Department
for Environment
Food & Rural Affairs

www.gov.uk/DEFRA

Atos IT Services UK Ltd

FEUS

Security Management Plan

Table of Contents

1. Executive Summary

This is the Security Management Plan (SMP) Outline for the delivery and operation of the DEFRA **FEUS** service which will be further developed during the Transition period. As such, this is not exhaustive and does not entail all service relevant details. The document is set out in alignment with ISO:IEC 27001 standards.

The scope of this SMP is the operation and administration of the DEFRA **FEUS** services as defined in the service contract. This SMP will be periodically updated, and reviewed at least annually, throughout the lifetime of the DEFRA **FEUS** contract.

The Atos Security Management function will fulfil a Governance and Compliance role over service delivery.

Atos will have designated accountability and responsibility for the security management activities as defined within the DEFRA **FEUS** service schedules.

This Security Management Plan below is in direct response to that requirement and is structured in accordance with ISO/IEC 27001/2, the guidance provided in the security policy framework, and HMG information assurance standards and their associated NCSC and CPNI good practice guides.

The Client Security Manager will have responsibility for the Security Management activities as defined within **FEUSPP Call Off Schedule 13 (Security Requirements).**

2. Document Control

2.1 Version History

Version	Date	Comments
1.0	05 September 2024	Template Version finalised

2.2 Issue Control

Version	Author Name	Approver
1.0	Atos	ISST Version

2.3 Purpose

This document outlines the Information Security Management Plan that will be used to manage information security risks across the DEFRA **FEUS** services provided to DEFRA by Atos.

The purpose of this document is to outline how DEFRA's IT service provisioned by Atos will demonstrate an adequate level of security is achieved. It provides an overview of the direction and approach for managing the Information Security function and processes for the services provided by Atos. This will be in relation to the contractual requirements as outlined in

Information security is an important aspect of any system/service operation and without an adequate level of security a system/service would be potentially exposed to unnecessary risk. Security is not an 'add on' to system/service but must be an integral part of the service. The security of a service must consider the risks and address these accordingly and be planned. Without planning, security issues would be addressed in an ad hoc manner, which may not give consistent and complete coverage across the system.

The security of a system/service must be planned and cover the entire life cycle of the service.

The security of the Atos service provision to DEFRA is built upon the existing:

- DEFRA specific policies and procedures
- Atos policies and procedures where possible.

This document is primarily targeted at the Atos support staff involved with supporting DEFRA's **FEUS** Service.

This document will be maintained and issued by the Atos Client Security Manager (CSM).

2.4 Scope

2.4.1 Scope of the SMP

The scope of this document is limited to providing a Security Management Plan for the Atos service provision to DEFRA:

All sections of this plan apply to the services that Atos provides to DEFRA unless an exception is granted following the process explained in Section 2.5. This applies to all Atos projects and programmes, information systems, networks, employees, including: full-time, part-time, temporary, agents, contractors, suppliers and consultants that are or will support the DEFRA **FEUS** services provided by Atos to DEFRA.

In addition to this Security Management Plan document, the following documents relating to Atos' ISO 27001 certification are also relevant:

- Scope of the Atos UKI Information Security Management System
- Atos ISO27001 Statement of Applicability.

2.4.2 Scope of the Service

The Future End User Services scope comprises both the front-end support of the End User Devices, through Service Desk, Self-Help, and Onsite Support Services, and the Back-Office support of services and infrastructure used by the End User Device communities, including but not limited to Device, Application, and Security Management, in addition to support for physical services, such as Comms Rooms, Body Worn Cameras, and Managed Meeting Rooms.

The scope of this Security Management Plan identifies the governance applied across these services as part of the overall security management of the service.

2.5 Exceptions

Policy exceptions may be obtained from the DEFRA Security Working Group (SWG). The appropriateness of these exceptions will be considered and reviewed by the SWG forum on at least an annual basis. Supporting evidence must be retained for both the exception and the annual review.

In addition, policy exceptions may originate direct from teams within Defra Group Security secured with the approval of the appropriate Business/Risk Owner.

2.6 Glossary

Term	Description
CSM	Client Security Manager
DEFRA	Department for the Environment Food and Rural Affairs
ISO	International Standards Organisation
SWG	Security Working Group
UKI	UK & Ireland

3. Information Security Management System

3.1 General Controls

All foundation security policies are derived from the Atos Information Security Management System (ISMS) which is externally certified to ISO27001:2022.

Information Security within Atos is initiated and controlled by a global Security Management Group which promotes good security practices across the organisation. There are Security Managers appointed at country level. The Chief Security Officer for the UK is also Head of the UK Security Directorate, ensuring service line responsibility for information security, and reports into the Chief Operating Officer at UK board level.

Atos will maintain the confidentiality, integrity and availability of the DEFRA services and data whilst complying with UK law, relevant industry appropriate standards, and good practice guides in accordance with the DEFRA **FEUS** services contract.

3.2 Client Specific Controls

Where DEFRA require controls over and above the Atos Baseline, bespoke policies will be created to reflect these requirements and referenced in the induction and training material provided to all staff working on the DEFRA **FEUS** services contract. Bespoke policies are subject to customer review and agreement.

In the case of any conflict between DEFRA and Atos information security documentation, the following will apply (in descending order of precedence); security controls will always be maintained in line with the Atos ISMS as a minimum standard:

- DEFRA ISMS and appropriate contractual Security schedule
- Atos ISMS policies and standards.

The availability of quality information security documentation that is well maintained is one key component of an effective information security management system for DEFRA; other key components are the production and maintenance of Information Assurance documents, as agreed, which offer a proportionate level of risk management and risk assessments by appropriately qualified personnel.

Institution, and regular review, of a clear information security management organisation, conducting regular updates of information security risk assessment and management review results.

CREST, CHECK or Tiger ITHC Testing, where stated as required in contract schedule across the Services and sub-contractors, are performed at least annually. The Atos Client Security Manager (CSM) is responsible for ensuring all related Information Security Policies and processes are communicated, and validating the adherence of Atos, partners, and subcontractors to them.

4. Organising Atos Information Security

4.1 Security Management Structure and Responsibilities

4.1.1 Atos Client Security Manager (CSM)

The Atos DEFRA CSM has day-to-day responsibility for Information Security and its implementation for the IT service provision. The Atos CSM will liaise with and report to the Atos Operations Manager, who has overall responsibility for information security and its implementation within DEFRA.

The CSM will ensure and validate that all managers and staff are aware of and comply with the appropriate policies and procedures which include DEFRA's IS Security Policy, Information Security Classification Standards, and Privacy and Data Protection Policy.

The CSM will produce and maintain a set of Assurance documents in line with DEFRA requirements The CSM will attend the monthly Security Working Group (SWG) including ownership and remediation of any actions arising from these meetings. The SWG membership will consist of the following:

- Atos CSM
- DEFRA Security Manager
- Atos Service Manager on request.

4.1.2 Atos DEFRA Service Director

The Atos DEFRA Service Director will be responsible for the day-to-day maintenance and implementation of DEFRA’s environment, along with the Atos support, infrastructure (i.e. the connections to and between Atos locations) from which remote support is provided to DEFRA. Overall Atos responsibility rests with the Atos DEFRA Service Director, while day-to-day activities are delegated to the Atos Operations Manager and Atos Support Team members (see below).

4.1.3 Atos Operations Manager / Support Team

The Atos Operations Manager is responsible to the Atos Service Director for the operation of the DEFRA environment, support and infrastructure. The Atos Operations Manager will be responsible for:

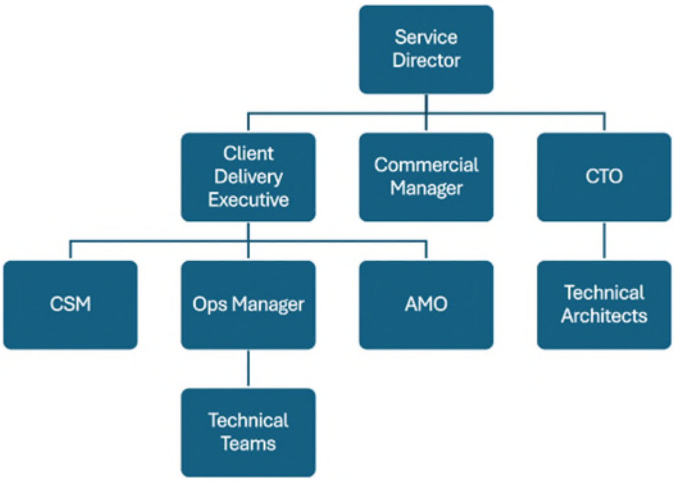
- Ensuring the configuration and control of the infrastructure hosted by Atos, and IT management systems, and all media associated with the systems, and their maintenance are in a secure state
- Managing changes to the configuration and operation of the applications and associated infrastructure, and associated systems. Ensuring the IT and associated infrastructure and IT management systems, are configured in accordance with these, and associated Atos Security Operating Procedures (SyOPs)
- In co-operation with the Service Providers and Facilities Manager (FM), authorising physical access to the restricted areas where IT equipment for DEFRA is located
- Assisting with the enforcement of DEFRA’s information security policies and procedures
- Ensuring the approved configuration of DEFRA’s infrastructure and associated systems is maintained

- Assisting with regular checks of the configuration of DEFRA's infrastructure, IT management systems and annual audits of the configuration against the configuration management records
- In liaison with the Service Providers and FM Manager for the location, maintaining the physical security of each IT/communications room
- Monitoring and controlling all maintenance work for DEFRA and associated infrastructure and related systems within the IT/communications rooms
- Notifying the CSM and Facilities Manager when any user no longer requires access to the restricted areas and taking necessary steps to change and/or recover keys that may have been issued to that person.

Changes to the DEFRA environment are only permissible through a valid and approved change request.

All members of Atos staff and all contractors working within the DEFRA environment are responsible for adhering to DEFRA's Information System Security Standards, HMG and NCSC policy and standards, including its supporting documentation (including information security guidelines) where appropriate.

Fig.1 Sample account structure



4.2 Information Security Incident and Problem Reporting

Any suspected Information Security incident or weakness associated with the DEFRA service which is identified or suspected by Atos staff will be reported to the Service Desk who will then follow the escalation procedures for Incident and Problem Management, whilst ensuring reporting is escalated to the Atos CSM who has the responsibility in managing the incident and informing DEFRA.

All security incidents must be reported to the Atos Client Security Manager and DEFRA following the DEFRA and Atos Security Incident Management Procedures/Policies as described in Section 11: Information Security Incident Management.

4.3 Vulnerability Management

DEFRA assets should be patched in a manner compliant with both the contractual requirements and the Patch Management Policy. Atos will report compliance to these monthly, in line with stipulated contractual requirements, to the Security Working Group forum with scope of forum and attendees set out in the SWG Terms of Reference.

The Atos Client Security Manager will work with the Atos Operations Manager to address any significant vulnerability identified and report progress through the SWG forum and/or Defra Operational Security team where appropriate.

4.4 Agreements on External (Third) Party Access

The Atos CSM will ensure all arrangements involving external (third) party sub-contracted access are based on a formal contract, containing at least the following information security requirements:

- The contractor must comply with the Atos and DEFRA Information Security Policy and associated documents
- The contractor must obtain appropriate clearance as required by DEFRA
- The contractor must comply with relevant legislation and regulation.

The Atos Client Security Manager is responsible for ensuring that any new arrangements or changes to external (third) party access contracts adequately reflect the relevant security requirements. The process for identifying and managing any security Risks from any Sub-contractors and third parties will follow the DEFRA Risk/Assurance model.

Key contract sub-contracts are identified in FEUSSP Order Form Attachment 5 (Key Supplier Personnel and Key Sub-contractors) which is included as an appendix to this document.

4.5 Location of Service Provision

The management of security will remain delivered within the UK.

Where Atos intends to use offshore support facilities from Atos offshore locations this will be agreed in advance with Defra Security.

4.6 Responsibility/Accountability

For Organising Atos Information Security:

Responsibility	Atos CSM
Accountability	Atos Client Executive Partner

5. Asset Management

5.1 Inventory of Assets

The Atos Operations Manager will have overall responsibility, with the asset managers, for ensuring applicable assets are recorded within the Asset Management Systems, in line with the DEFRA Asset Management Policy.

5.2 Acceptable Use of Information and other Assets

The Atos Global Information Security Policy; the Atos UK Information Security Policy; the Atos Global IT Acceptable Use Policy; the Atos UK Computer Usage Policy require all employees to handle information in a manner appropriate to its classification. The Atos CSM will be responsible for ensuring this is adhered to by all the Supplier's staff.

The Atos Computer Usage Policy states the employees' responsibilities in all aspects of computer usage. These policies provide the overall framework for several detailed specific policies and applies to all permanent and temporary employees whether employed directly by Atos or subcontracted. Breach of these Policies will be considered a disciplinary issue.

Should Atos wish to deviate from NCSC/CESG guidance this will only be done with prior written agreement from the Authority, following an assessment of the Residual Risk involved.

The Atos UK Computer usage policy contains the following two paragraphs - "You must not use Company or Customer IT and communications systems, whether alone or in conjunction with any other device, to gain unauthorised access to, or make disclosure or copy of, confidential information belonging to the Company or Customer.

The unauthorised disclosure or copying of information belonging to the Company or Customer is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct."

Any Device used to access or manage Authority Data and services must be under the management authority of Authority or Supplier and have a minimum set of security policy configuration enforced in line with the NCSC End User Device Platform Security Guidance. These devices must be placed into an Authority approved 'known good' state prior to being provisioned into the management authority of the Authority.

5.3 Return of Assets

All employees, contractors and third-party users are required to return all the organisation's assets in their possession upon termination of their employment, contract, or agreement. The access rights of all employees, contractors and third-party users to information and information processing facilities are removed upon termination of their employment, contract, or agreement, or adjusted upon change.

The Atos Joiner and Leavers Process (JML) documents the processes for when an Atos Employee (including Administrators) leaves the organisation.

5.4 Information Classification

<Refer to Security Aspects Letter detailing classification>

Atos Global Information Classification Policy and the Atos Country Specific (where issued) Classification Policy ensure that the appropriate level of protection is given to DEFRA information, according to the potential harm that might be caused by its loss or unauthorised disclosure along with compliance with UK data law and GDPR regardless of delivery location.

N.B. The Cabinet Office document "Government Security Classifications - May 2018" will take primacy over internal Atos Classification documents.

Atos will:

a. only handle Authority Data classified at OFFICIAL which is detailed in Government Security Classification Policy. The Authority may choose to limit the handling of Authority Data to a 'need to know' basis which will be indicated by the ‘OFFICIAL-SENSITIVE' classification. When the Supplier receives information marked as 'OFFICIAL – SENSITIVE' the Supplier shall immediately seek additional specific guidance from the Authority.

b. apply the ‘principle of least privilege’ (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of ICT systems which will process or store Authority Data.

Atos binding corporate rules

Atos is the first IT company to have obtained approval of its Binding Corporate Rules (BCRs) by European data protection authorities both as a data controller and a processor. This approval evidences Atos’ commitment to the protection not only of its own data but also that of its clients: all Atos entities provide a very strong level of protection to personal data, regardless of their location in the world.

Atos binding contract rules have EU approval for compliance with EU law; additionally, Atos has a global GDPR program for compliance. Post-Brexit, Atos will continue to comply with all Contractual and legal requirements.

5.5 Responsibility/Accountability

For Asset Management:

Responsibility	Atos CMDB team
Accountability	Atos Client Executive Partner

6. Human Resources Security

The Atos UK Security Control guidelines document covers the areas listed below in its guidelines for line managers. Additional controls/procedures will be developed and maintained as required in conjunction with DEFRA to ensure that Atos employees fully comply with Atos and DEFRA Human Resources security requirements.

All HR Related Policies and Processes are available in the HR portal for all Atos employees to read and understand.

6.1 Terms and Conditions

The Atos Operations Manager will ensure appropriate terms and conditions and role descriptions for Atos staff working on the DEFRA **FEUS** services will be clearly defined.

6.2 Staff vetting

All Atos staff and subcontractors working on the DEFRA account will be cleared to the appropriate level as stated by contractual terms and/or stated in Security Aspects Letter.

The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearance from accessing systems which store, process, or are used to manage Authority Data except where this is agreed with the Authority in writing.

6.3 Information Security Awareness and Training

The Atos Global Safety and Security guidelines and The Security Awareness and Training Policy document the standard Atos awareness and training requirements around information security. Where DEFRA specific security training is required, this will be provided by the Atos Client Security Manager.

6.3.1 Unattended user equipment

The Atos CSM will ensure that Atos staff (and any contractors/subcontractors) are aware of their responsibilities with regards not leaving any of their equipment unattended:

- DEFRA Atos Security Operating Procedures (SyOPs)
- Atos Global Information Security Policy
- DEFRA Organisation Security Policy.

6.3.2 Clear Desk Policy

The Atos CSM will ensure that Atos staff (and any contractors/subcontractors) are aware of their responsibilities with regards to keeping their work areas and screens clear:

- DEFRA Atos Security Operating Procedures (SyOPs)
- Atos Global Information Security Policy
- DEFRA Organisation Security Policy / Clear Desk and Clear Screen Policy.

6.4 Disciplinary Process

Atos Service Manager or Line Managers (as appropriate) will invoke the HR related processes regarding disciplinary proceedings as part of the DEFRA account. These may result in disciplinary action, up to and including termination of employment.

The Atos UK HR Disciplinary Policy and Procedure documents the details of the Atos disciplinary process.

Implementation of recommendations following the disciplinary process are expected to be implemented on the account within 1 working day of being issued.

6.5 Monitoring of Personnel

The Atos Operations Manager will follow appropriate management and HR process (the Atos Group HR Performance Management Guidelines to ensure all staff working on the DEFRA maintain the appropriate level of skills, as well as ensuring the working environment is in keeping with personal goals and development.

Although staff may expect privacy of email, and other related usage of IT equipment, where necessary, and following approved HR procedures, investigations may be carried out where required.

6.6 Termination of Employment

The Atos Operations Manager will follow standard HR procedures as part of staff termination. This will cover the removal of access, suspension of accounts, and any other DEFRA specific access that needs to be revoked. Terminations will be communicated to appropriate DEFRA and Atos personnel via the Atos CSM as needed.

The Atos Leavers Procedures documents the processes for when an Atos Employee (including Administrators) leaves the organisation. All delivery locations must follow the Atos Global Identify and Access Management Policy.

6.7 Security Access Cards/Building Passes

All Atos employees are issued with an identity card to enter corporate office locations. Only those Atos employees with a requirement to enter data centres are issued with security passes. All other Atos, DEFRA, or contractor employees require a change request to enter the computer room and are escorted at all times if they are not cleared to SC or above.

The Atos Global Access Control Policy details the processes for restricting and gaining physical access to Atos owned and managed locations.

6.8 Physical Access to areas containing DEFRA equipment.

All DEFRA equipment is physically located in the UK. Unattended access to DEFRA equipment is limited to those Atos employees with SC clearance and an operational or business requirement to enter to the sites/work areas used to provide services to DEFRA.

6.9 Responsibility/Accountability

For HR Security:

Responsibility	Atos CSM and Atos HR
Accountability	Atos Client Executive Partner

7. Physical and Environmental Security

Atos has a range of measures in place on different sites to enhance physical security of premises. The measures vary depending on the type of building, its location and the nature of the work undertaken there.

All Atos sites have building access control systems to protect against unauthorised entry and reception desks that are staffed, at a minimum, during business hours.

All the company's major sites are regularly inspected and reported on by specialist security advisors, who are employed by the company's Security Directorate for this purpose.

The security advisors all have lengthy experience in the management of security measures at high-security sites and are qualified ISO 27001 internal auditors.

As part of Atos' ISO 27001 Certification programme, all certified sites are regularly subject to internal and external audit.

Atos data centres maintain a high level of physical security. Access to data centres is strictly controlled and must follow change control and allows only authorised users into specific areas relating to their approved change.

The Atos Global security team will ensure, on behalf of the UK Security Directorate, the following site-specific items are performed:

- Information security awareness and training
- Site security procedures
- Information security risk assessments
- Information security incident reporting and handling
- Site security reviews
- Business continuity planning and testing
- Internal audits in support of the Atos ISO/IEC 27001 certification.

The Information Security Management Business manual details these and other responsibilities.

Further documentation is found in Baseline Physical and Environmental Security Standard, Physical Access Control, CCTV Policy, Management of Security Systems and Procedures. These documents detail the various physical security controls in place at Atos locations, along with standard site requirements such as access control processes, entry point protection, equipment logging and controls. These documents are available from the ISMS and Property and Facilities Management (PFM) portals.

Atos will prevent unauthorised physical access to Sites (to the extent that they are under Atos control).

7.1 Physical and environmental security control implementation

Atos employs various physical security controls at all its sites, in the form of either Radio-frequency Identification (RFID) or swipe access, additionally where appropriate Personnel Identity Number (PIN) entry systems (i.e. All Data Centres have RFID and PIN Systems).

All sites also implement the following physical security controls;

- Access control system implemented in all sites
- 24X7 monitoring by physical security
- CCTV surveillance system for monitoring/recording/playback
- Dedicated and isolated production area within production are provided to customer with additional access control system for sensitive projects
- Entry to visitors inside production area is prohibited unless approved
- Only authorised removable electronic devices are allowed after appropriate validation
- Unattended confidential printed documents are monitored
- Asset movements
  - Gate pass with limited authorised signatories
  - Storage media formatted / removed before release.

There must also be a sanctioned change request to gain entry to any Atos data centre.

The access rights of all employees, contractors and third-party users to Atos information processing facilities are removed upon termination of their employment, contract, or agreement, or adjusted upon change.

7.2 Physical Security Perimeter

Atos Facilities Management will take steps to ensure the site perimeters of its locations are controlled and monitored in a manner suitable to the building operations. This covers features such as CCTV implementations, 24/7 security guard monitoring and regular patrols and monitoring of all boundaries and entry points.

The Atos Global Physical Environmental Security Policy and the Baseline Physical Environmental Security detail the requirements for Atos owned and managed locations.

7.3 Physical Entry and Other Controls

Physical access controls are in place at Atos sites to restrict access to key areas based on an individual's requirements and clearance levels. This is controlled at Atos sites by keypads, proximity access tokens and mantraps (mantraps are limited mainly to Data Centres but are also deployed where needed for other secure sites).

The document Atos Baseline Physical and Environmental Security Standard documents the requirements for Atos owned and managed locations.

7.4 Working in Key Rooms/Areas

This is achieved by standard Atos procedures, requiring change approvals for access, as well as signing for token access and approval to enter the restricted area.

Atos Baseline Physical Environmental Security documents the requirements for Atos owned and managed locations.

7.5 Equipment Siting and Protection

The Atos Operations Manager will ensure that all equipment used to provide support within the Atos locations will be positioned and contained in a secure environment, in accordance with DEFRA requirements.

7.6 Intruder Detection Alarms

Atos Facilities Management will ensure Atos locations have a combination of 24/7 security guard patrols, CCTV, and intruder alarms.

The Atos Global Physical Environmental Security Policy and the Baseline Physical Environmental Security documents the requirements for Atos owned and managed locations.

7.7 Protection of Equipment against Theft

Atos maintains an inventory of all assets, the Atos Global Physical Environmental Security Policy and the Baseline Physical Environmental Security documents the requirements for Atos owned and managed locations.

7.8 Equipment Removal

Atos will ensure (through department managers and onsite guard force) processes are in place to ensure equipment is not removed from site without prior approval. Checks in this area will be carried out as part of regular site audits. Permission for equipment removal will be logged as part of a change process; any additional controls required by DEFRA will be co-ordinated by the Atos Client Security Manager.

The Baseline Physical Environmental Security documents the requirements for Atos owned and managed locations.

7.8.1 Secure disposal or re-use of equipment

Atos will ensure processes are in place that meet DEFRA policy to ensure equipment that is no longer required is disposed of securely, or if it is to be reused this too is done securely ensuring any previous data is wiped off. The following policies cover this requirement:

- Atos Media Disposal Requirements Specification
- Atos Asset Movement and Disposal Policy.

This area is also covered below in Management of Removable Media and Secure Re-use or Disposal of Media.

7.9 Hardware Access Controls

Atos will take steps to ensure all relevant hardware assets controlled and secured. Any instances identified as being different to this will be reported to the Atos Client Security Manager for remediation and investigation (this could be part of the Site Security Advisor audits).Tamper Detection

Atos (Site Security Advisors, Support Teams, and Facilities Management) will undertake regular Atos site audits. As part of these audits and patrols, any evidence or suspicion of tampering will be reported and actioned accordingly. The Atos Client Security Manager will also ensure awareness of tampering is covered as part of the information security awareness programmes.

Atos Site Security Advisor Audits document details the Atos audit scope and checks that take place;

- Atos Audit Report Template
- Atos Audit Corrective Action Plan Template.

7.10 Maintenance and Repair

All access to facilities and other restricted areas will require the change control process to be followed for access to be granted. The Atos Client Security Manager will form part of the change board and will ensure appropriate controls are in place for both Atos and 3rd Party Staff as required.

7.11 Power Security

Atos Facilities Management will take steps to implement appropriate redundant power supplies based on the function of the locations in scope. These solutions are based on industry best practice and customer requirements. These controls will be routinely inspected as part of site audits and tested as part of BCP testing.

7.12 Fire Security

Atos locations are all no smoking locations. Atos Facilities Management will also take steps to ensure environments operate in a structured, secure, and tidy manner to reduce possible fire risks, even though fire protection systems are in place. These will also be checked as part of site audits.

7.13 Water/Liquid Security

Atos Facilities Management will implement controls appropriate to the risk of water flooding and liquid related issues in the related Atos facilities and locations based on specific risk assessments. All equipment installed will be maintained and installed to the supplier's documented procedures.

7.14 Cabling and Related Item Security

Atos Facilities Management and network teams will ensure all Atos power and telecommunications cabling carry data and supporting IT services are protected from tampering and damage. Safety Alerts

Atos (via the Security Directorate and line managers) will operate a very security aware organisation, with all staff understanding the responsibility to question anything that appears different to the norm or suspicious. Instructions on the procedures for reporting incidents will be explained at induction along with the appropriate evacuation procedures.

7.15 Responsibility/Accountability

For Physical and Environmental Security:

Responsibility	Atos CSM
Accountability	Atos Client Executive Partner

8. Communications and Operations Management

The Atos Global Information Security Policy covers various aspects around change control procedures, segregation of duties and other key operational areas.

8.1 Operational Procedures and Responsibilities

8.1.1 Change Control Procedures

The Atos change management team will ensure all systems have documented operating procedures and all changes to systems are strictly controlled by documented change control procedures. These procedures will be documented and controlled by the Service Desk function.

8.1.2 Operating Procedures

Atos will ensure that its security operating procedures for the provision of the Services are signed by all Supplier and Sub-contractor personnel prior to those Supplier and Sub-contractor personnel being given access to the Supplier or Authority systems or data.

8.2 Segregation of Duties and Areas of Responsibility

Atos will create job descriptions to cover everyone’s job specification and responsibility. Steps will also be taken, where appropriate, to separate roles, tasks, and responsibilities to prevent individuals subverting company or customer critical processes. As a minimum the security audits must remain independent and segregated from the security function. Also, segregation can be applied by Key Users as and when required by them and when a segregation capability described above is required to be implemented within the Atos Solution, Atos shall provide independent assurance that Authority Data traffic is segregated.

8.2.1 Separation of Development, Test and Operational Environments

Atos will adhere to DEFRA specific policy and good security practices by ensuring different environments exist for different activities, such as, production and non-production whenever applicable.

8.3 System Planning and Acceptance

8.3.1 Capacity Planning

The Atos capacity planning team will ensure adequate facilities are in place to monitor and forecast capacity requirements. DEFRA will be made aware of issues relating to capacity requirements as part of the service provided by Atos:

- Atos ASMM Capacity Management Process documents the process.

8.3.2 System Acceptance

As the service provider, Atos will take steps to ensure rigorous acceptance testing is undertaken internally and with DEFRA to ensure the systems function as proposed. Testing will be co-ordinated for DEFRA, and all findings will be reported and communicated via the appropriate channels. All such testing will be in accordance with the requirements detailed within appropriate contractual schedules.

8.4 Protection against Malicious and Mobile Code

8.4.1 Prevention

The Atos Operations Manager will ensure that all equipment used to deliver the services are using authorised software; that controls are in place to prevent unauthorised changes and alterations by malicious code The Atos Client Security Manager will also be responsible to detail the risks and steps to be taken.

8.4.2 Detection

The Atos Operations Manager will ensure all systems relating to DEFRA will have approved and adequate controls in place to meet the requirements listed in DEFRA Antivirus and Malware policies. This will be verified by audits co-ordinated / conducted by the Atos Client Security Manager.

8.4.3 Recovery

The Service Desk will provide initial support to users who suspect infection of malicious code, and will provide steps to resolve the incident, and block access to malicious sites\domains.

8.5 IT Component Start-up and Close Down

The Atos Operations Manager will ensure that the hardware used to deliver service to DEFRA is built and operates based on agreed builds reviewed and signed off by the DEFRA Lead Architect and DEFRA Technical Director as part of service delivery. These will feature best practice processes, vendor configuration guidance, HMG / NCSC policy and where appropriate DEFRA specific requirements as part of the supported build.

8.6 Media (including Document) Security

8.6.1 Management of Removable Media

The Atos Operations Manager will ensure all staff working on the DEFRA account, are aware of the appropriate controls and methods that should be used, particularly around any media containing business critical information.

Further information can be found in the following Atos and NCSC documents:

- Atos Encryption Policy
- Atos Removable Media Disposal and Destruction of Sensitive Data
- Secure Sanitisation of Storage Media – Secure Sanitisation of Protectively Marked or Sensitive Information. https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

When Authority Data resides on a mobile Device (including removable storage media) it must be stored encrypted in accordance with the Government Security Classification Policy using a product or system component which has been formally assured through a certification process recognised by NCSC or equivalent.

This area is also covered in 7.8.3 Secure disposal or re-use of equipment.

8.6.2 Printed Output

The Atos Operations Manager will ensure all staff working on the DEFRA account, are aware of the appropriate controls and methods that should be used to ensure the printed output is handled and stored in accordance with its Data Classification. Destruction must take the form of, shredding, pulping or incineration, to prevent reconstruction in line with NCSC guidance.

8.6.3 Secure Re-use or Disposal of Media

The Atos Client Security Manager will ensure media and hardware will be securely disposed of or recycled for use in line with Atos and DEFRA policies, and HMG / NCSC policy when Re-Using and Disposing of Media.

Further information can be found in the following Atos and NCSC documents:

- Atos Encryption Policy
- Atos Removable Media Disposal and Destruction of Sensitive Data.

For clarification:

a. all information assets and business assets (including Devices, any form of storage device, media and hard copy) used to store Authority data, are securely sanitised in accordance with HMG IA Standard No.5.

b. sanitisation – whether destructive or non-destructive as required by HMG IA Standard 5 - is verified and audited by the Supplier.

c. sanitisation is performed using products that have been assured in accordance with the requirements of HMG IA Standard 5.

d. Authority Data is securely erased or protected against unauthorised access as agreed with the Authority when services in cloud-hosted or other shared environments are terminated.

8.7 Secure Sanitisation of Protectively Marked or Sensitive Information Exchange of Information

The Atos Client Security Manager will ensure staff are made aware of appropriate email usage and etiquette; these are communicated through awareness and documentation Atos Messaging Policy and Atos Email Etiquette Policy and any specific DEFRA requirements.

8.8 Monitoring

8.8.1 Accounting and Audit

Atos regularly carries out internal and external audits by various Certification bodies. Internal audits are the responsibility of the Security Site Advisor as documented in Atos Site Security Advisor Audits. In addition to these more physical audits, logical logs are recorded and monitored on all critical systems. The Atos Client Security Manager will review physical and logical logs and share testing and audit results with DEFRA where appropriate, to meet DEFRA requirements.

8.8.2 Clock Synchronisation

Atos will synchronise all computer clocks with a recognised central time source as standard to ensure log timing accuracy exists when reviewing logs and carrying out investigations.

The Atos Operations Manager will ensure a clock re-synchronisation and check takes place after every change to daylight saving hours, and from daylight saving hours to GMT.

8.9 Operator Logs

The Atos Operations Manager will ensure operator activities will be logged through a combination of change controls and tickets within the Service Desk for all DEFRA related activities.

8.10 Fault Logging

The Atos Operations Manager will ensure that all faults are recorded with the Service Desk.

8.11 Encryption

Inter site traffic must be encrypted in a manner compliant with DEFRA Policies for support office locations.

Removable media and assets that leave any DEFRA office location must be encrypted in a manner compliant with the Atos Encryption Policy and NCSC policy, except where the SIRO or delegate has given an exemption for business purposes.

Any Authority Data transmitted over any public or untrusted network (including the Internet, mobile networks, or un-protected enterprise network) or to a mobile device must be encrypted in accordance with the Government Security Classification Policy using a product or system component which has been formally assured through a certification process recognised by NCSC or equivalent.

8.12 Network Security Management

The Atos Operations Manager will ensure network security management which will include the security of network controls and network services as well as segregation between networks:

- Atos Communications and Operations Security Policy
- Atos Global Information Security Policy
- DEFRA Network - IT Network Security Policy.

Atos will:

- ensure that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Best Practice.
- When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) Atos will follow Best Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification for all bespoke or complex components of the Supplier Solution.
- follow NCSC guidance on architectural patterns e.g. for system administration capability.
- use independently assured products in the design and delivery of the solution through schemes such as NCSC Commercial Product Assurance or other schemes e.g. Common Criteria.
- enforce system to system authentication and encryption in transit when communications are transiting less trusted networks.

8.13 Responsibility/Accountability

For Communications and Operations Management:

Responsibility	Atos DEFRA Service Director
Accountability	Atos Client Executive Partner

9. Security Controls

Atos will deliver the following security services to meet DEFRA's security requirements as detailed in appropriate contractual schedules. The list below serves as an outline and an example and will be further elaborated and expanded during Transition period.

9.1 Vulnerability Management

Atos will receive vulnerability scanning results from on in-scope assets delivered through DEFRA Microsoft Defender from DEFRA SOC and perform associated and required remediation activities.

9.2 Data Loss Prevention

Atos will utilize DEFRA M365 Purview to provide O365 Data Loss Prevention services.

9.3 Responsibility/Accountability for Security Controls:

Responsibility	Atos Delivery Teams
Accountability	Atos Client Executive Partner

10. Access Control

10.1 User Account Management

10.1.1 User Account Requests and creation

All user account requests will be formally raised in the service desk system.

The Atos Account Service Manager/ Line Manager will be responsible for the requesting of Privileged accounts for Atos staff. This will ensure the least privilege access for the user, along with recording of access permissions granted.

Privileged accounts are only granted when approved by both Service Manager and CSM and are subject to audit by the CSM.

10.1.2 Review, Disabling and Deletion of User Accounts

The Atos Client Security Manager will ensure regular reviews are conducted on user account usage and requirements in accordance with the Assurance or Routine Compliancy Review policy, DEFRA Security Standards, and related documents.

Where Atos or Sub-Contractors grants increased IT privileges or access rights to Atos Personnel, those Supplier Personnel are granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges, or leave the organisation, their access rights shall be revoked within one (1) Working Day of the account being informed.

Likewise, where staff are removed from the account either through non-compliance to clearance requirements or due to disciplinary processes being enforced their access rights shall be revoked within one (1) working day of the account being informed.

Privileged access rights to the Supplier System will be reviewed on a quarterly basis.

10.2 Access Control Configuration

Access control shall be as per Atos ISMS Access Control Policy, all users are assigned unique usernames and provided the minimum access required to complete their role, no shared user accounts are permitted and access to information is provided on a “need to know” basis.

10.3 Password Management

10.3.1 Control and Implementation

Atos user account and password management will follow standard procedures for all accounts used:

Atos Password Policy

We also implement the advice given by https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

10.3.2 Password Generation

Atos (through support teams) will generate passwords in accordance with DEFRA Password Policy

10.3.3 Password Storage and Transmission

The Atos Operations Manager will distribute DEFRA related user account and password information. Privileged user information relating to DEFRA will be provided and stored in accordance with specific DEFRA Polices.

10.3.4 Changing Passwords

Atos (through support teams) will manage passwords in accordance with DEFRA Polices. The Atos Operations Manager has overall responsibility for ensuring this is accomplished.

10.3.5 Review of Passwords

The Atos Client Security Manager will take steps to enforce password change management. In the event a password has changed from the password guidelines; the forcing of password policy will be implemented.

10.3.6 Maintenance Passwords (Service Accounts)

The Atos Client Security Manager will ensure the disabling and enabling of maintenance passwords relating to DEFRA on an ‘as required’ basis. This will be controlled and monitored though standard change controls procedures.

10.3.7 Service Accounts Passwords

The Atos Client Security Manager will ensure the service accounts for machine-to-machine interaction will be regularly reviewed. This will be controlled and monitored though standard change controls procedures.

10.3.8 Privileged User/System Management Supervisory Passwords

The Atos Client Security Manager will ensure privileged accounts relating to systems and infrastructures are only held by Atos individuals assigned to support the services. These Privileged Users will always be identifiable and can be held responsible for their actions.

10.4 Network Access Control

The Atos Operations Manager has overall responsibility for ensuring network access control requirements in relation to DEFRA are maintained in accordance with HMG and NCSC Security Standards and related documents.

10.4.1 General

Atos will ensure that the all networking infrastructure is documented as per the requirements of the HMG and DEFRA standards. This documentation will cover justifications for any diagnostic points, along with methods for ensuring the infrastructure meets DEFRA requirements. These activities will be co-ordinated by the Atos Client Security Manager. Atos will operate an access control regime to ensure that Supplier Personnel do not use business-related authentication information for non-business purposes and will ensure that multi-factor authentication is required for all administrative access to Authority and Supplier systems.

10.4.2 External Connections

The Atos Client Security Manager will ensure all external connections under Atos supervision are configured and have the appropriate rule agreed with the DEFRA security stakeholders.

10.5 Information Security Conditions for Connection

The Atos Client Security Manager, will, where appropriate, ensure that the DEFRA Code of Connections document and agreements are completed and approved by DEFRA.

10.6 Remote Access

Only Atos staff may connect to the Atos Private Network, and this is ensured via two factor authentication methods; once connected, security will be established via an IPSEC VPN. The Atos Client Security Manager will ensure any remote support / access to the DEFRA environment will follow the security requirements detailed in DEFRA and NCSC security policy documents.

Any additional remote connectivity to DEFRA resources will be subject to DEFRA Security Assessor approval. All DEFRA laptops must have their hard disk encrypted with a NCSC approved full disk encryption product:

10.7 Operating System, Application and Information, Access Control

The Atos Operations Manager will ensure all equipment used as part of the DEFRA services will be based on a signed off build, with appropriate controls to protect information, applications systems, and functionality.

10.8 Mobile Computing and Teleworking

10.8.1 Laptop Security

The Atos Client Security Manager will ensure all DEFRA related Atos users are made aware of the various risks associated with using laptops outside of the office through information security awareness and training. The main areas of focus will cover what information shouldn’t be stored on the laptop, care of ownership whilst out of the office, risks of shoulder surfing, and other security risks of which users should be aware. All laptops must have their hard disk encrypted with an NCSC approved full disk encryption product:

Atos Laptop Code of Conduct documents the Atos standards on laptop due care.

Government Security Classifications April 2014
NCSC . Guidance on protecting-bulk-personal-data-main

- NCSC - 10 Steps: Home and Mobile Working
- NCSC - End User Devices Security Guidance: Windows 7
- ICO Guidance on Data Protection.

Where mobile working solutions are required in any part of the Supplier solution the Supplier shall:

a. ensure Supplier Personnel use multi-factor authentication for all administrative access or remote access to the Supplier System.

b. When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted in accordance with the Government HMG Security Classification Policy using a product or system component which has been formally assured through a certification process recognised by NCSC or equivalent.

10.9 Responsibility/Accountability

For Access Control:

Responsibility	Atos CSM
Accountability	Atos Client Executive Partner

11. Information Security Incident Management

The following documents are the Atos procedures for handling an Information Security related incident:

- Atos Security Incident Reporting
- Atos Major Incident Process (Security Directorate)
- Atos Serious Incident Procedure Checklist
- Atos Major Incident Response Procedure.

The procedures to be followed for DEFRA will be documented in the DEFRA Information System Security Standards

11.1 Information Security Incidents and Weaknesses

The Atos Client Security Manager will be the main point of contact and co-ordinator for all DEFRA related incidents. The Atos Client Security Manager will be responsible for communicating with the appropriate parties, leading the investigation from an Atos perspective and using appropriate Atos documentation to track and report the incident response. Service Desk is the repository for all security incidents. The DEFRA Security Working Group (SWG) is the forum for discussing security incidents.

11.2 IT/Networking Malfunctions

The Atos Client Security Manager will be the main point of contact and co-ordinator for all DEFRA related incidents. The Atos Client Security Manager will be responsible for communicating to appropriate parties, leading the investigation from an Atos perspective and using appropriate Atos documentation to track and report the incident response. Service Desk is the repository for all problem incidents. The DEFRA Security Working Group (SWG) is the forum for discussing problem incidents.

11.3 Learning from Information Security Incidents

The Atos Client Security Manager will review the actions and results of a security incident relating to DEFRA and identify lessons learned to reduce the possibility of recurrence. Lessons learned for other engagements will also be utilised to benefit DEFRA by identifying any security related weaknesses. These will be raised via the SWG.

11.4 Disciplinary Process in context of Information Security Incidents

The Atos Operations Manager, will as appropriate, invoke HR related processes regarding disciplinary proceedings as part of the DEFRA **FEUS** service. These may result in disciplinary action, up to and including termination of employment. This process will be facilitated by the line manager.

11.5 Responsibility/Accountability

For Information Security Incident Management:

Responsibility	Atos CSM
Accountability	Atos Client Executive Partner

12. Business Continuity Management

12.1 Business Continuity Planning

Specific Atos Site based business continuity plans are developed using the standard Security Directorate approved Template, Atos Site Business Continuity Plan.

- Atos Business Continuity Planning Checklist documents the BCP checklist for all sites regardless of location
- Atos Business Continuity Management.

12.2 Back-up Procedures

The Atos Operations Manager will take steps to ensure Atos DEFRA support staff suitably backup all critical systems, and transport and store the media securely. This process is verified as part of routine audits and backup verification testing. Any specific DEFRA backup requirements will be followed as documented in the DEFRA services contract and associated work instructions.

12.3 Escrow

The Atos Escrow Deposit procedure guarantees the availability of Authority data in the event of Atos ceasing to trade.

12.4 Emergencies and Breakdowns

12.4.1 Hardware Failures

In the event of hardware failure, the Atos Operations Manager will follow the appropriate steps to resume service in line with predefined SLAs. The steps taken will be recorded in the appropriate logs, and support staff will be notified as required.

12.4.2 Software Failures

In the event of software failure, the Atos Operations Manager will follow the appropriate steps to resume service in line with predefined SLAs. The steps taken will be recorded in the appropriate logs, and support staff will be notified as required.

12.4.3 Fire/Building Evacuation

As part of the induction process, Atos staff will be given instructions and briefings regarding fire and building evacuation. Staff working on the DEFRA Service will comply with Atos evacuation procedures as appropriate. The Atos Operations Manager will ensure appropriate inductions are initiated.

12.5 Responsibility/Accountability

For Business Continuity Management:

Responsibility	Atos Service Delivery Director
Accountability	Atos Client Executive Partner

13. Compliance

13.1 Compliance with Legal Requirements

The Atos Client Security Manager will ensure appropriate compliance with legal, regulatory, and contractual requirements are met as described in the DEFRA Service contract documents. This will include making appropriate information available for DEFRA information security compliance reviews.

13.2 Compliance with Information Security Policies and Standards, and Technical Compliance

Atos ensures compliance with various regulations through its use of internal and external audits against published policy. Where appropriate, the Atos Client Security Manager will assist DEFRA to meet compliance requirements documented in the DEFRA Security Standards where responsibility lies with Atos.

13.3 Protection of System Audit Tools

The Atos Client Security Manager will ensure system audit related tools are not installed and operational on a permanent basis in the DEFRA Service environment. Access and usage are controlled and approved through appropriate change control procedures.

13.4 Document Configuration Feedback

The Atos Client Security Manager will be responsible for informing the DEFRA Service teams in relation to any changes, and/or recommendations to this document and those documents referenced from this document.

13.5 Document Configuration Changes

The Atos Client Security Manager will ensure any appropriate changes to this document and those documents referenced from this document are understood and communicated to the DEFRA Service staff.

13.6 Responsibility/Accountability

For Compliance:

Responsibility	Atos CSM
Accountability	Atos Client Executive Partner

14. Appendix 1 – Key Sub-Contractors

A list of key sub-contractor will be managed by the account and management on compliance requirements will be enforced through contractual terms. Sub-contractors can be served notice to complete audit activities to validate compliance terms upon request through the contract term.

FEUSPP Order Form
Attachment 5 (Key Su

15. Appendix 2 - Risk Management Approach

The corporate Risk & Issue Management (RIM) process will be adopted with operational risks and issues, and their associated assumptions and dependencies, managed in line with corporate Risk Policy.

Risk Management processes are defined to:

Identify risks by their source from a contractual or operational perspective

Assess risks to quantify probability of occurrence

Mitigate risks through appropriate treatment

Monitor risks through the lifecycle of the service

Risk management is built into the business services delivered and resultant findings are included into the account risk management process and resultant risk register.

Risk identification forms an integral part of security services, from Impact Assessment processes completed for the implementation of new incremental services, change notice review, incident and problem ticket resolution, vulnerability management, service reporting.