D3 – Encrypted Data at Rest

Applicant to detail how they encrypt data at rest, describing the processes and technology to prevent structured and unstructured data from being accessed, modified or stolen (either digitally or physically) by unauthorised actors. This covers cloud storage, file hosting services, databases, data warehouses, spreadsheets, archives, tapes, off-site backup or mobile devices and portable storage devices.

For the purposes of this question, data-at-rest and data-in-use are considered the same

2 page A4 Arial 11 2%

Excellent scores will be awarded where Applicants;

- *Demonstrates their capability to encrypt at rest*
- *Provides technical details of how this is achieved including details of the cryptography protocols, ciphers and hashes*
- *Demonstrate where this capability has been deployed. To cover cloud storage, file hosting services, databases, data warehouses, spreadsheets, archives, tapes, off-site backup or mobile devices and portable storage devices*
- *Provide a robust description of the process the organisation uses to manage this capability*

We have put in place encryption and security certificates which are managed by our Managed Service Provider (MSP).

There are appropriate controls in place to ensure the keys are adequately protected in the lifetime of the keys. We have an established process which ensures that encryption should be at least AES 256 for data at rest. We utilise several protocols and support a variety of encryption standards dependent upon the platform and the task.

For instance, where we utilise Office 365, email, SharePoint, Teams, OneDrive, Windows 10/11, Mobile devices, Backups & USB devices then the Microsoft approved standards are used, AES256 and FIPS 140-2. Bitlocker is the standard product for Microsoft base encryption.

TLS version 1.2 or above is used for traffic, and other encryption-based services are used, such as Mimecast, for email as required.

Salesforce: Multi-Factor Authentication is supported, and the following verification methods can be used: Time-based one-time passcode (TOTP) authenticator apps like Salesforce authenticator, Google Authenticator, Microsoft Authenticator, and Authy. Salesforce supports the use of third-party authenticator apps that generate temporary codes based on the OATH time-based one-time password (TOTP) algorithm (RFC 6238). Security keys that support WebAuthn or U2F.

These are small physical devices that support security keys that are compatible with FIDO U2F. This standard uses strong public-key cryptography to protect users from man-in-the-middle attacks and malware.