List of measures to be observed by Barristers and Attorneys submitting documents in electronic format to the Employment Relations Tribunal (ERT) through *ert@mail.gov.mu*

1. All Barristers and Attorneys are encouraged to submit statements of case and documents to the Employment Relations Tribunal through the ERT's official e-mail address ***ert@mail.gov.mu***

2. Prior to the start of submitting such documents electronically, all Barristers/Attorneys or other interested parties are requested to provide in writing to the ERT relevant information which includes their mail address, phone numbers including a mobile phone number and the e-mail address which will be used in such correspondences. Information should be submitted using the form "***Barristers and Attorneys Contact Details Form***" (available on the website http://ert.gov.mu). Following submission of the above information, Barristers/Attorneys will be able to forward documents to the ERT solely from their officially submitted e-mail address.

3. All e-mails received by the ERT from Barristers/Attorneys officially submitted e-mail address will be deemed emanating from the said person. Barristers/Attorneys should be fully accountable for their e-mail addresses. They should ensure that their e-mail accounts are secured, having adequate password (See item number 10) which are only accessible to authorised person. It is a good practice for Barristers/Attorneys to use e-mail addresses known by a limited number of people. Ideally the submitted e-mail address should be used to correspond with the ERT only.

4. All e-mails sent to the ERT must be copied to the other party/ies and this must be apparent on the e-mail received. The ERT, ***in no circumstances***, will be responsible for copying or sending the e-mail received to another party.

5. Barristers/Attorneys need to ensure that e-mails sent to relevant parties are properly addressed. The ERT accepts no responsibility if e-mails sent have been improperly addressed to the ERT or third parties.

6. Barristers/Attorneys should **not** send confidential information such as copies of pay slips by e-mail. The ERT will ***in no circumstance*** be responsible for any liability which may occur following dissemination of confidential information. Likewise, the ERT will not accept any responsibility for the dissemination of offensive mails by Barristers/Attorneys and reserves the right to take any appropriate action which it may be advised against the perpetrator.

7. The ERT reserves the right to request for physical production of documents in case of any breakdown of the system whereby the ERT is temporarily unable to receive documents by electronic means.
   Barristers/Attorneys are recommended to phone at the ERT on the **2080091 or 2128286** to ensure that their e-mails have been properly received.
   In cases where the application itself (or dispute referred voluntarily by the parties) has been made online, the relevant party/ies have the responsibility to ascertain on the same day that the application has been properly received.

8. Prior to sending electronic documents to the ERT, Barristers/Attorneys should ensure that:
    - The PCs from which the documents will be sent should have an updated antimalware (antivirus) solution. Barristers/Attorneys should scan documents to be submitted to the ERT using that software prior to sending.

9. Barristers/Attorneys are encouraged to password protect documents sent through e-mail. The password can be communicated to the Registrar of the ERT who is the responsible officer for facilitating the communication of documents.

10. Passwords can be created in line with the following Password Creation Guidelines to ensure that passwords cannot be easily guessed.
    - Passwords should ALWAYS contain: at least 8 characters, both upper and lower case letters, at least one number and at least one special character (for example # $ %{ +?)
    - Passwords should NOT: be based on personal information such as names of family, dates, addresses, phone numbers, be based on work information such as room numbers, building name, co-worker's name, phone number and use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, abcABC123

An approach to devise hard to guess password is to make use of passphrases.
One example of a passphrase is: ***My Password is Strong***
Another way is by taking the first character of each word in a sentence to construct a password. For example: ***A child of 3 years likes to eat ice cream!*** becomes ***Aco3ylteic!***