Department
for Environment
Food & Rural Affairs

Defra group Security:
Security Policy

Owner	Defra Senior Security Advisor (SSA)
Document Author	Defra Security Team
Document Approval	Defra Senior Security Advisor (SSA)
Version / Date	PLIS002 v7.0
Next Review Date	February 2020

Department
for Environment
Food & Rural Affairs

1 Table of Contents

Department
for Environment
Food & Rural Affairs

2 Change control

Date	Author	Version	Change reference
23/3/2011	Alec Anderson	V2.0	Content and Format updated in line with new Defra Group & policies. Replaces the following policies: PLIS001 Information Security and Assurance, PLRM005 Removable Media, PLPS001 Personnel Security, PLTA001 Training and Awareness, PLDR001 Disposal and Re-use, PLLD00A IT Lockdown, PLBR002 Business Continuity and Disaster Recovery.
19/4/13	Suzie Price	V2.1	Issued for peer review
26/6/13	Suzie Price	Draft V2.2	Updated Version
03/09/2013	Andrew Miles	V3.0	Final version.
20/01/2014	Andrew Miles	V3.1	Updated in line with new GSC coming in April.
02/05/2014	Andrew Miles	V3.2	Comments collated and policies updated.
13/06/2014	Andrew Miles	V3.3	Further comments used to update policy.
07/07/2014	Andrew Miles	V4.0	Final version.
08/03/2016	Suzie Price/ Andrew Miles	V5.0	Final version.
04/08/2016	RPA Design Publications	V6.0	Formatting changes, no change to content.
23/02/2018	Michelle Wheeler	V7.0	Final version
2/03/2019	Michelle Wheeler	V8.0	

Table 1 – Document change control record

2.1 Document Control Statement

The following outlines the access, handling, communication and disposal guidelines that apply to this document.

2.1.1 Access Guidelines

There are no restrictions on internal Defra Group employee access to this document, or to contractors/consultants, third parties and any other agency or body with access to Defra Group assets or data handling facilities.

2.1.2 Handling and Disposal Guidelines

To be handled and disposed of in accordance with the Government Security Classification procedures for OFFICIAL information.

2.1.3 Communications Guidelines

All Defra Group security policies must be communicated within the organisations and be available to interested parties, as appropriate. Care should be taken not to disclose sensitive information and must be produced in protected PDF format.

3 Definitions

- "Defra Group" includes the core Department and the following Delivery Partners;
  - Animal Plant and Health Agency
  - Centre for Environment Fisheries and Aquaculture Science
  - Environment Agency
  - Kew Royal Botanical Gardens
  - Marine Management Organisation
  - Natural England
  - Rural Payments Agency
  - Veterinary Medicines Directorate
- "Defra Senior Security Advisor" refers to the Senior Security Officer, who is responsible for overall Defra-wide, day to day security.

4 Overview

4.1 Defra Group has a number of business assets, including buildings, physical items, ICT services and systems, information and personnel, all of which have a high value to the Department and therefore need to be suitably protected.

4.2 This policy has been developed to ensure an adequate level of protection for these business assets from a wide range of threats and events which may jeopardise Defra Group activities. Defra Group employs a risk management approach to the implementation of physical, procedural, technical and personnel security controls across the Department. This ensures that all risks pertinent to Defra Group's business assets are identified, prioritised and managed in an effective and consistent manner, thereby maintaining their confidentiality, integrity and availability, as appropriate.

5 Purpose

5.1 This document forms the Security Policy for Defra Group and is a statement of the Department's commitment to establish and maintain the security and confidentiality of information, information systems, applications, network and physical assets and buildings owned or held by Defra Group by:

5.1.1 Achieving a secure and confidential working environment;

5.1.2 Ensuring the availability of systems and information to authorised individuals;

5.1.3 Ensuring compliance with legal, regulatory and contractual requirements;

5.1.4 creating and maintaining within Defra Group a level of awareness of the need for Information, Physical and Personnel Security as an integral part of the day to day business, by ensuring that Defra Group employees are aware of and fully comply with applicable legislation as described in this and the relevant security policies maintained by the Defra Group;

5.1.5 Maintaining the reputation and operation of Defra Group in the eyes of the Department's customers, end-users and stakeholders;

5.1.6 ensuring there is a consistent level of security for Defra Group information assets to ensure the confidentiality, integrity and availability is maintained, whilst minimizing the risk of compromise from unauthorised disclosure and access, thereby ensuring data quality is preserved;

5.1.7 Ensuring breaches of information security and suspected weaknesses are reported and investigated;

5.1.8 Ensuring Business Continuity and Disaster Recovery plans are established, maintained and tested.

This policy applies to all information held in both physical and electronic form.

5.2 Legal requirements

Some aspects of information security are governed by legislation, the most notable UK acts are;

- The General Data Protection Act (2018)
- Computer Misuse Act (1990)
- Regulation of Investigatory Power Act (2000)
- Freedom of Information Act (2000)

6 Scope

6.1 The scope of this policy applies to:

6.1.3 All Defra Group staff, contractors, temporary staff and external third party suppliers who require logical or physical access to Defra Group information systems or premises;

6.1.4 To all colleagues, contractors/consultants, contractual third parties and any other agency or body with access to Defra Group information, information assets, IT equipment or data handling facilities.

7 Applicability

7.1 This Defra Group Security Policy applies to:

7.1.1 All Defra Group employees, including Civil Servants, Defra Group system users, casuals, consultants and contractors and visitors who have access to Defra Group business assets, who are responsible for reading and implementing the measures described within this policy and affording the appropriate level of protection to Defra Group's business assets;

7.1.2 All systems, products, services and processes owned or commissioned by Defra Group or acquired from an external supplier, including Cloud Based Infrastructure managed by Defra Group employees, security issues must be considered throughout their life-cycle, from inception through to de-commissioning;

7.1.3 All Defra Group locations from which Defra Group systems are accessed (including home use or other remote use). Where there are links to enable non-Defra Groups (to have access to Defra Group information) Defra Group must confirm the security policies they operate to meet the Defra Group security requirements set out in this policy and the risks are understood and mitigated.

8 Policy Statements

Physical and Environmental Security

Physical and Environmental security measures must be implemented to prevent unauthorised physical access, damage and interference to the Defra Group buildings.

8.1 It is the policy of Defra Group to ensure that:

8.1.1 Physical and Environmental controls are enforced at all locations where Defra Group information, physical or personnel assets or systems maintain a presence, in order to prevent the unauthorised access, modification, loss or destruction of business assets;

8.1.2 A layered approach to physical security is taken, combined with an approach to ensure that all measures are commensurate with the asset(s) being protected;

8.1.3 The physical measures enforced will prevent, deter, delay and/or detect, attempted or actual unauthorised access, acts of damage and/or violence being conducted towards Defra Group business assets;

8.1.4 Access to Defra Group premises, information data and information systems will be limited to authorised personnel only. Authorisation will be demonstrated through the use of authorisation credentials by common access control pass / security pass that have been issued by Defra Group. Passes must be visibly displayed at all times, whilst on Defra Group premises to demonstrate authorisation, and removed when leaving Defra Group premises;

8.1.5 In the event that visitors need access to the Defra Group premises, information data or information systems, those visitors must have prior authorisation, must be positively identified, and must have their authorisation verified before physical access is granted. Once access has been granted, visitors must be escorted and their activities monitored at all times*;*

8.1.6 Physical assets must be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access;

8.1.7 Equipment used to handle, store, transmit and process Defra Group data must be correctly maintained and protected from power failures and other disruption caused by failures in supporting utilities, to ensure its continued availability;

8.1.8 Physical access control measures are implemented and tested to ensure they are fit for purpose and offer the required protection;

8.1.9 Critical, sensitive or security classified business assets will be located in a secure area within a defined security perimeter protected by appropriate level of physical controls, determined by associated risks;

8.1.10 all networked file servers/central network equipment will be located in secure areas with restricted access, confined to designated employees whose job function requires access to that particular area/equipment.

Asset and Software Registers

8.2 Equipment Inventory

7.2.1 Defra Group assets associated with information and information processing facilities must be identified and an inventory of these assets must be maintained.

8.3 ICT Security

It is the policy of Defra Group to ensure that:

8.3.1 All Defra Group systems are subject to a risk assessment, and must be performed when the system processes or holds personal data, the risk management approach will be appropriate and decided by Defra Group Security.

All Defra Group systems and infrastructure will be considered for scope within IT Security Health Checks at least annually, or as required on any major system change, to ensure that the technical implementation of the system is secure and compliant with Defra Group policies;

8.3.2 The technical measures applied to Defra Group systems are to be consistent with the requirements outlined in each system risk assessment. As a minimum, the following measures will be applied:

8.3.2.1 All Defra Group systems will employ identification and authentication controls to enable the management of user accounts, manage the need-to-know requirement and manage the risk of unauthorised access;

8.3.2.2 All Defra Group ICT equipment, including laptops, desktop PCs, servers, Mobile Devices and Defra Group hardware (e.g. Defra Group appliances, firewalls, routers, hubs and switches) that processes Defra Group information and systems will be locked down in accordance with accepted best practice to restrict services and ensure the need-to-know requirement is implemented. The term “locked down” refers to the secure configuration of the device/system in order to minimise risks from misuse, which may compromise the integrity, confidentiality and availability of the information being processed by or stored on the device;

8.3.2.3 Measures must be in place to ensure that the latest vulnerabilities and threats that have the potential to affect Defra Group systems and its infrastructure can be identified, assessed and acted upon accordingly;

8.3.2.4 All Defra Group systems will be appropriately patched and kept up to date to fix known issues or security weaknesses throughout the lifetime of the product to reduce the risk from known vulnerabilities;

8.3.2.5 Defra Group systems and all associated infrastructure will have a protective monitoring policy applied that is in line with HMG policy, and as a minimum, ensures that any breach of the confidentiality, integrity and availability of that system and its information assets can be reliably and quickly detected and that the integrity of the audit trail is ensured;

8.3.2.6 There will be effective configuration management through a formal change control and asset management process, where all changes to ICT systems/applications will be subjected to a security impact assessment;

8.3.2.7 Measures must be in place to protect Defra Group's business assets from modification, damage or loss due to malicious software, including viruses, spyware and phishing;

8.3.2.8 Measures must be in place to ensure that Defra Group communications facilities (including the use of Email, Internet and Intranet) are used in an efficient, effective, ethical and lawful manner and in accordance to the PSN CoCo requirements.

8.3.3 All Defra Group systems will employ boundary security devices, where appropriate, to ensure protection from untrusted Organisations.

8.3.4 The use of removable media is not permitted except when the conditions below are met:

- Seek permission where necessary from the relevant IAO, especially if it concerns personal data, sensitive information;
- minimise their use;
- only use them where there is a good business reason;
- always use the most appropriate and secure type of removable media;
- Apply encryption for sensitive information or personal data if it must be saved to removable media.

8.3.5 Where a removable device/medium is used, it must be owned or issued on behalf of the Department and only used for Departmental business purposes. Media containing information must be protected against unauthorised access, misuse or corruption where possible.

8.3.6 Use of personally owned devices/media to hold or carry Defra Group information or connect to Defra Group systems is not permitted under any circumstances.

8.3.7 Defra Group-approved removable media devices should not be connected to non-Defra Group systems or personally owned devices unless explicit prior authorisation has been given. This includes Defra provided BlackBerrys and smartphones.

8.3.8 Where removable media is received from outside the Department the recipient must be expecting it, must have adequate assurances that it has been scanned for malicious content, and it must be for business, not personal use.

8.3.9 Users must not use Defra Group provided/approved devices to download data or information that contravenes the Acceptable Use Policy.

8.3.10 Users are formally made aware that it is a breach of security to download files which disable the network or which have the purpose of compromising the integrity and security of Defra Group file servers or to intentionally introduce files which cause system disruption could be prosecutable under the Misuse of Computer Act 1990.

8.3.11 Defra Group systems must have a formal registration and de-registration process in place to control access. Periodic review of user access rights must be undertaken, including those with privileged access rights.

Defra Group employees, contractors and temporary staff working for the Department and its delivery partners must only access systems for which they are authorized.

Information Assurance

8.4 It is the policy of Defra Group to ensure that:

8.4.1 There is a consistent level of security for all Defra Group information assets, thereby minimising the risk of compromising their confidentiality, integrity and availability. In particular:

8.4.1.2 The confidentiality of information and other business assets is maintained, by protecting Defra Group's information assets from unauthorised disclosure and unauthorised access;

8.4.1.3 The integrity of information and data quality is preserved, by ensuring that it is accurate, up to date and complete;

8.4.1.4 The availability of information assets, systems and services to authorised users is maintained.

8.4.2 All employees, contractors and temporary staff working for the Department and its delivery partners must be made aware of their duty to safeguard the Confidentiality, Integrity and Availability of the information that they store, handle or process.

8.4.3 All security related risks to Defra Group information assets will be managed in accordance with Defra Group's Information Risk Policy.

8.4.4 A whole-life, systematic and layered approach of technical, procedural, personnel and physical security measures is implemented to ensure the protection of end-user information (in particular personal and sensitive personal information as defined by the UK Data Protection Act 2018) and Defra Group information assets from unauthorised access or disclosure. All Defra Group business assets must be protected in line with the Government Security Classifications scheme.

8.4.5 All media devices holding personal data and/or sensitive material must be encrypted.

8.4.6 All information assets and business assets used to store personal data and/or sensitive material, must be securely disposed of in accordance with HMG IA Standard No.5 when no longer required.

8.4.7 All information assets and business assets used to store personal and/or sensitive data must not be left unattended and will be appropriately secured when not in use in line with the Defra Group Clear Desk and Clear Screen Policy.

8.4.8 Access to information assets that are subject to the 'need-to-know' principle will be restricted to authorised personnel who have the need to know that information to fulfil their role.

8.4.9 Incident Management procedures must be established to ensure that all breaches or suspected breaches of ICT, Information Security, physical assets and information loss are reported (if necessary, anonymously), recorded, investigated and mitigated quickly and effectively. Incident Management procedures must outline reporting requirements in the event the incident impacts Data Protection Act, PSN etc. A cultural change programme must be undertaken to raise awareness amongst all Defra Group, contractors and third party staff of the relevant security policies and procedures adopted by Defra Group.

8.4.10 Information security education and training must take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

8.4.11 A data retention policy is established and enforced (with exception to RPA) to ensure compliance to statute and the UK Data Protection Act 2018.

8.4.12 All contractual, regulatory and legislative requirements are met, to ensure that Defra Group and its Delivery Partners retain their organisational status, as appropriate e.g. Paying Agency accreditation status.

8.4.13 All risks associated with the sharing of Defra Group information assets are reviewed, managed and authorised by the relevant Information Asset Owner, thereby ensuring that information is only used within the law for public good.

Business Continuity

8.5 It is the policy of Defra Group to ensure that:

8.5.1 Business Continuity plans (BCP) and Disaster Recovery (DR) plans are produced, maintained and exercised for Defra Group's business assets, to minimise damage and ensure that Defra Group's business operation can be effectively recovered/restored in the event of a major failure or disaster;

8.5.2 Employees are aware of the existence of the plans and their specific responsibilities in the event of a disaster and BCP or DR plans being invoked;

8.5.3 BCP and DR plans are formally reviewed as required and as a minimum on an annual basis, by the relevant business area to ensure they are up-to-date and fit for purpose.

The complete Business Continuity Policy can be located here.

Personnel Security

8.6 It is the policy of Defra Group to ensure that:

8.6.1 Personnel controls are applied to all Defra Group employees, contractors and visitors;

8.6.2 The identities of all employees, contractors and temporary staff working for the Department are assured, in terms of their trustworthiness, integrity and reliability;

8.6.3 The level of clearance required for each employee and/or contractor with access to Defra Group business assets is determined on a case by case basis according to the role being fulfilled. As a minimum, all personnel must be subject to the Baseline Personnel Security Standard (BPSS) before the commencement of employment. Full implementation of BPSS, including a 100% application of 'unspent' criminal record check, is explicitly mandated as part of the security policy framework;

8.6.4 Defra Group/Delivery Partners shall ensure all new employees are made aware of their security responsibilities as part of their induction;

8.6.5 Defra Group/Delivery Partners shall ensure that staff are made aware of their responsibility to report any behaviours of security concern relating to colleagues or visitors.

Third Party Service Providers

8.7 It is the policy of Defra Group to ensure that:

8.7.1 All Service Providers are responsible for complying with Defra Group's Security Policy, and all associated security policies and procedures.

8.7.2 All Service Providers are responsible for ensuring that all Service Provider employees or contractors, who require access to Defra Group's business assets, are subject to the Baseline Personnel Security Standard as a minimum, before access is granted.

8.7.3 No access will be granted to any of Defra Group networks without formal authority.

8.7.4 Documentary evidence is obtained from all Service Providers on a yearly basis, to demonstrate compliance with established and agreed Defra Group's policies and procedures.

8.7.5 Defra Group will regularly monitor, review and audit Service Providers to gain assurance of compliancy to regulatory and legal requirements, including adherence to Defra Group policies and procedures.

9 Compliance, Governance and Monitoring

9.1 Compliance will be governed by the following Policy and standards:

9.1.1 HMG Security Policy Framework

9.1.2 ISO/IEC 27001:2013

9.2 In order to ensure compliance with these policies, Defra Group reserves the right to:

9.2.1 Monitor the use of Defra Group systems, respond to concerns regarding alleged or actual violations of this policy; and, if necessary, take appropriate action;

9.2.2 Monitor and record access to Defra Group sites and premises using monitoring and access control systems;

9.2.3 Monitor Defra Group's electronic communication systems and to enforce policies relating to the use of electronic information and those communication systems;

9.2.4 Access an individual's account, with the exception of the designated locations used to store personal information, via the electronic systems, including when that individual is not available;

9.2.5 Conduct compliance visits and audits against Defra Group policies and procedures to ensure they are being conformed too;

9.2.6 Consideration of ITHC when new systems are developed, upgraded or when significant changes occur;

9.2.7 Co-operate fully with any police enquiry or other lawful enquiry into alleged illegality arising as a result of prohibited use, recognising that this may assist in the criminal prosecution of any Defra Group employee(s) involved.

9.3 Non-compliance with this policy or other Defra Group security policies, unless by prior arrangement with Defra Group SSA, will be reported to the relevant delivery partners Security Risk Owner. Where the minimum requirements of the Security Policy Framework are not met in full, or are adapted, Defra Group will inform the Cabinet Office in writing.

9.4 All employees are responsible for information security and therefore must understand and comply with this policy and the supporting policies available. It is the duty of each employee who uses or has access to information to be aware of, and abide by, the policies and arrangements concerning the secure use and protection of Defra Group Assets.

It is the responsibility of each Line Manager to ensure that all employees who they are responsible for are trained and supported in information security requirements. It is the responsibility of DEFRA Group to provide employees with the necessary guidance, awareness and, where appropriate, training in relation to all applications, systems and Organisations they have access to; and employees will adhere to and abide by the rules controlling applications, systems and Organisations.

All personnel or suppliers providing a service for Defra and the Defra Group have a duty to:

- Safeguard hardware, software and information in their care;

- Prevent the introduction of malicious software on the Defra Group's information systems;
- Report any suspected or actual breaches in security.

All managers are directly responsible for implementing the policy and ensuring employees compliance within their respective departments.

Failure to observe or comply with the standards set out in this policy may be regarded as gross misconduct and any breach may render an employee liable to disciplinary action under the Defra Group or Local Delivery Partners disciplinary procedures, which may result in dismissal.

Third party contractors/consultants and any other agency or body accessing Defra Group assets or data handling facilities must have disciplinary procedures in place to cover breaches to the Defra Group's Security Policies by their employees.

10 Exceptions

Compliance to the principles within this policy is mandatory for all staff, contractors and third party suppliers and they are set to protect both the information assets we have and the systems that hold them. Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or increase costs. These will need to be risk assessed on a case by case basis. Where there are justifiable reasons why a particular Policy requirement cannot be implemented, a policy exception may be requested to the local security representative. Exceptions may be granted to an individual, a team/group or a service area or Directorate and may be for a temporary period or on a permanent basis, but subject to review.

11 Supporting Documentation

All other Defra Group Security Policies support this overarching document.

- Security Policy Framework.
- Government Security Classification scheme
- ISO/IEC27001:2013
- CESG Good Practice Guides (GPG)
- HMG Information Assurance documentation