- Hexaware's stakeholders must not engage in any actions or transactions which lead to financial or reputational loss to the Company or are blatant acts of fraud. All corporate records of Hexaware must be true, accurate and complete, and the Company data must be promptly and accurately entered in our books in accordance with Hexaware's and other applicable accounting principles, applicable laws and regulations. We must not improperly influence, manipulate or mislead any audit, nor interfere with any auditor engaged to perform an independent audit of Hexaware's books, records, processes or internal controls. No Employee in any way will cause the Company's accounts or other records to not clearly describe and properly state the true nature and timing of a business activity or transaction.
- Hexaware will make certain that all disclosures made in financial reports, public documents or any regulatory filings are full, fair, accurate, timely and understandable. This obligation applies to all Employees, including all financial executives, with any responsibility for the preparation for such reports or filings, including drafting, reviewing and signing or certifying the information contained therein. No business goal of any kind is ever an excuse for misrepresenting facts or falsifying records.

## GLOBAL CODE OF CONDUCT

---

Employees must inform the management, Human Resource department and Compliance Officer if they learn that information in any filing or public communication was untrue or misleading at the time it was made or if subsequent information would affect a similar future filing or public communication.

### **8. Building a great Hexaware**

We are obligated to protect & promote human rights amongst our employees (permanent, , retainers, trainees & employees of subcontractors), suppliers & customers. We nurture sustainable long-term relationships across the ecosystem in which we operate.

#### **8.1. Diversity Equity Inclusion- DEI**

- Hexaware Technologies Limited is an equal opportunity employer and supports a diverse workforce across all levels. We believe that Diversity Equity & Inclusion (DEI) is associated with our core values, and it is instrumental in our growth journey. We are committed to providing a workplace that is free from all forms of harassment. Employees are assured a workplace free of harassment irrespective of their gender, race, social class, caste, creed, and religion, place of origin, sexual orientation, disability or economic status with a zero-tolerance policy to any kind of workplace harassment.
- The basis for recruitment, hiring, placement, development, training, compensation and advancement at the company is solely based on qualifications, performance, skills and experience.

Refer Hex 5729 Diversity, Equity and Inclusion Policy

#### **8.2. Modern slavery**

- Hexaware's culture & philosophy is based on promoting human rights & as part of it we are committed to prohibiting modern slavery & human trafficking.
- We are signatory to the United Nations Global Compact (UNGC) & are committed to protecting & preserving human rights as per UN Guiding Principles & the International Labour Organization's Declaration on Fundamental Principles & Rights at Work.
- We are committed to exhibit zero tolerance towards all facets of modern slavery, as elaborated under the Modern Slavery Act 2015 UK (designed to tackle slavery, servitude and forced or compulsory labor and human trafficking, including provisions for the protection of victims), Commonwealth Modern Slavery Act 2018, the UN Declaration of Human Rights and the conventions of the International Labour Organizations specific to forced or compulsory labour.

For more details, please refer to the Slavery & Human Trafficking statement available on Hexaware website.

---

**GLOBAL CODE OF CONDUCT**

---

**8.3. Child labour**

- Hexaware is committed to strict prohibition of child laborers.
- Hexaware does not employ any person below the permissible age in the country where it is operating. We comply with all the relevant and applicable laws and regulations pertaining to child labor in the countries of our presence.

**8.4. Anti-bullying & prevention of sexual harassment**

- Hexaware forbids and does not expect employees to tolerate harassment or bullying in their employment. If an employee has a complaint of bullying, discrimination, sexual or other harassment, or other forms of violence or offensive conduct the employee is expected to report it to any Human Resources representative or a senior manager or the Head of the business unit, or in accordance with specific reporting practices as per the policy.
- Complaints of violence, offensive or improper conduct are taken seriously and investigated thoroughly, without retaliation.
- Employees are expected to familiarize themselves with Hexaware's Prevention of Sexual Harassment policy & Hexaware's anti-harassment policy, which can be viewed on the Hexaware Portal.
- It is mandatory for all employees to complete all training & assessments as outlined in the location specific guidelines.

India -> Refer Hex 5732 Prevention of Sexual Harassment at Workplace Policy

Global -> Hex 5734 Anti - Harassment Policy

**8.5. Abuse of managerial authority**

- Hexaware expects its managers to perform their managerial duties diligently & not misuse their managerial authority. They should conduct themselves professionally, which will protect the employee's dignity. Some examples of managerial abuse include-
  - i. Making demands that are unreasonable and/or outside of the associate's role; or
  - ii. Demanding to perform an action that is in breach of the principles of any policy of Hexaware
  - iii. Excessively, destructively or inappropriately criticizing or reprimanding them, or excessively scrutinizing their work, or
  - iv. Humiliating or undermining the reporting person

**8.6. Healthy & safe environment**

- Hexaware is committed to providing a safe, healthy and hygienic environment for its workforce.

**GLOBAL CODE OF CONDUCT**

Hexaware seeks to minimize the adverse environmental impact by conducting its operations in a safe manner. It strives to prevent all possible accidents, incidents, injuries and occupational illness. For more details, please refer Hex 5759 Occupational Health & Safety policy  
 Path-> StationH→ Resources → Apps → Quality Portal → PRIME→ Enterprise processes→ Occupational health & safety policy

**8.7. Abuse free workplace**

- All Hexaware premises across the globe are No Smoking zones. Possession or use of alcohol in the work area is strictly prohibited. Beer and wine can be served as an exception as per the customary practice in the country we operate for social purposes only, but not in the Hexaware work area. The illegal possession, use, sale, manufacture or distribution of illegal drugs at company premises or while on company business activities is prohibited.

**8.8. Freedom to express & social dialogue**

- We are committed to making Hexaware a great place to work with the help of our passionate and engaged workforce. In this process, we have equipped the workforce with their right to express & are fostering a culture of open dialogue. We promote open dialogue by encouraging employees to express their views, opinions & thoughts openly without any fear in all forums with various stakeholders.

**9. Environment, Social & Governance (ESG) management**

- We at Hexaware, are committed to imbibe the philosophy of sustainability as an integral part of our business and earnestly commit ourselves to uphold this as governing framework for all our business endeavors. We have established a Sustainability policy which defines the framework for sustainability at Hexaware and works in conjunction with various other policies in existence to create long lasting value for the environment, business and society at large. This policy will also facilitate us to promote diversity, equity and inclusion, enhance environmental performance, mitigate future risks, and improve economic prosperity.
- For more details, please refer to Hex 5730 Sustainability policy.  
 Path: StationH→ Resources → Apps→ Quality Portal → PRIME→ Enterprise processes→ Sustainability policy

**10. Confidentiality**

- In the course of employment with Hexaware, employees will have access to information that is considered confidential and/or proprietary. Generally, confidential and proprietary information is

**GLOBAL CODE OF CONDUCT**

any Company information that is not public. As a policy of the Company every employee must sign a Non-Disclosure Agreement before joining the services of the company and abide by the same. Employees are expected to use appropriate discretion to discuss terms and conditions of their employment in accordance with applicable law.

- Confidential and proprietary information is information about Hexaware or Hexaware's customers that includes, but is not limited to:
  - ✓ Research and development, such as project descriptions, plans, drawings, reports, notebooks, computer files and programs, and investment amounts
  - ✓ Trade secrets, including business practices, technical processes and applications, service and restoration procedures, operations procedures, software specifications and designs, and equipment uses
  - ✓ Hexaware intellectual property, including patented, trademarked, and copyrighted material Procedures and practices related to management of Hexaware's network, communications, data centers, command centers, and other technical equipment
  - ✓ Non-public information about products, service alliances, and customers, including marketing plans and sales
  - ✓ Prospects, product and service strategy, and software specifications
  - ✓ Confidential and proprietary organizational and business information, such as budgets and other financial data and records, rate and cost data, customer lists, services provided, and personnel data, including employee records and lists
  - ✓ Information received/receiving from or about customers and potential customers
- Employees have the responsibility to protect confidential and proprietary information from theft, disclosure, or inappropriate use. They are expected to store confidential and proprietary information in a safe place as identified and follow the information security and other related policies. They should use extreme caution while discussing business or using a cell phone or other portable communications device in public places, and never discuss Hexaware' or its customers' confidential and proprietary information with friends or acquaintances.
- Before releasing confidential or proprietary information or permitting anyone from outside Hexaware to use a Hexaware trademark or copyrighted work, employees must first obtain appropriate management approval and make sure the party receiving the information has signed a non-disclosure and a license agreement approved by the legal department.
- Employees must immediately notify the legal department if they discover that Hexaware' confidential and proprietary information, trademark, copyright, patent, name, or logo has been improperly used or disclosed.
- Employees must protect Hexaware's customers' and prospective customers' confidential and proprietary information. They are expected to never use another party's trademark, name, logo, or copyrighted material without the owner's prior written permission, and never remove copyright notices from computer or other materials.

**GLOBAL CODE OF CONDUCT**

---

- When (employee's) employment with Hexaware ends, all documents, records, and other information and property belonging to Hexaware must be returned. Even after the employee leaves the employment of the Company, they have a continuing obligation to safeguard and not use or otherwise disclose Hexaware' and its customers' confidential and proprietary information to anyone.
- The work for which employees are employed is and will be of a private nature, and in connection with the performance of their services on behalf of Hexaware, its subsidiaries and affiliates (together with their predecessors and successors, the "Company"), the Company, may make available information of a private nature which is including, but not limited to Company's customers' and prospective customers' business, strategies, methodologies, operations, technologies (including computer software), financial affairs, organizational and personal matters, policies, procedures, trade secrets, programs, operations, customers, prospective customers, employees and other non-public matters, including those concerning third parties ("Private Information"). Employees agree that they shall receive in strict confidence all such private information belonging to the company or to its customers or prospective customers. Employees further agree to use their best efforts to maintain and to assist the Company in maintaining the confidentiality of all such private information, and to prevent it from getting into unauthorized hands.
- Employees shall ensure that their respective salary shall always be kept confidential and should not be disclosed to any colleagues or anybody else unless local law specifically allows for salary sharing.
- Employees further agree that:
  - I. They shall neither copy nor distribute any material, or other information constituting private information which comes into their possession because of their employment by the company, other than for the company use.
  - II. They shall, not only during the period of employment by the Company but even at any time thereafter, directly or indirectly, disclose to others and / or use for their own benefit or for the benefit of others, private information acquired by them during the period of their employment, except to the extent as may be reasonably necessary in the ordinary course of performing their duties as an employee of the company.
  - III. They shall not disclose to the Company or attempt to induce the Company to use any private information or material to which the Company is not entitled.
  - IV. Upon termination of their employment with the Company, they shall return to the Company or to the customer or prospective customer/s all materials and information that constitutes private information and any copies thereof and certify to the company that they no longer have any rights to such materials or information, and they will represent that the original and all copies of such materials and information have been returned to the company or to the customer/s or



---

**GLOBAL CODE OF CONDUCT**

---

prospective customer/s.

Employees also acknowledge, undertake and agree as follows:

- I. Employees shall not use any knowledge, trade secrets or other information that is treated confidentially by the company or its customers including, but without limitation to, information on the company's knowledge bases except in the proper course of their duties or as otherwise permitted by the company. Confidential information does not extend to information already in the public domain unless such information has arrived there by unauthorized means.
- II. Without limiting the previous clause employees undertake that they shall not attempt to:
  - a. remove or take any such confidential information; or
  - b. disclose confidential information to any third party other than in the proper course of their duties or as otherwise permitted by the company; or
  - c. gain personal advantage from trading in or based on confidential information; or
  - d. Cause or procure any other person to deal in the securities of any company on the basis of confidential information.
  - e. obtain nor claim any ownership interest in any knowledge or information obtained from Hexaware and its knowledge bases either during or even after the termination of employees' relationship with the company
  - f. Employees cannot disclose to any future employer or use for their own purposes any confidential information they may have access to during their relationship with the company.

**11. Intellectual property rights & ownership**

- All intellectual property created in the course of employment belongs to Hexaware. All computer equipment, software and facilities used by employees are also proprietary to Hexaware, including all documents, materials and Emails created.
- Hexaware also reserves the right to withdraw any of the facilities provided if it considers that employees' use of it is in some way unacceptable.
- For details, please refer to the Hex 5706 Intellectual Property Rights (IPR) Policy available on StationH.

**12. Non-solicitation of employees**

**GLOBAL CODE OF CONDUCT**

- During the term of employment and in the event of ceasing the services of the company for whatsoever reason, the employee agrees that, in addition to any other limitation during the term of the employee's employment and for a period of one year after their termination, the employee will not directly or indirectly-
  - Solicit or accept employment with any Hexaware or its subsidiaries ('Hexaware') customer to which the employee has provided services as Hexaware employee.
  - On the behalf of the employee or as a partner or as an officer, director, an employee, agent or shareholder or any other entity; or person or as a trustee, fiduciary of other representative or any other person or entity.
  - Employee, solicit the employment of, or encourage or aid any other party to employ or solicit the employment of any Hexaware employee to terminate employment with Hexaware.
  - Contact any persons or companies which are customers or prospective customers of Hexaware or any of its affiliates or subsidiaries for the purpose of soliciting the customers or prospective customers in competition with Hexaware its affiliates or subsidiaries nor solicit or divert or cause ~~anyone~~ to solicit or divert, any such customers or prospective customers from Hexaware its subsidiaries, affiliates.

**13. Information Security, Data privacy & Data protection**

- Information Security means protecting information and the related information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The term Information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity, and availability of information. Information Security is concerned with the confidentiality, integrity, and availability of data regardless of the form the data may take electronic, print or other forms.
- The information created and used by Hexaware is one of our most valuable assets. Damage or loss of these assets could severely impact our customers, violate laws and regulations and negatively affect the company.
- Given the competitive nature of our business, Hexaware's information assets must be protected. All Hexaware employees, consultants, trainees must take the necessary steps to ensure that the company's assets are properly protected from threats that exist. For further details on Information Security employees are expected to refer to the Information Security Policy document available in Intranet.
- Employees are expected to ensure that they nominate themselves for the awareness training on Information Security that is held periodically.
- E-mail
 

Hexaware provides E-mail systems to employees to facilitate the performance of company work and their contents are the property of Hexaware. Management reserves the right to retrieve the contents for legitimate reasons, such as to find lost messages, to comply with investigations of wrongful acts or to recover from system failure.

## GLOBAL CODE OF CONDUCT

---

- Internet browsing

The browsing facility shall be provided for carrying out the company's business and usage is subject to monitoring. Any inappropriate usage shall result in warnings, removal of browsing facility and other disciplinary action.

- Login ID & passwords

- ✓ Employees shall ensure that Hexaware password rules are followed.
- ✓ Employees shall enable password protected screen saver.
- ✓ Employees shall not share their passwords.
- ✓ Employees shall change passwords at regular intervals and whenever there is any indication of possible system or password compromise.
- ✓ Employees shall avoid keeping paper record of passwords.
- ✓ Employees shall change temporary passwords on first log on.
- ✓ Employees are solely responsible for all actions committed using ID and hence expected to not to share their passwords with others or leave logins unattended.
- ✓ Employees shall not include passwords in any automated log-on process, e.g., stored in a macro or function key.

- Visitors

Employees shall not take visitors into the office premises without security authorization.

- Clean desk policy

- ✓ Employees shall lock away all confidential and /or restricted information outside office hours.
- ✓ They must not leave sensitive information in the open while they are away from their desk.
- ✓ Employees should log out and switch off their PC at the end of the day.
- ✓ Printers should be cleared of sensitive data.
- ✓ Employees shall use shredders for destroying confidential data.

- Licensed software

- ✓ Employees shall ensure that only authorized and licensed software is loaded on the computer system assigned to them
- ✓ Employees shall not make unauthorized copies of copyrighted software.

- Anti-virus

- ✓ Ensure that the latest licensed anti-virus software is installed and always enabled on your PC.

- Incident reporting

- ✓ If employees become aware of any breach of security of any kind, or any incident of possible misuse or violation of this policy, they must report to the Information Security Team.

- New installations

**GLOBAL CODE OF CONDUCT**

- ✓ No hardware changes are allowed to the workstation /PC. Installation of modems network connections, if not provided are prohibited.
- Social media obligations
  - ✓ All employees are expected to familiarize themselves with social media policy available on intranet portal & follow it without fail.
- Public speaking & press enquiries
  - ✓ All media relations activities throughout Hexaware are conducted and managed in adherence with the principles of honesty, integrity and transparency. Competitive international benchmarking on the best communication practices is always encouraged at Hexaware. Information dissemination to the media and resolution of media queries must be comprehensible, factual and completed within reasonable time deadlines.
  - ✓ All media relations activities including communication during crisis situations at Hexaware are routed through the Corporate Communications Department. The Corporate Communications Department is responsible for planning, directing and monitoring the activities of corporate press releases and communication.
  - ✓ For details, please refer to the Hex 5442 Social Media Policy available on StationH.)
- Data Privacy & Data protection
  - ✓ Hexaware's Data privacy policy details personal & sensitive personal data collection & processing, cookie policy, our policy on children, Data Transfer and disclosure of Personal Data etc.
  - ✓ Hexaware takes reasonable steps to protect information. The company has put in place appropriate physical, electronic and managerial procedures to safeguard and secure the Information from loss, misuse, unauthorized access or disclosure, alteration or destruction.
  - ✓ For more details, please refer data privacy policy available on Hexaware website ([Privacy Policy | Hexaware](#))

**14. Reporting of unlawful and unethical behaviour, whistle blower policy**

- Hexaware expects employees to:
  1. report promptly and in good faith, any actual or suspected violation by an employee of the standards, requirements or expectations set out in this code of conduct; and
  2. Encourage other employees to do the same.
- Hexaware has constituted Whistleblower Policy as a mechanism to encourage a climate of open communication within the Company to report concerns at the earliest opportunity including any unethical practice or behavior, actual or suspected Fraud or violation of the Company's code of conduct or ethics policy

## GLOBAL CODE OF CONDUCT

---

and thus avert a larger issue in the future.

- The purpose of the Whistle Blower Policy is to enable a person who observes an unethical practice or behavior (whether or not a violation of law), actual or suspected Fraud or violation of the company's code of conduct or ethics policy to approach the Whistleblower Committee of the Company without necessarily informing their supervisors.
- For more details, please refer to Hex 5870 "Whistleblower policy" available on StationH.

### 15. Organization discipline & decorum

#### **Personal Appearance**

- While the company fully subscribes to the view that what employees wear is their own concern but, in consideration of the image of the company, employees are expected to demonstrate professionalism and excellence in all aspects of their behavior including the attire while at work and while on official duty. Considering the prevailing trends in business attire Hexaware recommends some norms which are outlined in the Dress code policy & guidelines. (Path: StationH – Resources- Documents-HR Policies & Processes – India – My Onboarding – Dress code policy & guidelines).

#### **Office Discipline**

- Employees are expected to help maintain a quiet environment and a clean desk.
- Smoking within the office premises is strictly prohibited and playing of computers games is not allowed.
- Office equipment must be handled carefully. PCs should be switched off before leaving the premises.

#### **Working Hours**

The company has flexi timing policy and observes a 5-day week. Working hours are country/ location/ customer specific, whichever is applicable.

If a customer requires alternate working hours, the customer's required working hours will supersede.

#### **Access card and Attendance**

Employees are expected to display their ID card while they are in the office premises. Also, they are expected to observe security regulations as intimated time to time.

As they come in, they must:

## GLOBAL CODE OF CONDUCT

---

- Register their attendance with the help of the Access Card and swipe it every time they enter or leave the office premises.
- They are expected to display their card while they are in the office premises. In case they are on official outdoor duty or forget to bring the access card then they must follow the process as per Hexaware's policy in this regard.
- Employees are expected not to swipe access cards for others. This will be considered as serious misconduct and will invite disciplinary action.
- In cases where the place of work is not the designated office, the employee is expected to use any such systems which are designed and implemented for the purpose of marking attendance. For details, please refer to the Attendance Policy & Guidelines available on StationH.

### Time Sheet

- All Hexaware employees (Regular – Up to G12) & Retainers are expected to fill their Time Sheet.
- To fill your time sheet, Login to Teams on your mobile phone -Time App -Login – Fill in the details.
- Employees working on client site, must fill client time sheet (as per client requirement) and Hexaware Time Sheet.
- Incase if you fail to fill your Time Sheet within the stipulated time, you will be marked as Defaulter.

### Phone Calls

- Phones must be utilized for official purposes and personal calls must be kept to a minimum.
- Employees are expected to pick up a ringing telephone at the earliest. In case the concerned employee is not available, the other employee should take the message.

### General

- Employees are expected not to discuss their problems, if any, whether personal or organizational, with the customers / customers.
- Collection, betting and trading within the office are strictly forbidden. Under special circumstances certain collections i.e., for charity, disasters, wedding gifts etc. may be permissible but only when authorized by the Head of the Unit/ Head of Administration.

Hexaware forbids actions or content connected to illegal activities. Employees cannot use

## GLOBAL CODE OF CONDUCT

---

messaging services to publish posts, distribute or disseminate defamatory, infringing, obscene, or other unlawful material or discussion. This ban strictly includes, but is not limited to, child pornography, illegal drugs, software piracy, and physical harassment.

- Employees shall not use Hexaware web or messaging services for the purpose of linking to external sites that violate this code of conduct.
- Employees should not upload files or post messages that contain photos, music, software or other material protected by intellectual property laws, rights of privacy or publicity, or any other applicable law unless they own or control the rights there to or have received all necessary consents. Hexaware is not liable for any use of material posted by users.
- Employees should not post or promote any materials that could damage or dislocate another user's computer or would allow others to wrongly access software or web sites.
- In addition to upholding this code of conduct, employees are responsible for adhering to all local and national laws that pertain to their working location / conditions whether in India or during visit / deputation / transfer abroad for short term or long term.

### Personal Property

- To lose anything, however small it may be, is an unpleasant experience. But this may happen to any employee. Securing personal property is primarily the responsibility of the individual employees.
- Personal Search: Even though this is an extreme step, the company reserves the right to search for any employee if such search is warranted for legitimate reasons.
- Lost and Found: All items of lost property are to be handed over to the Administration representatives of respective locations, which will be retained by them until their rightful owner with proper identification claims them.

### Acts of Misconduct

The following acts and omissions shall be treated as misconduct. This list includes but is not limited to:

- ✓ Willful in-subordination or disobedience, whether alone or in combination with others, to any lawful and reasonable order of a superior
- ✓ Theft, fraud or dishonesty in connection with the Hexaware's business or property
- ✓ Willful damage to or loss of Hexaware's goods or property
- ✓ Taking or giving bribes or any illegal gratification
- ✓ Habitual absence without leave or absence without leave for more than 10 days
- ✓ Habitual late attendance
- ✓ Habitual breach of any law applicable to the Hexaware

**GLOBAL CODE OF CONDUCT**

- ✓ Riotous or disorderly behaviors during working hours at the establishment or any act subversive of discipline
- ✓ Habitual negligence or neglect of work
- ✓ Frequent repetition of any act or omission
- ✓ Striking work or inciting others to strike work in contravention of the provision of any law, or rule having the force of law
- ✓ Misrepresentation or giving false statements about personal/professional background or suppression of relevant facts during the selection process or at the time of joining or concealing any information that would have played a role in selection / rejection of the candidature for employment
- ✓ Involvement in criminal offences
- ✓ Violation of the terms of employment and undertaking given at the time of joining/thereafter or violation of the service agreement
- ✓ Abetting or inciting others to disobedience or misconduct
- ✓ Conflict of interests with Company's business interests
- ✓ Any harassment at workplace

In case of employees violating any of the above acts or found indulging in any of the above misconduct; company reserves the right to take an appropriate disciplinary action commensurate with the act of commission and omission after doing the enquiries/investigation.

No notice of termination shall be necessary if an employee is dismissed from service for proven misconduct, breach of code of business conduct, violation of service agreements, violation of confidentiality agreement or disobedience of written instructions.

**Violations of this code**

Violations of this code shall be reported as per the Whistle blower policy. In applicable cases it will also have consequences in employment law and may lead to external investigations and legal proceedings shall be initiated against the employees who violate any legal or contractual agreements/obligations with the Company.

**16. Training & certification**

- a) The HR function must ensure to inculcate all the principles as laid down in the code and other ethics and compliance policies of the Company by imparting trainings as follows:
  - i. To all new joiners covering Hexaware's code of conduct, Anti- Bribery and Anti-corruption Policies, Anti Money Laundering Policy and other related policies, within 30 days of joining.



## **GLOBAL CODE OF CONDUCT**

---

- ii. Annual refresher training to all the Employees to educate them on the requirements and obligations as laid down by the company's code and all the other ethics and compliance policies and procedures as well as rules and requirements of all the applicable laws and regulations.
- b) Upon joining Hexaware each Employee will be provided with a copy of the code of conduct and required to sign an acknowledgement. On an annual basis, each employee will be required to recertify compliance with the code. Annual execution of a statement of compliance with the code [including any policies and procedures referred therein] shall be a condition of your continued employment with the Company.

### **17. Review of the code**

Hexaware will periodically review this code and make amendments as considered necessary in the interest of governance and in accordance with the relevant laws and regulations.

### **18. Administration of the policy**

The code is accessible to all the employees on the company's intranet. The company must also inform all the third parties about this policy or any amendments thereof, through online upload of the code on the company's website or any other mode as may be deemed to be necessary in this regard.

Any questions, exceptions or evaluations related to this code must be forwarded to the Compliance Officer, by means, such as email, by phone or in person.

### **19. Annexure 1- Statement of compliance**



GLOBAL CODE OF CONDUCT

Hexaware Technologies Limited
Code of Conduct
Annual Statement of Compliance
<p>This is to acknowledge and certify that:</p> <p>I have received and reviewed Hexaware’s Code of Conduct. I agree to comply with the standards referenced in the Code and all related policies and procedures referred to herein. I acknowledge that the Code is a statement of principles for individual and business conduct and does not constitute an employment contract. I further acknowledge that it is my responsibility to understand and follow compliance standards and to adhere to the ethical principles outlined in the Code of Conduct.</p> <p>I will comply with all relevant Anti-Bribery and Corruption laws including all laws, regulation and other requirements as applicable to the respective geographies in connection to our work with the Company.</p> <p>I will not offer, pay, promise, solicit, provide, accept, or authorize, directly or indirectly, any illegal bribe, kickback, or other improper or illegal payment to any person including any Public Official (Government Official<sup>1</sup>) in connection with our work with the Company.</p> <p>I will not authorize, offer, promise or make any payment or give anything of value<sup>2</sup> directly or through a Third Party a commercial party, in order to induce a Government Official to do or omit to do any act in violation of a duty or other obligation or to influence or reward an action or decision of the Public Official (Government Official) or any non-government/ commercial party or to gain an improper business advantage.</p> <p>I will not deal with any Government Official who has a direct or indirect legal or beneficial interest in the business of the Company.</p> <p>I will advise the Company immediately if these certifications change and/or no longer remain accurate during the term of the employment.</p> <p>I will report any potential or actual violation of which I become aware promptly in accordance</p>

<sup>1</sup> For purposes of this certification, “Government Official” shall mean an officer or employee of a government or government agency of any level, whether by appointment, by election or by agreement; an officer or employee of a body corporate that provides a service to the public; exercising a public function or acting in an official capacity on behalf of a government; a party official or candidate for political office; an officer or an employee of a public international organization, such as the World Trade Organization and the United Nations; or an employee, officer, or director of a state-owned or state-controlled enterprise

<sup>2</sup> For purposes of this certification, the term “anything of value” should be interpreted broadly to include anything that might be of value to the recipient, including (but not limited to) cash, future business, gifts, travel expenses, entertainment (e.g., sporting events, concerts, etc.), offers of employment or internships, business meals, sponsorships, and cash or in-kind charitable contributions. This also includes things of value provided indirectly, such as business opportunities to business partners; gifts or hospitality to a spouse; or internships or jobs for children of the intended bribe recipient

GLOBAL CODE OF CONDUCT

Hexaware Technologies Limited	
Code of Conduct	
Annual Statement of Compliance	
with Hexaware's Whistle Blower Policy. I understand that Hexaware maintains a policy of non-retaliation provided that the report is made in good faith. I understand that any violation of the Code or any ethics or compliance policy or procedure is grounds for disciplinary action, up to and including termination of employment.	
I confirm that to the best of my knowledge:	
<ul style="list-style-type: none"><li>I am not involved in any situation that conflicts or might appear to conflict with the Code.</li><li>I have promptly disclosed to you all conflicts or potential conflicts with the Code that I have been involved in since the date of the last Statement of Compliance signed by me and such conflicts have been resolved to the Company's satisfaction.</li></ul>	
I also agree to notify Compliance Officer immediately of any change that might adversely affect my compliance with the Code.	
Employee Name	Thamocharan Chandran
Employee ID	
Job Title	
Department	
Location	
Date	
Signature	

20. Frequently asked questions (FAQ)

Why do we have a code?

The Code serves as a guide to how employees should conduct themselves as a member of the Hexaware team. Preserving our corporate culture and ensuring compliance with legal, regulatory and fiduciary duties is vital to the organization and following the Code helps us do that.

Who must follow the code?

This Code applies to Hexaware Technologies Limited, its subsidiaries and affiliates operating across all geographical regions (referred to as the "Company"). It thereby applies to all employees of the Company

---

## GLOBAL CODE OF CONDUCT

---

regardless of their location.

### **What are responsibilities laid down by the code?**

Employees have two responsibilities. First, all the employees must follow not only the letter of the Code, but its intent and spirit as well and certify the commitment/compliance on an annual basis. Second, if you suspect someone may be violating the Code or any other compliance and governance policies laid down by the Company, employees have an obligation to report it. To make a report, follow the section of the Code: "Reporting of Unlawful and Unethical Behavior, Whistle Blower Policy".

### **How will an employee know if there is a problem?**

The Code attempts to deal with the most common issues that an employee may encounter, but it cannot address every question that may arise and hence the Code is by no means a substitute for our good judgment. When an employee is not sure what to do, they ask themselves the following questions:

- ✓ Is it illegal?
- ✓ Does it feel like the wrong thing to do?
- ✓ Would you feel uncomfortable if others knew about it?
- ✓ Will it have the potential to create a negative perception of themselves or the Company?
- ✓ Do you have a personal interest that has the potential to conflict with the Company's interest?

If answer to any of these questions is "yes", then the proposed conduct may violate the Code and you should ask for help.

### **How should I ask for help?**

If an employee has any questions about the Code, any policies or guidelines referred to herein, or about the best course of action to take in a particular situation, employee should seek guidance from their supervisor/immediate superior or Compliance Officer.

### **What if an employee would like to make an anonymous report?**

An employee may make an anonymous report by any of the means or channels as defined in Hexaware's Whistle Blower Policy. If an employee chooses to make an anonymous report, their anonymity will be protected to the fullest extent possible as permitted by law. Keep in mind, however, that maintaining your anonymity may limit the Company's ability to investigate your concerns.

### **What are the consequences for violating the code?**

Violations of the Code or any of the policies and guidelines incorporated by reference herein, can vary in its consequences. Hexaware reserves the right to take appropriate action for violation of this code that fits the

**GLOBAL CODE OF CONDUCT**

---

nature and particular facts of the violation including reprimand or other disciplinary action such as termination of your employment at the company. Certain violations of the code also contravene applicable laws and therefore can have severe consequences outside of Hexaware. Depending on your actions, failing to comply with the code could lead to civil or criminal prosecution, which could result in substantial fines, penalties and/or imprisonment

Certificate Of Completion		
Envelope Id: 95F02123408E4EB59A6E28A93168B66B		Status: Delivered
Subject: Welcome To Hexaware- Mandatory Joining Documents		
Source Envelope:		
Document Pages: 61	Signatures: 0	Envelope Originator:
Certificate Pages: 5	Initials: 0	Prasanna P
AutoNav: Enabled		PrasannaP1@hexaware.com
Envelopeld Stamping: Enabled		IP Address: 208.127.31.73
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi		
Record Tracking		
Status: Original	Holder: Prasanna P	Location: DocuSign
5/27/2024 7:08:12 PM	PrasannaP1@hexaware.com	
Signer Events	Signature	Timestamp
Thamotharan Chandran		Sent: 5/27/2024 7:08:21 PM
methamu8601@gmail.com		Viewed: 5/27/2024 7:58:28 PM
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure:		
Accepted: 5/27/2024 7:58:28 PM		
ID: 47c433d8-9279-4d34-9c63-5ff006f3eab1		
In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Sathish	COPIED	Sent: 5/27/2024 7:08:21 PM
sathish2@hexaware.com		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure:		
Not Offered via DocuSign		
Prasanna P	COPIED	Sent: 5/27/2024 7:08:22 PM
prasannap1@hexaware.com		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure:		
Not Offered via DocuSign		
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/27/2024 7:08:22 PM
Certified Delivered	Security Checked	5/27/2024 7:58:28 PM
Payment Events	Status	Timestamps



## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Hexaware Technologies Ltd (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**



Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

#### **How to contact Hexaware Technologies Ltd:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [contracts@hexaware.com](mailto:contracts@hexaware.com)

#### **To advise Hexaware Technologies Ltd of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [contracts@hexaware.com](mailto:contracts@hexaware.com) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

#### **To request paper copies from Hexaware Technologies Ltd**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [contracts@hexaware.com](mailto:contracts@hexaware.com) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

#### **To withdraw your consent with Hexaware Technologies Ltd**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to [contracts@hexaware.com](mailto:contracts@hexaware.com) and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Hexaware Technologies Ltd as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Hexaware Technologies Ltd during the course of your relationship with Hexaware Technologies Ltd.