3rd Party External data hosting requirements

The following conditions must be met when BT data is

- Hosted in an external environment (Non BT Data Centre)
- Transferred between Data Centre's (DC) (Non BT Data Centre)
- Transferred between Data Centre's and back up facilities. (Non BT Data Centre)

It applies to all BT 'In Confidence (IC) data, BT 'In Strictest Confidence' (ISC) data and BT Personal data. See the 3rd Party Information Classification and Handling Specification http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm for definitions. There are additional controls for Sensitive Personal Data.

Ref	Control	Reason
EDH10	BT's Security requirements must be contractually agreed by the supplier or relevant sub-contractor.	To make sure the Supplier is aware of, and has agreed to the security controls that are in place to protect the data
EDH20	If the external hosting is compromised and BT data is stolen or modified, a process must be in place to ensure BT is notified as per the contract, with sufficient level of detail as per clause 3.8 of BT's Security Requirements.	To make sure BT is quickly made aware of a potential incident /data theft.
EDH30	The Data Centre should hold a valid ISO 27001 certificate for security management (or certification(s) that demonstrate equivalent controls, supported by independent auditors report)	ISO27001 demonstrates that a best practice information risk management framework of controls is in place.
EDH40	BT IC or ISC data in transit must be encrypted (256AES), end to end (such that no BT data passes over the suppliers network in the clear). Anything transmitted outside of the BT network including the suppliers internal network is considered un-trusted.	To protect the data if it's intercepted while in transit and/or prevent the data being tampered with
EDH50	Data must be encrypted when stored in an external data hosting environment. (See the 3rd Party Information Classification and Handling Specification http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm for minimum requirements)	To protect the data at rest
EDH60	Management of cryptographic keys must meet the requirements of the Cryptography Specification at the end of this document.	Cryptography best practice
EDH70	Logical user access for Administration purposes must be role based and use industry standard 2-factor authentication e.g. one time password tokens or certificates issued by recognised trusted root certification authorities. Lists and files of trusted root certification authorities can be found at - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Weak access control could result in unauthorised access.

EDH80	Controls must be in place to mitigate, detect and prevent unauthorised access. Controls must: create an audit trail where the integrity is protected from modification Show who the user was (e.g. user account ID) What asset they were accessing (e.g. data), When (e.g. time-stamp)	To provide an audit trail to show who the user was, what asset they accessed, where from, & when
EDH90	Administration of externally hosted applications or data must be via a secure (encrypted) connection and use 2 factor authentication as per EDH70.	To make sure remote access support is as secure as local access.
EDH100	Any remote direct access to data where, BT data is in transit or at rest must be from within the same country as the DC or in a country or territory that ensures an adequate level of protection for the BT data	To minimise the risk of not meeting country data protection laws.
EDH110	All physical and logical access must have a change request or fault ticket. Access must only granted for the duration of the fault and removed when the fault is fixed	To minimise the risk of unauthorised changes being made.
EDH120	All physical and logical access must be logged, with log files retained for 1 year (minimum)	To make sure log files are available to support potential incident investigation.
EDH130	Back-up data storage must be encrypted (256AES) at the media level, e.g. tape, disks etc., and off-site storage must be within the same country as the Data Centre or in a country or territory that ensures an adequate level of protection for the BT data	To protect BT data and minimise the risk of not meeting country data protection laws
EDH140	All storage devices containing BT data must be erased/deleted as specified by the 3rd Party Information Classification and Handling Specification http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	To minimise the risk of data leakage if an unauthorised person was able to recover the data at the end of its lifecycle.

Additional controls for Sensitive Personal Data

EDH150	On reasonable request the supplier must allow BT access to carry out an on-site security audit	So BT can check the security controls and make sure they adequately protect the data

General Cryptography Controls. (EDH60)

Ref	Control	Reason
C1.10	Current Cryptographic libraries must be used	Cryptographic libraries are updated regularly. In addition to updating software packages in-line with vendor direction cryptographic packages should be reviewed and updated regularly.
C1.20	Only use approved industry standard cipher suites for encryption. E.g. for TLS SSLv2	Non approved ciphers may introduce vulnerabilities
C1.30	The latest version of TLS must be used for new deployments. SSL V1,2 & 3 must not be used	Earlier versions, up to and including TLS1.0 are no longer considered secure
C1.40	Perfect Forward Secrecy must be enabled	Perfect forward secrecy algorithms prevent captured messages being decrypted even if the

		authentication private key is compromised in the future
C1.50	Self-signed certificates must not be used	Self-signed certificates negate the benefit of end-point authentication and also significantly decrease the ability for an individual to detect a man-in-the-middle attack.
C1.60 **GTS2.370**	An industry standard certification authority must be used for certificate management. E.g. verisign	To maintain an inventory of certificates issued for vulnerabilities and certificate expiry
C1.70	Passwords must be protected using a non-reversible one way mathematical function (e.g. Hashing algorithm) with a unique randomising factor (Salt) per password. NB. SALT is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase.	Stored password files can be extracted and as such all entries must be protected to prevent recovery of clear text passwords
C1.80	Protected passwords as per C1.70 must be stored away from a system's configuration files and have access control implemented so that only appropriate privileged users can read or copy the contents.	It must never be possible to retrieve protected passwords by directory traversal, SNMP walk, configuration dump, or other mechanism, which might allow attempts at offline cracking.