Ministry of Defence

Industry Security Notice

Number 2024/06 dated 06/06/2024

Subject: **Cloud security control requirements for handling of OFFICIAL MOD Information**

Introduction

1. This Industry Security Notice (ISN) outlines the minimum requirements for cloud security controls and the individual responsibilities to allow for handling[1] of OFFICIAL (including OFFICIAL-SENSITIVE) MOD information in cloud services used by Defence suppliers, to ensure that it is appropriately protected. Additional responsibilities are set out in DEFCONs and other contractual mechanisms.

2. For any storage of NATO Unclassified and NATO Restricted material, the Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems (AC/322-D(2021)0032) and any other relevant NATO standards and directives must be complied with.

3. Any provisions set out in Security Aspects Letters take precedence over the requirements in this ISN where there is any difference between them. If the content of this ISN conflicts with a contract-specific Security Aspects Letter, DEFCONs or other contractual mechanisms, or for any further information/clarification, please refer to the MOD Delivery Team.

Scope

4. This ISN addresses the use of cloud services by Defence suppliers. It applies to all

[1] The generation, storage, use, processing and/or transmission of MOD information either in hardcopy or electronic form.

Cloud service models which are[2]:

a. Software as Service: The consumer is able to use applications running on cloud infrastructure.

b. Platform as a Service: The consumer is able to deploy onto the cloud infrastructure consumer-created or acquired applications.

c. Infrastructure as a Service: The consumer is provided with processing, storage, networks and other computing resources where the consumer is able to deploy and run software.

5. This ISN applies to both existing and new cloud services being used by Defence suppliers. If a Defence supplier's use of existing cloud services is not compliant with this ISN, the supplier shall engage with MOD Delivery Team to agree a plan for improving its level of compliance.

6. This ISN does not address the requirements for cloud services being supplied as deliverables to MOD; the MOD Delivery Authority should be consulted for these.

Background

7. Cloud usage continues to grow steadily, both in volume and the type of services being built and hosted in it. Cloud is usually the preferred option when organisations procure new IT services. Use of cloud also has the potential to improve the security of information[3] if the security risks of cloud usage are effectively managed.

Action by Industry

8. To aid the decision making about which cloud provider and service to use, any service designed, built and operated by the cloud provider shall be aligned with the NCSC Cloud Security Principles[4].

9. The Defence supplier should seek confirmation from the cloud provider that they align with the NCSC Cloud Security Principles including evidence of measures that the cloud provider has taken to meet them. If possible, this confirmation should be obtained before the Defence supplier decides which cloud provider to use. The Defence supplier shall ensure that the cloud provider complies with any other required control measures.

10. The Defence supplier shall ensure that they provide MOD with the required written evidence and/or documentation of alignment with the NCSC Cloud Security Principles. This evidence should be supplied to the relevant MOD Delivery team before the start date of the contract that the Defence supplier has with MOD. This also applies to Defence

---

[2] As defined by the NIST Special Publication 800-145 – SP 800-145, The NIST Definition of Cloud Computing | CSRC

[3] Security benefits of good cloud service whitepaper - NCSC.GOV.UK

[4] National Cyber Security Centre 14 Cloud Security Principles.

suppliers in any other tiers of the supply chain where MOD information is processed.

11. The Defence supplier must understand the country (or countries) where the data will be processed, and also the country (or countries) of any customer support service desks, and ensure appropriate controls are in place to protect the data from unauthorised access. Specifically:

a. The Defence supplier shall ensure that there are no obligations upon the cloud provider to share or allow access to MOD information in a manner incompatible with UK laws/regulations (NCSC Cloud Principle 2.1: physical location and legal jurisdiction). This applies to any locations used for the processing and/or storage of MOD information.

b. Where the legislative position of an international cloud provider's home country is not equivalent to the UK data and information protection landscape, the Defence supplier shall consider whether this rules out doing business with them, or if this can be provided for by way of imposing contractual obligations in lieu of legislative obligations.

c. When storing or processing personal data outside of the UK, the supplier shall follow UK data protection legislation, refer to the ICO guidance on international transfers and seek further guidance from legal advisors and/or Data Protection Officers as to how this applies to data transfer requirements.

12. MOD may make additional enquiries to the Defence supplier about how MOD information is stored, processed, transited and accessed, and the measures the supplier has in place to mitigate the risks to MOD information. Responses to these enquiries, or the inability to respond to enquiries (for example, if some parts of the answers to these enquiries are not known), may result in additional measures/controls or changes being imposed in any relevant contracts, subject to any agreement required for changes to existing contracts or how contracts are delivered. Any additional measures, controls or changes would be specific to a particular contract and where they are required, the Defence supplier should discuss them with the relevant Delivery Team.

13. Regardless of the location of data storage and processing, the Defence supplier shall as a minimum ensure that the personnel security controls described in NCSC Cloud Principle 6: Personnel security are met.

14. The Defence supplier shall comply with any applicable UK and/or international partners' export controls legislation.

15. The Defence supplier is not required to provide MOD with an F1686 form regarding sub-contracting or collaborating with overseas contractors, for cloud services used by the Defence supplier which are not being provided as deliverables to MOD.

16. The shared responsibility model[5] between the Defence supplier and their cloud

[5] https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model

provider regarding how the security of the cloud is to be managed must be agreed. The cloud service model should be taken into account when allocating responsibilities[6]. Responsibilities shall be documented, they should include but are not limited to the following:

a. Application configuration.

b. Identity and access controls including enforcement of least privilege, authentication and who will manage encryption keys.

c. Application data storage.

d. Application.

e. Operating system.

f. Network flow controls.

g. Host infrastructure.

h. Physical security.

17. In addition to the agreement of responsibility (individual or shared) of the areas detailed in paragraph 16, the responsibility (individual or shared) for delivering the following cloud service requirements must be identified and allocated:

Cloud service requirements	
Security Operations	Secure Operations Centre
	Log collection
	Log analytics
	Security monitoring
	Incident management
Protective Security Services	Threat detection capabilities
	Patching
Boundary Protection Services	Ingress services
	Gateway services
Artefact repository	Code repository
	Software repository
Support	User support
	Administration
Change management	Request fulfilment
Business Continuity and Disaster Recovery	Business Continuity and Disaster Recovery planning
	Business Continuity and Disaster Recovery exercises
	Backups and archives
	Restore
Assurance	Confidence that effective policy is enforced

18. The Defence supplier shall ensure that there is a regular assurance process to ensure ongoing management of security risks and to check that all relevant parties are

[6] Cloud security guidance - NCSC.GOV.UK

performing their responsibilities, with assurance reviews being carried out whenever a significant change is made and also every year as a minimum. The Defence supplier shall notify the MOD Delivery Team of any significant issues (including any potential issues or risks that might be significant) discovered during assurance activities.

19. All information systems and services shall be managed throughout their lifecycle, including prompt updating and patching, and adoption of the latest good practice configuration in accordance with NCSC guidance (in NCSC Cloud Principle 5: Operational security and Vulnerability management) and vendor direction.

20. The Defence supplier shall ensure that it is notified by the cloud provider of any security incidents. It is the Defence supplier's responsibility to report these to the Defence Industry Warning Advice and Reporting Point (WARP) in accordance with DEFCON 658.

21. If the Defence supplier becomes aware of any intended, planned or actual change in control of their cloud provider (such as change in ownership), the Defence supplier shall notify MOD at the point of contact set out below.

Validity / Expiry Date

22. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

23. The point of contact in respect of this ISN is:

Info & Info-Cyber Policy Team
Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence
email: UKStratComDD-CyDR-InfoCyPol@mod.gov.uk (Multiuser).