MEMSET®
GOVERNMENT HOSTING

Cloud Service Security Principles
Memset Statement

www.memset.com

Summary - March 2014

The Cabinet Office has produced a set of fourteen Cloud Service Security Principles to be considered when purchasers are evaluating the security features of cloud services (https://www.gov.uk/government/publications/cloud-service-security-principles).

Memset's GCloud services conform to all of the Cloud Service Security Principles. Our services all fall within the scope of our ISO27001 Certification, and additionally our IL2 and IL3 accredited services have CESG Pan Government Accreditation (PGA) to IL2 or IL3 as appropriate. ISO Certification is granted by an independent external assurer, and PGA accreditation is external and supported by IT Health Checks undertaken by independent CHECK consultants. Hence the security of our services has been rigorously assured by independent external bodies and consumers can be confident that we conform to the Principles.

As we conform to the Cloud Service Security Principles, our services are suitable for use with OFFICIAL data. IL3 accredited services are suitable for all OFFICIAL data, IL2 accredited services are suitable for OFFICIAL data which is moderately sensitive and our IL0 services can be used for OFFICIAL data not requiring particular protection. Data owners will need to decide on the most suitable services based on the particular nature of their data.

The following additional information on each of the Security Principles is intended to help consumers to decide which service is most suitable for their circumstances. Memset is happy to discuss the services or provide additional information as required to enable consumers to be sure they are selecting the most appropriate service for their needs.

Memset's GCloud services conform to all of the fourteen Cloud Service Security Principles as follows:

1. Data in transit protection

IL3 services are only available via PSN which provides assured protection between our locations and the consumer's locations. Our systems provide the protection required to achieve their level of certification. Consumers can add end-to-end encryption over our IL0 and IL2 services if they wish. Customers are responsible for the management of data in transit protection required for the accreditation of their solution.

2. Asset protection and resilience

Appropriate physical security measures are in place with access control to office and data centre environments. For our IL3 services, we have protective measures in place which provide for aggregation of IL3 data. We are a UK company with our data centres and office being UK-based. Our data centres and service management facilities are subject to ISO 27001, IL2 and IL3 assurance as appropriate to the service, covering confidentiality, integrity and availability aspects.

3. Separation between consumers

Appropriate separation and segregation has been designed into our systems from the outset and has been assured through the ISO27001 and PGA accreditation processes, including our IT Health Checks. Each consumer has dedicated server resources, and infrastructure and network resources have separation suitable for the type of service (ie public or private cloud).

4. Governance

Our security governance framework is well established and conforms to ISO27001 and CESG requirements. We have a named Senior Information Risk Owner (SIRO) and Security Manager, and they and other appropriate roles have defined responsibilities for the security of our cloud services.

5. Operational security

We have assured processes, procedures and tools in place covering all aspects of operational security including the management of change, configuration, vulnerabilities, incidents and protective monitoring.

6. Personnel security

All Memset staff are checked to the Baseline Personnel Security Standard (BPSS) and staff who potentially have access to data in the IL3 domain also have Security Check (SC) clearance. A role-based approach is taken to ensure that staff are appropriately cleared and only have access to the systems and data they require for their role.

7. Secure development

All aspects of the development of our services are protected and security is regularly reviewed, evolved and maintained to meet new threats.

8. Supply chain security

Our supply chain is covered by the scope of our certifications and accreditation so is externally assured as being suitably protected to support our services. Our supply chain is simple, thus making it easier to ensure that it is suitable for our services.

9. Secure consumer management

We provide consumers with the tools they need to securely manage their use of our services through management and support channels and make clear their responsibilities for the protection of their own data.

10. Secure on-boarding and off-boarding

Our services are provisioned in a known good state and make clear the customers' responsibility for further hardening to their specific requirements. We handle the deletion of data when they leave the service, and the destruction of physical media, in an approved and assured manner.

11. Service interface protection

All interfaces and connections are protected by means appropriate to the level of the service, such as firewalls and access controls, and have been assured through our certification and accreditation processes.

12. Secure service administration

Networks, connections, devices and processes used for service administration have been designed and implemented to be secure and have been externally assured.

13. Audit information provision to tenants

Consumers can be provided with the information they require to monitor the access to the services they have obtained from us. Services are self-managed by the consumers who as such have freedom to implement the monitoring framework most suited to their needs. Responsibilities for the monitoring of access and use of the customer's services are clearly defined.

14. Secure use of the service by the consumer

Our agreements set out the requirements on the consumer to ensure that they are using our services in an appropriate manner to deliver a secure overall solution incorporating our services. Consumers of our IL3 services must have signed up to a PSN Code of Connection.

Further Information

For further information on the way Memset meets the principles or a more general discussion on the security of our services, please contact a Memset sales person, your account manager or submit a support ticket.

MEMSET®
GOVERNMENT HOSTING

Get in touch:

www.memset.com
sales@memset.com

0800 634 9270 (Freephone)
+44 (0)1483 608010 (International)

Registered company No. 4504980
VAT number: GB 794 1313 25

Crown
Commercial
Service
Supplier

bsi.

ISO 9001 Quality Management	ISO 14001 Environmental Management	ISO/IEC 27001 Information Security Management
FS 600656	EMS 600657	IS 588114