Chapter 8: Information Security

Contents

Introduction ................................................................. 1
Data Protection .............................................................. 2
Right of Access Requests .................................................. 3
DWP Contract ...................................................................... 3
Minimum Security Requirements ........................................ 5
Staff Vetting ......................................................................... 5
Confidentiality ...................................................................... 5
Training and Awareness ..................................................... 5
Access Controls ............................................................... 6
Security Incident Management ........................................... 6
Security Incident Reporting ................................................ 6
Changes to Provider Security Plans (including Offshoring) .... 6
Communications Management ............................................ 7
Use of Social Media ......................................................... 7
Sharing Information .......................................................... 7
Email Security ...................................................................... 8
Claimant CV and Name Unencrypted Email Exemptions .... 8
Supply Chain and Third Party Unencrypted Email Exemptions 9
Claimant Data Not Permitted via Unencrypted Email .......... 11
Unencrypted Emailing of Data to DWP .............................. 11
Sending Clerical Information ............................................. 12
Retention, Storage, Archiving and Destruction .................... 12
Document Retention ........................................................ 12
Portable Media .................................................................... 12
Premises .............................................................................. 13
Annex 1: Security Incident Report Form ............................. 14
Annex 2: Security Plan Change Request Form ..................... 15
Annex 3: When to Seek DWP Approval for use of Third Party Electronic Services ........................................ 16

Introduction

1. Notwithstanding information and agreed measures included in your contract and the Contract Security Plan/Risk Management Information Asset Assessment (RMIAA), the following is provided as generic guidance for all providers delivering national employment programmes on behalf of Department for Work and Pensions (DWP). This guidance should be read in conjunction with the relevant provision specific guidance and your contract which may permit further exceptions.

2. DWP requires all prime providers and their subcontractors and service delivery partners to operate appropriate technical and organisational measures; including secure systems and processes for handling and storing claimant or participant information in line with your contract, DWP
Standards and the Data Protection Act and General Data Protection Regulation (GDPR). The risk of loss of public confidence through failure to protect sensitive or personal information remains a key risk for DWP and its supply chain.

3. Our business is about people and we regard their personal data as a valuable and sensitive asset which has been entrusted to us. We take data protection extremely seriously, and we require you (and your subcontractors and service delivery partners) to apply the high standards that we ourselves apply.

4. Equally important is that you ensure all your staff and personnel throughout the supply chain (including subcontractors and service delivery partners) consistently understand the need for security compliance.

5. This section provides information on data security and details your responsibilities with regards to:
   - The secure collection, transfer; storage and disposal of information;
   - The reporting of security incidents; and
   - The request to change any aspect of your security plan agreed with DWP.

6. As a prime provider to DWP, you will have access to claimant and for some programmes, non-claimant’s personal data and DWP information. You will therefore need to comply with the Data Protection Act, GDPR and the minimum security standards that you are required to meet and continue to meet. Further information on what is required of you in respect of Data Protection, GDPR, Data Security and Freedom of Information is contained in the Terms and Conditions of your contract and the DWP Security Standards.

Data Protection

7. You must ensure that personal data is processed in accordance with the Data Protection Act and other relevant legislation. Appropriate technical and organisational measures must be implemented to protect personal data against accidental loss, destruction, damage, alteration and theft. In most contracts you are acting as data processors for DWP, and DWP remains the data controller. You are only permitted to process personal data for which DWP is the data controller as specified by, and for the purposes of, the contract. Use of this personal data for any other purpose must be approved by DWP. Individual contracts will specify whether you are acting other than solely as DWP’s data processor.

8. If a claimant or participant asks you for a copy of their personal data for which DWP is the data controller through a Right of Access request you should forward this to the DWP Right of Access Gateway Team immediately for a decision on releasing the data. Please refer to para 11.
9. DWP is the Data Controller in regard to the personal data processed under contract for DWP’s purposes. If you are a processor, the General Data Protection Regulation places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. You and your subcontractors or service delivery partners must not report incidents to the Information Commissioner, that is our responsibility and we will decide each case on its individual circumstances. All incidents must be reported to DWP as soon as discovered. Please see Security Incident Reporting.

Right of Access Requests

10. Right of Access requests replace what was previously known as Subject Access Requests following the introduction of General Data Protection Regulation 25 May 2018.

11. Where possible claimants should be directed to the Right of Access online form which is submitted directly to DWP.

12. If you receive a Right of Access request from a claimant or participant solicitor or third party you must forward immediately to the Right of Access Gateway Team at rightofaccess.requests@dwp.gov.uk. The Gateway Team has 30 days in which to respond to the Right of Access request and communicate this to you.

DWP Contract

13. The terms and conditions of your contract detail DWP’s security requirements, for example:

- The name and contact details of the individual who will act as the first point of contact with DWP for security issues,
- Security of Premises – maintaining the security of premises used for the delivery of the service and security for storage of information including archived information,
- Security Requirements and your Security Plan/Risk Management Information Asset Assessment (RMIAA),
- These documents set out the security measures that you will implement and maintain in relation to all aspects of the services and all processes associated with the delivery of services. All members of staff must be aware of and act in accordance with the content of your Security Plan/RMIAA,
- Audit and testing of the Security Plan/RMIAA,
- Malicious software – requirement to use the latest versions of anti-virus and software from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of malicious software, and

14. You must inform DWP when you are considering any changes to processes which may affect the handling of DWP/Authority Data. DWP/Authority Data is defined as:

a) “the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:

   i) supplied to the Contractor by or on behalf of the Authority; or

   ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or

b) any Personal Data for which the Authority is the Data Controller”.

15. You must inform DWP of security incidents and breaches immediately. A security incident or breach is defined as:

   Any circumstance that has arisen contrary to policy and that has the potential to compromise DWP assets. Assets include people, property or information. The circumstance may include actions that were actual or suspected; accidental, deliberate or attempted. “Compromise” is to bring the asset into disrepute or danger. Security Breach is the confirmed compromise of DWP assets without permission or authority.

Examples of security incidents and breaches: (NB – this is not an exhaustive list)

- Loss or theft of IT assets that permit access to DWP data (for example: Laptop, Tablet, PC, mobiles and so on),
- Unauthorised access to systems and services used to deliver DWP contracted provision,
- Loss or theft of DWP data,
- Unauthorised disclosure of DWP/Claimant data,
- Unauthorised access or deliberate amendment to systems and services/records (such as browsing records) used to deliver DWP contracted provision,
- Intruder or break-in at premises used to deliver DWP contracted provision,
- Cyber-attack – malware, virus, phishing.

Any queries regarding potential incidents please contact wpd.security@dwp.gov.uk

Please note instances of a single letter wrongly posted to another claimant or participant containing the name and address of a different claimant or participant only is not a reportable incident.
Should there be further identifiable claimant data in the letter such as NINO, data of birth, bank details or other sensitive personal information then this is a reportable incident.

Minimum Security Requirements

16. The following covers key areas of information security that you must adhere to:

**Personnel Security** – Before allowing staff and your subcontractor or service delivery staff access to DWP data, the measures detailed below must be in place:

**Staff Vetting**

17. Baseline Personnel Security Standard (BPSS) – covering pre-employment checks:

- Identity,
- Employment history (minimum of 3 years),
- Nationality/immigration status and
- Criminal records.

18. Please note that it is a legal requirement for enhanced Disclosure and Barring Service (DBS) checks to be completed for all of your staff and any subcontractor/service delivery staff dealing with vulnerable people.

19. As part of this process, the contractor’s declaration must be completed and returned to DWP on an annual basis; see the BPSS guidance.

**Confidentiality**

20. You will have signed a confidentiality agreement as part of your contract with DWP.

21. In addition, as part of the contract, you may be required to obtain individual confidentiality statements from staff that have access to DWP data.

**Training and Awareness**

22. Personnel within your organisation and supply chain must understand their obligations when handling DWP data and be aware of their legal and contractual responsibilities including at the start and termination of employment including the Computer Misuse Act and Data Protection Act and GDPR.

23. You must ensure all staff, including subcontractor and service delivery partner staff handling DWP data receive information security training on induction to the company and regular refresher training must be in place.
Access Controls

24. DWP requires that User Access Controls and Procedures are in place to monitor access to DWP data ensuring access is granted to and removed as job responsibilities demand.

25. Where relevant to your contract, access to the PRaP system by anyone other than your authorised staff is prohibited. You will ensure that your staff will not allow any unauthorised person who has not been granted access to PRaP by DWP, to gain access to PRaP.

Security Incident Management

26. You must ensure that all necessary systems and processes are in place for reporting incidents against the handling and storing of DWP data including your subcontractors and service delivery partners. All incidents must be reported to DWP as soon as discovered. Please see Security Incident Reporting.

27. You must have incident handling processes in place to identify and resolve any security weaknesses.

28. You must have procedures in place to identify software and system faults and failures including the identification of malicious software.

Security Incident Reporting

29. Provider security incidents should be reported immediately using the reporting stencil at Annex 1 and emailed to wpd.security@dwp.gov.uk where this will be acknowledged and a reference number allocated. Additional remedial actions may be specified by DWP to resolve the incident. Please contact the inbox should you wish to utilise a more secure transmission method.

30. When reporting an incident DWP claimant or participant data must not be contained within the report.

Changes to Provider Security Plans (including Offshoring)

31. You should complete the template at Annex 2 along with a Risk Management Information Asset Assessment document (RMIAA) when requesting any change, modification or refinement to any aspect of your security plan and IT system. Please contact the WPD Security inbox to request the latest RMIAA. You may also find Annex 3 useful if seeking use of third party electronic services.

32. Completed change request documents should be sent to wpd.security@dwp.gov.uk. You should supply as much information about the proposed change as possible including the name and contact details of the individual within your organisation leading on the change.
33. This also includes offshoring DWP data, use of a product or service with an offshore element or use of landed resources in delivery of your DWP contract(s). Offshore is deemed by the Cabinet Office as outside the UK. All offshore proposals must be reviewed and approved by DWP and in some circumstances Cabinet Office prior to use.

34. You must seek and receive approval should any of your subcontractors and service delivery partners wish to use offshore.

35. As part of the offshore proposal DWP will require full details of the data held under the contract, this should detail what data is involved including whether a particular data field is a marker or actual data and the volumes. Please ensure this is provided when you submit the Offshore Questionnaire in addition to the Change Request and RMIAA documents.

36. Please note that for products with multiple configuration profiles DWP may require you as part of the condition of approval to undertake an IT Health Check within 3 months of using the product with the results reviewed by DWP. This provides assurance around correct configuration.

37. Please see the DWP Offshore Policy – Guide for Contractors for further details. Please submit the completed Offshore Questionnaire and all accompanying documentation to wpd.security@dwp.gov.uk.

38. Should you feel a more secure transmission method is appropriate please contact wpd.security@dwp.gov.uk to discuss.

Communications Management

39. You must have policies and guidelines in place with regard to the use of office systems such as the use of electronic media and telephonic.

40. All media used in delivery of your DWP contract must be controlled and comply with all applicable legal requirements.

Use of Social Media

41. When using Social Media for business reasons (both internal and external) please note you are only allowed to:
   - Advertise local information that may help with job seeking activities,
   - Promote and support the delivery of our business and make the Department more open and accessible.

42. You are not allowed to use Social Media sites to track claimants or participants; this includes claimants or participants you believe are in employment but have not informed you.

Sharing Information
43. You must have policies and controls to manage information sharing with DWP, subcontractors, service delivery partners and other third parties. This includes the need for procedures and policies for the use of encryption where appropriate. DWP requires that encryption certified and configured to FIPS 140-2 standard is met by you.

44. You may only share information in line with your DWP contract. DWP is the Data Controller in regard to the contract unless specified otherwise and is responsible to the Information Commissioner for the security of information. More information can be found at: The ICO webpage: Our approach to encryption

45. You must follow processes and procedures that you have agreed with DWP when returning data to DWP (including Jobcentre Plus).

**Email Security**

46. When sending DWP data by email you must first ensure that the recipient is entitled to receive that data and has a legitimate business need.

47. The sender is responsible for ensuring the safe transmission of DWP data ensuring all relevant standards are adhered to at all times.

48. The method that you choose must be the most secure method available to you and have been reviewed and approved by DWP during the life of the contract.

49. You should only send the minimum amount of data needed to make the communication effective.

50. Any failure to follow these standards will result in a reportable security incident occurring. Should you have any queries regarding these standards please contact wpd.security@dwp.gov.uk.

**Claimant CV and Name Unencrypted Email Exemptions**

51. The following claimant or participant CV and claimant or participant name unencrypted email standards apply to all provision.

**Claimant or Participant CV Exemption**

The unencrypted emailing of a claimant or participants CV to their email account. The following conditions must be adhered to:
- Only one CV to be sent per email,
- The individual must have requested their CV to be emailed to them - CVs must not be emailed without the individual’s prior consent - i.e. they must not be sent unsolicited,
- A confirmation will need to be kept that the individual is content for their CV to be sent by email to their stated email address,
- The following must not be included: date of birth, NINO, bank details, medical information, ethnicity and criminal record information.
Claimant or Participant Name Exemption
The unencrypted emailing of a full claimant or participant name to an employer or within your supply chain or to DWP provided the following conditions are adhered to:

- Only one claimant or participant name per email,
- Claimant or participant name only,
- If any other identifiable claimant data is included within the email or subject line then encryption must be applied unless you have specific written permission from DWP to the contrary,
- Confirm who the email recipient will be and that the email is received.

Supply Chain and Third Party Unencrypted Email Exemptions

52. Provider, subcontractor and service delivery partner staff are permitted to send an unencrypted e-mail within their supply chain or to a third party containing information about individual data subjects for the following situations:

- up to 10 CV’s,
- up to 10 application forms,
- up to 10 letters and
- lists of claimant or participant names (up to 500)

For emailing of DMA, Exit Reports, Change of Circumstances and Benefits Cap Notification please refer to provision specific guidance.

53. You must ensure you continue to adhere to the security requirements in your contract and associated guidance; if a Security Plan Change Request is required please follow the change process detailed in this chapter.

Emailing up to 10 CV’s

54. You may send up to a maximum of 10 CV’s by unencrypted email. This may comprise of CVs and or information directly extracted from a CV (single data set) but must not exceed the 10 CV/data set limit in a single email.

55. Failure to adhere to this constitutes a reportable incident.

Emailing up to 10 Application Forms

56. You may send up to 10 application forms in one unencrypted email; for example to a prospective employer.

57. Application forms must contain the minimum information to make the communication effective. You must not include NINOs, bank details or date of birth however the age of the claimant or participant may be included where appropriate.

58. Where application forms are for couples (each form includes data about two persons) then you must limit the number of forms to 5 applications per
email to ensure each email contains information on no more than 10 claimants or participants in total.

59. Failure to adhere to this constitutes a reportable incident.

**Emailing up to 10 of the following types of letters**

- Interview Letters,
- Job Offer letters,
- Appointment Letters.

60. No other letters are permitted to be sent by unencrypted email and using unencrypted email to send letters containing significant sensitive personal data is not permitted.

61. Limited personal data can be included to make routine communications effective however information about substance addiction or mental health issues for example are not suitable for transmission by unencrypted email.

62. NINOs and bank details must not be communicated by unencrypted email by yourself or your supply chain to employers for claimants or participants successful at interview.

63. Where there is a concern about the sensitivity of particular correspondence you should send it by more secure means such as encrypted email or by Royal Mail or a similar secure service.

64. Failure to adhere to this constitutes a reportable incident.

**Emailing Lists of Claimant or Participant Names (up to 500)**

65. You may send a list of up to 500 claimant or participant names in 1 unencrypted email however you must always follow DWP guidance;

> “In the case of a list of information about more than one data subject, and these are claimants: surnames and initials, or forenames, NINOs and/or reference numbers (additional simple details such as date of interview/appointment may be included if necessary) may be sent”.

66. There must be no reference to benefits payment amounts, child support payment amounts, or any additional personal details such as date of birth or home addresses, home or mobile telephone numbers or other contact details in these correspondences.

67. The maximum number of data subjects which may be included in a list in a single unencrypted e-mail is 500. Any emails containing only a list of
NINOs and no other information about the data subjects are not subject to this limit.

68. Failure to adhere to this constitutes a reportable incident.

Claimant or Participant Data Not Permitted via Unencrypted Email

69. The following DWP claimant or participant data must **not** be included in unencrypted email when exchanging information with your supply chain or third parties unless you hold prior DWP approval to do so;

- Date of birth,
- Bank account details,
- Medical history/mental health issues,
- Substance abuse,
- Criminal records,
- Benefit payment details,
- Children’s names and dates of birth/age,
- Ethnicity,
- Sexual orientation.

National Insurance Number

70. NINOs must not be communicated by unencrypted email unless otherwise specified in the above exemptions or you hold prior DWP approval to do so.

Unencrypted Emailing of Data to DWP

71. You are permitted to use unencrypted email when sharing the following data with DWP:
   a) Submission of UCNEA1s,
   b) Submission of European Social Fund and European Social Fund (ESF) Match Funded Provision Good News Stories.

72. When emailing any of the above you must only attach one UCNEA1 or Good News Story per email.

73. The Supply Chain and Third Party Unencrypted Email Exemption - Emailing Lists of Claimant or Participant Names (up to 500) paras 65-68 of this guidance has been extended to permit you to use unencrypted email when sharing this data with DWP for ESF, New Enterprise Allowance 2 (NEA2) and Work and Health Provision (WHP) only.

74. Please ensure you use clear and concise email header titles so it is clear to the recipient your emails intent.
75. Failure to adhere to this constitutes a reportable incident.

Sending Clerical Information

76. Documents may be posted by adhering to the following principles:
   - Always use a fully tracked service when sending claimant data about 50 or more individuals together (in the same envelope),
   - A fully tracked service must be used as standard for items going to or from storage or archiving facilities,
   - All staff must ensure that correct courier or postal addresses are used,
   - If incorrectly addressed mail is received; you must ensure appropriate care is taken to safeguard the package until the correct recipient is known. The package should then be sent to the correct recipients using a similar ‘fully tracked’ service,
   - It is the sender’s responsibility to consider the scale and sensitivity of the information that is being sent, and whether additional security (i.e. using a fully tracked service) is required.

Retention, Storage, Archiving and Destruction

77. You must have procedures and policies in place to provide secure retention, storage, archiving and destruction of DWP data. You must have:
   - A documented clear desk policy in operation;
   - Lockable storage available to store DWP data; and
   - Procedures in place for the safe destruction or re-use of redundant media including hard disks, CD’s, hard-copies and any other storage used to process DWP data (DWP reference HMG Information Assurance Standard 5 - Secure Sanitisation).

Document Retention

78. Your specific contract or provider guidance will have detail around what documents must be retained and for how long and must be adhered to.

79. Clarification must be sought from your DWP Performance Manager regarding the use of electronic document retention.

80. If you are delivering an ESF contract then you must adhere to specific requirements relating to document retention; see Generic Guidance Chapter 11- ESF requirements.

Portable Media

81. You must ensure that equipment; systems and services are protected from unauthorised access, theft, interference or damage.

82. Portable media includes laptops, memory sticks, smartphones or similar handheld devices, mobile phones, CD’s and hard-copy documents.
83. If your personnel are working outside your main delivery sites and accessing DWP data via portable media you must ensure that:

- Equipment must be sited in a secure area and cannot be seen by unauthorised persons,
- Procedures must be in place to record the removal of equipment/software from site,
- You must ensure the appropriate level of protection is given to the data i.e. encryption for electronic records and devices. Electronic records and devices must be encrypted at all time; and
- Information stored on portable media must be kept to an absolute minimum and meets business needs.

Premises

84. To ensure that information, systems and services are protected from unauthorised access, theft, interference or damage you must ensure the following:

- **Perimeter:** Controls and procedures are in place to secure the perimeter of site, building or office,
- **Access Control:** Controls and procedures are in place to allow only authorised personnel to enter site, building or office i.e. visitors must be signed on and off site at all times,
- **Secure Areas:** Controls and procedures are in place to allow only authorised personnel into secure areas; and
- **Delivery and Collection of Data:** DWP data is safeguarded from unauthorised access, accidental or deliberate loss or damage i.e. controls are in place for the delivery and collection of data.
Annex 1: Security Incident Report Form

Please email immediately to: wpd.security@dwp.gov.uk
Please contact the inbox should you wish to utilise a more secure transmission method.

Date:  
Completed by:

<table>
<thead>
<tr>
<th>Contract(s) Title including end date(s) and Provider Contact</th>
<th>Location data lost/compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Detail and timeline of incident** – please provide as much detail as possible

**Description of any data lost** – description of the data set(s) in question. **Do not** include the actual data set.

**Any notifications carried out to-date** – e.g. Police/individuals affected. If the Police please include the crime reference number.
Annex 2: Security Plan Change Request Form

Please email this request to: wpd.security@dwp.gov.uk
Please contact the inbox should you wish to utilise a more secure transmission method.

Date:          Completed by:

<table>
<thead>
<tr>
<th>Provider Name and Contact</th>
<th>DWP Contracts Affected</th>
<th>DWP Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DWP use</td>
</tr>
</tbody>
</table>

**Full Description of Change Requested:**
Please provide as much information as possible about the proposed change including any appropriate building layouts, IT architecture plans and audits/testing scope relevant to this request. Please also include a data dictionary if applicable.
Annex 3: When to Seek DWP Approval for use of Third Party Electronic Services

The following diagram provides a basic guide to determining whether DWP is required to review and approve your change. Please contact DWP if in any doubt.

Will service involve DWP data being shared or disclosed?  
- **Yes**
  - Will service involve DWP data being created or received? (includes MI)  
    - **Yes**
      - Will the security plan change as a result of using this service?  
        - **Yes**
          - Will DWP claimants or participants be required or compelled to use service? (Alternatives/choices MUST be offered)  
            - **Yes**
              - Does the service involve subcontracting? (not incl. use under license)  
                - **Yes**
                  - DWP approval required  
                - **No**
                  - No DWP approval required  
          - **No**
          - No
        - **No**
        - No
    - **No**
  - **No**
- **No**

**No DWP approval required**
- Do not use DWP branding,
- Ensure claimants are clearly advised of: options/alternatives, terms of use, privacy and cookie policies,
- Provider conducts own assessment of adequacy.