Frequently asked Information Information security questions

GENERAL

Which layers are provided by mea; SaaS, IaaS, PaaS ? And who manages the different tiers?

mea manages the software, the platform and the hardware stack for the solution. This ensures the clients will only need to login using their credentials and the entire stack is managed and maintained securely by mea

PEOPLE/ ROLES

Does an Organization Chart exist for mea and can it be produced for review?

Yes and this is available

Does a mea employee list exist and can be produced for review?

Yes and this is available

Is the engineering function established as a distinct entity in the overall mea organization?

Yes

Is there a background check or vetting process for new mea employees?

Yes, mea follows a rigorous vetting process for new employees

Does mea have a full time Security Administration function with personnel tasked with responsibility and accountability for data privacy and cyber security?

Yes, mea has a full time security admin role, who overlooks the end to end security needs of the organisation. This also includes the full security management of the Software, Hardware, Platform stack, data privacy, cyber security, web security reporting to the Chief Security Officer

POLICIES/ PLANS

Does mea have corporate policies for Information security, Patching, Email, Privacy, Internet and can be produced for review?

Yes, mea has all these policies in place and takes full responsibility to patch all the software and firmware stack to ensure the system is free from all critical or major vulnerabilities in a time bound manner

Does mea have corporate policies for Data privacy, Cyber security and Data retention and can be produced for review?

Yes, mea has all these policies in place

Does mea have disaster recovery IT plans and can they be produced for review?

Yes, mea platform runs within a secure dedicated AWS instance. As part of AWS solution, mea has enabled the Disaster recovery process to ensure we always have the platform available in a different region to manage the disaster scenario

Has mea suffered a data security control failure (i.e Hack, Data Breach) ever?

No never

Do you have a Data Breach response plan?

Yes, mea follows a detailed standard data breach response plan. The complete mea data breach response plan can be found in the mea Data breach document

Does mea have an ongoing data privacy and security training/awareness to staff

Yes, mea has a regular data privacy and security training that each of the personal engaged in maintaining the security needs of the organisation need to adhere

Does mea have policies for user access privileges to systems.

Yes, mea uses least privileged access and has defined a set of User access policies that clearly defines each users roles and responsibilities. These policies controls users from accessing only those systems and resources they are entitled to access.

Does mea have policies in place to assess if sub-contractor’s security environment meets applicable data laws and regulatory requirements.

Yes, mea defines the sub-contractor process and guidelines strictly. Every sub-contractor is defined specific roles and given permissions that limits them to view or access only certain system/resources

CERTIFICATIONS AND TESTING/ AUDITS

Is mea ISO 27001 certified, SoC2 certified, HIPPA certified and GDPR compliant and can produce the relevant certification?

Yes, mea is certified for ISO 27001, SoC2 and HIPPA and is GDPR compliant

Does mea have ISO standards for access control including access management in the following areas ?

Yes, mea follows a very strict access control policy management as defined in the mea information and security policy document

Do you have independent audits performed annually?

Yes, mea engages 3rd party auditors to perform Audits and re-certifications annually

Does mea have an annual independent control assessment report?

Yes, mea has external and internal security control assessments

Does a Third Party perform penetration tests for mea and is a redacted copy available?

Yes, this is available on request

Is Anti-Virus and anti-malware installed, current, running and actively maintained on all hardware in all environments including servers, laptops and virtual machines

Yes, mea ensures that anti-virus and anti-malwares are installed to their latest versions on every system/resource being used in the mea platform

Are Intrusion Detection Systems (IDS) deployed and active within mea?

Yes, we use AWS WAF and AWS shield in order to address the IPS and IDS

Are Intrusion Protection Systems (IPS) deployed and active within mea?

Yes, we use AWS WAF and AWS shield in order to address the IPS and IDS

Does mea encrypt non-public data in transit

Yes, by default all data is encrypted during transport

Does mea encrypt non-public data at rest

Yes, by default all data is encrypted at rest

Does mea have a secure data disposal policy that is implemented and functioning as intended

Yes, for every component storing data we have secure data disposal policy configured and running

HOSTING

Is client data is hosted within mea systems on an internal only standardised and secure architecture

Yes, on a secure architecture, hosted on AWS with dedicated hosts

Does mea have outstanding known vulnerabilities within its environment?

mea ensures all vulnerabilities are addressed within a time abound period. However, there might be few low vulnerabilities that might exist and such a list will be published till it is addressed periodically

FUTURE PLANS

Does mea have any plans in place to advance security, data privacy and retention?

Yes, mea has an extensive forward looking plans that can be shared upon request.

Please contact infosecurity@meaplatform.com for more information