

## Chapter 8 - Information Security

### TABLE OF CONTENTS

Introduction.....	1
General .....	2
Data Protection.....	2
DWP Contract .....	2
Minimum Security Requirements.....	4
Staff Vetting.....	4
Confidentiality.....	4
Training and Awareness.....	5
Access Controls .....	5
Security Incident Management.....	5
Security Incident Reporting .....	5
Changes to Provider Security Plans.....	6
Use of Office Systems.....	6
Sharing Information .....	6
Sending Information .....	7
Retention, Storage, Archiving and Destruction.....	8
Document Retention.....	8
Annex 1 .....	10
Definition of a Security Incident .....	10
What is a Security Incident? .....	10
Definition of an Asset.....	10
Concept of Loss.....	11
Does an incident require staff involvement? .....	11
Examples of Security Incidents.....	11
Disclosure .....	11
Unauthorised access to data .....	12
Fraud/irregularity or unauthorised modification.....	12
Theft .....	12
Loss .....	12
Provider Process/Procedure Failure .....	12
Damage .....	13
Annex 2 .....	14
Security Incident Report.....	1
Annex 3 .....	15
Provider Security Plan Change Request .....	15

### Introduction

1. Notwithstanding information and agreed measures included in your contract and the Provider Referral and Payment System (PRaP) Security Plan, the following is provided as generic guidance for all providers delivering Welfare to Work programmes to Department for Work and Pensions (DWP).

2. The Department requires all prime contractors and their sub contractors and service delivery partners to operate appropriate, secure systems and processes for handling and storing participant information in line with DWP Standards and the Data Protection Act. The risk of loss of public confidence through failure to protect sensitive or personal information remains a key risk for the 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. So we take data protection extremely seriously, and we require you (and your sub-contractors and service delivery partners) to apply the high standards that we ourselves apply.
4. Equally important is the need for providers to **impress the need for strict security compliance on their staff their sub contractor and delivery partners and their staff.**

## General

5. This section provides information on data security and details your responsibilities with regards to:
  - the secure collection, transfer; storage; disposal of information;
  - the reporting of Security incidents; and
  - request to change to any aspect of your security plan agreed with the Department.
6. As a supplier to the DWP, you will have access to participant's personal data and DWP information. You will therefore need to comply with the Data Protection Act and there are also minimum security standards that you are required to meet and continue to meet. Further information on what is required of you in respect of the Data Protection, Data Security and Freedom of Information is contained in the Terms and Conditions of your contract.

## Data Protection

7. You must ensure that you process data in accordance with the provisions of the Data Protection Act and implement appropriate technical and organisational measures to protect the data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure.

## DWP Contract

8. The terms and conditions of your contract detail the Department's security requirements, including:

## DWP Provider Guidance Chapter 8

- 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;
  - Security Requirements and Plan;  
(i.e. the plan sets 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, and act in accordance with the content of the Security Plan.)
  - 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;
  - audit and testing of the Security Plan; and
  - compliance with ISO/IEC:27002 (Information Security Code of Practice) and ISO/IEC 27001 (Information Security Requirements Specification) (Standard Specification), if applicable.
9. As a provider you must inform DWP if/when you are considering any changes to processes which may affect the handling of Authority Data. *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”.*
10. You must inform DWP of security incidents immediately. **A Security incident is defined as:**

“A deliberate attempt, whether successful or not, to compromise DWP data or assets. This includes DWP data and assets in the possession of a contractor/provider or their sub contractors/service delivery partners.

Any incident resulting in a loss of DWP data or assets. This includes DWP data and assets in the possession of a contractor/provider or their sub contractors/service delivery partners

## DWP Provider Guidance Chapter 8

A breakdown in provider systems/processes that has resulted in DWP data becoming exposed/potentially exposed to external sources.”

Further information can be found below Security Incident Reporting and at [Annex 1](#).

## Minimum Security Requirements

11. The following cover the key, non-technical, areas of information security that Providers to DWP must adhere to:

**PERSONNEL SECURITY** – Before allowing staff and your sub-contractor staff access to DWP data, the measures detailed below **must** be in place:

### Staff Vetting

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

- Identity;
- employment history;
- nationality/immigration status; and
- criminal records.

13. Please note that an enhanced CRB check needs to be completed for all of your staff and any sub-contractor staff dealing with vulnerable people.

14. As part of this process, the contractor’s declaration must be completed and returned to DWP on an annual basis see Annex D of the [BPSS guidance](#).

### Confidentiality

15. You will have signed a confidentiality agreement as part of your contract with the Department.

16. In addition, as part of the contract, you may be required to obtain individual confidentiality statements from staff that have access to Authority Data.

## DWP Provider Guidance Chapter 8

### Training and Awareness

17. Your personnel must understand their obligations when handling DWP data, being aware of their legal and contractual responsibilities including at the start and termination of employment including the [Computer Misuse Act](#) and [Data Protection Act](#).
18. You must ensure all staff, including sub contractor and service delivery partner staff handling Authority Data receive information security training on induction to the company and regular refresher training must be in place.
  - The DWP Supply Chain Information Assurance Team (SCIAT) has developed a data security training and awareness slide pack for suppliers and their employees delivering DWP contracts. Suppliers can use the slides as training material for their employees.  
[Data protection and information security - DWP](#)

### Access Controls

19. DWP requires that User Access controls and procedures are in place to monitor access to Authority Data ensuring access is granted to and removed as job responsibilities demand.
20. Where relevant to your contract, access to the PRaP System website by anyone other than your authorised staff is prohibited. You will ensure that your staff will not allow any other member of your staff, or any third party who has not been granted access to the PRaP System website by the DWP, to gain access to the PRaP System website.

### Security Incident Management

21. You must ensure that all necessary systems and processes are in place for reporting incidents to the handling, storing participant information including your sub contractors and service delivery partners.
22. You must have incident handling processes in place to identify and resolve any security weaknesses.
23. You must have procedures in place to identify software and system faults and failures such as the identification of malicious software.

### Security Incident Reporting

24. Provider security incidents should be reported immediately using the reporting stencil at [Annex 2](#) and emailed to [wpd.security@dwp.gsi.gov.uk](mailto:wpd.security@dwp.gsi.gov.uk)

## DWP Provider Guidance Chapter 8

where this will be acknowledged and a reference number allocated to it. Provider remedial actions may be specified by DWP to resolve the incident.

25. When reporting an incident DWP customer data should not be contained within the report unless essential or asked to do so by DWP and must be [encrypted to the required standard](#).
26. Full details including a definition of a security incident can be found at [Annex 1](#).
27. **Under no circumstances should you; sub contractors or service delivery partners report incidents to the Information Commissioner. DWP is the Data Controller and it is our responsibility to report any data loss to the Information Commissioner where appropriate.**

## Changes to Provider Security Plans

28. Providers should complete the template at [Annex 3](#) when requesting any change, modification or refinement to **any aspect** of the Security Plan agreed with the Department.
29. Completed templates should be sent to [wpd.security@dwp.gsi.gov.uk](mailto:wpd.security@dwp.gsi.gov.uk). Providers should supply as much information about the proposed change as possible along with the name and contact details of the individual within the Providers organisation leading on the change request.

## Communications Management

30. To ensure the integrity, availability and reduce risks to DWP data using media which must be controlled and comply with all applicable legal requirements.

## Use of Office Systems

31. You must have policies and guidelines in place with regard to the use of office systems such as the use of electronic media such as telephone, fax, e-mail and hard copy post.

## Sharing Information

32. You must have policies and controls to manage information sharing with DWP, Jobcentre Plus, sub-contractors and other third parties. This includes the need for procedures and policies for the use of Encryption. DWP requires that FIPS 140-2 standard is to be met by you.

## DWP Provider Guidance Chapter 8

33. Providers may only share information in line with their contract with DWP and DWP is the Data Controller in regard to the contract 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](#)
34. The following exemption applies to all DWP Welfare to Work providers and allows the emailing of unencrypted customer CV's to potential employers. The following conditions must be adhered to:
- Only one CV to be sent per email
  - Limit the type of data that a client includes on their CV i.e. ensure that the following is not included: date of birth, National Insurance number, bank details, medical information, criminal record information.
  - Ensure that the client is aware that their CV will be sent via email and provides a disclaimer to that effect.
  - Confirm who the email recipient will/should be and that the email is received.

## Sending Information

35. Documents must be sent in batches rather than on an individual basis, but should not be stockpiled, and following the principles detailed below:
- Always use a fully tracked service when sending **personal data** about 50 or more individuals together (in the same envelope);
  - A fully tracked Service should also be used for smaller numbers for more **sensitive personal data** i.e. Transfers containing name along with for example, National Insurance Number, health records, financial records, work history, personal email etc (**20 or more items**);
  - A fully tracked service must be used as standard for items going to/from storage/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 be sent using a similar 'fully tracked' service. This approach will avoid any risk to the personal/sensitive data that may be contained within the package; and
  - 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.
36. More information can be sent to you on request.

## Retention, Storage, Archiving and Destruction

37. You must have procedures and policies in place to provide secure retention, storage, archiving and destruction of Authority Data.

You must have:

- a documented clear desk policy in operation;
- lockable storage available to store Authority Data; and
- procedures in place for the destruction or re-use of redundant media including hard disks, CD's, hard-copies and any other storage used to process Authority Data.

### Document Retention

38. Your specific contract will have detail around what documents must be retained and for how long.

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

40. 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

41. To ensure that equipment, systems and services are protected from unauthorised access, theft, interference or damage.

42. Portable media includes laptops, memory sticks, blackberries or similar handheld devices, mobile phones, CD's and hard-copy documents.

43. If your personnel are working outside your main delivery sites and accessing Authority 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 right 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

## DWP Provider Guidance Chapter 8

- Information stored on portable media must be kept to an absolute minimum and meets business needs.

### Premises

44. To ensure that information, systems and services are protected from unauthorised access, theft, interference or damage.

45. 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

### Definition of a Security Incident

#### What is a Security Incident?

A Security Incident is defined as:

- a deliberate attempt, whether successful or not, to compromise DWP data or assets. This includes DWP data and assets in the possession of a contractor/provider or their subcontractors; and
- any accident resulting in a loss of DWP data or assets. This includes DWP data and assets in the possession of a contractor/provider or their subcontractors.
- a breakdown in provider systems/processes that has resulted in DWP data becoming exposed/potentially exposed to external sources.

The following are only examples of which have resulted in loss of DWP data:

- The employee of a provider loses their work briefcase. It contains no DWP information therefore there is no requirement to report to DWP as the briefcase and contents aren't DWP assets; and
- The employee of a provider loses their work briefcase. It contains a small amount of DWP information thus making it a requirement to report to DWP. DWP's interest is the information; a DWP asset, the briefcase belongs to the provider thus isn't a DWP asset;
- The employee of a provider fails to adhere to the email encryption standards specific to the DWP programme contract resulting in customer details being transmitted via the external internet.

DWP will always ask questions about the secure transport and storage of DWP information by providers and their staff and their sub contractors/service delivery partners and their staff. In the case of the briefcase examples above, it would be about treatment of the briefcase by provider staff and their sub contractors/service delivery partners and their staff in use and storage. In terms of the email it would be why has this happened, is it systemic failure or a lack of awareness on the employees part etc?

#### Definition of an Asset

An asset is any item of departmental property that has a value. Assets include:

## DWP Provider Guidance Chapter 8

- physical property and equipment;
- all information and documents; and
- other DWP valuables.

The definition includes information held clerically or electronically and owned by DWP.

### **Concept of Loss**

The concept of loss is not solely concerned with the physical loss of an asset. It also includes loss:

- of confidentiality of information through accidental or deliberate disclosure to someone not authorised to receive it;
- because the asset is not available for use; this may be because it has been lost or stolen, or accidentally deleted from a PC disk and there is no backup copy. It may be because it is damaged and cannot be used until it is repaired, replaced or there may be some other fault that makes the asset unusable; and
- of trustworthiness and reliability (integrity) of information.

### **Does an incident require staff involvement?**

Incidents occur when an attempt whether successful or not to compromise DWP data or assets occurs. The cause does not negate the need to make a report. Suspected dishonesty or corruption on the part of provider and their staff must be reported as incidents.

### **Examples of Security Incidents**

#### **Disclosure**

When information is deliberately or accidentally divulged to unauthorised persons e.g.

- participant details sent to wrong participant;
- inappropriate disclosure to a third party including bogus callers. DWP expect you to mitigate against disclosure to bogus callers by applying all checks they deem appropriate to verify caller/recruiter; and
- leaks – where protectively marked or sensitive information is disclosed without authority to a third party usually the media.

## DWP Provider Guidance Chapter 8 **Unauthorised access to data**

When information is accessed without a valid business reason but the information is not disclosed to other persons.

### **Fraud/irregularity or unauthorised modification**

Any actual attempted or suspected changes to data or software without a valid business reason e.g.

- unauthorised change to a participant's data;
- unauthorised change to software; and
- introducing spurious information such as bogus vacancies (where a vacancy is suspected not to be genuine). Please follow Jobcentre Plus/DWP PMD guidance on this matter.

### **Theft**

A third party or employee stealing assets such as a laptop containing DWP data from a car etc.

The concept of theft can also be applied to data, for example an employee leaves to set up his own business and takes a copy of the client list (DWP data).

### **Loss**

When any type of asset has been lost that could have security implications for DWP or DWP participant's. This includes documents lost within the office or remote storage facilities.

DWP takes the view documents known to be in an office or remote storage facility but misfiled thus not immediately available are not lost just misplaced in a secure facility. Evidence of loss is based on an ability to audit trail a document to a point where it was known to be secure and analysis of the circumstances surrounding the loss.

### **Provider Process/Procedure Failure**

An action by a provider's employee failing to adhere to the security policy in a way that exposes/potentially exposes DWP customer data to external sources such as correct encryption not being applied or protective markings not being applied etc.

## Damage

Any incident that causes damage or loss to a service or asset, for example a member of staff deliberately destroys a computer containing DWP data or documents damaged in transit etc.

DWP requires all such instances to be reported as this can indicate issues with a provider's processes which may need Account Management involvement to resolve.

**Please note all of the above is to try and give an indication of what a security incident is but please bear in mind it is impossible to provide a full definitive list of examples etc due to instances of random incidents.**

## Annex 2

COMMERCIAL IN CONFIDENCE

Incident ref. (DWP Use)
----------------------------

### Security Incident Report

Please email immediately to [WPD.SECURITY@DWP.GSI.GOV.UK](mailto:WPD.SECURITY@DWP.GSI.GOV.UK)

Date:                      Completed by:

Contract Name and Director	Contract site	Location data lost/compromised

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

**Description of any data lost** - provide full description of the data types lost ie names/addresses/bank account details/prisoner records etc.

**Any notifications carried out to-date** – e.g. police/individuals affected.

### Annex 3

COMMERCIAL IN CONFIDENCE

#### Provider Security Plan Change Request

Please email immediately to [wpd.security@dwp.gsi.gov.uk](mailto:wpd.security@dwp.gsi.gov.uk)

Date: Completed by:

Provider Name and Director	Provider Contact for This Request	Change Request Ref (DWP Use)
<p><b>Full Description of Change Required:</b>                      Provider should include as much information as possible about the proposed change including:</p> <ul style="list-style-type: none"> <li>- Whether the change impacts on all programmes currently delivered by the provider or 1 programme</li> <li>- Is it a software change</li> <li>- How many people and/or sites in your organisation are impacted by the proposed change – will the change for example require staff training</li> <li>- How will information about DWP participant currently held on your systems be impacted and protected during the change process.</li> <li>- Will the way in which DWP participant Data is held on your systems change if so, how</li> <li>- If this is change to systems do you anticipate there being any requirement for testing, including penetration testing.</li> </ul>		
<p><b>Will this change result in any loss of service to the participant over the implementation period?</b></p>		