Term & Conditions of Working in Microsoft Account

Name of the Employee: Kapil Bohra

Location: Lucknow

Date: 3/22/2021

HCL Employee id: 51880206

HCL Email id: kapil.bohra@hcl.com

Microsoft V- id: v-kapilbohra@microsoft.com

For Execution by all the employees assigned / working in Microsoft Account

Undertaking

As a condition and consideration of my association with Microsoft Account in a responsible position. I hereby agree to the following:

Employee Services Special & Unique: I recognise the duties and services to be performed by myself as an employee or associate of Microsoft Account which are special, unique, and intellectual in nature.

Conditional information shall include all

- Production Processes, marketing techniques and arrangements, mailing lists, purchasing information, pricing policies, quoting procedure, financial information, funding information, customer and prospect names and requirements, employee, customer, agents, supplier and distributor data, business strategies ,plans, assets, liabilities, revenues, profits price lists and other material or information relating to Microsoft Account and the manner in which Microsoft Account carries out its operations.
- Source & object code, flowcharts, algorithms, coding sheets, routines, compilers, assemblers, design concepts and related documentation and manuals.

All ideas which are derived from or related to my access to or knowledge of any of the above enumerated materials and information.

The absence of any marking or statement that particular information is confidential information shall not affect its status as confidential information.

I understand that "Confidential Information "for the purpose shall mean and include all information, regardless of the form and whether oral, written, stored, in a computer databases or otherwise, which has been disclosed by HCL & its affiliates/ Subsidiaries / Microsoft or any of its employees to myself. I understand that confidential information does not include any of the foregoing items, which has become publicly known and made generally available through no wrongful act of mine or of others who were under confidentiality obligations as to the item or items involved or independently

developed without use or reference to such Confidential Information; or rightfully disclosed by a third party without any restrictions on disclosure.

I hereby accept the responsibility for maintaining the secrecy and confidentiality of such information and all portions thereof shall survive for a period of five (5) years. Further I undertake to abide by all the HCL information security, data protection, data classification and data privacy policy; moreover, I have also gone through below mentioned Do's and Don'ts and aware of repercussions of not adhering to it.

Do's-

- Know and comply with the Information security policy of HCL & its Microsoft
- Ensure your Desktop / Laptop are locked during your absence.
- Ensure protection of your company assets while in transit and in public places
- Protect HCL's and Microsoft Asset, PR and proprietary information from unauthorized access / disclosure.
- All Media containing confidential information should be handled diligently and securely disposed, when it is no longer required.
- Report promptly any suspected Information Security Incident on Incident Management System in the following path:
- For Apps, Infra & ERS employees: My HCL >> My Transactions>>Others>>Security Incident Management>> Raise Incident
- For BSERV employees: I Assist Home Page>> Applications>> Report security Incident>> Raise Incident.
- Change your HCL & MS passwords frequently & ensure that HCL and MS V-dash id passwords are different.

Don'ts

- ➢ Don't allow tailgating
- ➢ Don't share user ID's, passwords & any authentication credentials / devices
- ➢ Don't use Generic / Common user ID's
- ➢ Don't open suspicious emails & links.
- ➢ Don't visit / download from prohibited / unauthorised sites.
- ➢ Don't send emails from HCL / Microsoft domains to other domains.
- ➢ Don't copy/ paste Microsoft business data on any personal devices / blogs/ social network sites / internet.
- ➢ Don't download unlicensed software / freeware.
- ➢ Don't carry unauthorised media devices into the facility & Microsoft operations areas.
- ➢ Don't share personally identifiable information (PII) belonging to you, your colleagues or Microsoft data without appropriate authorisation over internet.
- ➢ Don't leave your company assets (Laptop / Data card) unattended while in transit & in public places

➢ Don't put any organisational or Client specific document or information in public & personal domain or social networking sites i.e. Google Drive, GIT HUB, Facebook, WhatsApp, Twitter etc.

Incidents	Action
Violation of Non-disclosure agreement & HCL/ Microsoft Information Security Policy	**Termination**
Misuse of Classified business & proprietary information belonging to HCL or Microsoft.	**Termination**
Access / Storing pornography	**Termination**
Downloading & installing unauthorized software	**Termination**
Posting of classified HCL / Microsoft information on Internet	**Termination**
Hacking / reverse engineering HCL / Microsoft systems	**Termination & Legal Action**
Password Sharing	**Appraisal cycle to be extended by a period of 6 months / 1 year or Termination**
Unauthorised Media access, Like USB, CD, ROM etc.	**Appraisal cycle to be extended by a period of 6 months / 1 year or Termination**

Signature :-

DocuSigned by:

Kapil Bohra

2274188D8BEC4D9...