e2e Secure Cloud Connect Service – Terms and Conditions Document

e2e Secure Cloud Connect Service - Terms and Conditions Document

Service Specific Terms and Conditions

On-boarding	On-boarding is included with the following scope: e2e will support the customer in connecting/enrolling the requested fixed VPNs, mobile VPNS and mobile devices into the service. Optionally we can also migrate data into the service on a time and material basis. Examples of this would be connecting to an existing customer active directory service which would be charged on a time and material basis. MDM On-boarding is included with any initial standard applications (creating an allow list) – Any applications which require more complex configuration would be chargeable.
Off-boarding	Off-boarding is included with the following scope: all user access will be revoked and any e2e cloud connect components containing customer data will be wiped and factory reset. All customer data will be removed. The customer is expected to migrate their own data out of the service prior to the end of the service. Optionally we can also migrate the data out of the service (such as historical access logs) on a time and material basis.
Backups	All e2e managed devices are backed up to support the availability of the service.
Disaster recovery	The service can be split across two UK datacentres if required.
Service lead time	Typically, 10-30 working days from acceptance of order.
Minimum term	The service has a minimum term of 6 months.
Early exit charge	One month of service cost.
Termination charge	Termination before initial 6 months incurs early exit charge
Consumer responsibilities	The control and management of end users of the service and any VPN components installed or provisioned on customer equipment including end user devices Provision of any internet connectivity to the e2e cloud Desirable to provide separate out of band connectivity with a fixed IP address ASDL line to the VPN CPA Device
Technical requirements	To manage the service the user is required to enrol with our two-factor authentication service and connect to the service using one of the following: Windows, Linux, MAC, IOS, Android and Blackberry. To create a fixed VPN the customer is required to either provide a NCSC CPA foundation level approved device (IPsec Security Gateway) or allow e2e to supply and provision one. To create a mobile VPN the customer us required to either provide and support a NCSC CPA foundation level approved device (IPSec VPN for remote working) or allow e2e to supply one.

Networks and Connectivity	e2e services are designed and assured to connect to the following networks. Please contact e2e for further details. • Public Services Network (PSN) • Government Secure intranet (GSi) • Police National Network (PNN) • New NHS Network (N3) • Joint Academic Network (JANET)
Ordering and Invoicing	Monthly in arrears by Purchase Order or Direct Debit.
Data restoration/service migration	Data can be migrated into and out of the service using the VPN access methods provided. e2e can assist with this process on a time and materials basis if required.
Financial recompense model	If the service level falls below the stated availability (excluding planned or emergency maintenance and excluding any fault that is not the responsibility of e2e or e2e components), consumers will be eligible for a service credit. Service credits are provided as professional service credits that can be used for any support, design or security activities and are calculated at a value of 10% of service spend on the particular service.
Training	The customer can choose to purchase training days.
Trial Service	There is no trial service available.

More information and contact details

Enquiries, and more information is available on request, email info@e2e-assure.com with any queries.