1.6.2 Tenderers should describe their procedures for storing, retaining and transmitting data between the Contractor, the Framework Public Bodies (and sub-contractors where applicable) to ensure compliance with the Statement of Requirements (Schedule 1) and to ensure continuity of service and protection against cyber-attacks

At MediaCom, we believe it is the responsibility of every employee to take the same level of care as the company over online security and the management of clients data. As such, upon employment, every MediaCom employee is issued both the GroupM Blogging Policy and the GroupM IT Code of Ethics to read and sign.

The purpose of this is to outline the legal implications of blogging and include recommended best practices for employees, consultants, contractors and non-GroupM employees who maintain or blog on work-related internal or external blogs, as well as for employees, consultants, contractors and non-GroupM employees who maintain personal blogs. In addition, it is to establish the minimum requirements for the use of GroupM information systems, and is a summary of the IT Security Policy to be followed by all employees, consultants, contractors and non-GroupM employees who access GroupM resources.

These Guidelines are read together with WPP Code of Business Conduct, WPP Policy Handbook and GroupM policies to ensure a fully informed view. GroupM are also certified under the UK Government Cyber Essentials Scheme (Certificate No [redacted]) we are currently in the process of certification for 2019. All the software we use is validated against security check points prior to development and purchasing of 3rd party software.

Where will data be stored

We use file structures and data repositories that are structured to ensure data relating to a specific client is separated from other clients' data. These structures allow us to ensure that access to client data is granted on an as needed basis and is restricted to appropriate individuals. Access to client data can only be granted via the [redacted] central helpdesk, this requires approval from the relevant client account lead. This process ensures formal records of the request and approval are documented and auditable.

WPP have a strategic partnership in place with [redacted] covering the management and maintenance of our technology infrastructure. Contracts with third party vendors and clients include adequate consideration of confidentiality and data protection requirements, including mutually binding confidentiality agreements.

How will data be securely transmitted

Sensitive data and deliverables are encrypted in transit via a secure file transfer system, SFTP or via a client preferred method. Opportunistic TLS is enabled to ensure secure email transfer is available where possible. Client sensitive data is encrypted in transit via a secure file transfer solution in line with industry standards. Encryption of data on file servers and SAN is not standard and we perform an information security risk assessment and ensure countermeasures are established to mitigate identified information security risks. All client data is stored in secure data centres in line with the requirements of the WPP Information Security policy. Processes are also in place to ensure all traffic between systems is transported over https and encrypted.

How will data be secured

Sensitive data and deliverables are encrypted in transit via a secure file transfer system, SFTP or via a client preferred method. Opportunistic TLS is enabled to ensure secure email transfer is available where possible. Client sensitive data is encrypted in transit via a secure file transfer solution in line with industry standards. Encryption of data on file servers and SAN is not standard and we perform an information security risk assessment and ensure countermeasures are established to mitigate identified information security risks. All client data is stored in secure data centres in line with the requirements of the WPP Information Security policy.

Processes, including assessing future risks

GroupM's parent company, WPP, operates a well-established and formally approved information security management framework which comprises information security policies, risk assessment and independent assurance processes. The WPP information security management framework is mandated across all WPP companies and compliance with the framework is subject to periodic independent review by WPP Internal Audit, with findings tracked to resolution.

Disaster recovery policies

Our BCP DR is designed to ensure we continue to have systems and procedures in place, to combat business interruption and allow us to communicate quickly and efficiently with each other and with our operating companies and suppliers. Our BC Team (Business Continuity Team) ensure all aspects are the business are captured to ensure BC can be maintained. Our BCP must also meet control requirements as set out by WPP's General Computing Controls. Each control test is audited by WPP annually to ensure our BCP continues to meet these requirements

Back-up and continuity to deliver services

GroupM's parent company, WPP have a strategic partnership in place with [redacted] covering the management and maintenance of our technology infrastructure (including backups).

Mitigating against cyber-attack and crime

Vulnerabilities and potential vulnerabilities in both infrastructure and applications are identified through a managed Vulnerability Management Service (VMS). Such items are evaluated and remediated through a standard process. Services are kept up to date with security patches through the standard patch management service (incorporating a Security Advisory and Integrity Service). A Malware Defence Management Service (MDMS) ensures that a secure Server environment is maintained. This protects against malicious code such as malware, viruses and intrusion (this includes the provision and maintenance of anti-malware services, along with segregation/filtering through firewalls). Manual ethical hacking is scheduled and performed on systems based on risk.

Destruction policies

GroupM have mechanisms in place to ensure that data is handled in line with guidance from WPP legal and relevant regulatory and client contractual requirements. The complexity of the services we provide to clients does not lend itself to third party assurance reports, which are primarily designed to provide independent assurance over commodity services such as IT or finance operations.

On this basis we do not seek to employ third party reports to provide assurance over our control environment. We have a formal General Computer Controls framework in place which defines the minimum standard of IT and information security controls applied across our business. Adherence to

our General Computer Control framework is subject to periodic independent review by WPP Internal Audit, with findings tracked to resolution.

GDPR

GroupM has an extensive GDPR Programme running across all agency networks. The GDPR Programme is led by the GroupM Global legal team. We have a broad advisory and implementation team, including IT, Compliance, Finance, Trading, Digital Risk, Data, HR, Communications, [m]Platform, and Privacy. We have appointed a Data Protection Officer who covers all of GroupM and have GDPR coordinators in each of our markets to help run the programme ensuring compliance at every level.