D4 – Encrypted Data in Transit

Applicant to detail how they encrypt data in transit. The Applicant must describe the techniques, technology and processes to protect against tampering and eavesdropping over public and private networks.

As defined by 'Principe 1 of the National Cyber Security Centre's cloud security guidance'.

2 page A4 Arial 11 2%

Excellent scores will be awarded where Applicants robustly;

- *Demonstrates their capability to encrypt data in transit*
- *Provide technical details of how this is achieved including details of the cryptography protocols, ciphers and hashes*
- *Demonstrates that all data in transit (either internally or externally across the internet) is and remains encrypted.*
- *Provides a detailed description of the ISMS (Information Security Management System) process the organisation uses to manage this capability.*

We employ several methods to ensure the confidentiality, integrity, and availability of our data. Where we must transfer data outside of the business to a third party, we will ensure this is done using encryption (for instance when sending files via emails, we will use Mimecast Large File Transfer which encrypts and securely transfers the data).

We also employ the use of VPN or TLS 1.2 or above for data transfer security and manage this via our MSP. There are policies in place for guiding acceptable use of facilitating transfer of data and this guides the requirements for in-house and external network services.

Where we transfer data using a secure file transfer protocol, a change request will be instituted by our MSP for review and approval and where no longer required, we will wipe irretrievably.

Email can be sent securely via Mimecast or Microsoft services where required. Utilising AES archives and TLS transport protocol.

Secure File Transfer Protocol (SFTP) is used where appropriate for major transfers of data. Normally via a VPN.

The Group utilise MGS-POL-IT-008 Cryptographic Controls Policy to manage the usage of encryption controls.

The scope of this policy applies to:

Any of M Group Services premises where electronic information is stored, and the employees work.

M Group Services employees, temporary staff, contractors, and service providers utilising the companies' information systems.

Information system resources, including data networks, LAN servers, personal computers (stand-alone or network-enabled) mobile devices (including, iPads and iPhones), located at M Group Services offices and non-group locations, where these resources are under the jurisdiction and/or ownership of the group, and any personal computers, servers and portable computerised media authorised to access the companies' data networks. Third parties with access to critical or sensitive data owned by M Group Services companies shall also adhere to this policy.

Electronic information resources of critical or sensitive data, where: o Critical can be defined as information which is of commercial, strategic, or significant monetary value to the companies.

Sensitive can be defined as information of which disclosure would either contravene the Data Protection Act 2018 and/or the General Data Protection Regulation (2018) or cause measurable damage to the companies' reputation or that of its customers or suppliers if it were to fall into the public domain.