Hi Team,

CBA has provided approval to "WORK FROM HOME" based on certain conditions which need collective adherence by HCL and all HCL Employees working in CBA account.
All conditions and service levels as accepted in MSA and SOW need to be adhered to without any dilution.

Please read this mail thoroughly and send acknowledgment mail stating that "I have READ, UNDERSTOOD AND will FOLLOW these guidelines" to PMO.
You can also use "Yes" or "No" voting button on confirming the above statement. 'yes' – I agree to the above statement and will comply. 'No'- I do not agree and cannot comply.
If 'NO' – then send a specific issue copying your platform leads and PMO.

This need to be completed before onboarding into CBA.

Your minimum obligations includes (and other requirements as per HCL and CBA polices)

1. Complete all CBA Mandated Mandatory training
2. Complete all HCL Mandated Mandatory training on Information security and Data Protection
3. Disclose your correct residence address (place you are currently working) from where you are performing your duties to HR/PMO.
4. DO NOT work in any place other then disclosed place of residence.
5. Perform your CBA related work only from approved location (your disclosed residence as mentioned in point 3 or CBA ODCs)
6. Keep CBA information and data confidential while working from home – Not to share/ discuss any details with family members
7. DO NOT share credentials (VDI, Passwords, RAS Token etc.) with anyone
8. DO NOT send any emails to Non CBA domain (external mail) from CBA Mail ID/Device
9. Connect to VDI only through HCL VPN and not directly access VDI through internet or from personal devices.
10. Inform your managers and create Info security incidents immediately within HCL or CBA in case you commit/ notice any violations.

Following is the additional risk and security requirements set out in the Bank's approval to Work from Home
Key aspects which need your attention have been marked below.

(a) The Supplier must inform the Bank immediately if the Supplier has any cyber or data privacy concerns.

(b) To the extent reasonably possible, the Supplier must maintain similar levels of control over the equipment and usage in respect of the approved Supplier Personnel and locations to the controls in respect of the Approved Facilities.

(c) The Supplier must not allow Supplier Personnel to share credentials or RAS tokens or codes with each other.

(d) The Supplier must not attempt to disable or bypass any Bank security controls.

(e) The Supplier is not authorised to establish direct connection from approved device to VDI. All

connections to VDI must be routed through HCL VPN. The Bank will establish appropriate controls to limit direct access to VDI for connections not routed via HCL VPN.

(f) This approval does not allow or provide for additional CBA LAN accounts, VDI accounts, CBA devices, access to MyRas or CBA Jumphots in order to access the CBA network or environment. Requests for additional access are to follow standard CBA process with priority to be given to RUN/Critical resources to keep the Bank operational.

(g) The Supplier is to monitor capacity and performance of their work from home technology solution. If capacity is impacting performance due to increased usage, the Supplier must prioritise connections and usage for essential supplier staff identified as critical to support the CBA account. These are staff members identified in the Supplier's BCP as critical (supporting RUN functions of the bank). This is to minimise disruption risk to the Bank. The Supplier is to immediately inform CBA of performance related matters that pose a risk to critical service delivery.

(h) The Supplier is to immediately inform CBA of identified security control weaknesses or incidents. Depending on severity of the incident or weakness, CBA may revoke approval for the work from home solution.

(i) For all Supplier staff working from home, the Supplier must take all reasonable steps to ensure that staff access is appropriate for the role. The Supplier will continue to provide the Bank, role and access details of Supplier personnel working in the engagement. Wherever notified, the Bank will take appropriate steps to ensure access rights are reduced to the minimum required for the role.

(j) The Supplier must issue staff working from home with education/guidance that communicates the below (at a minimum):

(i) Supplier staff must keep CBA information and data confidential while working from home. I.e. not visible to other people in residence and ensure particular care is taken if other members of the family are working for corporate accounts which are CBA competition.

(ii) CBA information and data is to remain on the supplier managed device. CBA information and data is not to be stored on personal devices.

(iii) CBA information or data is not be sent to external email addresses.

(iv) Work from home is limited to the supplier staff member's place of residence.

Acceptance of Accountabilities Team Member: (Must be a Technology Partner staff member who is working on CBA premises) I have read and understood my responsibilities and agree to comply with these guidelines regarding working in shared premises		
Name with SAP Number	Signed	CBA Joining Date