Annex 5 – External Data Hosting Requirements

These requirements are applicable to the hosting of all **BT 'In Confidence' (IC)** or **'In Strictest Confidence' (ISC)** applications and data in any location that is not BT owned or managed. This includes but is not restricted to Cloud Services where a) the data in transit is secure and protected from interception typically using an encrypted protocol, and b) the BT data is encrypted at rest within the cloud service.

The following conditions apply to In Confidence applications and data hosted outside BT:

- The Data Centre should hold a valid ISO 27001 certification (or certification(s) that demonstrates equivalent controls) for security management or shall comply with the Security Requirements of ISO 27001 certification or security policies aligned to ISO27001 and/or working towards ISO27001 within a timeframe agreed with BT;
- Data 'in transit' must be strongly encrypted to protect the BT data between the point of egress from BT, and the DC boundary (typically the load balancer and decryption device located behind the DC boundary firewall);
- DC engineers with physical access to the servers should not have logical access to the production environment, and administrators with logical access to the systems should not have physical access to the DC.
- All logical access should be controlled by an account security system to ensure the management of passwords is controlled and the appropriate authorisation process is implemented to ensure the identity of the requestor e.g. CyberArk.
- For privileged access (including but not restricted to DBA) management of passwords should be time bound and where possible implement additional restrictions on the source IP address.
- Any privileged access e.g. DBA, ASG etc. to systems that process BT information must comply with the requirements in Annex 1 - information classification.
- For remote access, a secure Virtual Private Network must be used in conjunction with role based two-factor authentication; additionally all remote third party privileged access may only access the systems where BT data is in transit or at rest from within the same country as the DC, or a country or territory that ensures an adequate level of protection for the BT data;
- Implement whole life cryptographic key management processes that are commensurate with industry best practice;
- Any physical access to areas or equipment where BT information is stored or processed must have an auditable process e.g. change request, to ensure access is only granted for the minimum duration required e.g. no permanent access;
- Off-site back-up data storage must be encrypted in-line with the requirements of Annex 1;
- Controls must be in place to mitigate, detect and prevent unauthorised access. Controls must create an audit trail using the" Who What Where When" principle.
- Who the user was e.g. user account ID;
- What asset they were accessing e.g. data;
- From Where they accessed the asset e.g. IP address; and
- When e.g. time-stamp.
- All physical and logical access must be logged, with log files retained for 1 year (minimum);
- In the event of a breach where BT data is compromised, stolen or modified, a process must be in place to ensure BT is notified within a reasonable amount of time, with sufficient level of detail;

Where there is ISC information the following additionally applies -

- the Data Centre must pass an on-site security inspection ;
- Application servers, databases etc., should be on dedicated, not multi-tenanted, infrastructure and should be hosted in a dedicated rack within a secure cage. Where this requirement can't be met, a BT Risk Assessment must gain assurance demonstrating adequate separation of BT data from other customers' data sharing the same environment ensuring that DBAs must not have login access to customer's instances and not see customer data in an assembled manner. Database tables and rows must not reflect the view of a single customer instance.

Processes must be place to ensure that ISC data is deleted securely at the end of its lifecycle in the cloud; All storage devices containing ISC data must be erased/deleted