Security Standard – Cloud Computing (SS-023)

Chief Security Office

Date: 20/03/2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

Contents

1. Introduction 6
2. Purpose 6
3. Exceptions 6
4. Audience 7
5. Scope 7
6. Security Controls Assurance 7
7. Technical Security Control Requirements 7
8. Application Programming Interfaces Security* 7
8.1. Application Security 7
8.2. Customer Access Requirements 8
8.3. Data Integrity & Security 8
9. Audit Assurance & Compliance 8
10. Business Continuity Management & Operational Resilience 8
10.1. Business Continuity 8
10.2. Data Centre & Environmental Conditions & Risks 9
10.3. Documentation 9
10.4. Equipment 9
10.5. Impact Analysis 9
10.6. Policy 10
11. Change Control & Configuration Management 10
11.1. New Development & Acquisition 10
11.2. Outsourced Development 10
11.3. Quality Testing 10
11.4. Unauthorised Software Installations 11
11.5. Production Changes 11
12. Data Security & Information Lifecycle Management 11
12.1. Classification 11
12.2. Data Inventory & Flows 11
12.3. Ecommerce Transactions 12
12.4. Handling Labelling and Security Policy 12
12.5. Non-Production Data 12
12.6. Ownership & Stewardship 12
12.7. Secure Disposal 12
13. Data Centre Security 12
13.1. Asset Management 12
13.2. Controlled Access Points 13
13.3. Off-site Authorisation & Equipment 13
13.4. Policy 13
13.5. Secure Area Authorisation 13
13.6. Unauthorised Persons Entry 13
13.7. User Access 13
14. Encryption & Key Management Entitlement 14
14.1. Entitlement 14
14.2. Key Generation 14
14.3. Sensitive Data Protection 14
14.4. Storage and Access 14
15. Governance & Risk Management 14
15.1. Baseline Requirements 14

15.2. Data Focused Risk Assessments 15
15.3. Management Program Oversight Support & Involvement 15
15.4. Policy & Policy Enforcement 15
15.5. Policy Impact on Risk Assessments & Reviews 16
15.6. Risk Assessments 16
15.7. Risk Management Framework 16
16. Human Resources Security 16
16.1. Asset Returns 16
16.2. Background Screening 16
16.3. Employment Agreements & Termination 16
16.4. Mobile Device Management 17
16.5. Non-Disclosure Agreements 17
16.6. Roles & Responsibilities 17
16.7. Technology Acceptable Use 17
16.8. Training & Awareness 17
16.9. User Responsibility 18
16.10. Workspace 18
17. Identity & Access Management 18
17.1. Audit Tools Access 18
17.2. Credential Lifecycle & Provision Management 18
17.3. Diagnostic / Configuration Ports Access 19
17.4. Policies and Procedures 19
17.5. Segregation of Duties 19
17.6. Source Code Access Restriction 19
17.7. Third Party Access 19
17.8. Trusted Sources 20
17.9. User Access Authorisation Reviews & Revocation 20
17.10. User ID Credentials 20
17.11. Utility Programs Access 21
18. Infrastructure & Virtualisation Security 21
18.1. Audit Logging / Intrusion Detection 21
18.2. Change Detection 21
18.3. Clock Synchronization 21
18.4. Information System Documentation 21
18.5. Vulnerability Management 21
18.6. Network Security 22
18.7. OS Hardening and Base Controls* 22
18.8. Production / Non-Production Environments 22
18.9. Segmentation 22
18.10. VM Security - Data Protection 22
18.11. Hypervisor Hardening* 23
18.12. Wireless Security* 23
18.13. Network Architecture 23
19. Interoperability & Portability 23
19.1. Use of APIs 23
19.2. Data Request 23
19.3. Policy & Legality 24
19.4. Standardised Network Protocols 24
19.5. Virtualisation 24

20. Mobile Security* 24
20.1. Anti-Malware 24
20.2. Application Stores 24
20.3. Approved Applications 24
20.4. Approved Software for BYOD 25
20.5. Awareness and Training 25
20.6. Cloud Based Services 25
20.7. Compatibility 25
20.8. Device Eligibility, Inventory & Management 25
20.9. Encryption 25
20.10. Jailbreaking and Rooting 26
20.11. Policy & Legal 26
20.12. Lockout Screen 26
20.13. Operating Systems & Passwords 26
20.14. Remote Wipe 26
20.15. Security Patches 26
20.16. Users 27
21. Security Incident Management, E-Discovery & Cloud Forensics* 27
21.1. Contact / Authority Maintenance 27
21.2. Incident Management & Reporting 27
21.3. Incident Response Legal Preparation 27
21.4. Incident Response Metrics 28
22. Supply Chain Management, Transparency & Accountability 28
22.1. Data Quality and Integrity 28
22.2. Incident Reporting 28
22.3. Network / Infrastructure Services 28
22.4. Provider Internal Assessments 28
22.5. Supply Chain Agreements & Governance Reviews 28
23. Compliance 29
24. Accessibility 29
25. Security Standards Reference List 29
26. Reference Documents 29
27. Definition of Terms 30
28. Glossary 30
29. Controls Catalogue Mapping 30

1. Introduction

1.1. This Security Standard provides the list of controls that are required to secure Cloud based services to a Department of Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data to be stored with a Cloud platform. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

1.2. For further clarity and relevance, this standard has alignment to the Departments internal technical strategy paper, the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for Cloud security and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for Cloud deployments.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

3. Exceptions

3.1. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.3. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for Suppliers, developers, security groups, and also IT staff such as Security Compliance Teams, involved in securing environments for DWP systems and applications.

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All of the organisation's Cloud implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all Cloud systems that are provisioned for departmental use.

5.3. In the In the event of uncertainty on the controls laid out in this standard please contact the Security Advice Centre for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section 3 on exceptions above).

8. Application Programming Interfaces Security*

*For full technical detail on best practices please refer to the SS-003 Security Standard – Software Development Lifecycle Security Standard and other relevant patterns for cloud deployment.

8.1. Application Security

Reference	Security Control Requirement
8.1.1.	Applications and programming interfaces (APIs) MUST be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

8.2. Customer Access Requirements

Reference	Security Control Requirement
8.2.1.	Prior to granting customers/citizens access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access MUST be addressed.

8.3. Data Integrity & Security

Reference	Security Control Requirement
8.3.1.	Data input and output integrity routines (i.e., reconciliation and edit checks) MUST be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
8.3.2.	Policies and procedures MUST be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.

9. Audit Assurance & Compliance

9.1. Risk Management & Audit Function

Reference	Security Control Requirement
9.1.1.	Audit plans MUST be developed and maintained to address business process disruptions.
9.1.2.	Auditing plans MUST focus on reviewing the effectiveness of the implementation of security operations.
9.1.3.	All audit activities MUST be agreed upon prior to executing any audits.
9.1.4.	Independent reviews and assessments MUST be performed at least annually to ensure that the organisation addresses nonconformities of established policies, standards, procedures, and compliance obligations.
9.1.5.	Organisations MUST create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework MUST be reviewed at least annually to ensure changes that could affect the business processes are reflected.

10. Business Continuity Management & Operational Resilience

10.1. Business Continuity

Reference	Security Control Requirement
10.1.1.	A consistent unified framework for business continuity planning and plan development MUST be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
10.1.2.	Business continuity and security incident response plans MUST be subject to testing at planned intervals or upon significant organisational or environmental changes. Incident response plans MUST involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

10.2. Data Centre & Environmental Conditions & Risks

Reference	Security Control Requirement
10.2.1.	Data centre utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) MUST be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorised interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.
10.2.2.	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster MUST be anticipated, designed, and have countermeasures applied.

10.3. Documentation

Reference	Security Control Requirement
10.3.1.	Information system documentation (e.g., administrator and user guides, and architecture diagrams) MUST be made available to authorised personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features

10.4. Equipment

Reference	Security Control Requirement
10.4.1.	To reduce the risks from environmental threats, hazards, and opportunities for unauthorised access, equipment MUST be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.
10.4.2.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.
10.4.3.	Protection measures MUST be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.

10.5. Impact Analysis

Reference	Security Control Requirement
10.5.1.	There MUST be a defined and documented method for determining the impact of any disruption to the organisation (cloud provider, cloud consumer) that MUST incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
	• Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption

10.6. Policy

Reference	Security Control Requirement
10.6.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organisation's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures MUST include defined roles and responsibilities supported by regular workforce training.
10.6.2.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures MUST be incorporated as part of business continuity planning and tested accordingly for effectiveness.

11. Change Control & Configuration Management

11.1. New Development & Acquisition

Reference	Security Control Requirement
11.1.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data centre facilities have been pre-authorized by the organisation's business leadership or other accountable business role or function.

11.2. Outsourced Development

Reference	Security Control Requirement
11.2.1.	External business partners MUST adhere to the same policies and procedures for change management, release, and testing as internal developers within the organisation (e.g., ITIL service management processes).

11.3. Quality Testing

Reference	Security Control Requirement
11.3.1.	Organisation MUST follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.

11.4. Unauthorised Software Installations

Reference	Security Control Requirement
11.4.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorised software on organisationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

11.5. Production Changes

Reference	Security Control Requirement
11.5.1.	Policies and procedures MUST be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures MUST be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorisation by, the customer (tenant) as per agreement (SLA) prior to deployment.

12. Data Security & Information Lifecycle Management

For further and more detailed guidance please refer to the SS-004 Security Standard – Secure Data Handling Standard

12.1. Classification

Reference	Security Control Requirement
12.1.1.	Data and objects containing data MUST be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organisation.

12.2. Data Inventory & Flows

Reference	Security Control Requirement
12.2.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider MUST inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

12.3. Ecommerce Transactions

Reference	Security Control Requirement
12.3.1.	Data related to electronic commerce (ecommerce) that traverses public networks MUST be encrypted, appropriately classified and protected from fraudulent activity, unauthorised disclosure, or modification in such a manner to prevent contract dispute and compromise of data.

12.4. Handling Labelling and Security Policy

Reference	Security Control Requirement
12.4.1.	Policies and procedures MUST be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance MUST be implemented for objects that act as aggregate containers for data.

12.5. Non-Production Data

Reference	Security Control Requirement
12.5.1.	Production data MUST not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and MUST comply with all legal and regulatory requirements for scrubbing of sensitive data elements.

12.6. Ownership & Stewardship

Reference	Security Control Requirement
12.6.1.	All data MUST be designated with stewardship, with assigned responsibilities defined, documented, and communicated.

12.7. Secure Disposal

Reference	Security Control Requirement
12.7.1.	Policies and procedures MUST be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

13. Data Centre Security

13.1. Asset Management

Reference	Security Control Requirement
13.1.1.	Assets MUST be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time MUST be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

13.2. Controlled Access Points

Reference	Security Control Requirement
13.2.1.	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) MUST be implemented to safeguard sensitive data and information systems.

13.3. Off-site Authorisation & Equipment

Reference	Security Control Requirement
13.3.1.	Authorisation MUST be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.
13.3.2.	Policies and procedures MUST be established for the secure disposal of equipment (by asset type) used outside the organisation's premises. This MUST include a wiping solution or destruction process that renders recovery of information impossible. The erasure MUST consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.

13.4. Policy

Reference	Security Control Requirement
13.4.1.	Policies and procedures MUST be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.

13.5. Secure Area Authorisation

Reference	Security Control Requirement
13.5.1.	Ingress and egress to secure areas MUST be constrained and monitored by physical access control mechanisms to ensure that only authorised personnel are allowed access.

13.6. Unauthorised Persons Entry

Reference	Security Control Requirement
13.6.1.	Ingress and egress points such as service areas and other points where unauthorised personnel may enter the premises MUST be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorised data corruption, compromise, and loss.

13.7. User Access

Reference	Security Control Requirement
13.7.1.	Physical access to information assets and functions by users and support personnel MUST be restricted.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

14. Encryption & Key Management Entitlement

14.1. Entitlement

Reference	Security Control Requirement
14.1.1.	Keys MUST have identifiable owners (binding keys to identities) and there MUST be key management policies defined and implemented.

14.2. Key Generation

Reference	Security Control Requirement
14.2.1.	Policies and procedures MUST be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider MUST inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.

14.3. Sensitive Data Protection

Reference	Security Control Requirement
14.3.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.

14.4. Storage and Access

Reference	Security Control Requirement
14.4.1.	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms MUST be required. Keys MUST not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage MUST be separated duties.

15. Governance & Risk Management

15.1. Baseline Requirements

Reference	Security Control Requirement
15.1.1.	Baseline security requirements MUST be established for developed or acquired, organisationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations MUST be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements MUST

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
	be reassessed at least annually unless an alternate frequency has been established and authorised based on business need.

15.2. Data Focused Risk Assessments

Reference	Security Control Requirement
15.2.1.	Risk assessments associated with data governance requirements MUST be conducted at planned intervals and MUST consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorised use, access, loss, destruction, and falsification

15.3. Management Program Oversight Support & Involvement

Reference	Security Control Requirement
15.3.1.	Managers MUST be responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.
15.3.2.	An Information Security Management Program (ISMP) MUST be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorised access, disclosure, alteration, and destruction. The security program MUST include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organisation of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance
15.3.3.	Executive and line management MUST take formal action to support information security through clearly-documented direction and commitment, and MUST ensure the action has been assigned.

15.4. Policy & Policy Enforcement

Reference	Security Control Requirement
15.4.1.	Information security policies and procedures MUST be established and made readily available for review by all impacted personnel and external business relationships. Information security policies MUST be authorized by the organisation's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.
15.4.2.	A formal disciplinary or sanction policy MUST be established for employees who have violated security policies and procedures. Employees MUST be made aware of what action might be taken in the event of a violation, and disciplinary measures MUST be stated in the policies and procedures.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

15.5. Policy Impact on Risk Assessments & Reviews

Reference	Security Control Requirement
15.5.1.	Risk assessment results MUST include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.
15.5.2.	The organisation's business leadership (or other accountable business role or function) MUST review the information security policy at planned intervals or as a result of changes to the organisation to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.

15.6. Risk Assessments

Reference	Security Control Requirement
15.6.1.	Aligned with the enterprise-wide framework, formal risk assessments MUST be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk MUST be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).

15.7. Risk Management Framework

Reference	Security Control Requirement
15.7.1.	Risks MUST be mitigated to an acceptable level. Acceptance levels based on risk criteria MUST be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

16. Human Resources Security

16.1. Asset Returns

Reference	Security Control Requirement
16.1.1.	Upon termination of workforce personnel and/or expiration of external business relationships, all organisationally-owned assets MUST be returned within an established period.

16.2. Background Screening

Reference	Security Control Requirement
16.2.1.	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties MUST be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.

16.3. Employment Agreements & Termination

Reference	Security Control Requirement
16.3.1.	Employment agreements MUST incorporate provisions and/or terms for adherence to established information governance and security policies and MUST be signed by newly hired or on-boarded workforce personnel (e.g., full

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
	or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.
16.3.2.	Roles and responsibilities for performing employment termination or change in employment procedures MUST be assigned, documented, and communicated.

16.4. Mobile Device Management

Reference	Security Control Requirement
16.4.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).

16.5. Non-Disclosure Agreements

Reference	Security Control Requirement
16.5.1.	Requirements for non-disclosure or confidentiality agreements reflecting the organisation's needs for the protection of data and operational details MUST be identified, documented, and reviewed at planned intervals.

16.6. Roles & Responsibilities

Reference	Security Control Requirement
16.6.1.	Roles and responsibilities of contractors, employees, and third-party users MUST be documented as they relate to information assets and security.

16.7. Technology Acceptable Use

Reference	Security Control Requirement
16.7.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organisationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) MUST be considered and incorporated as appropriate.

16.8. Training & Awareness

Reference	Security Control Requirement
16.8.1.	A security awareness training program MUST be established for all contractors, third-party users, and employees of the organisation and mandated when appropriate. All individuals with access to organisational data MUST receive appropriate awareness training and regular updates in organisational procedures, processes, and policies relating to their professional function relative to the organisation.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

16.9. User Responsibility

Reference	Security Control Requirement
16.9.1.	All personnel MUST be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment

16.10. Workspace

Reference	Security Control Requirement
16.10.1.	Policies and procedures MUST be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.

17. Identity & Access Management

17.1. Audit Tools Access

Reference	Security Control Requirement
17.1.1.	Access to, and use of, audit tools that interact with the organisation's information systems MUST be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.

17.2. Credential Lifecycle & Provision Management

Reference	Security Control Requirement
17.2.1.	User access policies and procedures MUST be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organisationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures MUST incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimisation or re-use when feasible • Authentication, authorisation, and accounting (AAA) rules for access to

Reference	Security Control Requirement
	data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorisation, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements

17.3. Diagnostic / Configuration Ports Access

Reference	Security Control Requirement
17.3.1.	User access to diagnostic and configuration ports MUST be restricted to authorized individuals and applications.

17.4. Policies and Procedures

Reference	Security Control Requirement
17.4.1.	Policies and procedures MUST be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies MUST also be developed to control access to network resources based on user identity.

17.5. Segregation of Duties

Reference	Security Control Requirement
17.5.1.	User access policies and procedures MUST be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.

17.6. Source Code Access Restriction

Reference	Security Control Requirement
17.6.1.	Access to the organisation's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software MUST be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.

17.7. Third Party Access

Reference	Security Control Requirement
17.7.1.	The identification, assessment, and prioritisation of risks posed by business processes requiring third-party access to the organisation's information systems and data MUST be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorised or inappropriate access. Compensating controls derived from the risk analysis MUST be implemented prior to provisioning access.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

17.8. Trusted Sources

Reference	Security Control Requirement
17.8.1.	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.

17.9. User Access Authorisation Reviews & Revocation

Reference	Security Control Requirement
17.9.1.	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organisationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components MUST be authorised by the organisation's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider MUST inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.
17.9.2.	User access MUST be authorised and revalidated for entitlement appropriateness, at planned intervals, by the organisation's business leadership or other accountable business role or function supported by evidence to demonstrate the organisation is adhering to the rule of least privilege based on job function. For identified access violations, remediation MUST follow established user access policies and procedures.
17.9.3.	Timely de-provisioning (revocation or modification) of user access to data and organisationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, MUST be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider MUST inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

17.10. User ID Credentials

Reference	Security Control Requirement
17.10.1.	Internal corporate or customer (tenant) user account credentials MUST be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimisation or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorisation, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

17.11. Utility Programs Access

Reference	Security Control Requirement
17.11.1.	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls MUST be restricted.

18. Infrastructure & Virtualisation Security

*For specific guidance on Docker and Microservices please refer to the following resources.

18.1. Audit Logging / Intrusion Detection

Reference	Security Control Requirement
18.1.1.	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviours and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.

18.2. Change Detection

Reference	Security Control Requirement
18.2.1.	The provider MUST ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images MUST be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity MUST be immediately available to customers through electronic methods (e.g., portals or alerts).

18.3. Clock Synchronization

Reference	Security Control Requirement
18.3.1.	A reliable and mutually agreed upon external time source MUST be used to synchronise the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.

18.4. Information System Documentation

Reference	Security Control Requirement
18.4.1.	The availability, quality, and adequate capacity and resources MUST be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements MUST be made to mitigate the risk of system overload.

18.5. Vulnerability Management

Reference	Security Control Requirement
18.5.1.	Implementers MUST ensure that the security vulnerability assessment tools or services accommodate the virtualisation technologies used (e.g., virtualization aware).

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

18.6. Network Security

Reference	Security Control Requirement
18.6.1.	Network environments and virtual instances MUST be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations MUST be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.

18.7. OS Hardening and Base Controls*

Reference	Security Control Requirement
18.7.1.	Each operating system MUST be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.

*For specific OS Hardening please refer to SS-008 Server Operating System Security Standard

18.8. Production / Non-Production Environments

Reference	Security Control Requirement
18.8.1.	Production and non-production environments MUST be separated to prevent unauthorised access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.

18.9. Segmentation

Reference	Security Control Requirement
18.9.1.	Multi-tenant organisationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, MUST be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations

18.10. VM Security - Data Protection

Reference	Security Control Requirement
18.10.1.	Secured and encrypted communication channels MUST be used when migrating physical servers, applications, or data to virtualized servers and, where possible, MUST use a network segregated from production-level networks for such migrations.

18.11. Hypervisor Hardening*

Reference	Security Control Requirement
18.11.1.	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems MUST be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).

*For specific security guidance on Docker, Hypervisor and Microservices please refer to the relevant standards.

18.12. Wireless Security*

Reference	Security Control Requirement
18.12.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorised traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorised (rogue) wireless network devices for a timely disconnect from the network

*For security guidance on Wireless Security Deployments please refer to SS-019 Security Standard – Wireless Network Security Standard.

18.13. Network Architecture

Reference	Security Control Requirement
18.13.1.	Network architecture diagrams MUST clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures MUST be implemented and MUST apply defence-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

19. Interoperability & Portability

19.1. Use of APIs

Reference	Security Control Requirement
19.1.1.	The provider MUST use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.

19.2. Data Request

Reference	Security Control Requirement
19.2.1.	All structured and unstructured data MUST be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).

19.3. Policy & Legality

Reference	Security Control Requirement
19.3.1.	Policies, procedures, and mutually-agreed upon provisions and/or terms MUST be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.

19.4. Standardised Network Protocols

Reference	Security Control Requirement
19.4.1.	The provider MUST use secure (e.g., non-clear text and authenticated) standardised network protocols for the import and export of data and to manage the service, and MUST make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.

19.5. Virtualisation

Reference	Security Control Requirement
19.5.1.	The provider MUST use an industry-recognised virtualisation platform and standard virtualisation formats (e.g., OVF) to help ensure interoperability, and MUST have documented custom changes made to any hypervisor in use and all solution-specific virtualisation hooks available for customer review.

20. Mobile Security*

*Full guidance and security requirements for mobile security please refer to SS-017 Security Standard – Mobile Device Security Standard.

20.1. Anti-Malware

Reference	Security Control Requirement
20.1.1.	Anti-malware awareness training, specific to mobile devices, MUST be included in the provider's information security awareness training.

20.2. Application Stores

Reference	Security Control Requirement
20.2.1.	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.

20.3. Approved Applications

Reference	Security Control Requirement
20.3.1.	The company MUST have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

20.4. Approved Software for BYOD

Reference	Security Control Requirement
20.4.1.	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.

20.5. Awareness and Training

Reference	Security Control Requirement
20.5.1.	The provider MUST have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider MUST post and communicate the policy and requirements through the company's security awareness and training program.

20.6. Cloud Based Services

Reference	Security Control Requirement
20.6.1.	All cloud-based services used by the company's mobile devices or BYOD MUST be pre-approved for usage and the storage of company business data.

20.7. Compatibility

Reference	Security Control Requirement
20.7.1.	The company MUST have a documented application validation process to test for mobile device, operating system, and application compatibility issues.

20.8. Device Eligibility, Inventory & Management

Reference	Security Control Requirement
20.8.1.	The BYOD policy MUST define the device and eligibility requirements to allow for BYOD usage.
20.8.2.	An inventory of all mobile devices used to store and access company data MUST be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.
20.8.3.	A centralised, mobile device management solution MUST be deployed to all mobile devices permitted to store, transmit, or process customer data.

20.9. Encryption

Reference	Security Control Requirement
20.9.1.	The mobile device policy MUST require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and MUST be enforced through technology controls.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

20.10. Jailbreaking and Rooting

Reference	Security Control Requirement
20.10.1.	The mobile device policy MUST prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and MUST enforce the prohibition through detective and preventative controls on the device or through a centralised device management system (e.g., mobile device management).

20.11. Policy & Legal

Reference	Security Control Requirement
20.11.1.	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy MUST clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required.
20.11.2.	The mobile device policy MUST require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).

20.12. Lockout Screen

Reference	Security Control Requirement
20.12.1.	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement MUST be enforced through technical controls.

20.13. Operating Systems & Passwords

Reference	Security Control Requirement
20.13.1.	Changes to mobile device operating systems, patch levels, and/or applications MUST be managed through the company's change management processes.
20.13.2.	Password policies, applicable to mobile devices, MUST be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and MUST prohibit the changing of password/PIN lengths and authentication requirements.

20.14. Remote Wipe

Reference	Security Control Requirement
20.14.1.	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device MUST allow for remote wipe by the company's corporate IT or MUST have all company-provided data wiped by the company's corporate IT.

20.15. Security Patches

Reference	Security Control Requirement
20.15.1.	Mobile devices connecting to corporate networks, or storing and accessing company information, MUST allow for remote software version/patch validation. All mobile devices MUST have the latest available security-related patches installed upon general release by the device manufacturer or carrier

Reference	Security Control Requirement
	and authorized IT personnel MUST be able to perform these updates remotely.

20.16. Users

Reference	Security Control Requirement
20.16.1.	The BYOD policy MUST clarify the systems and servers allowed for use or access on a BYOD-enabled device.

21. Security Incident Management, E-Discovery & Cloud Forensics*

*For the full set of security controls for this area please refer to the SS-14 Security Standard - Security Incident Management Standard.

The expected security controls that are listed here are particularly relevant for cloud deployments where shared responsibilities are critical for effective incident response.

21.1. Contact / Authority Maintenance

Reference	Security Control Requirement
21.1.1.	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities MUST be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.

21.2. Incident Management & Reporting

Reference	Security Control Requirement
21.2.1.	Policies and procedures MUST be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.
21.2.2.	Workforce personnel and external business relationships MUST be informed of their responsibilities and, if required, MUST consent and/or contractually agree to report all information security events in a timely manner. Information security events MUST be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.

21.3. Incident Response Legal Preparation

Reference	Security Control Requirement
21.3.1.	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach MUST be given the opportunity to participate as is legally permissible in the forensic investigation.

21.4. Incident Response Metrics

Reference	Security Control Requirement
21.4.1.	Mechanisms MUST be put in place to monitor and quantify the types, volumes, and costs of information security incidents.

22. Supply Chain Management, Transparency & Accountability

22.1. Data Quality and Integrity

Reference	Security Control Requirement
22.1.1.	Providers MUST inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers MUST design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.

22.2. Incident Reporting

Reference	Security Control Requirement
22.2.1.	The provider MUST make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).

22.3. Network / Infrastructure Services

Reference	Security Control Requirement
22.3.1.	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, MUST be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.

22.4. Provider Internal Assessments

Reference	Security Control Requirement
22.4.1.	The provider MUST perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.

22.5. Supply Chain Agreements & Governance Reviews

Reference	Security Control Requirement
22.5.1.	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) MUST incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships,

Reference	Security Control Requirement
	physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorisation of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organisation being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence • Where considered appropriate by the Department, the Cloud provider Must support independent monitoring and audit of the security posture of the services that they are providing.
22.5.2.	

23. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

24. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

25. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		
Standards Master List		

26. Reference Documents

Cloud Security Alliance Cloud Controls Matrix.

27. Definition of Terms

Term	Definition
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, non-repudiation and accountability; including, but not limited to: devices, products, systems, key variables and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).

28. Glossary

The glossary can be found alongside the published standards and patterns.

29. Controls Catalogue Mapping

For full traceability the table below is given to show how the controls in this standard map to the control points in Cloud Controls Matrix v3.01 referenced above, and the ISO/IEC 27002:2013.

CCM Security Control	ISO/IEC 27002:2013 Control & DWP Controls Catalogue.	Cloud Computing Security Standard Control Statement(s)
AIS-01	9.4.2, 9.4.1,12.6.1 14.2.1, 14.2.3,14.2.7 18.2.2	9.1.1
AIS-02	9.1.1	9.2.1
AIS-03	9.1.1, 9.4.1,10.1.1 13.2.1, 13.2.2,18.1.4	9.3.1
AIS-04	9.1.1, 9.4.1,10.1.1 13.2.1, 13.2.2,18.1.4	9.3.2
AAC-01	12.7.1	10.1.1-3
AAC-02	-	10.1.4
AAC-03	8.2.1, 18.1.1,18.1.3 18.1.4 ,18.1.5	10.1.5
BCR-01	17.1.2	11.1.1
BCR-02	17.3.1	11.1.2
BCR-03	11.2.2, 11.2.3	11.2.1
BCR-04	12.1.1	11.3.1
BCR-05	11.1.4, 11.2.1,11.2.2	11.2.2
BCR-06	11.2.1	11.4.1
BCR-07	11.2.4	11.4.2
BCR-08	11.2.2, 11.2.3,11.2.4	11.4.3
BCR-09	17.1.1, 17.1.2	11.5.1
BCR-10	6.1.1, 7.2.1, 7.2.2 12.1.1, 15.1.1,15.1.3	11.6.1
BCR-11	8.2.3 ,12.3.1,15.1.1 15.1.3	11.6.2
CCC-01	9.4.5,12.5.1, 14.1.1 14.2.1, 14.2.7,14.3.1 15.1.1, 15.1.3,18.1.3 18.1.4	12.1.1
CCC-02	9.4.5, 12.1.4,12.5.1	12.2.1

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

CCM Security Control	ISO/IEC 27002:2013 Control & DWP Controls Catalogue.	Cloud Computing Security Standard Control Statement(s)
	12.6.1, 14.1.1,14.2.1 14.2.2, 14.2.3,14.2.4 14.2.7, 14.2.9,14.3.1 15.1.1, 15.1.2,15.1.3 15.2.1, 15.2.,16.1.3 18.2.1, 18.2.2,18.2.3	
CCC-03	6.1.1, 9.4.5,12.1.1 12.1.4, 12.5.1,12.6.1 14.1.1, 14.2.2,14.2.3 14.2.4, 14.2.9,14.3.1 15.1.1, 15.1.3,16.1.3 18.2.2, 18.2.3	12.3.1
CCC-04	6.1.2, 9.4.1, 9.4.4 12.2.1, 12.5.1,14.2.1 14.2.4, 15.1.1,15.1.3	12.4.1
CCC-05	12.1.4, 14.1.1,14.2.1 14.2.2, 14.2.3,15.1.1 15.1.3	12.5.1
DSI-01	8.2.1	13.1.1
DSI-02	-	13.2.1
DSI-03	8.2., 13.1.1, 13.1.2 14.1.2, 14.1.3,18.1.4	13.3.1
DSI-04	8.2.2, 8.2.3, 8.3.1 13.2.1	13.4.1
DSI-05	8.1.3, 12.1.4, 14.2.2 14.3.1	13.5.1
DSI-06	6.1.1, 8.1.2, 18.1.4	13.6.1
DSI-07	8.3.2, 11.2.7	13.7.1
DCS-01	8.1.1, 8.1.2, 8.1.3 8.1.4, 15.1.1,15.1.3	14.1.1
DCS-02	11.1.1, 11.1.2	14.2.1
DCS-03	-	14.3.1
DCS-04	11.2.6, 11.2.7	14.4.1
DCS-05	8.1.1, 8.1.2, 15.1.1	14.4.2
DCS-06	11.1.1, 11.1.2,15.1.1 15.1.3	14.5.1
DCS-07	11.1.6	14.6.1
DCS-08	11.2.5 12.1.2	14.7.1
DCS-09	11.1.1 15.1.1 15.1.3	14.8.1
EKM-01	10.1.1, 10.1.2	15.1.1
EKM-02	8.2.3, 10.1.2,18.1.5	15.2.1
EKM-03	8.3.3, 10.1.1,13.1.1 13.2.3, 14.1.3,14.1.2 18.1.3, 18.1.4	15.3.1
EKM-04	10.1.1 10.1.2	16.4.4
GRM-01	14.1.1, 15.1.1,15.1.3 18.1.2, 18.2.3	16.1.1
GRM-02	8.2.2, 18.1.1, 18.1.3	16.2.1
GRM-03	7.2.1, 7.2.2, 9.2.5 18.1.2, 18.2.2	16.3.1

CCM Security Control	ISO/IEC 27002:2013 Control & DWP Controls Catalogue.	Cloud Computing Security Standard Control Statement(s)
GMR-04	6.1.1, 6.1.3, 6.1.4 13.2.4, 15.1.1,15.1.3 18.1.2, 18.2.1	16.3.2
GRM-05	-	16.3.3
GRM-06	5.1.1, 7.2.2,15.1.1 15.1.3, 18.1.2	16.4.1
GRM-07	7.2.3, 15.1.1,15.1.3 18.1.2	16.4.2
GRM-08	15.1.1, 15.1.3	16.5.1
GRM-09	5.1.2, 15.1.1,15.1.3 18.1.2	16.5.2
GRM-10	12.6.1, 14.2.3,15.1.1 15.1.3	16.1.1
GRM-11	12.6.1,15.1.1,15.1.3, 17.1.1, 18.2.2	16.7.1
HRS-01	8.1.1, 8.1.2, 8.1.4	17.1.1
HRS-02	7.1.1	17.2.1
HRS-03	7.1.2, 13.2.4	17.3.1
HRS-04	7.3.1	17.3.2
HRS-05	6.2.1, 6.2.2, 8.2.1 8.3.1, 8.3.2, 8.3.3 18.1.4	17.4.1
HRS-06	13.2.4	17.5.1
HRS-07	17.6.1	6.1.1
HRS-08	8.1.3	17.7.1
HRS-09	7.2.2	17.8.1
HRS-10	7.2.2, 9.3.1, 11.2.8	17.9.1
HRS-11	7.2.2, 9.3.1, 11.1.5 11.2.8, 11.2.9	17.10.1
IAM-01	9.1.1, 9.1.2, 9.2.1 9.2.2, 9.2.5, 9.4.1	18.1.1
IAM-02	9.1.1, 9.1.2, 9.2.1 9.2.2, 9.2.5, 9.4.1	18.2.1
IAM-03	9.1.1, 9.4.4, 13.1.1	18.3.1
IAM-04	9.2.1, 9.2.2, 9.2.3 9.2.4, 9.2.5, 9.2.6	18.4.1
IAM-05	6.1.2	18.5.1
IAM-06	9.4.5, 18.1.3	13.6.1
IAM-07	9.1.1, 9.2.1, 9.2.2 9.2.5, 9.2.6	18.6.1
IAM-08	9.2.1, 9.2.2, 9.2.3 9.2.4, 9.2.5, 9.2.6 9.3.1, 9.4.1, 9.4.2 9.4.3, 9.4.5	18.8.1
IAM-09	9.1.2, 9.2.1,9.2.2 9.2.3, 9.4.1	18.9.1
IAM-10	9.2.5	18.9.2
IAM-11	9.1.1, 9.2.1, 9.2.2 9.2.3,9.2.6	18.9.3
IAM-12	9.1.1, 9.2.1,9.2.2 9.2.4, 9.2.5, 9.2.6 9.4.2	18.10.1
IAM-13	9.1.2, 9.4.4	18.11.1
IVS-01	A.9.2.3, A.9.4.4,A.9.4.1	19.1.1

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

CCM Security Control	ISO/IEC 27002:2013 Control & DWP Controls Catalogue.	Cloud Computing Security Standard Control Statement(s)
	12.4.1, 12.4.2,12.4.3 15.1.1, 15.1.3,16.1.2 16.1.7, 18.2.3,18.1.3	
IVS-02	12.1.2, 12.4.1,12.4.2 12.4.3, 12.6.1,12.6.2 15.1.1, 15.1.3,16.1.1 16.1.2, 16.1.3,16.1.4 16.1.5, 16.1.6,16.1.7	19.2.1
IVS-03	12.4.1, 12.4.4,15.1.1 15.1.3	19.3.1
IVS-04	12.1.3, 15.1.1,15.1.3	19.4.1
IVS-05	15.1.1, 15.1.3	19.5.1
IVS-06	9.1.2, 12.4.1, 13.1.1 13.1.2, 13.1.3,14.1.2 15.1.1,15.1.3,18.1.4	19.6.1
IVS-07	12.1.4, 12.2.1 12.4.1, 12.6.1,15.1.1 15.1.3	19.7.1
IVS-08	9.1.1, 12.1.4,14.2.2 14.2.3,14.2.4,14.2.9 15.1.1, 15.1.3	19.8.1
IVS-09	9.4.1, 13.1.3,15.1.1 15.1.3, 18.1.4	19.9.1
IVS-10	12.6.1, 14.2.3,15.1.1 15.1.3	19.10.1
IVS-11	12.6.1, 14.2.3,15.1.1 15.1.3	19.11.1
IVS-12	8.1.1, 8.1.2,8.1.3 8.3.3, 9.2.1,9.2.2 10.1.1, 10.1.2,11.2.1 11.2.4, 12.4.1,13.1.1 13.1.2, 13.1.3,13.2.1 15.1.1, 15.1.3	19.12.1
IVS-13	15.1.1, 15.1.3	19.13.1
IPY-01	12.6.1, 14.2.3,18.1.1 18.2.2 ,18.2.3	20.1.1
IPY-02	12.6.1, 14.2.3,18.1.1 18.2.2 ,18.2.3	20.2.1
IPY-03	6.1.1, 6.1.3, 12.6.1 14.2.3, 18.1.1,18.2.2 18.2.3	18.3.1
IPY-04	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	20.4.1
IPY-05	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	20.5.1
MOS-01	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.1.1
MOS-02	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.1.1
MOS-03	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.3.1
MOS-04	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.4.1
MOS-05	12.6.1, 14.2.3,18.1.1	21.5.1

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

CCM Security Control	ISO/IEC 27002:2013 Control & DWP Controls Catalogue.	Cloud Computing Security Standard Control Statement(s)
	18.2.2, 18.2.3	
MOS-06	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.6.1
MOS-07	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.7.1
MOS-08	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.8.1
MOS-09	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.8.2
MOS-10	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.8.3
MOS-11	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.9.1
MOS-12	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.10.1
MOS-13	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.11.1
MOS-14	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.12.1
MOS-15	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.13.1
MOS-16	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.13.2
MOS-17	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.11.2
MOS-18	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.14.1
MOS-19	12.6.1, 14.2.3,18.1.1 18.2.2, 18.2.3	21.15.1
MOS-20	9.2.1, 9.2.2,12.6.1 14.2.3, 18.1.1,18.2.2 18.2.3	21.16.1
SEF-01	6.1.3, 6.1.4	22.1.1
SEF-02	16.1.1, 16.1.2	22.2.1
SEF-03	6.1.1, 7.2.1, 7.2.2 16.1.1, 16.1.2,16.1.3	22.2.2
SEF-04	7.2.2, 7.2.3,16.1.7 18.1.3	22.3.1
SEF-05	16.1.6	22.4.1
STA-01		20.1.1
STA-02		20.1.2
STA-03		20.1.3
STA-04		20.1.4
STA-05		20.1.5
STA-06		20.1.6
STA-07		20.1.7, 20.1.5
STA-08, STA-09		20.1.8
STA-01	12.6.1, 14.2.3,15.1.1 15.1.3, 18.1.1,18.2.2 18.2.3	23.1.1
STA-02	15.1.1, 15.1.3	23.2.1
STA-03	13.1.2, 15.1.1, 15.1.2, 15.1.3	23.3.1
STA-04	12.6.1, 14.2.3,15.1.1, 15.1.3, 18.1.1, 18.2.2, 18.2.3	23.4.1

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

CCM Security Control	ISO/IEC 27002:2013 Control & DWP Controls Catalogue.	Cloud Computing Security Standard Control Statement(s)
STA-05	9.4.1, 10.1.1, 13.2.2, 15.1.1, 15.1.2,15.1.3	23.5.2
STA-06	15.1.1, 15.1.3	23.5.2
STA-07	15.1.1, 15.1.3	23.6.1
STA-08	15.1.1, 15.1.3	23.7.1
STA-09	13.1.2, 15.1.1,15.1.2, 15.1.3, 15.2.1	23.7.2
TVM-01	12.2.1, 15.1.1,15.1.3	24.1.1
TVM-02	12.6.1, 14.2.2, 14.2.3, 15.1.1, 15.1.3	24.2.1-.2
TVM-03	12.2.1, 15.1.1,15.1.3	24.3.1