Companies and Intellectual Property Commission

a member of the dti group

NOTICE 55 OF 2019

IMPORTANT NOTICE TO CUSTOMERS – CIPC E-MAIL PROTOCOLS

In order to ensure that CIPC data and information is secured with the latest security protection against potential security breaches, CIPC has implemented an **enhanced cyber security solution**, in order to not only protect the CIPC environment, but more specifically the data of our clients which is under the custodianship of CIPC. As a result, clients may have noted that some e-mail transmission/s are affected due to these recent enhanced security features.

In some instances e-mails sent from CIPC to external clients may be diverted to the **"junk" or "spam" e-mail folder/s of the external recipients.** It may also appear as if e-mails sent to CIPC have not been received by CIPC officials.

In other instances, e-mails sent to CIPC may not be delivered at all, or if delivered, attachments thereto may have been removed.

To resolve the problems outlined above, users are requested to follow the steps outlined below.

Where e-mails sent from CIPC are diverted to the "junk" or "spam" folders of the external recipients:

- Go to https://outlook.live.com, where "*Outlook*" is the applicable e-mail application/service provider (the same process will apply to other service providers e.g. Yahoo, GMail, Hotmail, etc.);
- Sign into your account and click on the "*Settings*" icon in the top right of the screen;
- From the list at the bottom, click on "*View all Outlook Settings*";
- From the list of options, under Junk E-mail, select "*Safe Senders*";
- Into the field marked "*Enter a sender or domain here*", enter the domain name **cipc.co.za** and click on the "*plus*" icon;
- Click on the "*Save*" icon to save the settings.

Or where e-mails sent to CIPC are being rejected, attachments are being removed or e-mails sent to CIPC appear to have not been received by CIPC officials the following applies:

Although this error is shown at the recipient's side the correction here fore has to be done on the side of the sender/client/user's domain.
To resolve this:
- Confirm that the size of the attachment/s do not exceed 10 Megabytes (MB) in size;
- Verify the SPF record of the sender domain;
  - *Online tools such as https://mxtoolbox.com/spf.aspx could be used for such a SPF check.*
- Confirm that the e-mail originates from the IP address as reflected in the User/Service Provider (ISP) SPF record;
- Where there is any discrepancy with the IP address please log a call with your ISP to correct the record.
  If this is not corrected by your ISP, any other mail server/s - including those of CIPC – which verifies SPF records of incoming e-mails will reject all e-mails received from that domain.

If after following the steps outlined above, clients still experience challenges herein, kindly proceed to log an enquiry/ticket via the CIPC Enquiries System under the relevant department relating to the specific application (e.g. Companies and CCs/Company Registration, etc.).

The Enquiries system can be accessed by visiting www.cipc.co.za and clicking on "*Enquiries*", or using the link https://enquiries.cipc.co.za.

CIPC apologises for any inconvenience which may be caused by the implementation of these increased security measures, in order to ensure the safekeeping of all data managed by CIPC.

Yours sincerely

Andre Kritzinger
Executive Manager: BISG
27 September 2019