XPS Pensions Group

Information Security

August 2019

Information Security

XPS Pensions Group have a comprehensive information security programme designed to provide a layered defence so that all tools work together to protect both XPS Pensions Group and our client's data.

Network traffic is analysed using Darktrace Enterprise Immune system, a next generation AI and machine learning technology.

Information Governance and Risk Management

- XPS Pensions Group maintain an IS027001 Information Security Management System (ISMS) across the group. All information security risks are reported into a group level Risk & Audit committee, held in a central risk register, and the committee meet on a quarterly basis to review all risks across the business. The Risk & Audit committee report directly to the board.
- All security policies are reviewed on an annual basis and whenever there is a policy change to ensure that they meet both customer requirements and regulatory requirements e.g. GDPR.
- XPS Pensions Group use a number of 3rd party suppliers to provide services to both clients and the business. Where these providers have access to personal data we conduct annual security reviews and request penetration test results.
- As part of our recruitment and on boarding process all employees are subject to vetting which includes a criminal background check.

Network Security

- All laptops are configured with Windows 10 and encrypted with Microsoft BitLocker.
- Site-to-site traffic is secured over a private MPLS WAN. Personal and confidential data sent externally is encrypted using a minimum of AES 256-bit encryption.
- The perimeter is secured with Cisco managed firewalls and supplemented by a SonicWall Intrusion Detection/Intrusion Prevention System (IDS/IPS).
- Network traffic is analysed using Darktrace Enterprise Immune system, a next generation AI (artificial intelligence) and machine learning technology. The system learns all traffic (patterns of life) to detect suspicious activity and Darktrace Antigena provides a recommended response to mitigate the threat.
- Email security is provided by Mimecast Advance Threat Prevention configured to filter incoming/outgoing mail to reduce spam, archive mail and prevent attacks using malicious email attachments.
- Regular monthly server updates are implemented using Microsoft System Centre Configuration Manager.
- Wireless Security is provided using Meraki wireless access points. Corporate networks are hidden (restricted to domain authenticated devices/users) and secured with WPA2 encryption.
- Access to the internet is controlled using Zscaler cloud-based internet proxy which blocks all access to social media, cloud-based storage and webmail.

CYBER ESSENTIALS

User Education and Awareness

- Security training is provided to all new joiners via Astute-eLearning online security training and all users are required to undertake annual refresher training.
- Quarterly phishing tests are conducted from KnowBe4 platform.
- Security bulletins are issued on a routine basis to provide additional security guidance and training.

Malware Prevention

- All clients and servers are configured with Webroot Secure Anywhere agents. Webroot provides a next generation cloud-based anti-malware and journal based anti-ransomware solution.

Data Loss Prevention Controls

- Mimecast cloud-based email security is configured for DLP and enforces encryption for all unencrypted personal data.
- Access to USB is restricted via group policy and disabled for all users by default.

Secure Configuration

- Twice annual penetration testing of our perimeter and public IP addresses is conducted.
- Annual AAF01/06 audits are conducted for XPS Administration as recommended by The Pensions Regulator.
- In addition, we hold the UK government Cyber Essentials certification. XPS Administration are certified to ISO 27001 which is being rolled out to offices that were previously not in scope.
- All hardware and software changes are managed through Best Practice ITIL change control processes, therefore all changes require technical and security approval before implementation.
- Standard hardened images are used for all system builds.

Managing User Privileges

- All user accounts are controlled by Microsoft Default Domain Policy and Group Policy Objects to provide least privilege access to data and resources.
- Access is granted using the policy of 'least privilege' and includes regular reviews for all users.
- KeePass is used for administrative password management which helps to prevent uncontrolled storage of passwords and provide easy password auditing.

Incident Management

- Fully documented and updated Incident Management processes exist to manage security incidents which includes standing up a Cyber Incident Response Team (CIRT).
- System Backups are replicated between datacentres with Microsoft Data Protection Manager which can be used to recover systems if there is a virus or ransomware attack. Additional long-term backups are stored in a third external datacentre.
- BCP and DR plans are fully implemented and tested on at least an annual basis.

Home and Mobile Working

- Remote connectivity is secured via SonicWall GVPN and Barracuda client- based VPNs.
- Microsoft Intune is configured to provide mobile device management (MDM) and enforces encryption on mobile devices.

> Our processes also ensure that personal data is encrypted in transit through the use of encryption.

> Training on Cyber related issues is provided at induction and annually thereafter to enhance levels of awareness of risk and the associated process.

For further information

If you would like further details about XPS's approach to Information Security please contact XPS Information Security Team or your client account manager.

@xpsgroup

0118 918 5015

company/xpsgroup

it.security@xpsgroup.com