Dear all

In continuation of the IT Security steps that are being taken, let me provide an update for everyone's awareness and alignment.

- Enforcement of Data Classification and protocols and safeguarding highly sensitive data – Implemented and moving into BAU* mode.
- Internet access / web site filtering for all employees reviewed and updated - Implemented and moving into BAU* mode.
- Email transmission to open/free mail domains will go through an approval step. - Implemented and moving into BAU* mode.
- Email size restrictions applied across the group - Implemented and moving into BAU* mode.
- Minimum Password Length is set to '10' and complexity requirement maintained - Implemented and moving into BAU* mode.
- Data transfer to open and free data transfer / cloud storage sites will be blocked. - Implemented and moving into BAU* mode.
- IT Asset labelling to identify authorised devices. - This is work in progress and will be carried out by IT field Ops teams.
- **Multi Factor Authentication (MFA)** – Pilot users testing is completed successfully and we are moving to extend this to all remote users. This will apply to all devices that off LAN and also includes the mobile access to O365/email from smartphones. In addition to the password a secure token code / OTP mode is being enabled to provide us the required layer of protection. We will roll out in batches so the impacted community is supported as we transition.

**BAU – Business As Usual*

I also want to highlight and alert everyone to the cyber threats that are also being posted in the media related to COVID-19 Phishing attacks. Let me share the link to the published CERT advisory note.

CERT-In Advisory CIAD-2020-0040

In light of this threat, here are some of the recommended Best Practices to follow -

- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header). Block the attachments of file types, "exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf"
- Beware about phishing domain, spelling errors in emails, websites and unfamiliar email senders Check the integrity of URLs before providing login credentials or clicking a link.
- Do not submit personal information to unknown and unfamiliar websites.
- Beware of clicking form phishing URLs providing special offers like winning prize, rewards, cashback offers.
- Any unusual activity or attack should be reported immediately to ITSecurity@nestgroup.net.

The IT policy documents are made available on our Intranet page for your easy reference - http://home.nestgroup.net/it-policies.html.
(Note: The Intranet site is only accessible from the Office LAN).