Password-Protect Documents
Best Practice Guide

To protect the confidentiality of clients' personal information, given the current circumstances, iA has prepared this guide to ensure that advisors follow best practice while performing their professional duties, including password protection of documents containing confidential information.

Therefore, when carrying out your business duties, it is vital to keep in mind that it is your responsibility to maintain the confidentiality of clients' personal information irrespective of the tool or means of communication used.

1. **Password management**

To ensure document security, make sure passwords follow the important guidelines below:

- be at least 8 characters long
- include at least one uppercase letter, one lowercase letter and one special character (a number or a symbol)
- refrain from using the same password each time
- refrain from using personal information (SIN, DOB, etc.)

If your password does not follow the above-mentioned guidelines, your document will not be adequately protected, and you might risk client data breach.

There are only two secure methods of sharing a password with a client:

- verbally (telephone or videoconference)
- by using a question whose answer is only known to the advisor and the client – refrain from using easy-to guess information such as a child's name or date of birth

2. **Email management**

When an email is sent with a message or a document that contains personal data – i.e. information that can directly or indirectly identify individuals – such information must be absolutely saved in a password-protected file.

Examples of information that must be protected by a password are: name, contract number, physical or electronic address, telephone number, medical history, financial transactions, etc.

When an email containing confidential information is no longer relevant or necessary, it must be permanently deleted from the mailbox as well as the trash folder.