Standard

S1741 A2 Cloud cyber security

Contents

1 Purpose 2
2 Scope 2
3 Requirements 2
3.1 Cloud service models 2
3.2 Cloud responsibilities matrix: 3
4 SaaS requirements 3
5 IaaS and PaaS requirements 4
5.1 Application and interface security 4
5.2 Identity and access management 4
5.3 Cloud endpoint security 5
5.4 Network security 5
6 Supporting information 6
7 Person accountable for this document 6
8 Definitions 6
9 Abbreviations 7
10 References 7
11 Document history 7

1 Purpose

This standard details the cyber security requirements for all cloud deployment and how they must be implemented in line with TfL's cyber security policies.

2 Scope

The standard applies to all cloud based services and data owned by TfL or operated and supported by third parties for or on behalf of TfL, unless otherwise stated in contracts or covered by business unit specific operational policies or standards.

Any IT or Operational Technology which is built on or hosted using infrastructure, platform or software as a service (see 3.1) offering is defined as being cloud based.

Responsibility for security controls on cloud services is split between the TfL system owner and the service provider, depending on the level of control which has been procured. All contracts with suppliers for cloud services must clearly outline the boundary of responsibilities for security patching and include a security schedule.

3 Requirements

3.1 Cloud service models

3.1.1 Infrastructure as a Service (IaaS): The service provider or vendor offers computing resources (e.g. servers, storage, networks, processing power) in a virtualised environment. Users use these resources to build their own platforms and applications within the vendor or service provider's infrastructure.

3.1.2 Platform as a Service (PaaS): The service provider delivers a platform or environment with its underlying infrastructure where users can build and deliver applications.

3.1.3 Software as a Service (SaaS): Applications are hosted and delivered by a vendor or service provider. These applications are accessible via a network, typically the internet, for users to access.

3.2 Cloud responsibilities matrix:

Responsibility	SaaS	PaaS	IaaS	On-Prem
Data Governance & rights management	🟦	🟦	🟦	🟦
Client Endpoints	🟦	🟦	🟦	🟦
Datacentre location	🟦	🟦	🟦	🟦
Account & access management	◩	◩	◩	🟦
Identity & directory infrastructure	◩	◩	🟦	🟦
Application	⬜	◩	🟦	🟦
Network controls	⬜	◩	🟦	🟦
Operating System	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacentre	⬜	⬜	⬜	🟦

⬜ **Service Provider** 🟦 **TfL**

4 SaaS requirements

4.1 All SaaS instances must be risk assessed with the Cyber Security and Incident Response Team (CSIRT). This will set any specific security requirements, relevant to the purpose and environment of the service and based upon:

a) System access control – for further requirements, refer to the policy

b) Network security - for further requirements, refer to the policy

c) Malware prevention - for further requirements, refer to the policy

d) Secure builds and configurations - for further requirements, refer to the policy

e) Vulnerability management - for further requirements, refer to the standard

f) Security patching - for further requirements, refer to the standard

g) Encryption - for further requirements, refer to the Cryptography standard.

4.2 All SaaS procurement must be assessed with CSIRT to determine the relevant cyber security contractual clauses or obligations. Further requirements are available via the Third party cyber security policy.

4.3 All SaaS instances must allow:

a) Controls to limit access and control permissions for users

b) Security monitoring and alerting

c) Secure connections between ourselves and the service provider e.g. via the Application Programming Interfaces (APIs) or website utilising HTTPS.

5 IaaS and PaaS requirements

5.1 Application and interface security

5.1.1 Applications including APIs must be designed, developed, deployed and tested in accordance with relevant standards, i.e. the Open Web Application Security Project (OWASP) top 10 or the Web Application Security Consortium (WASC). This must be agreed with CSIRT based on the level of risk and must adhere to applicable legal, statutory, or regulatory compliance obligations.

5.1.2 Content of data either inputted to or outputted from cloud applications shall be filtered and validated to accept only the intended content type and form (dependent on field, context or application).

5.1.3 Applications must use a minimum of TLS 1.2 for all API communication and must be encrypted using AES 256 (further requirements are available via the Cryptography standard).

5.1.4 All API communication must be authenticated / authorised using CSIRT's authorised standards i.e. OAuthv2, OpenID Connect, SAML2.0 (Security Assertion Markup Language) for access control.

5.1.5 API keys and other sensitive data shall be encrypted using AES 256 at rest (further requirements are available via the Cryptography standard).

5.1.6 Where possible connections between the TfL estate and cloud systems must be via an express route or direct connection. Where this is not possible connections must be encrypted in accordance with the Cryptography standard.

5.1.7 Security certificates must be generated and managed securely in line with the Cryptography standard.

5.2 Identity and access management

5.2.1 Access to cloud hosted services must:

a) Adhere to the System access control standard

b) Have permissions assigned to groups and not directly to user accounts

c) Use Multi Factor Authentication (MFA) for privileged users

d) Not use personal email addresses to access or register for any cloud service or subscription.

5.2.2 Access to cloud hosted services for external users must:

a) Be granted through the provision of a TfL account and follow the requirements above in section 4.2; or

b) Be a CSIRT authorised cloud federation service, i.e. Microsoft Azure Active Directory (Azure AD) and Business to Business (B2B) collaboration, and Amazon Identity Access Management (IAM)

c) Use multi-factor authentication with either points a) or b) above.

5.3 Cloud endpoint security

5.3.1 All endpoints (as defined within the Secure builds and configurations policy) which are cloud based must have their builds vulnerability and risk assessments carried out prior to their live deployment and must be authorised by CSIRT. The assessment will determine which controls are mandatory, such as:

a) Host-based firewall

b) Full disk encryption (where data is being stored, transferred or processed)

c) Periodic vulnerability and risk assessments.

5.3.2 Endpoint protection must be deployed to:

a) Provide real-time protection to detect and block malware

b) Conduct scheduled scanning to periodically scan the entire system

c) Automatically update the latest protection signatures on a pre-determined frequency.

5.4 Network security

5.4.1 Web Application Firewalls (WAFs) must be deployed to protect all public facing web servers and web applications. WAFs must be configured to:

a) Block commonly known threats: see OWASP top 10

b) Log all user activities and executed actions

c) Provide zero day detection

d) Be able to test rules in passive mode

e) Implement geo-location rules or policies to restrict access when required

f) Provide malware protection

g) Blacklist and whitelist IP addresses

h) Use response scrub to protect against system data leakage.

5.4.2 CSIRT authorised Distributed Denial of Service (DDOS) protection must be deployed for public facing services to provide:

a) Protection against application layer, volumetric and protocol attacks

b) Protection against new and evolving threats

c) No disruption to legitimate traffic during an attack.

5.4.3 Firewalls must be deployed with the following requirements:

a) All firewalls must be configured to align with the requirements in the Network cyber security standard

b) All ingress and egress connection to and from services on OneLondon account or domain joined must be through the firewall in the enterprise management hub

c) Intrusion detection and prevention modules with policies configured must be used to detect and prevent malicious traffic or activities

d) Application control and web filtering must be enabled to ensure compromised URLs or applications are detected and blocked.

5.4.4 Patching and vulnerability management must align with the requirements in the Secure builds and configurations and Security patching standards.

6 Supporting information

6.1 Advice and guidance about this standard can be obtained from CSIRT by emailing cybersec@tfl.gov.uk.

7 Person accountable for this document

Name	Job title
Matthew Hudson	Chief Information Security Officer (CISO)

8 Definitions

Term	Definition	Source
Infrastructure as a Service	The service provider or vendor offers computing resources (e.g. servers, storage, networks, processing power) in a virtualised environment. Users use these resources to build their own platforms and applications within the vendor or service provider's infrastructure.	Glossary
Platform as a Service	The service provider delivers a platform or environment with its underlying infrastructure where users can build and deliver applications.	Glossary
Software as a Service	Applications are hosted and delivered by a vendor or service provider. These applications are accessible via a network, typically the internet for users to access.	Glossary

9 Abbreviations

Abbreviation	Meaning
CSIRT	Cyber Security and Incident Response Team
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
API	Application Programming Interface
OWASP	Open Web Application Security Project
WASC	Web Application Security Consortium
MFA	Multi Factor Authentication
IAM	Identity Access Management
WAF	Web Application Firewall
DDoS	Distributed Denial of Service
B2B	Business to Business
TLS	Transport Layer Security
HTTPS	Hypertext Transfer Protocol Security
AES	Advanced Encryption Standard
SAML	Security Assertion Markup Language

10 References

Document no.	Title or URL
P124	Secure builds and configurations policy
P125	Network security policy
P126	System access control policy
P128	Malware prevention policy
P132	Third party cyber security policy
S1736	Network cyber security standard
S1737	Secure builds and configurations standard
S1739	Security patching standard
S1740	Cryptography standard
S1745	Cyber security vulnerability management standard

11 Document history

Issue no.	Date	Changes	Author
A1	July 2017	New standard produced as per change No. 04917.	Paul Beverley CSIRT
A2	March 2018	Changes made to standard as per annual review. Change No. CR-10280	Haider Sarwar CSIRT