Background

The security and privacy of your data is of paramount importance to us. We provide a wide range of consultancy and support services, and while performing these services it is likely we will be acting in the role of a Processor* of data that you Control*, and very often the data we are processing will include Personal Data.*

* As defined by the GDPR

Interactions that we have with your data while engaged on Project work will be governed by terms set out in the relevant Project Initiation Document. This Client Access Request Process has been devised to ensure that all interactions that we have with your data while providing Support and ad-hoc Consultancy services are similarly properly authorised and auditable.

Requesting and Authorising Access

On each occasion that one of our consultants requires access to your systems and/or data to carry out Support or ad-hoc Consultancy work that is not governed by a current Project Initiation Document a form called a Client Access Request Form (CAR Form) will be generated and issued by email to the person requesting the work.

The CAR Form describes the work to be carried out and identifies the specific individuals from the LAKE team who require access. It must be approved in writing (usually by email reply) by an authorised officer of the client before technical connections are enabled or screen-sharing sessions arranged.

Denying Access

Please deny further access when the work in question is complete. We will submit a new CAR Form if we require changes to any aspect of the access being requested, including the name(s) of the Consultant(s) requiring access and the type and level of access being requested.

Traceability

Wherever possible and practicable, all access to your systems and network should be via accounts that are maintained in the consultant's own name. This ensures that it is always clear precisely who has made specific changes. This is particularly important when it comes to traceability of changes that may have been made to Personal Data that you Control.

Where it is not possible for you to offer named accounts in this way, generic or impersonal LAKE accounts (e.g. lakeuser1, lakeuser2, etc) may be used as long as you maintain an audit trail, recording which specific individuals used these impersonal accounts on any particular day. Whenever the work we are doing requires submission of a Professional Services Report (PSR) the LAKE consultant will provide additional audit evidence by including on the face of their PSR a note of the account they used to connect to your systems.

Named Accounts and Screen-sharing

If read-write access is required and the only route available for us is through a screen-sharing tool such as Teams or WebEx, the way the technology works means we can only connect to a host machine that is already logged in to your network.

Ideally the login for the session running on the host machine would be that of the LAKE consultant, but this is not possible without compromising his or her password. Every such session will therefore necessarily be running under a user account that is managed by you.

To work around this constraint, one of the following arrangements is recommended (in order of preference):

- A 'LAKE' account that allows very limited access (ideally only RDP or equivalent to allow the consultant to login to relevant servers under his or her own named account) is used as the host
- The host machine for the screen-sharing session is a virtual machine that allows very limited access (as above)
- All activity during the session is monitored by a user at your side with appropriate knowledge and experience
- A user at your side with appropriate knowledge and experience remains in control of the mouse and keyboard during the entire session, and we limit ourselves to the provision of advice and guidance only.

Replacing or Disabling Impersonal Accounts

Please take care before disabling or converting an impersonal Lake network or database account to replace it with another account. It is possible the original impersonal Lake account may have been used for scheduled tasks, services, backup or maintenance routines etc. and these will fail if the account is disabled.