FINANCIAL SERVICES COMMISSION

SECURITY PROTOCOL FOR

BENEFICIAL OWNERS REGISTRY

SECURITY PROTOCOLS: BENEFICIAL OWNERS REGISTRY

1.0 THE REGISTRY

The TCI's Beneficial Owners (BO) data registry will be housed and administered by the TCI Financial Services Commission in accordance with the protocols established between the TCI and the relevant UK authorities, and the provisions of the Companies Ordinance 2017.

2.0 SECURITY PROTOCOL

The Financial Services Commission has implemented a number of measures to safeguard client information stored on the BO database. The sensitive nature of the BO data requires that the risk of disclosure be minimised, if not eliminated. With this in mind, the Commission has put in place industry standard best practices to provide the highest level of security.

2.1 AIR GAPPING

Air gapping is a security measure that involves isolating a computer or network and preventing it from establishing an external connection. The BO network will be air gapped; it will be physically isolated from the Internet and the Commission's Local Area Network. All information uploaded into the BO database will be done via an Encrypted USB flash drive.

In the Commission's BO system architecture, both the application and the database for the BO system are isolated from the main KRegistry application and database. There is no link between the BO database and the KRegistry database. No external users (CSPs and their users) will have access to the BO system. No unauthorised users within the Commission will have access to the BO system.

The BO system will reside in **Providenciales** and be housed in one of the Commission's Server Room that is locked at all times. Only one IT Personnel will be tasked with maintaining the BO system and will not have any user credentials to the BO database.

2.2 ACCESSING THE BO DATABASE

Access to the BO system (uploads and searches) will always include two authorised people. A maximum of seven staff members - the Managing Director (MD), three management level staff and three officers - will be authorised to access the database. The management level staff are all subject to ongoing review by the Integrity Commission. Staff will be assigned on a two person rotational basis, a manager and an officer (with the MD as an alternate), to be responsible for access to the database. Only the assigned officer will have access to the database during that designated period, usually one month.

2.3 GENERATING DATA TO TRANSIT TO THE COMMISSION

The Commission will provide two methods that the CSPs can use to securely generate their data to be uploaded into the BO database.

i. The CSPs will be provided with a spreadsheet containing fields that can be populated manually or via direct interaction with their IT system. *A guide and sample were provided to assist with the population of the spreadsheet.*

ii. CSPs can use the portal through the Commission's online KRegistry System. The BO module on the KRegistry System, provides a user-friendly interface that allows CSPs to enter their BO information that will generate the required spreadsheet. The BO module of the KRegistry System is not linked to the BO database; hence, any pre-populated information, is obtained from the KRegistry Database. Pre-populated information will only include the entity name, entity number and entity address.

    Information entered via the BO module creates a temporary session online. The session will last until the spreadsheet has been created. Once the information has been entered and the spreadsheet generated, all data, logs and system files relative to the BO information entered by the CSP, will be deleted from the online system. The CSP will be required to save their spreadsheet.

Upon completion, the CSPs will have two options to submit their spreadsheet to the Commission.

a) The CSPs can save the spreadsheet to a flash drive. The flash drives will be sent or taken to the Commission's Providenciales office for uploading.

    The Commission recommends that CSPs use a 256-bit AES hardware encryption that is FIPS (Federal Information Processing Standards) 140 level 2 validated. This type of flash drive requires an alphanumeric password that will be used to encrypt and decrypt files on the flash drive and will be entered by the CSP. Once the data is encrypted on the flash drive, it will become undecipherable in the background and is locked away under encrypted storage within the drive. If the drive is stolen or misplaced, and someone tries to gain access to the data without the password, the attempt will be, by all practical means, impossible. Additionally, after a certain number of access attempts, the data will be automatically erased. Once the authorised personnel from the Commission receives the flash drive, he/she will call the client to obtain the password to decrypt the file. It is recommended that CSPs change their password for their flash drive after every update.

Flash drives submitted to the Commission will be stored in a locked vault that is accessible only by the officers on rotational duty during that period. The flash drives will be returned to CSPs after use. The Commission will try to conduct uploads of data at a set time each day (time to be advised to clients) to allow CSPs to be present and wait for their flash drive, at their option.

b) CSPs can email an encrypted spreadsheet to the Commission. The CSPs can encrypt the spreadsheet using Microsoft Office Password Protection 128-bit AES encryption. The emailed encrypted spreadsheet will only be accessed by authorised personnel from the Commission. CSPs can also consider using email encryption to encrypt their emails over the Internet. Once the spreadsheet is received by the authorised personnel in the Commission, the personnel will call the client to obtain the password to decrypt the file. The authorised personnel will be required to save the file directly to an encrypted flash drive and upload the information via the assigned computer machine. As a monitoring measure, at least two authorised personnel must be present when downloading the spreadsheet to the flash drive. Additionally, all spreadsheets will be deleted from the email account as soon as it is successfully transferred to the flash drive.

There will be three computer terminals dedicated to the operations of the BO process:

- One machine will have access to the BO system and will be used to upload the BO information and perform searches. This machine will not have any access to the Internet or to the Commission's Local Area Network.

- Another machine will be used as an intermediary. This machine will be used to copy the contents of the CSP flash drive to the Commission's flash drive. This is to avoid any inadvertent transfer of virus from the CSPs flash drive to the BO network. No information will be saved to the physical machine. This machine will not have any access to the Internet, the Commission's Local Area Network or the BO system.

- The last machine will be dedicated to access the BO email account only. This machine will be used exclusively for the CSPs who chooses to email their BO information as discussed above. This machine will not have any access to the Commission's Local Area Network or the BO network but will have access to the Internet.

The machines that will not have any Internet access will be located in a room that will be locked at all times and can only be accessible by Radio Frequency Identification (RFID) security. The RFID will identify the identity of anyone accessing the room. A camera will also be installed in this room. The camera will not face the monitor.

The machine that will have Internet access will be located outside of the locked room but will be monitored by a camera. Only authorised users will have access to the stand-alone machine.

2.4 ACCESS TO THE KREGISTRY SYSTEM

One of the methods for the CSPs to generate the required spreadsheet, is by accessing the KRegistry System *(stated in method 2.2 above under Generating Data to Transit to the Commission)*. Access to the KRegistry System can only be gained through the use of Digital Certificates that will be provided by the Commission. The Digital Certificates will be issued through a WebTrust-certified validation authority. The Digital Certificates will be stored on hardware tokens storing the certificate's private keys, meaning the cryptographic operations are now isolated and insusceptible to any attacks on the operating system. Using this type of control access will enforce a two-factor authentication which provides an additional layer of security. Hence, in order for CSPs to access the KRegistry system, they will be required to use a hardware token, as well as a login user name and password.

The KRegistry website will use the Secure Socket Layer (SSL) protocol. SSL is a standard security protocol that will establish an encrypted link between the Commission's web server and a browser in an online communication. The use of SSL technology ensures that all data transmitted between the web server and browser remains encrypted. CSPs can verify that the KRegistry website is secured by a SSL certificate by looking for 'HTTPS' (Hyper Text Transfer Protocol Secure) in the URL.

2.5 AUDITING AND ACCESS CONTROL MONITORING

The BO database has been designed to create audit logs to assist in keeping track of activities taking place on the database. These logs include:

i) BO user details (username of person performing search)
ii) Number of searches made by the BO user.
iii) Requestor details and the nature of the request.
iv) Date and time the request is made and responded to.
v) Time and date of search performed.
vi) Changes or updates within BO information.

2.6 INTERNAL SECURITY AND MONITORING CONTROLS

In order to minimise the risk of disclosing BO information, the Commission has put in place the following security and monitoring controls:

i) The Commission's BO users are not allowed to perform more than 10 searches per day. If additional searches are required, an override has to be performed by another authorised officer.

ii) Only encrypted flash drives will be used on all computer terminals engaged in the handling of BO information.
iii) Cell phones are not allowed in the room that will have access to the BO system.
iv) BO uploads will be performed in the presence of two persons; one of which can be the relevant CSP.
v) BO searches will be performed in the presence of two Commission officers, one of which will be a management level officer.
vi) Audit logs are generated and viewed by management periodically that gives basic information (name and entity) about the searches performed and the user details.

3.0 ADDITIONAL SECUIRTY

The Commission reserves the right to have in place or introduce additional security measures which are not disclosed in this document.

4.0 BENEFICIAL OWNER REQUESTS PROTOCOL

United Kingdom law enforcement authorities will be able to request from the Turks and Caicos Islands law enforcement authorities all of the current beneficial ownership information contained on the Commission's BO Platform on entities incorporated in the Turks and Caicos Islands.

The Commission and the TCI Police Force will establish designated points of contact, whose function will be to receive and respond to each law enforcement authorities' request for beneficial ownership information.