Template document for third parties handling PERSONAL DATA not through direct contract or on behalf of Welsh Government – delete or amend items in red, within brackets as appropriate

Llywodraeth Cymru
Welsh Government

Security Aspects Letter for ……[*reference for data access agreement and name of organisation*]……

Please note that **Cyber Essentials** certification must remain valid for the full duration of the work and it is the data processor's responsibility to ensure any recertification is undertaken at the appropriate time.

Welsh Government contact details [*lead analyst telephone number and email address plus alternative contact details*]

Introduction

The Welsh Government requires all suppliers, sub-contractors and service delivery partners to operate appropriate and secure processes for handling, storing and processing data and information owned by the Welsh Government. You are receiving this letter as you will be processing, for you own purposes as defined in the Data Access Agreement, personal information for which Welsh Government act as Data Controller.

This Security Aspects Letter (SAL) states how our information assets are to be handled

Please note that the term 'information' is used within this document to refer to all data and information handled.

Personal Information

As the data controller (as defined in the Data Protection Act 1998) for the personal information being handled in this contract, the Welsh Government requires the security measures specified in this document to be implemented in relation to the staff, systems and premises handling the information described in the data access agreement. These measures must be implemented to prevent unauthorised or unlawful processing of personal data and protect against accidental loss, destruction or damage to this information.

Specification of security measures required

The following security controls are based on commercial good practice, with an emphasis on staff to respect the confidentiality of all information.

Governance

1. A named individual must be appointed to the role of 'security lead' to take responsibility for the security aspects of this [*agreement*]. This named individual will be required to lead on any response required in relation to assessment of the measures in place during the term of the [*agreement*].

2. Any security breaches must be brought to the attention of the named security lead who is then required to report the incident to the Welsh Government contact at the earliest opportunity. Failure to do so could delay an effective response by the Welsh Government.

3. The OFFICIAL–SENSITIVE marking must be retained on all Welsh Government information which is marked as such.

Electronic information:

In addition to meeting the technical requirements prescribed by the **Cyber Essentials** certification the following protective measures must be applied:

4. If any information is stored or processed on equipment other than that owned by [*company name*] then assurance must be provided that partners and subcontractors also comply with Cyber Essentials or ISO27001 standards when processing the information needed to carry out this contract.

5. Storing or processing information on personally owned devices or email accounts is not permitted[1].

6. [If '*Cloud' storage services are to be used for sensitive personal information, evidence must be provided that the relevant Government Cloud Security Principles are applied].*

7. All sensitive or personal electronic information must be encrypted in transit. Data encryption services such as PGP or Egress Switch must be used when emailing information.

8. All sensitive or personal electronic information at rest on mobile devices handling Welsh Government information e.g. laptops, must be encrypted (minimum FIPS 140-2 / AES 256)[2].

---

[1] Personal equipment is defined as equipment which:
- is not a company asset **or**
- the configuration of the equipment is outside company control **or**
- it is used by those not employed by the company e.g. a sole trader who allows their 'work' laptop to be used by other family members. The risk being that Welsh Government personal information can be accessed by those not authorised to see it.

[2] For more information about encryption standards see the Information Commissioner's website - https://ico.org.uk/for-organisations/encryption/

9. Information at rest on servers/individual computers must be encrypted (minimum FIPS 140-2 / AES 256) unless the ICT equipment is located in secure premises with strong physical controls e.g. a data centre with access control measures, alarmed, arrangements for 24 hours security guards.

10. Access to the information involved in this contract must be on a 'need to know' basis. Only authorised staff who have received suitable training (see Personnel Security section) can be given access. A list of authorised staff must be provided within the Data Access Agreement.

11. If contacted by telephone, staff must verify the identity of the caller before discussing Welsh Government data. No personal data shall be passed to another party without absolute verification of the identity of the caller and that they have the authority to receive this information.

12. The information processed or collected under the terms of this contract must be deleted in accordance with the terms of the Data Access Agreement. This includes any information stored on servers, mobile devices or other storage media including CDs or DVDs, other removable media, hard copy [paper] or hard drives. Please confirm in writing when this has been done.

Physical Security:

13. Only authorised personnel can have access to restricted areas containing information systems, removable media or hard copy information relating to this contract. Plans and procedures for dealing with, and intercepting, unauthorised visitors and intruders must be in place and evidence provided to the Welsh Government on request.

14. If it is necessary to take hardcopy information outside the restricted areas this must be kept to the minimum required and protected in transit (e.g. by means of envelope / file / briefcase) to avoid information being visible and to reduce the likelihood of loss or misuse.

15. Local business processes must make it easy for staff to follow the rules (e.g. clear desk policies, separating publicly available printed information from the OFFICIAL-SENSITIVE papers, guidance and facilities for proper disposal etc.).

Personnel Security:

16. The Contractor must hold accurate and verified information for all staff working on this contract in relation to proof of identity, nationality/immigration status, unspent criminal convictions and employment history. Evidence must be provided on request and the Welsh Government may verify the validity and expiry dates of any existing clearances with the relevant holding agency.

17. Suppliers and their sub-contractors must have, or be able to obtain, sufficient staff who can achieve the appropriate security clearance prior to engagement with the Welsh Government.

18. All staff working on this data must be properly trained to understand that they have a duty of confidentiality and are responsible for safeguarding any WG information that they are entrusted with by applying the measures set out in this letter. The Security Awareness for Suppliers' Employees guidance document is available for reference.

19. On termination of involvement in this work user access privileges must be withdrawn and employees debriefed on their confidentiality responsibilities. This includes, but is not limited to, pin codes and any passwords known to the user.

Signatures

For and on behalf of service provider / supplier [Name of organisation]	
Signed	
Name [PRINTED]	
Date	
Position	

Annex A - Definitions of sensitive data

1. **Personal Information** -

The Data Protection Act [1998] regulates the use of "personal data". The definition provided by the Information Commissioner's Office makes it clear that personal data means data which relate to a living individual who can be identified [a] from those data, or [b] from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to:

[a] the racial or ethnic origin of the data subject,
[b] political opinions,
[c] religious beliefs or other beliefs of a similar nature,
[d] membership of a trade union [within the meaning of the Trade Union and Labour Relations [Consolidation] Act 1992],
[e] physical or mental health or condition,
[f] sexual orientation,
[g] the commission or alleged commission of any offence, or
[h] any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

2. **OFFICIAL – SENSITIVE**

Under the Government Classification System this handling caveat is used in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' principle as compromise or loss could have damaging consequences. This could include, but is not limited to, the following types of information:

1. The most sensitive corporate or operational information, e.g. relating to organisational change, contentious negotiations, major security or business continuity issues;
2. Policy development research and statistics;
3. Advice to ministers on contentious or very sensitive issues;
4. Commercial or market sensitive information that may be damaging to the WG or to a commercial partner if improperly accessed;
5. Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
6. Diplomatic activities or negotiating positions where inappropriate access could impact foreign relations or negotiating positions and must be limited to bounded groups;
7. Very sensitive personal data, where it is not considered necessary to manage this information in the SECRET tier.
8. Where the consequences of loss or inappropriate access to individual information assets may be particularly damaging [e.g. export licensing, witness data, information of use to terrorist / extremist targeting etc].