Work From Home - Guideline

Below are some of the basic requirements and guidelines to follow.

A. Wi-Fi Connectivity -Ensure you use a secure Wi-Fi network to connect to your organization network. Avoid Public Hotspots or open Wi-Fi.

B. Connected – Ensure you are connected to the internet and skype during routine office hours i.e. 10 AM to 7 PM (Lunch Break 1 PM to 1.30 PM)

C. Communicate – Ensure everyone have stand up meeting (video call/skype/phone) of about 5-15 max every day before they resume to their routine task with colleagues and supervisor.

D. Alert – Be alert on the skype and respond to the queries, questions discussed in the group or personal on skype / phone .

E. Reporting – Ensure that before end of day, you submit your report to your superior summarised what is done, what is pending, any queries, dependencies and next day plan .

For Development/QA Team below is the authority

1) To Respected project manager and CC to Dhaval
   nitin@fusioninformatics.com,
   Harpal.zala@fusioninformatics.com
   Dhaval@fusioninformatics.com

For Designer Team below is the authority

1) To respected superior and CC to Ashesh
   priyanka@fusioninformatics.com
   Ashesh@fusioninformatics.com

For Sales Team below is the authority

1) To respected superior and CC to Ashesh
   alok@fusioninformatics.com
   Ashesh@fusioninformatics.com

For Marketing Team below is the authority

1) To respected superior and CC to Ashish
   ashok@fusioninformatics.com
   ashiesh@fusioninformatics.com

F. Live Support Mandate

A. It is strongly recommended to establish 24*7 support to handle queries from top management in case of emergency.

G. Basic Mandate Hygiene–for organisations and employees alike

A. Enforce strong password policies
B. Change your router password, and Encryption should be set to WPA2 and WPA3.
C. Set up session time-out on all remote connections and automatic screen locking feature on all computers.
D. Turn off networking capabilities (such as Bluetooth) for mobile and laptop when not necessary for work.
E. Turn on personal firewalls, if available
F. Restrict other applications allowed on the mobile device
G. Add additional security authentication layers to company data on mobile devices.
H. Set up restrictions to keep unknown or unnecessary browser extensions from being installed. Many extensions have tracking codes which users are unaware of, while others are used to spread malware. Stick with trusted and needed browser extensions only.
I. If possible, physically secure computers with locking cables
J. Employees should know how to spot and respond to unusual computer activities, which can be an indicator for any suspicious activity.
K. Employees must be aware whom to contact for IT support, how to verify the genuinity of the person asking for access to their computer.
L. Avoid clicking on links in unsolicited emails and be wary of email attachments. See ‘Using Caution with Email Attachments’ and ‘Avoiding Social Engineering and Phishing Scams’ for more information.
M. While checking personal emails on work machine, be extra cautious and make sure you open attachments only from known and verified senders.
N. Use this as a thumb rule everywhere -neither click on any link nor open any attachment from an unknown source.
O. Use customized spam filter settings for personal email accounts.
P. In case of financial approvals/ dispatch of payments, please cross verify with the concerned person before you issue any payments.
Q. While working from home, should take care of the confidentiality of valuable transactions and sensitive confidential documents.
R. Avoid delivery of sensitive physical documents other than office address and collect them as required with utmost care.
S. No recording of client calls, no screen recording, no clicking pictures, and video capturing

T. Screen capture functionality should be disabled on mobiles
U. Enforce strict email policies with visual markings enablement to restrict print, snip and saving confidential emails.
V. Closure of Unwanted Ports – It is strongly recommended to close unnecessary network ports with the help of your IT/Security teams.
W. Antivirus should be up to date with remote access policy configuration for auto-update of virus definition, client machine should be properly patched before connecting to the organization network.
X. Choose secured and trusted third-party services .It is noteworthy to document remote access requirements, authorize remote access before allowing connections, monitor and control remote access, encrypt remote access connections from the organization's firewall and threat detection. Try to ensure systems/desktops are fully protected and has the same protection as office workstations.
Y. Ensure that all applications and data are stored on the portal's server and cannot be downloaded or saved on an device without permission.

It is every employee's responsibility to follow the same best practices.

Right Work Environment Working from home also largely involves sharing the space with other family members/housemates. It's important to set guidelines to indicate when you are at work so as not to be disturbed. Hence there must be an isolated space for work.

The right set of tools and environment should be available to ensure smooth functioning, like a wireless headset for call center operations, quiet workplace, allowed only whitelisted devices in USB ports; Sys Admins should be proactive and allow USB ports only for authorized devices.

Please review and seek clarity for NDA/ legal undertaking to protect client/business information that you have signed while joining, and it is every employee's responsibility to adhere to it strictly while working from home.