DMS Information Security Questions and Answers

OPEN BANKING

Question	Answers
Who is the entity responsible for the day-to-day operation of DMS?	Resolving Group 56 Ayres Street, London SE1 1EU, United Kingdom Open Banking will provide first line of support thus should be first port of call, contactable by emailing: Servicedesk@openbanking.org.uk
Where does DMS reside?	The service resides within the European Economic Area.
Who is responsible for the data stored within DMS?	All data shared between users of the DMS system is owned by the entity that generated it. The DMS service applies the appropriate controls to protect this data in transit and at rest. On resolution of the issue/dispute, data is automatically removed from the DMS system. Neither Resolving UK, nor Open Banking users have access to the data.
Who has access to the data with DMS?	Data entered into the DMS by its users is only visible to parties involved in the dispute and authorised support personnel involved in issue resolution.
How long is the data within DMS retained?	DMS data is encrypted and retained for the lifetime of the dispute. All relevant records are removed from the system upon resolution of the dispute.
How is the data within DMS protected in transit and at rest?	Data at rest and in transit is encrypted using industry standard protocols.
Is DMS subject to PCI DSS controls?	No, the service does not fall within the scope of PCI DSS.
What are cloud entry controls applied on DMS?	The service resides behind a web application.
Has DMS been Penetration Tested?	Yes, a full penetration test has been conducted. Major changes or releases will trigger further penetration testing exercises.
Has DMS been subjected to a code review?	Yes, all repositories, packages and dependencies have been reviewed. Regular code reviews are conducted after any major release change.
Does DMS employ Anti-Virus/Malware services?	Antivirus/malware services are deployed on all user and service endpoints. **NB.** DMS does scan uploaded files for viruses/malware; however, the integrity and validity of the evidence uploaded into DMS is the responsibility of the information owner.

DMS Information Security Questions and Answers

OPEN BANKING

Question	Answers
What access controls are in place for DMS?	Robust access controls are in place, including highly complex passwords, multi-factor authentication and monitoring controls.
Is an appropriate change control system in place for DMS?	Yes, automated controls are in place to support change control, including compliance auditing, security analysis, change management, and operational troubleshooting.
Does DMS employ security monitoring?	Continuous security event monitoring, management and alerting is in place to monitor for malicious activity, potential threats or unauthorized behaviour.
Does DMS employ application protection?	All services are continuously audited and assessed for overall compliance with policies and standards.
What intrusion detection/prevention mechanisms are employed on DMS?	Web application firewall and monitoring controls are in place to protect DMS from common exploits that could affect application availability or compromise security
What is the user password policy for DMS?	Users should satisfy the following conditions to set the strong/quality password. • 8 characters minimum • One uppercase character • One lowercase character • One special character • One number
Are password issued directly to the DMS users?	DMS will not send passwords to users via email or any other intermediary. Users will be asked to automatically validate/confirm their email and set their password via the application. This feature is same for reset password functionality as well.
Has a Consensus Assessments Initiative Questionnaire (CAIQ) been completed for DMS?	The CAIQ is an assessment of security requirements compliance of cloud providers. Authored by the Cloud Security Alliance it focuses on providing industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings. As DMS does not fall into any of these categories, a CAIQ response is not required.