**DSD002 Annex One – DIP On-Boarding Non-Functional Checks**

**Amendment Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description of Change | Approval Reference |
| 0.1 |  | Issue 101 Consultation | - |
| 0.2 |  | Issue 101 Report | - |
| 0.3 |  | Shared with Ofgem |  |
| 0.4 |  | P474 |  |

**Contents**

[1 Non-Functional Checks 3](#_Toc161132885)

# Non-Functional Checks

The following shall be checked during DIP On-Boarding and each year thereafter as part of a Code-of-Connection Self-Assessment Document (CoCo SAD):

1. the requirements of DSD002 Annex 2 ‘Detailed DIP Operational Requirements’ and DSD002 Annex 3 ‘The DIP-PKI (Public Key Infrastructure) Policy’ are in place;
2. Statements of Applicability demonstrating that all applicable ISO/IEC 27001 controls have been applied, where appropriate (where an organisation is ISO 27001 certified);
3. evidence of compliance with other recognised security frameworks such as Cyber Essentials or Cyber Essentials Plus;
4. written confirmation that the DIP Rules have been read and understood;
5. documents and processes are in place to ensure compliance with Data Protection Legislation. The DIP User shall provide, on request, evidence of compliance including relevant data protection policies, processes and, where applicable, data protection impact assessments. DIP Users acknowledge and agree that, notwithstanding the DIP Manager undertaking non-functional checks in accordance with this section, compliance with Data Protection Legislation remains the responsibility of the DIP User, and the DIP Manager checks shall not constitute validation of the completeness or correctness of a DIP User’s documentation or approach;
6. process for retaining all audit logs of basic user activities (e.g., logon, logoff, failed attempts) and security events for all information systems and services that interact with the DIP, within legal constraints, for a minimum of 3 months of live data and 12 month archived;
7. demonstration of logical network schematic of the information systems and services in scope that interact with the DIP, and include:
8. services and functionality;
9. gateway/boundaries functionality;
10. processes are in place for key management – demonstrable by written processes, logical diagrams and, at DIP Manager’s discretion (if possible), demonstration of process to place messages in storage;
11. process for retention of security events for all information systems and services that interact with the DIP – demonstrable by production of written process and, at DIP Manager’s discretion, demonstration of how record is accessed;
12. DIP Users systems are backed-up in accordance with best practice – demonstrable by adherence to ISO 27000 series processes and production of written process to back up systems, to include logical process diagrams;
13. processes, protocols and liabilities between the DIP User and any third Party they have contracted with - demonstrable by production of written documents (within limits of confidentiality); DIP Manager may contact the third party directly for verification at their discretion;
14. DIP User has a Cyber Incident Response Plan – demonstrable by production of written documents;
15. DIP User is aware of their responsibilities as a Data Processor/Controller in accordance with relevant Data Protection Legislation – demonstrable by production of applicable documentation detailing the DIP User’s responsibilities – this may be part of a wider document;
16. DIP User shall have processes in place to deal with breaches of DIP Data. This shall include process for informing relevant authorities and stakeholders, including the DIP Manager –demonstrable by production of written processes and, if applicable, any evidence that the DIP User has already carried out such processes; and
17. adherence to the Authority’s data best practice – demonstrable by production of written procedures and demonstration of examples of adherence.

DIP Users do not need to have ISO 27000 series (or equivalent) certification – see DSD002 ‘DIP Connection and Operations for further details.

The CoCo SAD will be a self-attestation by the DIP User that they remain compliant with the requirements of DSD002 ‘DIP Connection and Operations and the Annexes in particular. CoCo SADs are required to be retained for a minimum of 5 years and shall be produced as required by the DIP Manager.

The DIP Manager publishes guidance on completing the annual CoCo SAD, including a template to be completed by DIP Users.

Where ISO numbers are used, they shall for the purposes of the DIP Rules be deemed to include references to updated ISO numbers and/or replacements and/or amendments to them.

DIP Users will be expected to comply with all such ISO numbers applicable from time to time.