

Framework Schedule 6

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	DBT MacBook Air and MacBook Pro Project _2740
THE BUYER:	Secretary of State for the Department for Business and Trade
BUYER ADDRESS	Old Admiralty Building, London, SW1A 2DY
THE SUPPLIER:	Kingsfield Computer products Ltd
SUPPLIER ADDRESS:	16-18 Midland Street, Manchester, M12 6LB
REGISTRATION NUMBER:	03357539
DUNS NUMBER:	519903041
SID4GOV ID:	

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 21 July 2023. It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

- Lot 2 Hardware & Associated Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

- 1 This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
- 2 Joint Schedule 1(Definitions and Interpretation) RM6068
- 3 The following Schedules in equal order of precedence:
 - Joint Schedules for **Project _2740**
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 10 (Rectification Plan)

Framework Schedule 6

- Joint Schedule 11 (Processing Data)
 - Call-Off Schedules for **Project _2740**
- 4 CCS Core Terms (version 3.0.6)
- 5 Joint Schedule 5 (Corporate Social Responsibility) RM6068

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Special Term: All devices must include 3 years warranty from the date of delivery.

CALL-OFF START DATE: by 31 August 2023

CALL-OFF EXPIRY DATE: Contract will expire when the goods have been delivered.

WARRANTY PERIOD: 3 Years

CALL-OFF INITIAL PERIOD: N/A

CALL-OFF OPTIONAL EXTENSION N/A

PERIOD

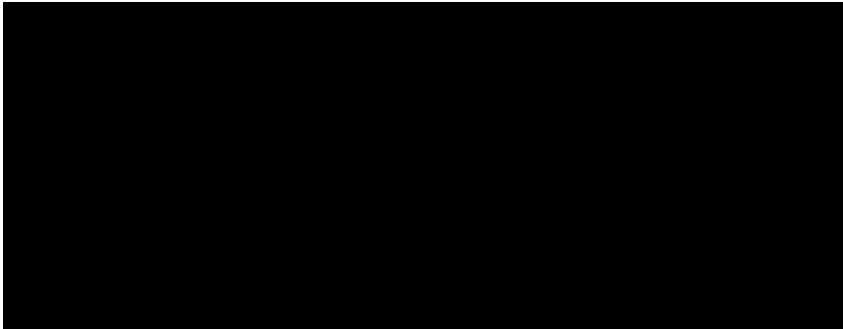
CALL-OFF DELIVERABLES

GOODS/SERVICES DESCRIPTION
25 units of MacBook Pro (no colour preference) -- Apple M2 chip <ul style="list-style-type: none">• 8-core CPU with 4 performance cores and 4 efficiency cores• 10-core GPU• 16-core Neural Engine• 100GB/s memory bandwidth• 16 GB RAM Retina display <ul style="list-style-type: none">• 13.3-inch (diagonal) LED-backlit display with IPS technology; 2560x1600 native resolution at 227 pixels per inch with support for millions of colours• 500 nits brightness• Wide colour (P3)• True Tone technology 8GB <ul style="list-style-type: none">• 8GB unified memory Configurable to: 16GB or 24GB

Framework Schedule 6

25 units of MacBook Air (no colour preference) -- (M2, 2022) Model Identifier: Mac14,2 Total RAM:16.0 GB Drive Capacity:256.0 GB
--

LOCATION FOR DELIVERY



DATES FOR DELIVERY OF THE DELIVERABLES

Delivery date estimated by 31st August 2023

TESTING OF DELIVERABLES

N/A

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be 3 years from date of delivery.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Charges used to calculate liability is the total contract value of £52,593.49 excl VAT

Framework Schedule 6

BUYER'S AUTHORISED REPRESENTATIVE



BUYER'S ENVIRONMENTAL POLICY

N/A

BUYER'S SECURITY POLICY

DBT Information Security Policy

Departmental Security Team

Note: This Policy should be read in conjunction with the policies and guidance documents listed within this document.

Date of Issue: November 21

Framework Schedule 6

Document control

1	Title:	Information Security Policy
2	Summary:	DBT safeguarding & protecting information and other assets
3	Policy owner:	Departmental Security Team
4	Responsible Director:	Finance and Business Services
5	Applies to:	All staff & authorised personnel handling DBT information & other assets
9	Version:	v.01
13	Date of next formal review:	November 2022

Document Revision History

Version	Date	Author	Summary of changes
0.1	Oct 21	Security Team	Updated policy and alignment to Corporate Policies Framework

Contents:

1. Introduction
2. Scope of the policy
3. Objectives of Information Security
4. Governance Framework
 - 4.4. Principles
 - 4.6. Information Risk Management
5. Roles and responsibilities
 - 5.7. Access to DBT Information Assets by Third- Party Suppliers
6. Protection of DBT systems & network
7. Legal Compliance
8. Monitoring
9. Applicable Policies
10. Review

Framework Schedule 6

1. Introduction

- 1.1. The Department for International Trade is responsible for promoting UK trade across the world and encouraging economic growth, and inward investment. It uses Information to support day-to-day business objectives and to enable the continued development and provision of products and services; to meet the future needs and prosperity of the wider UK economy and international partners. As a government department, DBT has a duty of care to protect all sensitive and valuable information from unauthorised disclosure, loss, alteration, or destruction. This includes all information handled as part of our daily business.
- 1.2. The purpose of the Information Security Policy is to protect DBT from all information security threats, whether internal or external, deliberate, or accidental. This policy is to ensure security is achieved and maintained where all DBT information (or other assets), are handled, making them less likely to be compromised, corrupted, or disclosed to unauthorised persons and its origin is authenticated.
- 1.3. DBT is committed to developing and implementing effective Information Security controls to safeguard and protect all Information assets and business interests from harm. DBT will foster a culture that values, protects, and uses information appropriately.

2. Scope of the policy

- 2.1. This policy applies to all DBT staff, suppliers, consultants, contractors and employees from external organisations, including all who have a legitimate business need to handle DBT information; enter DBT premises, or access any other DBT assets, as authorised representatives. All are collectively referred to as staff or authorised representatives throughout this policy.
- 2.2. This policy sets out how DBT staff and authorised representatives of the department handling DBT assets, shall manage and protect DBT information. It also details the requirements that various functions have for ensuring the safety and security of all information handled and other assets, on behalf of the department.
- 2.3. This policy applies to all aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store,

Framework Schedule 6

process, transmit or receive information. This policy applies to all DBT information and data that is handled or processed internally or shared externally with authorised partners or organisations.

3. Objective of Information Security

- 3.1. The objective of information security is to achieve and maintain a condition where all information is handled safely and securely by those who have legitimate need to access it in a way that it is less likely to be corrupted or disclosed to unauthorised persons and its origin is authenticated.
- 3.2. DBT requires that all Information Assets are protected from all threats, whether internal or external, deliberate, or accidental. Therefore, all systems handling information assets must be managed securely.
- 3.3. By implementing this Information Security Policy, DBT will operate in line with Government standards and best practice for securing information. DBT is committed to ensuring that effective security arrangements are implemented and regularly reviewed to reduce the threats and manage risks to all assets including:
 - DBT staff and authorised users
 - The information that DBT collects, creates, shares, processes, and stores
 - DBT's physical assets and resources
 - DBT's digital, IT and communication systems
 - Premises that DBT uses to accommodate its operations, people, and visitors

4. Governance Framework

- 4.1. DBT has developed a control framework of policies, procedures, and guidelines for Information security across the whole department. This is achieved through implementation of a combination of independent, but mutually supportive risk managed technical controls and measures; processes and procedures designed to detect, deter, and delay security attacks and facilitate investigation.

Framework Schedule 6

4.2. DBT security policies and procedures are implemented for the protection of all assets including detecting, reporting, responding to and handling security incidents and breaches.

4.3. The protection is designed for the preservation of:

- **confidentiality** – ensuring that information is only accessible to authorised persons protecting sensitive information from unauthorised disclosure or interception
- **integrity** – safeguarding the accuracy and completeness of information and processing methods, free from tampering
- **availability** – ensuring that authorised users have access to information and associated assets when required and ensuring that vital services remain available
- **non-repudiation** – the reasonable assurance that, where appropriate, a user cannot deny being the originator of a message after sending it.

4.4. Principles

4.5. This policy is based upon the following principles:

- DBT has a duty to provide a secure environment for all those in scope for handling information assets.
- All those in scope are expected to observe the highest standards of ethical, personal, and professional conduct, including all staff and authorised representatives
- All information assets shall have an Information Asset Owner
- Access to information assets shall only be granted to those staff, third parties, consultants /contractors or other representatives who have a proven documented and authorised requirement to access the information legitimately to fulfil their role function
- Levels of protection and risk reduction measures will be derived from a risk and threat analysis
- Neither this policy nor any standard evolved from it shall take precedence over the requirements of law

4.6. Information Risk Management

4.7. DBT risk assessment system must be used and carried out where this involves information or information processing systems. Information and Risk Assurance Process ([IRAP](#)), sets out DBT procedures for risk assessing and assuring new and existing projects and initiatives, before they are purchased, build or

Framework Schedule 6

used in DBT. This includes, any function involving digital, data and technology or the processing of information.

4.8. The purpose is to mitigate any risks identified; controls are specified and implemented within the project timescales. Security risk management's objectives are to:

- Ensure all DBT Information assets undergo a formal risk management process
- Ensure that all those who have been authorised to access DBT's information assets are aware of, and fully comply with relevant legislative requirements; and government security policies and instructions, relating to the protection of the department's assets.
- Delivery of appropriate mitigation of information security risks within DBT and suppliers to acceptable levels, by risk management and the use of [HMG Security Classifications](#); HMG standards; Physical controls & Cyber technical controls.
- Ensure all those to whom the policy applies are aware of their responsibilities for Information security risk management

5. Roles and responsibilities

5.1. This Policy is founded on the principle that security is everyone's responsibility and an integral part of everyone's role i.e. all staff and authorised representatives. This enables DBT to operate effectively and securely.

5.2. **Senior Security Adviser (SA)** - is responsible for articulating the security needs of the department, overseeing, and reporting on the delivery of services to agreed standards, including being the responsible owner for local security policies. Acting as an intelligent customer for the department. The SA supports the Department's security infrastructure and procedures through recognition of the security profession and implementation of the Government Functional Standard – [Security 007](#).

5.3. **Data Protection Officer (DPO)** - is responsible for advising The Permanent Secretary /Accounting Officer and senior boards (such as ExCo) about DBT's compliance with UKGDPR & Data Protection 2018 Act and best practice, including explaining residual risk and addressing privacy requirements.

Framework Schedule 6

- 5.4. **Head of Knowledge and Information Management (KIM)** - has responsibility for the exploitation of DBT information. To work with the department to make sure data and records are created, protected, and used in a compliant way. To enable our people to access the right information easily and transparently to gain maximum value from our corporate memory.
- 5.5. **Information Asset Owners (IAO)** - must identify and understand DBT's information assets and are responsible for ensuring information assets are handled and managed appropriately. This means making sure information assets are properly protected and their value to DBT is fully exploited. IAOs are supported by Information Asset Managers (IAM) who will have hand on knowledge and duties associated with an asset.
- 5.6. **All Staff** (and authorised representatives) – must comply with the information security policy and procedures, to safeguard all information which they have legitimate access to - including any other DBT assets, which they are entrusted with. Each individual has personal responsibility to ensure no breaches occur as a result of their actions.

5.7. Access to DBT Information Assets by Third- Party Suppliers

- 5.8. All DBT third-party suppliers or contractors personnel must be authorised to access information and have the appropriate level of security clearance to ensure the protection of DBT assets throughout the duration of the contract.

All suppliers must maintain the safety of DBT information to protect them from unauthorised access, loss, or disclosure, when handled or shared on behalf of DBT. Suppliers must be made aware of their responsibilities regarding information security

Suppliers handling DBT Information or providing a service to DBT must adopt a proportionate risk-based approach to information security risk management, by adopting HMG standards or internationally recognised standards and controls, to mitigate risks.

No external entities shall be given access to any of DBT's information assets unless that body has been formally authorised to have access by the appropriate Information Asset Owner or contract manager via the official DBT procurement process.

6. Protection of DBT systems & network

Framework Schedule 6

6.1. DBT has Cyber security policies and procedures for the protection of all IT systems and devices which contain or process information assets, including detecting, reporting, responding to and handling security incidents and breaches.

Cyber Policies ensures:

- Correct and secure operations of information processing facilities by regulating, monitoring, and reviewing the implementation of protective measures
- The protection of information in networks and any supporting information processing facilities and maintain the security of information transferred within DBT and with any external entity
- That information security is integral to information systems across the entire lifecycle of acquisition, development, maintenance and decommissioning of systems

7. Legal Compliance

7.1. All staff and authorised representatives must comply with relevant legislation, regulations, and central government policy, covering information governance and security.

7.2. DBT shall develop and improve information security to provide appropriate protection for information consistent with legal requirements and central government standards. The following legislation applies:

- Freedom of Information Act 2000
- UK General Data Protection Regulation and Data Protection Act 2018
- Public Records Act 1958
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Human Rights Act 1998
- Civil Service Code

8. Monitoring

8.1. This policy applies to All DBT staff and authorised representatives. Anyone who fails to comply with these standards and procedures will be subject to disciplinary action.

Framework Schedule 6

8.2. Failure to comply with this policy constitutes a security breach. Serious or repeated breaches of security, which include deliberate or damaging behaviour, may lead to a review of, or if a serious incident, the withdrawal of an individual's security clearance and the individual may also be subject to disciplinary action as detailed in the DBT Disciplinary Policy.

All staff and authorised representatives are responsible for reporting any security breaches.

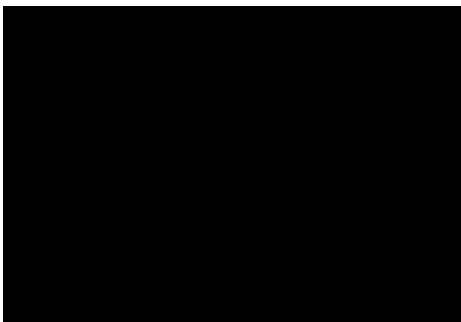
9. Applicable Policies

- Acceptable Use Policy
- Security Breach Policy
- Social Media Policy
- Security Incident & Reporting Policy
- Access Control Policy
- Personnel Security Policy
- Cyber Security Monitoring Policy
- Information and Records Management Policies

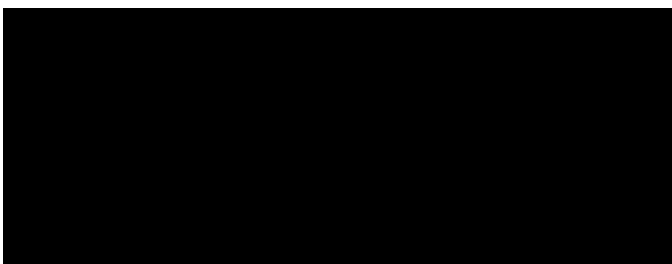
10. Review

DBT security policies will remain under review and will undergo formal review every 12 months or after a major incident. The policy may be modified as appropriate when any changing issues or and circumstances are identified which impacts on the policies or procedures.

SUPPLIER'S AUTHORISED REPRESENTATIVE



SUPPLIER'S CONTRACT MANAGER



Framework Schedule 6

PROGRESS REPORT FREQUENCY

N/A

PROGRESS MEETING FREQUENCY

N/A

KEY STAFF

N/A

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

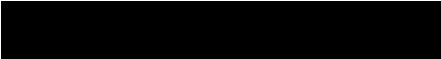
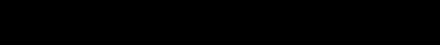
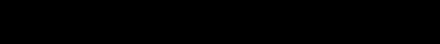
GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

N/A

For and on behalf of the Supplier:

Signature: 
Name: 
Role: 

Date: 22/7/2023

Framework Schedule 6

For and on behalf of Buyer:

Signature:

Name:

Role:

Date: 24/7/2023