PENSION SCHEMES

Cyber Security Compliance

Trustee Checklist

Cyber security presents a serious risk to pension schemes, with the potential implications of a cyberattack resulting in loss of member data, pensioners not getting paid and risk to investments.

This document provides a checklist of tasks to ensure trustees meet minimum standards with regards to managing cyber risk. The Essential Foundations are fundamental steps which all trustees should implement as part of their cyber risk management. These steps form part of our Cyber Security Package offering, and we have template documents that we can offer clients at a fixed fee.

The next steps, Best Practice Building Blocks, provide trustees with an indication of practices they should be aiming to adopt to ensure that cyber risk management is a priority. We can provide practical help and guidance with implementing these steps.

If you would like more information about our Cyber Security Package offering then please get in touch.

Initial Steps – Essential Foundations		
Cyber Security Policy	This comprehensive document sets out how the pension scheme manages and mitigates its cyber risk. It should be reviewed and updated at least annually.	
Cyber Security Incident Response Plan	This plan sets out how trustees will respond to a cyber security incident, including what support trustees will need and where it would come from. It should be reviewed and updated at least annually.	
Cyber Security Best Practice Framework and Assessment	This document supports trustees in building their pension scheme's cyber resilience in line with best practice. It then enables them to assess and monitor their pension scheme's cyber resilience. It should be reviewed and updated at least annually.	
Cyber Hygiene Quick Reference Guide	This is a quick reference guide which: • Provides an overview of the pension scheme's approach and key cybersecurity documents; • Sets out practical tips which trustees can refer to on a day-to-day basis; and • Contains contact details for key advisers and stakeholders in the event of a cyber security incident. It should be updated as and when necessary.	
Basic Cyber Security Training	Trustees should receive regular cyber security training, to ensure they understand the nature and impact of cybercrime and its evolving threats. Trustees should be aware of and familiar with tPR's guidance on cyber security principles.	

Next Steps – Best Practice Building Blocks		
Data and Asset Mapping	A detailed mapping exercise should be carried out on flows of data, assets, and other critical information, to help trustees understand their exposure.	
Risk Register	This should record the cyber risk that the pension scheme faces through its key functions, systems and assets. It should be reviewed and updated at least annually.	
Data Protection Documents	A Data Protection Policy and fair processing notice – which should have been implemented following GDPR compliance requirements in 2018 – should be reviewed to ensure their provisions remain up-to-date and fit for purpose. We can provide template documents, if necessary.	
In-depth Cyber Security Training	Cyber-attack simulation training assesses the incident-readiness of trustees and their pension scheme, focusing on the scheme's cyber resilience. Trustees should also consider GDPR refresher training.	
Review of Third Parties	Trustees should understand how cyber security issues are reflected in the provisions of the pension scheme's third-party contracts, and should ensure that these contracts contain robust cyber security clauses.	
Cyber Security Insurance	Trustees should consider the insurance cover the pension scheme has in place in relation to cyber security and renew or extend cover as appropriate. If the pension scheme does not have cyber security insurance in place, the trustees should consider whether it is appropriate for the pension scheme.	

Get in touch

If you would like to find out more about our Cyber Security Package offering, please do not hesitate to get in contact with one of the team below, or your usual Burges Salmon contact.

Richard Pettit
Partner

T +44 (0)117 902 6674
M +44 (0) 7814 703 625
E richard.pettit@burges-salmon.com

David Varney
Partner

T +44 (0)117 902 7261
M +44 (0) 7980 980 102
E david.varney@burges-salmon.com

Samantha Howell
Senior Associate

T +44 (0)117 902 7267
M +44 (0) 7815 465 359
E samantha.howell@burges-salmon.com

Amy Khodabandehloo
Senior Associate

T +44 (0)117 939 2215
M +44 (0) 7812 001 888
E amy.khodabandehloo@burges-salmon.com