Request for allowlisting

Email content distribution and data protection overview

What is 'allowlisting'?

When you arrange for your servers to recognise particular email addresses and domains, it's called allowlisting. By making sure Fidelity email addresses are on your list of approved contacts, you're making sure all plan communications issued by us can be safely received by your employees.

We've made a list of the domains and email addresses for you to give to your IT department:

Domain

- @fidelity.co.uk (Including sub domains below):
  - @email.fidelity.co.uk
  - @message.fidelity.co.uk
- @fil.com

Sender address:

- email.co@fidelity.co.uk
- email.wi@fidelity.co.uk
- email.wi@email.fidelity.co.uk
- Fidelitysecurity@fidelity.co.uk
- notification@email.fidelity.co.uk
- notification@message.fidelity.co.uk
- FidelityPlanViewerAdministrator@fil.com
- Pensions.Service@fil.com
- feedback@fil.com

Email content distribution

Like most businesses, we use third party solutions to help us deliver market-leading services. All third parties go through strict vetting procedures and due diligence checks before we use any of their solutions in our business.

When we communicate by email, for example, we use multiple vendors and software applications, including, Marketo and IMI Connect. Both of these use a multi-layered approach to protect and monitor any data we share.

It's just the distribution that's managed by third parties; the information shared is managed by Fidelity. Fidelity employees process and load the data, define the rules that drive the segmentation and complete the transfer of information to the distributor.

Fidelity's responsibility for the protection of data extends to our suppliers and service providers, so external arrangements must be reviewed as part of Fidelity's security policies. These policies define the necessary oversight and due diligence actions to be performed.

Sending domain

The emails are sent by FIL Life Insurance Ltd and the domain is our own. We take security very seriously at Fidelity and have invested in sophisticated communication tools to increase security and to verify that content being sent is from Fidelity.

Security of our members' personal data

External Security Reviews (ESRs) are conducted to assess Fidelity's third-party suppliers for effective supplier risk management. Reviews like these identify, document, and manage the risk posed by each of Fidelity's suppliers to Fidelity.

The assessment during the review builds a holistic view of the supplier's control environment and Fidelity's potential risk exposure. Ensuring the confidentiality, integrity and availability of members' personal data is our paramount concern, which is why we have a comprehensive information security framework backed up by a wide variety of security policies, standards and procedures. Fidelity prescribes the minimum level of protection required to mitigate the risks associated with accidental or unauthorised use, disclosure, modification, or destruction of information, and for ensuring the confidentiality, availability and integrity of our information and information systems.

WI1125/WF2125842/SSO/1126

Fidelity™ INTERNATIONAL