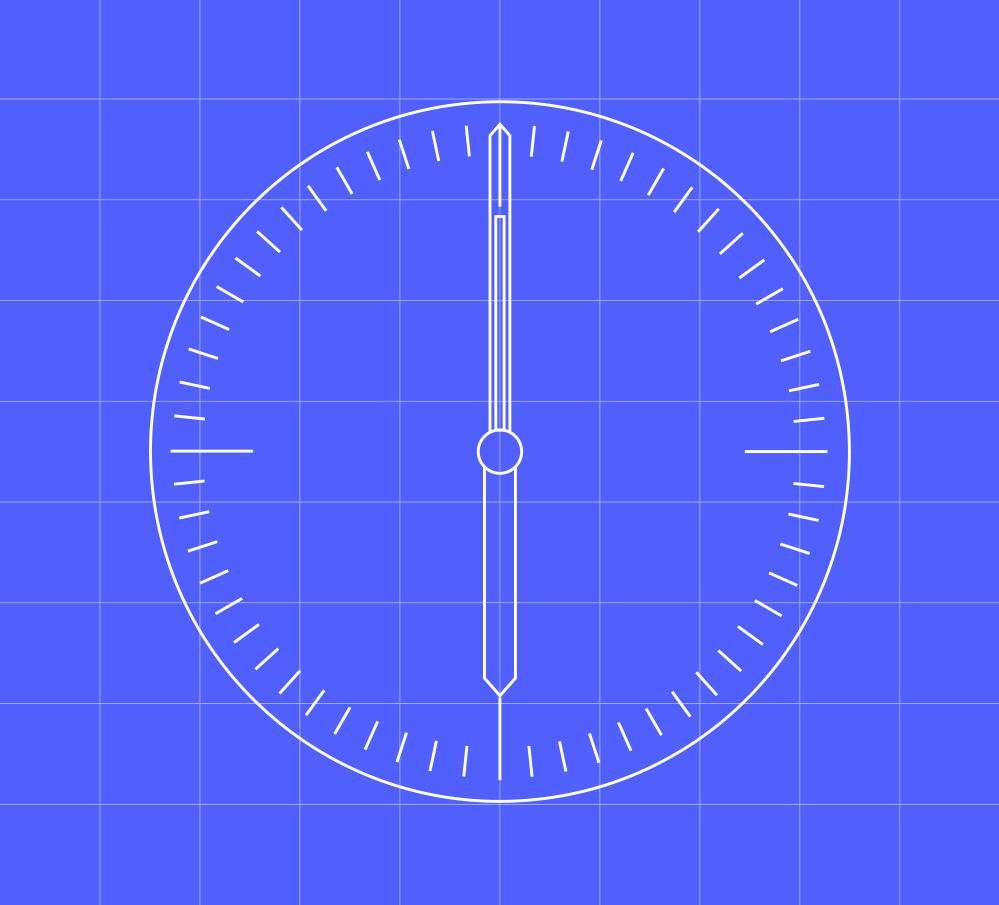
****MHHS DIP End-to-End Security Requirements****



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document owner | Document number | Version | Status: | Date |
| **Kevan Gleeson** | **MHHS-DIP005** | **Version 1.4** | **Draft** | **14th September 2022** |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Document owner | Document number | Date |
|  |  |  |

Contents

[Contents 2](#_Toc99111758)

[1.1 Change Record 7](#_Toc99111759)

[1.2 Reviewers 7](#_Toc99111760)

[1.3 References 7](#_Toc99111761)

[1.4 Terminology 7](#_Toc99111762)

[2 Background 8](#_Toc99111763)

[3 Introduction 8](#_Toc99111764)

[3.1 Purpose 8](#_Toc99111765)

[3.2 Scope 9](#_Toc99111766)

[3.3 Logical overview 9](#_Toc99111767)

[4 Programme Oversight 11](#_Toc99111768)

[4.1 Design Authority Group (DAG) 11](#_Toc99111769)

[4.2 Security Design Working Group (SDWG) 11](#_Toc99111770)

[5 Determining the Security Requirements 12](#_Toc99111771)

[5.1 Security Requirements for Market Participants 12](#_Toc99111772)

[5.2 Security Requirements for an Interface 12](#_Toc99111773)

[5.3 Security Requirements for the system. 12](#_Toc99111774)

[5.4 Enrolment Requirements 12](#_Toc99111775)

[5.5 DIP Security requirements 12](#_Toc99111776)

[6 Secure Code Development 13](#_Toc99111777)

[6.1 Developer Security Testing 13](#_Toc99111778)

[6.2 Secure Code Scanning 14](#_Toc99111779)

[7 Security Governance 14](#_Toc99111780)

[7.1 NCSC CAF 14](#_Toc99111781)

[7.2 NCSC Cloud Security Guidance 14](#_Toc99111782)

[7.3 Security Design Principles 15](#_Toc99111783)

[7.4 Compliance 15](#_Toc99111784)

[7.5 DIP Alignment with SPaR 16](#_Toc99111785)

[7.5.1 Security, Privacy and Risk Impact Guidance 16](#_Toc99111786)

[7.6 Privacy Classification 17](#_Toc99111787)

[7.7 GDPR 18](#_Toc99111788)

[7.7.1 Privacy Impact Assessment 18](#_Toc99111789)

[7.8 Supply chain 18](#_Toc99111790)

[7.9 Rules of Behaviour 19](#_Toc99111791)

[7.10 Outsourced Security Services 19](#_Toc99111792)

[8 Operational Security controls 19](#_Toc99111793)

[8.1 Risk Assessment 19](#_Toc99111794)

[8.1.1 Risk Management 19](#_Toc99111795)

[8.1.2 Risk Management Process 20](#_Toc99111796)

[8.1.3 Risk Analysis 20](#_Toc99111797)

[8.1.4 Risk Assessment Activities 21](#_Toc99111798)

[8.2 Data Protection 21](#_Toc99111799)

[8.2.1 Data Residency 21](#_Toc99111800)

[8.2.2 Data Hosting 21](#_Toc99111801)

[8.2.3 Data Environments 21](#_Toc99111802)

[8.2.4 Data Ownership 21](#_Toc99111803)

[8.2.5 Data Confidentiality and Integrity 21](#_Toc99111804)

[8.2.6 Data at Rest 22](#_Toc99111805)

[8.2.7 Data Loss Prevention 22](#_Toc99111806)

[8.2.8 NDA 22](#_Toc99111807)

[8.2.9 Non-repudiation 22](#_Toc99111808)

[8.2.10 Data Retention and Removal 22](#_Toc99111809)

[8.2.11 Asset Management 22](#_Toc99111810)

[8.2.12 Configuration Management 22](#_Toc99111811)

[8.2.13 Incident Response 23](#_Toc99111812)

[8.2.14 External Removable Media 23](#_Toc99111813)

[8.3 System and Information Integrity 23](#_Toc99111814)

[8.3.1 System Hardening 24](#_Toc99111815)

[8.3.2 System Clock 24](#_Toc99111816)

[8.3.3 System Defaults 24](#_Toc99111817)

[8.3.4 End Point Protection 24](#_Toc99111818)

[8.3.5 Backup Protection. 24](#_Toc99111819)

[8.3.6 Defect Remediation / Root Cause Analysis 25](#_Toc99111820)

[8.3.7 Security Monitoring Tools and Techniques 25](#_Toc99111821)

[8.3.8 Protective Monitoring Facilities 25](#_Toc99111822)

[8.3.9 Anomalous Activity 25](#_Toc99111823)

[8.3.10 Deviation from Configuration 26](#_Toc99111824)

[8.3.11 Alerts and Advisories 26](#_Toc99111825)

[8.3.12 Security Function Verification 26](#_Toc99111826)

[8.3.13 Software and Information Integrity 26](#_Toc99111827)

[8.3.14 Unused components 26](#_Toc99111828)

[8.4 Information Security Management System (ISMS) 27](#_Toc99111829)

[8.4.1 Security Planning 27](#_Toc99111830)

[8.4.2 ISMS Update: 27](#_Toc99111831)

[8.4.3 Security Documentation (Standards / Patterns) 27](#_Toc99111832)

[8.4.4 Information security policy 28](#_Toc99111833)

[8.5 Identity and Access Control (IDaC) 28](#_Toc99111834)

[8.5.1 Policy and Procedures 28](#_Toc99111835)

[8.5.2 Identification and Authentication 28](#_Toc99111836)

[8.5.3 Management connectivity 28](#_Toc99111837)

[8.5.4 Manage User Identifiers: 29](#_Toc99111838)

[8.5.5 Authentication Management 29](#_Toc99111839)

[8.5.6 Encryption 29](#_Toc99111840)

[8.5.7 Public Key Infrastructure (PKI) 29](#_Toc99111841)

[8.5.8 Account Management 30](#_Toc99111842)

[8.5.9 Access Enforcement 30](#_Toc99111843)

[8.5.10 Separation of Duties 30](#_Toc99111844)

[8.5.11 RBAC / Least Privilege 30](#_Toc99111845)

[8.5.12 Unsuccessful Login Attempts 30](#_Toc99111846)

[8.5.13 System Use Notification 31](#_Toc99111847)

[8.5.14 Concurrent Session Control 31](#_Toc99111848)

[8.5.15 Session Lock 31](#_Toc99111849)

[8.5.16 Session Termination 31](#_Toc99111850)

[8.5.17 Supervise and Review 31](#_Toc99111851)

[8.5.18 Permitted Actions 31](#_Toc99111852)

[8.5.19 Automated Marking 31](#_Toc99111853)

[8.5.20 Remote Access 32](#_Toc99111854)

[8.5.21 Secure Device 32](#_Toc99111855)

[8.5.22 Wireless 32](#_Toc99111856)

[8.5.23 Portable and Mobile Devices 32](#_Toc99111857)

[8.5.24 Personally Owned Systems 32](#_Toc99111858)

[8.6 Audit and Accountability 32](#_Toc99111859)

[8.6.1 Policy and Procedures 32](#_Toc99111860)

[8.6.2 System Management Audit 33](#_Toc99111861)

[8.6.3 Content of Audit Records 33](#_Toc99111862)

[8.6.4 Storage Capacity and Retention 33](#_Toc99111863)

[8.6.5 Processing, Monitoring, Analysis, and Reporting 33](#_Toc99111864)

[8.6.6 Reduction and Report Generation 34](#_Toc99111865)

[8.6.7 Date/Time Formats 34](#_Toc99111866)

[8.6.8 Protection of Audit Records 34](#_Toc99111867)

[8.7 External interface and Communications Protection 34](#_Toc99111868)

[8.7.1 Policy and Procedures 34](#_Toc99111869)

[8.7.2 Application Partitioning 34](#_Toc99111870)

[8.7.3 Security Function Isolation 34](#_Toc99111871)

[8.7.4 Resource-Priority 35](#_Toc99111872)

[8.7.5 Unauthorised Connections 35](#_Toc99111873)

[8.7.6 Unauthorised Network Services 35](#_Toc99111874)

[8.7.7 Boundary Protection 35](#_Toc99111875)

[8.7.8 Transmission Integrity 36](#_Toc99111876)

[8.7.9 Transmission Confidentiality 36](#_Toc99111877)

[8.7.10 Network Disconnect 36](#_Toc99111878)

[8.7.11 Cryptography 36](#_Toc99111879)

[8.7.12 Message signing 36](#_Toc99111880)

[8.7.13 Public Access Protections 36](#_Toc99111881)

[8.7.14 Collaborative Computing 37](#_Toc99111882)

[8.8 Contingency Planning 37](#_Toc99111883)

[8.8.1 Policy and Procedures 37](#_Toc99111884)

[8.8.2 Contingency Plan 37](#_Toc99111885)

[8.8.3 Training 37](#_Toc99111886)

[8.8.4 Testing 37](#_Toc99111887)

[8.8.5 Plan Updates 38](#_Toc99111888)

[8.8.6 Alternate Sites 38](#_Toc99111889)

[8.8.7 ISP Services 38](#_Toc99111890)

[8.8.8 Backup, Recovery, and Reconstitution 38](#_Toc99111891)

[8.8.9 Failure scenarios 39](#_Toc99111892)

[8.9 Maintenance 39](#_Toc99111893)

[8.9.1 Policy and Procedures 39](#_Toc99111894)

[8.9.2 Periodic Maintenance 39](#_Toc99111895)

[8.9.3 Remote Maintenance 40](#_Toc99111896)

[8.9.4 Maintenance Personnel 40](#_Toc99111897)

[8.9.5 Timely Maintenance 40](#_Toc99111898)

[8.10 Personnel Security 40](#_Toc99111899)

[8.10.1 Policy and Procedures 40](#_Toc99111900)

[8.10.2 Position Categorisation 41](#_Toc99111901)

[8.10.3 Service Personnel 41](#_Toc99111902)

[8.10.4 Personnel Screening 41](#_Toc99111903)

[8.10.5 Changes in Personnel 41](#_Toc99111904)

[8.10.6 Access Agreements 42](#_Toc99111905)

[8.10.7 Third-Party Personnel 42](#_Toc99111906)

[8.10.8 Personnel Sanctions 42](#_Toc99111907)

[8.11 Certification and Accreditation 42](#_Toc99111908)

[8.11.1 ISO27001 42](#_Toc99111909)

[8.11.2 Policy and Procedures 42](#_Toc99111910)

[8.11.3 Security Assessments 42](#_Toc99111911)

[8.11.4 NCSC CHECK Assessments (Penetration Testing) 42](#_Toc99111912)

[8.11.5 Vulnerability Assessments 43](#_Toc99111913)

[8.11.6 Security Patching 43](#_Toc99111914)

[8.11.7 Connectivity to the DIP 44](#_Toc99111915)

[8.11.8 Certification and Accreditation 44](#_Toc99111916)

[8.11.9 Plan of Action (POA) 44](#_Toc99111917)

[8.11.10 Continuous Monitoring 44](#_Toc99111918)

[8.12 Awareness and Training 44](#_Toc99111919)

[8.12.1 Policy and Procedures 44](#_Toc99111920)

[8.12.2 Security Awareness Training 44](#_Toc99111921)

[8.12.3 Security Training and Records 44](#_Toc99111922)

[8.12.4 Lessons Learned 45](#_Toc99111923)

[9 Reports, Dashboards and KPIs 45](#_Toc99111924)

[Appendix A – End to end security requirements 46](#_Toc99111925)

[Appendix B – PKI Certificate Services. 46](#_Toc99111926)

[Appendix C – Failure scenarios (Examples) 46](#_Toc99111927)

[Appendix D – OFGEM DPIA 46](#_Toc99111928)

## Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Detail |
| 10 November 2021 | KG | 0.1 | Initial draft |
| 28 January 2022 | KG | 0.2 | Updated based on feedback from peer review. |
| 16 February 2022 | KG | 0.3 | Updated post first review with procurement |
| 17 February 2022 | KG | 0.4 | Updated post first review with SDWG |
| 20 February 2022 | KG | 0.5 | Updated formatting, added section 8.2.14. |
| 4 March 2022 | KG | 0.6 | Added section 8.2.14, added Appendix B & C |
| 23 March 2022 | KG | 0.7 | Updated post review with LDP |
| 25 March 2022 | KG | 1.0 | Set to version 1.0 |
| 6th May 2022 | KG | 1.1 | Updated based on bidders feedback |
| 10th May 2022 | KG | 1.2 | Updated based on bidders feedback |
| 14th September 2022 | KG | 1.3 | Removed references to message encryption |
| 3rd November 2022 | KG | 1.4 | Updated post SDWG Assurance Forum |

## Reviewers

|  |  |
| --- | --- |
| Reviewer | Role |
| Robert Golding | Solution architect |
| Ian Smith | Design manager |
| SDWG | Security Design Working Group |

## References

|  |  |  |  |
| --- | --- | --- | --- |
| Document/Link | Publisher | Published | Additional Information |
| E2E Security requirements | DCC | 03/05/201 |  |
| NCSC Cloud Principles | NCSC | Current version as of December 2021 | [Implementing the Cloud Security Principles - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles) |
| Cyber Assessment Framework | NCSC | CAF v3.0 | [Cyber Assessment Framework - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework) |
| Data Best Practice  Supporting Information v0.3 | Proposed Version May 2021 |  | <https://www.ofgem.gov.uk/sites/default/files/docs/2021/05/data_best_practice_supporting_information_v0.3_0.pdf> |
| MHHS DIP003 - End to End Security Architecture | MHHS | v1.0 |  |
| MHHS DIP001 - Functional specification | MHHS | v1.0 |  |
| MHHS DIP004 - Cyber Security Connection Guidance | MHHS | v1.2 |  |

## Terminology

|  |  |
| --- | --- |
| Term | Description |
| CAF | Cyber assessment framework (currently v3.0) |
| DIP | Data integration platform |
| DPIA | Data Protection Impact Assessment |
| EDA | Event-Driven Architecture |
| ESO | Enduring Service Owner |
| FIM | File Integrity Monitoring |
| FIPS | Federal Information Processing Standards |
| HIDS | Host-Based Intrusion Detection |
| IGP | Indicators of Good Practice |
| ISO | Information Security Officer |
| ISP | Internet Service Provider |
| IT | Information Technology |
| MHHS | Market Wide Half Hourly Settlement |
| NCSC | National Cyber Security Centre |
| NISR | Network and Information Systems Regulation |
| NIST | National Institute of Standards and Technology |
| SpaR | Security, Privacy and Risk |
| ISMS | Information Security Management System |
| UEBA | User and Entity Behaviour Analytics |
| XDR | Extended Threat Detection and Response |

A full glossary of all terms used can be found here:

<https://mhhsprogramme.sharepoint.com/sites/Market-wideHalfHourlySettlement/SitePages/Programme-Glossary1.aspx>

# Background

At the core of this architecture is the Data Integration Platform (DIP), responsible for brokering the communication between all industry participants operating under the TOM. The working assumption is that the DIP will be a cloud-hosted, serverless/containerised, compute/messaging system that will leverage the benefits of distributed cloud architectures to achieve the resilience, availability, security, and scalability required.

# Introduction

## Purpose

This document was developed to identify the security requirements for all data services of the new DIP, the interfaces between Market Participants and the organisations developing, operating and using those systems and interfaces, along with connectivity requirements for service providers and third parties.

The document was created during the early phases of the MHHS Programme to describe security objectives for the DIP and the systems and services participating in the DIP. Consequently, the information relied upon in this document was necessarily conceptual and focused on alignment with Good Industry Practice.

This security requirements document supports the MHHS Programme's requirement for a solution neutral position, which does not influence the shape of Request for Proposal responses or constrain innovation. As a result, the security requirements document aims to not unduly influence, or constrain, the solution towards a specific technology or architecture.

The Security Requirements are to:

Describe functional and non-functional and derived requirements that need to be satisfied to achieve the security objectives for the DIP.

Provide pertinent information for Security Architects and Solution Architects to ensure that security requirements are included in the design of solution and security architecture documents.

Show traceability between security risks and controls in concert with the Business Attributes defined in the End to End Security Architecture.

The security requirements are described in this Word document, and a summary can be found in the End to End Security Requirements spreadsheet in Appendix A.

Some of the key points to note are as follows:

In this document, security requirements equate with demonstrating compliance with a recognised industry security standard. ISO/IEC 27001 and consideration given to NCSC CAF, NCSC Cloud Security Principles, CIS and NIST Cyber Security Framework.

For the purpose of this document, it is assumed that Market Participants will already have undertaken a risk assessment as part of the on-boarding process under the relevant code body (SECAS, REC code, BSC code)

Where Market Participants choose to use a third party for connectivity to the DIP (DIP Connection Providers), The DIP connection providers will be required to register with the BSCCo and will be responsible for their own security requirements. (See MHHS-DES004 - Cyber Security Connection Guidance for further details)

The consumption data, MPAN and any PII is considered to be personal data and therefore covered by GDPR.

The DIP must have an application-level means with heuristic capability of detecting Threshold Anomalies with respect of the security of the DIP and of presenting warnings and/or preventing these anomalies...

Data in transit between systems in the DIP Solution must be encrypted at the transport level and all messages digitally signed.

Unauthorised access or attempted unauthorised access must be detected by the systems.

Implementation of an Information Security Management System.

## Scope

The components within scope can be broadly categorised as follows:

Systems/services:

* + Service providers / third parties
  + Cloud infrastructure
  + Communications (ISP)
  + Market Participants connections

Interfaces:

* + Between Market Participants (Publishers) and the DIP;
  + Between the DIP and Market Participants (Consumers)
  + Between the DIP and service providers / third parties.

## Logical overview

The following diagrams are for illustration purposes and serve only to provide visual context of the new DIP:

* Components of the new DIP – Figure 1
* Service Orientated View of the new DIP – Figure 2
* Connectivity to the DIP – Figure 3



Figure 1 – Components of the new DIP



Figure 2 - Service Orientated View of the new DIP

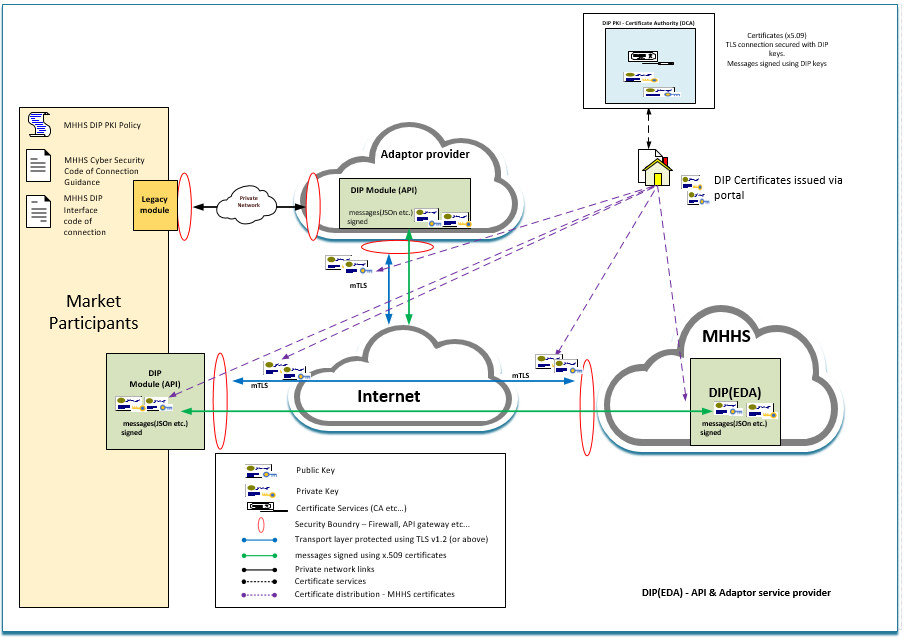


Figure 3 – Connectivity to the DIP

# Programme Oversight

The following section 4.1 and 4.2 are for information purposes only and serve to highlight the structure that the DIP service provider will need to be familiar with.

## Design Authority Group (DAG)

The MHHS DAG’s role is to oversee, review, consult and approve, the MHHS Programme development of the end-to-end business processes, system, security and data architecture that delivers the detailed system design that enables all programme participants to design, build and test their individual system and business changes.

The purpose of the DAG is to provide advice and oversight for the Security Design Working Group.

## Security Design Working Group (SDWG)

The purpose of the SDWG is to manage the development of the security architecture and artefacts, maintain compliance with regulatory standards, and ensure adequate performance of the cyber security program at DAG.

The SDWG supports action and coordination of the cyber security program policy, technical, and operational activities. The SDWG is charged with:

Advising the DAG on cyber security issues and implement their decisions, agree upon DIP implementation patterns for cyber security, and ensure that cyber security is tailored to the needs of the industry

Provide strategic and tactical direction and support, and serve as architects of the DIP cyber security program.

Meet monthly, at a minimum, to develop cyber security program approaches and initiatives, monitor progress, schedule and performance, and address current and evolving cyber security issues.

Develop and monitor the implementation of prioritised plans of actions linked to resources and implementation schedules for the DIP cyber security program.

Enable threat mitigation best practices, incident reporting and analysis, and information sharing across the DIP and Market Participants.

Integrate and institutionalise the cyber security program with aligned resource planning and architectural processes and artefacts.

Ensure that contractors and other interconnected organisations and entities implement adequate controls to safeguard the DIP, including Market Participants.

# Determining the Security Requirements

Continuous improvement of security will help ensure the DIP is resilient and able to avoid disruption through a cyber-attack that could have a severe impact on the MHHS settlements systems.

## Security Requirements for Market Participants

At a high level, the requirements that Market Participants must achieve to use the DIP can be broken down into two specific areas:

Compliance with requirements of that will be set as obligations by what is expected to be the BSC Code

Meeting the Code of Connection (CoCo) that will be defined during the design phase.

## Security Requirements for an Interface

The security requirements for an interface apply to the physical connection, the transport layer and the application layer of the network itself as well as the access to the network from the systems at either end. The detailed requirements for each interface will be defined in the Code of Connection which will be developed during the design phase.

## Security Requirements for the system.

The detailed security requirements for the DIP systems (Instances) can be found in section 8.

## Enrolment Requirements

To participate in the DIP, the DIP Service Provider must:

Have utilised an industry recognised information risk management framework such as ISO/IEC 27005: 2011.

Show compliance with aspects of the chosen information risk management framework (ISO/IEC 31000:2018 standard) that are relevant to the DIP Programme.

Have conducted a Data Protection Impact Assessment (DPIA) and an Information Risk Assessment (IRA) with respect to the data being held and processed, with security controls being implemented accordingly.

## DIP Security requirements

The security requirements for the DIP fall into the following categories and are described in detail in this document. A spreadsheet containing a summary of the security requirements can be found in Appendix A - End to End security requirements. (This can be provided in alternative formats if required)

Secure development

Governance

Risk Assessment;

Data Protection;

Systems and information integrity

Information Security Management System (ISMS)

Identity and access control

Audit and accountability

External interface and communications Protection

Contingency planning

Maintenance

Personnel security

Certification and accreditation

Awareness and Training

# Secure Code Development

System Development Lifecycle means, in relation to any System, the whole of the life of that System from its initial concept to ultimate disposal, including the stages of development, specification, design, build, testing, implementation, maintenance, modification and decommissioning.

The DIP Service Provider shall ensure,

1. At each stage of the System Development Lifecycle, the DIP service provider designs and operates the solution so as to protect it from being compromised.
2. All code is developed securely in-line with industry best practice regarding secure code development (OWASP, CERT, Microsoft SDL)
3. Detect security defects early in development via the use of secure code analysis (SAST) / software composition analysis (SCA).
4. Infrastructure-as-code (IaC) is used for secure deployment where applicable.
5. Undertake penetration testing of the systems prior to operational running.

## Developer Security Testing

The DIP Service Provider shall;

1. Create a security test and evaluation plan.
2. The security test and evaluation plan must be executed, at a minimum, on an annual basis.
3. Prior to operational running
4. The results of the plan need to be used in support of the certification and assurance process.

## Secure Code Scanning

The DIP Service Provider shall ensure that they perform secure code scanning reviews as part of the software development life cycle to ensure they are effectively identifying potential issues within the code.

# Security Governance

## NCSC CAF

The full set of NCSC CAF Technology objectives identified by the AWG that are applicable to the solution are listed in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **NCSC CAF Objective** | **Category** | **Section** | **Applicable to Service Provider** |
| A.1 Governance | Process & People | 7 | Yes |
| A.2 Risk Management | Process | 8.1 | Yes |
| A.3 Asset Management | Technology & Process | 8.2.11 | Yes |
| A.4 Supply Chain | Process & People | 7.8 | Yes |
| B.1 Service Protection Policies & Processes | Technology | 8.4 | Yes |
| B.2 Identity & Access Control | Technology | 8.5 | Yes |
| B.3 Data Security | Technology | 8.2 | Yes |
| B.4 System Security | Technology | 8 | Yes |
| B.5 Resilient Networks & Systems | Technology | 8.8 | Yes |
| B.6 Staff Awareness & Training | People | 8.12 | Yes |
| C.1 Security Monitoring | Technology | 8.3, 8.11.10 | Yes |
| C.2 Proactive Security Event Discovery | Technology | 8.3.8 | Yes |
| D.1 Response & Recovery Planning | Technology, Process, People | 8.8 | Yes |
| D.2 Lessons Learned | Process & People | 8.12.4 | Yes |

Table 1 – NSCS CAF v3.0

***Link to descriptions:***

<https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework>

## NCSC Cloud Security Guidance

If the solution architecture is constrained or dependant on cloud components then the following principles should be included. The AWG recommendation on principles in scope of the DIP are listed in the table below.

|  |  |  |
| --- | --- | --- |
| NCSC Cloud Security Principle | See Section | Applicable to Service Provider |
| 1. Data in Transit Protection | 8.7.8 | Yes |
| 2. Asset Protection & Resilience | 8.8 | Yes |
| 3. Separation between Users | 8.5 | Yes |
| 4. Governance Framework | 7 | Yes |
| 5. Operational Security | 8 | Yes |
| 6. Personnel Security | 8.10 | Yes |
| 7. Secure Development | 7.11, 7.12 | Yes |
| 8. Supply Chain Security | 7.8 | Yes |
| 9. Secure User Management | 8.5 | Yes |
| 10. Identity & Authentication | 8.5 | Yes |
| 11. External Interface Protection | 8.7 | Yes |
| 12. Secure Service Administration | 8.5 | Yes |
| 13. Audit Information for Users | 8.6 | Yes |
| 14. Secure Use of Service | 8.5 | Yes |

Table 2 – NCSC Cloud Principles

## Security Design Principles

The DIP Service Provider shall follow the NCSC secure by design principles;

***Establish the context:*** The business process mapping will define the scope and data used in the DIP. SPaR will be used (as recommended by the AWG) to identify the Security, Privacy and Risk impact of each business process. Where required a DPIA will be completed.

***Making compromise difficult:*** The DIP will follow a defence in depth approach of leveraging a series of layered, redundant defensive measures to protect sensitive data following industry best practice. (NCSC cloud security principles, NIST, CIS etc.)

***Make disruption difficult:*** the DIP will be designed to an acceptable level of disruption, using multiple layers of redundancy with resilient regions, zones, compute, network paths, storage arrays, online and offline backups. With additional emphasis on the management systems necessary to administer the DIP.

***Make compromise detection easier:*** The design of the DIP will ensure the management infrastructure can be queried at each layer of the stack and the relevant logs are sent to a central log collection and analysis platform for incident detection and investigation.

***Reduce the impact of compromise:*** The DIP will be designed to make the best use of replication, snapshots, and high availability to speed system recovery (Giving cloud-based systems an edge over traditional infrastructure).

***Risk management:*** A robust risk process will be established to identify the risks posed to the DIP when connecting Market participants. Guidance will be provided as to the minimum security requirements the Market Participant must meet in order to be connected to the DIP.

## Compliance

The DIP Service Provider shall demonstrate compliance with the security requirements at specific points in the Programme by undergoing an audit of key controls and making its results available to the MHHS Programme Team for assurance purposes. This must be done:

Prior to participating in testing

Prior to operating the production system; and

Once per year when in live operation.

## DIP Alignment with SPaR

SPaR is a framework recommended by OFGEM. Each architectural component that describes data in transit and data at rest. The data should be assessed to determine which of the following Impact Types are applicable and then in addition, to what risk level.

### Security, Privacy and Risk Impact Guidance

The following data assessment was provided by the AWG.

|  |  |  |
| --- | --- | --- |
| Impact  Type | Risk Impact Levels: | Applicable to  The DIP |
| Public  Confidence | 1: Likely to reduce an individual citizen’s perception of that service | Yes |
| 2: Likely to reduce the perception of that service by many citizens | Yes |
| 3: Likely to result in undermined confidence in the service provider generally | Yes |
| 4: Likely to result in undermined confidence in the service at a national level | No |
| 5: May lead to a loss of public trust in the service severe enough to cause a noticeable drop in citizens using DGE services through mistrust, with consequent risk to life | No |
| 6: May lead to a loss of public trust in the service severe enough to cause a noticeable drop in citizens using DGE services through mistrust, with consequent risk to life | No |
| Public  Privacy | 1: Loss of control of a citizen’s personal contact information | No |
| 2: Loss of control of a citizen’s personal identifiable data | Yes |
| 3: Loss of control of a citizen’s personal data | Yes |
| 4: Loss of control of a large group of citizens’ personal data | Yes |
| 5: Loss of control of citizens’ personal data nationally | Yes |
| 6: Complete loss of control of citizens’ personal data | No |
| Public  Finance | 1: Minor loss of money for an individual, no more than an individual annoyance | Yes |
| 2: Major financial loss for an individual, but not involving any financial hardship, or minor loss for a small group of individuals | Yes |
| 3: Significant loss of income for an individual, such that it has a short-term impact on the individual’s way of life or causes some financial hardship | No |
| 4: Significant loss of income for a group of individuals that causes financial hardship. Financially devastating for an individual for example personal bankruptcy and home repossession | No |
| 5: Financially devastating for a large group of individuals for example wide spread personal bankruptcy and repossession of homes | No |
| 6: Financial impacts are wide spread to the extent that major long-term damage is caused to the UK economy | No |
| Industry  Credibility | 1: Likely to reduce an individual company’s perception of a specific service provided | Yes |
| 2: Likely to reduce the perception of a specific service by several companies | Yes |
| 3: Likely to result in undermined confidence in the provided services generally | Yes |
| 4: Likely to result in undermined confidence in the service at a national level with some impact on market performance | No |

Table 3 - SPaR

## Privacy Classification

The DIP Service Provider shall hold a register of data classifications and review regularly with the Enduring Service Owner. (At least annually)

|  |  |  |
| --- | --- | --- |
| Type | Category | Description |
| Information  Security  Classification | Restricted | For information that is confidential to a group of individuals. |
| Confidential | For information not Restricted but which should not be shared outside of a named process or organisation unit. |
| Commercial in Confidence | For information that may be shared with commercial partners. |
| Public | For all other information. |
| GDPR | PII  (personally identifying information) | As defined by the UK DPA 2018 and GDPR, all PII data items shall be classified as:  Restricted  Confidential  Commercial in Confidence    Each data item must be identified and/or tagged (i.e. within a catalogue) to indicate it falls within the definition of PII. |

Table 4 – Privacy Classifications

Note: Please refer to the Information Commissioners Office for the definition of PII classification.

[https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/key-definitions/what-is-personal-data/](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/)

Note: Privacy Classification as a security guideline meets the existing NCSC objectives:

CAF B.3a – Data Security

Cloud Security Principle 2 – Asset Protection and Resilience

## GDPR

The DIP service provider shall be responsible for the role of Data Protection Office for the DIP and shall undertake the required Data Protection Impact Assessment (DPIA) and Privacy Impact Assessment (PIA).

The DIP service provider shall define their role as DPO as either Data Controller/Processor as identified in the DPIA for all identified PII, MPaN and consumption data for those systems which hold this data.

The DIP Service Provider shall ensure compliance with general data protection regulation (GDPR)

The DIP Service Provider(s) contracts will define the GDPR contractual obligations.

See Appendix D for further detail on the OFGEM DPIA for MHHS.

### Privacy Impact Assessment

The DIP Service Provider shall ensure that a Data Protection Privacy Impact Assessment must be carried out in order to assess privacy risks related to Personal Data

## Supply chain

The DIP Service Provider shall ensure where service providers / 3rd party personnel have access to the DIP and its associated data and systems, there needs to be a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service providers / 3rd parties and must meet the requirements set out in the NCSC CAF section A4.a Supply Chain.

## Rules of Behaviour

The DIP Service Provider will make readily available to all Market Participants a set of rules that describes:

1. Responsibilities and expected behaviour with regard to DIP system usage

The DIP Service Provider receives signed acknowledgement from Market participants indicating they have:

Read

Understand, and;

Agree to abide by the rules of behaviour, including consent to monitoring, before authorising access to the DIP.

Link to descriptions:

[https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloudsecurity-principles](https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles)

## Outsourced Security Services

The DIP Service Provider shall ensure monitoring of security control compliance from outsourced services and any third-party providers of security services employ adequate security controls in accordance with:

Directives, policies, regulations, standards, guidance, and established service level agreements.

Where the DIP service provider relies on third parties to provide security services; the DIP service provider remains responsible for ensuring the security of the DIPs systems and information by overseeing the effectiveness of the services provided by the outsourced security services provider.

# Operational Security controls

## Risk Assessment

### Risk Management

The DIP service provider will follow a risk management approach composed of four distinct areas:

1. Assessment
2. Mitigation
3. Evaluation
4. Continuous assessment

Each area of the DIP Risk Management approach requires a cost-effective structured process for:

1. Identifying
2. Analysing; and
3. Reducing the potential impact of risk events

The DIP service provider must ensure that all systems are assured by the Enduring Service Owner and any risk assessment activities must be completed prior to any system becoming operational.

### Risk Management Process

The DIP service provider will follow a Risk management approach that is applicable to all systems regardless of their stage in the system life cycle.

A uniform risk management process permits the DIP service provider to:

1. Effectively secure the DIP and all assets.
2. Make informed risk management decisions and focus on mitigating current risk factors
3. Ensure interoperability and portability
4. Understand total operational and residual risk.

This approach includes:

1. Identifying system and environmental threats and vulnerabilities
2. Documenting decisions on the adequacy and maintenance of security controls
3. Determining cost implications of enhanced protection
4. Accepting residual risk
5. Providing continuous monitoring of the system and environment to ensure that controls are performing as required and changes in cloud computing and/or operations do not have an adverse impact on the system.

### Risk Analysis

The DIP service provider will be responsible for conducting risk management analysis including:

Risk Assessment:

1. Identify and describe all systems connecting to the DIP.
2. Assess threats, vulnerabilities, likelihood of adverse actions, and potential consequences
3. Quantify the level(s) of risk based on the assessment
4. Develop a set of security controls based on the level(s) of risk
5. Document decisions made during the assessment

Risk Mitigation:

1. Evaluate security controls and select those that provide the greatest level of risk reduction at the lowest cost
2. Identify appropriate security controls and assign responsibility to those individuals who will implement and maintain those controls
3. Implement security controls and document the implementation to provide input to the configuration baseline.

Evaluation and Assessment:

1. The first two activities (risk assessment and risk mitigation) are properly documented and reflected in the system baseline
2. Security controls are implemented

Continuous Assessment

1. Perform ongoing assessments and analysis of the effectiveness of the DIP security controls
2. Provide ongoing reports on the security posture of the DIP systems
3. Support risk management decisions to help maintain risk tolerance at acceptable levels

### Risk Assessment Activities

The DIP service provider must conduct risk assessment activities;

1. Prior to operational running.
2. On at least an annual basis.
3. On any occasion on which it implements a material change to the solution; and
4. On the occurrence of any Major Security Incident in relation to the solution.

## Data Protection

### Data Residency

The DIP Service Provider shall ensure the DIP is hosted, operated and maintained from within the United Kingdom.

### Data Hosting

Data hosting to be provided from a public cloud provider (Azure, AWS, GCP etc.) from within the UK.

### Data Environments

The DIP Service Provider shall ensure Production systems shall be separated from those systems used for testing, training and development.

Production data should not be used in non-production environments

1. Non production environments should only be populated with synthetic “test” data.
2. Unless programme exception is granted by the ESO.

### Data Ownership

The DIP Service Provider shall ensure Data owners/stewards are clearly identified, and be responsible for the security of the data within the system

The DIP Service Provider shall ensure that data owners must be clearly identified, and be responsible for the security of the data within the system

### Data Confidentiality and Integrity

The DIP Service Provider shall ensure data confidentiality mechanisms are used to protect sensitive data from inspection by unauthorised entities. The DIP Service Provider shall ensure data is protected using approved FIPS140-2 compliant encryption algorithms for the following:

1. All data traveling over the Internet or other public network
2. All sensitive data being processed through the DIP; that should not be viewed by MHHS, Service Providers or third party personnel who have access to the DIP system resources; i.e. Cloud engineers, network operations personnel or system administrators.
3. If sensitive data is being stored, it should be secured with a level of encryption which is aligned to NCSC guidance.

### Data at Rest

The DIP Service Provider shall ensure All sensitive data being stored, is secured with a level of encryption which is aligned to NCSC guidance, and ensure

1. Archived messages must be marked as immutable.
2. All information stored on systems with, file system, network share, application, or database-specific access are protected with control lists.
3. Controls enforce the principle that only authorised individuals should have access to the information based on their need to access the information as a part of their responsibilities.

### Data Loss Prevention

The DIP Service Provider shall ensure sufficient data loss protection mechanisms are in place to detect any instance of data leaving it by any means, including (but not limited to) network transfers and the use of removable media without authorisation.

1. Sufficient data protection is required to ensure the system is capable of detecting any instance of data leaving it by any means.
2. Including (but not limited to) network transfers and the use of removable media without authorisation.

### NDA

In accordance with the data classification scheme, sensitive Information shared with third parties must be subject to a Non-Disclosure Agreement

### Non-repudiation

The DIP Service Provider shall ensure the DIP can provide proof of the origin of messages and of the integrity of message data content.

### Data Retention and Removal

The DIP Service Provider shall ensure that in accordance with the Data Retention Policy, any Data no longer required, is securely deleted in accordance with NCSC guidance.

### Asset Management

The DIP Service Provider shall ensure that an Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the DIP Service Provider to establish and maintain a register of the physical, virtual and information assets on which it relies for the purposes of the Authorised Business (including a record of the member of Personnel who has responsibility for each such asset).

### Configuration Management

The DIP Service Provider shall ensure they follow a recognised configuration management process consisting of:

1. Identifying and controlling assets (including a record of the member of Personnel who has responsibility for each such asset).
2. An asset register which defines all DIP resources and information assets along with a maintenance inventory.
3. Connectivity information (APIs, Policy enforcement device etc.)
4. Equipment type or software release versions
5. the System is capable of identifying any deviation from its expected configuration; and

i) any such identified deviation is rectified; and

ii) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of the solution.

The DIP Service Provider shall, provide the capability and procedures to control the assets and resources by Initialising, operating, reconfiguring, and shutting down cloud resources from a centralised network management workstation. The functional capabilities include the following (but not limited to):

1. Bootstrap.
2. Performing software verification checks of resource entities;
3. Supporting deployment of new software and resources in the DIP
4. Supporting connectivity provisioning;
5. Providing database administration; and
6. Maintaining software, and firmware inventory.

### Incident Response

The DIP Service Provider shall ensure the DIP continues to operate with the ability to detect, analyse, contain, respond to, and recover from events that could have a negative impact on the DIP. Those events, referred to as incidents, include the introduction of malicious code such as Ransomware into the DIP, network-based attacks aimed at denying or degrading the DIP service, and incidents of unauthorised access or unauthorised usage. The DIP Service Provider is responsible for managing the DIP-wide incident reporting and response. Part of that capability is a Security Incident and Advisory function, which provides warnings, analysis, and assistance to Market Participants regarding security incidents. The DIP Service Provider uses the Security Incident Response Plan, to provide the incident detection and response capabilities mentioned above.

The DIP Service Provider has the ability to gather and analyse data from:

1. All DIP resources
2. Physical/Virtual resources such as (but not limited to), firewalls, API gateways, IPS, switches.
3. Contracted service providers, such as ISPs.
4. The DIP Service Provider also reports on incidents as outlined in the ISMS.

All service contracts, such as one’s between the DIP Service Provider and an ISP, have contract language to ensure: Event data can be exchanged between the service provider and the DIP. Course of action in the event of service disruption or cessation by the provider.

### External Removable Media

The DIP Service Provider shall ensure systems are configured not to write data to external removable media.

## System and Information Integrity

### System Hardening

The DIP Service Provider shall propose a suitable recognised standard such as NIST/CIS to adhere to, and provide rationale for the choice, ensuring all assets are hardened in accordance with the standard and documented in the ISMS.

### System Clock

The DIP Service Provider shall ensure all system clocks within the solution are connected to a common, reliable and suitable time source.

1. All network devices MUST be synchronised to the same network clock by using Network Time Protocol (NTP) to enable accurate and effective event correlation.

### System Defaults

The DIP Service Provider shall ensure they DO not use vendor-supplied defaults and removes all unnecessary accounts before activating the system on the network.

1. This applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, application and systems accounts, SNMP community strings etc.

### End Point Protection

The DIP service provider shall ensure that dependent on chosen architectural pattern, the solution shall be designed to protect against malware, ransomware, zero day threats and includes at a minimum:

1. on-access scanning
2. daily scheduled scan
3. daily signature updates (with critical updates immediately when required)
4. anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or
   1. deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

DIP service provider personnel that are permitted to gain access to the DIP through the use of remote access must have the appropriate:

1. Software Firewalls Enabled.
2. Anti-Virus Software Enabled and signatures are up-to-date.
3. Anti-Spyware Software Enabled and signatures are up-to-date.

### Backup Protection.

Where the DIP Service Provider carries out a backup, they shall ensure that the data which is backed-up:

1. Contains all system data and is automatically backed up on a regular basis.
2. Contains all of the organisation's key systems and are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
3. Is protected in accordance with the Information Classification Scheme, including when being transmitted for the purposes of Back-Up; and
4. Is stored on media that are located in physically secure facilities, at least one of which facilities must be in a different location.

### Defect Remediation / Root Cause Analysis

The purpose for defect remediation is to efficiently identify and correct defects and share information on defects identified within the Security Incident Capability.

The DIP Service Provider shall:

1. Centrally manage the defect remediation process and install updates automatically without individual user intervention.
2. Employ automated mechanisms too periodically and, upon command, determine the state of system components with regard to defect remediation.

### Security Monitoring Tools and Techniques

The DIP Service Provider shall ensure Internet access points have a network-based intrusion detection systems and require all Internet-accessible Cloud computing resources to have an IPS, host-based intrusion detection / prevention in place and functioning and

1. Connect all individual intrusion detection / prevention tools into a system-wide intrusion detection system using common protocols.
2. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
3. Employ automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks.
4. All security tools are kept up to date.

### Protective Monitoring Facilities

The DIP Service Provider shall detect malicious activity affecting, or with the potential to affect, the operation of the DIP even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable) and;

The DIP Service Provider shall ensure,

1. All systems are protectively monitored in accordance with NCSC guidance
2. They fully understand which systems should and should not communicate and when
3. They routinely search for system abnormalities indicative of malicious activity in the DIP and systems supporting the DIP, generating alerts based on the results of such searches.
4. The protective monitoring solution records all system activity (including all attempts to access resources, or Data held, on it) in audit logs;
5. The protective monitoring solution detects any attempt by any person to access resources, or Data held, on it without possessing the authorisation required to do so; and
6. That the incident response capability prevents any such attempt at unauthorised access.

### Anomalous Activity

The DIP Service Provider shall propose a suitable recognised standard such as the MITRE Att&ck framework to adhere to, and provide rationale for the choice, ensuring all assets are monitored in accordance with the standard and documented in the ISMS and;

The DIP Service Provider shall ensure that the System includes the capability to detect anomalous activity. Using appropriate combinations of static configuration, signature and heuristic-based methods, the system shall monitor:

1. Audit logs of each component of the System;
2. Error messages generated by each device which forms part of the solution;
3. Patterns of traffic over any interfaces
4. Large volumes of supplier switching activity

### Deviation from Configuration

The DIP Service Provider shall ensure that:

1. The System is capable of identifying any deviation from its expected configuration; and
2. Any such identified deviation is rectified; and
3. An up-to-date list of all hardware, software and firmware versions and patches, which form part of the configuration of the solution is documented in the ISMS.

### Alerts and Advisories

The DIP Service Provider shall receive security alerts/advisories for all system components of the DIP on a regular basis, and issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

1. The DIP Service provider must make security alerts and advisories available for all system components of the DIP as needed.

### Security Function Verification

The DIP Service Provider shall document security functionality controls in the ISMS. All information systems must verify the correct operation of security functions, either upon system start-up and restart, upon command by user with appropriate privilege, or at least quarterly;

1. All Cloud resources must notify the system administrator upon system shutdown or restart when anomalies are discovered.
2. Automated mechanisms are used to provide notification of failed security tests.
3. Employment of automated mechanisms to support management of distributed security testing.

### Software and Information Integrity

The DIP Service Provider shall detect and protect against unauthorised changes to software and information.

1. Enforce explicit rules governing the downloading and installation of external software by users.
2. Application whitelisting software must ensure that only authorised software libraries (such as \*.dll, \*.ocx, \*.so, etc.) are allowed to load into a system process.
3. If the solution detects any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and
4. Where any such software has been installed or executed, to take appropriate remedial action.

### Unused components

The DIP Service Provider shall ensure that:

1. Only components and services required for the operation of the DIP are enabled.
2. Any unused components are disabled or uninstalled

## Information Security Management System (ISMS)

The DIP Service Provider shall develop, implement and maintain an [Information Security Management System](https://www.isms.online/solutions/isms/) that demonstrates the approach to information security and privacy to address the threats around the DIPs information and related assets. The DIP SP will be ISO27001 cetified.

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update Security Planning policies, procedures, and practices that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Coordination among Market Participants
* Compliance

### Security Planning

The DIP Service Provider shall provide a plan which describes how the Information Security Management System shall be implemented and operated and:

1. Describes the security requirements for each system.
2. Describes the security controls in place for each system.
3. Describes the roles and responsibilities of who will review and approve the plan for each system.

### ISMS Update:

The DIP Service provider shall define and document procedures to review the ISMS, at least annually, and to revise the plan to address significant changes and problems identified during planning the implementation of security control assessments.

### Security Documentation (Standards / Patterns)

The DIP Service Provider shall develop, document and maintain within its ISMS the standards (patterns) for each system in the DIP.

The DIP Service Provider shall ensure that adequate documentation of the DIPs security systems and constituent components is available, protected when required, and distributed to authorized personnel.

1. Establish secure configurations for all device types
2. Establish secure configurations for all software and databases used in the DIP
3. Document the functional properties of the security controls employed within DIP with sufficient detail to permit analysis and testing of the controls is available.
4. Document the design and implementation details of the security controls with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components) is available.

### Information security policy

To be provided by Elexon

## Identity and Access Control (IDaC)

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update Identification and Authentication policies, procedures, and practices that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Coordination among Market Participants
* Compliance

The DIP Service Provider shall document within the ISMS the Authentication controls for all systems within the DIP and ensure;

1. Distinct user IDs that are unique to each user or group for user identification
2. A user authentication mechanism that is unique to each Market Participant for primary access to all system resources in the DIP.
3. Any associated equipment that relies on passwords as the means to authenticate users must implement effective password management.

### Identification and Authentication

The DIP Service Provider shall ensure each:

1. User is uniquely identified and authenticated (or processes acting on behalf of users) on all systems.
2. User has multi-factor authentication configured and enabled.
3. Device is Identified and Authenticated before establishing a connection.

### Management connectivity

The DIP Service Provider shall ensure all connectivity to the DIP for management purposes is secured and authenticated in accordance with NCSC guidelines.

1. Scan all devices remotely logging into the DIP network(s) prior to accessing DIP resources to ensure security policies have been enforced. (Defined in the ISMS for each device.)
2. All system management access must be over a secure channel.
3. All system management access requested must use multi-factor authentication.

### Manage User Identifiers:

The DIP Service Provider must ensure for each user identifier;

1. The user has been verified by the ESO
2. The user identifier is issued to the intended party
3. Identifiers are disabled after a reasonable period of inactivity.
4. Identifiers are archived once notified by the ESO to do so.

### Authentication Management

The DIP Service Provider shall manage system authenticators (Multi-factor authentication) by:

1. Defining initial authenticator content
2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators
3. Changing default authenticators upon system installation.
4. Electronic authentication methods to provide services to citizens must comply with NIST SP 800-63, Electronic Authentication Guideline.

### Encryption

The DIP Service Provider shall ensure all systems, requiring authentication, that the authentication credentials are encrypted using approved cryptographic technologies that are compliant with FIPS 140-2.

The DIP Service Provider shall ensure only standardised and extensively reviewed encryption algorithms are used.

### Public Key Infrastructure (PKI)

The DIP Service Provider shall ensure they develop and implement a certificate service, policy and certification practice statement for the issuance of public-key certificates used in the DIP and ensure certificates are based on the X.509 framework. With separate certificates used in each environment (UAT, Pre Production, Production etc.)

The PKI infrastructure provides:

1. Public key certificates
2. Certificate repository
3. Certificate revocation
4. Key backup and recovery
5. Support for non-repudiation of digital signatures
6. Automatic update of key pairs and certificates
7. Management of key histories
8. Support for cross-certification
9. Client-side software interacting with all of the above in a secure, consistent, and trustworthy manner.

Further detail on the PKI requirements of the DIP can be found in Appendix B – PKI Certificate services

### Account Management

The DIP Service Provider shall manage system accounts, including establishing, activating, modifying, reviewing, disabling, expiration date and removing accounts and document the procedures for managing the accounts and

1. Automatically terminate temporary and emergency accounts after a reasonable period as specified by the DIP Service Provider in its ISMS.
2. Automatically disable inactive accounts after a reasonable period as specified by the DIP Service Provider in its ISMS.

#### Privileged Accounts

The DIP Service Provider shall ensure,

1. Privileged accounts shall be dedicated to the Systems and must always be allocated to named administrators or systems
2. All privileged access must have multi-factor authentication enabled (administrator, audit, assessment accounts)
3. All users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

Consideration should be given to implementing Just In Time (JIT) access for privileged activities.

### Access Enforcement

The DIP Service Provider shall enforce assigned authorisations for controlling access to the system in accordance with applicable policy.

1. Access to security functions (deployed in Cloud, software, and firmware) is restricted to authorised personnel (e.g., security administrators).

### Separation of Duties

The DIP Service Provider shall enforce separation of duties through assigned access authorisations when accessing the DIP.

1. Groups of information services, users and information systems shall be appropriately segregated on different networks

### RBAC / Least Privilege

The DIP Service Provider shall enforce the most restrictive set of rights/privileges using Role-Based Access Controls (RBAC) by users when accessing the DIP.

### Unsuccessful Login Attempts

The DIP Service Provider shall document in the ISMS and enforce a limit of, 3, consecutive invalid access attempts by a user. The system will automatically lock the account/node until released by an administrator when the maximum number of 3 unsuccessful attempts is exceeded.

### System Use Notification

The DIP Service Provider shall display an approved system-use notification message before granting system access informing potential users:

1. The user is accessing any system in the DIP
2. System usage may be monitored, recorded, and subject to audit
3. Unauthorised use of the system is prohibited and subject to criminal and civil penalties
4. Use of the system indicates consent to monitoring and recording.
5. System use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the system.

The DIP Service Provider shall ensure systems display a warning banner (or close approximation) at login and require users to electronically acknowledge the warning (such as clicking on “OK” or “I agree” button to proceed):

***For example;***

\*\*WARNING\*\* this is an MHHS computer system. MHHS computer systems are provided for the processing of official MHHS information only. All data contained within this computer system is owned by MHHS, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorised personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on MHHS computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORISED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY. \*\*WARNING\*\*

### Concurrent Session Control

The DIP Service Provider shall limit the number of concurrent sessions for any user as defined in the ISMS.

### Session Lock

The DIP Service Provider shall prevent further access to the DIP by initiating a session lock that remains in effect until the user re-establishes access using appropriate identification and authentication procedures.

### Session Termination

The DIP Service Provider shall automatically terminate a session after a period of inactivity specified in the ISMS.

### Supervise and Review

The DIP Service Provider shall supervise and review the activities of users with respect to the enforcement and usage of system access controls. Employ automated mechanisms to facilitate the review of user activities.

### Permitted Actions

The DIP Service Provider shall identify specific user actions that can be performed on the system without identification or authentication. The DIP Service Provider shall permit actions to be performed without identification and authentication only to the extent necessary to accomplish the required task.

### Automated Marking

The DIP Service Provider shall mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

### Remote Access

The DIP Service Provider shall document, monitor, and control all methods of remote access (e.g., API, VPN) to the DIP including, remote access for privileged functions and;

1. Authorises each remote access method
2. Authorises only the necessary users for each access method.
3. Automates mechanisms to facilitate the monitoring and control of remote access methods.
4. Uses encryption to protect the confidentiality of remote access sessions.

### Secure Device

The DIP Service Provider shall ensure all privileged tasks can only be undertaken from a secure device such as a Jump box or a Citrix server which is hardened to allow only authorised services and applications to run.

### Wireless

The DIP Service Provider shall ensure no wireless technologies are enabled / used within the DIP and;

1. Automated mechanisms should be configured to identify wireless networks
2. Any Wireless networks identified must be disabled

### Portable and Mobile Devices

The DIP Service Provider shall establish usage restrictions and implementation guidance for portable and mobile devices. Document, monitor, and control device access to the DIP.

The DIP service Provider shall ensure:

1. Appropriate "Service Provider Personnel" authorise the use of portable and mobile devices.
2. Policies and procedures are created for the protection of portable/mobile devices that may currently or in the future contain potentially sensitive but unclassified data and/or personally identifiable information.
3. The data that is being stored is encrypted to Protect information residing on portable and mobile devices.

### Personally Owned Systems

The DIP Service Provider shall prevent the use of personally owned systems.

## 8.11Audit and Accountability

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update Audit and Accountability policies and controls that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Compliance

### System Management Audit

The DIP Service Provider shall document within the ISMS, for each system, which events generate auditable records and ensure:

1. The solution records all system activity (including all attempts to access resources, or Data held, on it) in audit logs;
2. The solution detects any attempt by any person to access resources, or Data held, on it without possessing the authorisation required to do so; and
3. The solution prevents any such attempt at unauthorised access
4. The solution compiles audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.
5. The solution can manage the selection of events to be audited by individual components of the system.
6. The solution is periodically reviewed and the list of system-defined auditable events is updated

### Content of Audit Records

The DIP Service Provider shall document within the ISMS, each system, and what the content of each auditable records contains. All Audit records must:

1. Capture sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
3. Provide the capability to centrally manage the content of audit records generated by individual components throughout the system.

### Storage Capacity and Retention

The DIP Service Provider shall allocate sufficient audit record storage capacity and configure auditing to prevent such capacity being exceeded. And:

1. All configurations must be documented within the ISMS.
2. Is consistent with the DIP retention periods to provide support for after-the-fact investigations of security incidents and meet any regulatory retention requirements.
   * + 1. Minimum 3 months of audit logs searchable and available immediately.
       2. Minimum 12 months of audit logs archived

### Processing, Monitoring, Analysis, and Reporting

The DIP Service Provider shall ensure,

1. In the event of an audit failure or audit storage capacity being reached, all systems will alert appropriate personnel and take the appropriate actions specified by the ISMS (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)
2. They regularly review/analyse audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
3. Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
4. Employ automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.

### Reduction and Report Generation

The DIP Service Provider shall provide an audit reduction and report generation capability for each system.

1. Provide the capability to automatically process audit records for events of interest-based upon selectable, event criteria.

### Date/Time Formats

The solution shall apply a date and timestamp to all interface interactions sent and received. The date and timestamp shall use Coordinated Universal Time (UTC) as defined by International Telecommunications Union Recommendation (ITU-R TF.460-6). See section 8.3.2

### Protection of Audit Records

The DIP Service Provider shall employ mechanisms that protect system audit information and audit tools from unauthorised access, modification, and deletion.

1. Audit logs must be tamper-proof, and
2. The ability to remove sensitive logs should be restricted.

## External interface and Communications Protection

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update System and Communication Protection policies that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Coordination among Market participants
* Compliance

The DIP Service Provider shall document System and Communication Protection procedures, within their ISMS, and associated System and Communication Protection controls for the DIP.

### Application Partitioning

The DIP Service Provider shall separate user functionality (including user interface services) from the DIP management functionality.

### Security Function Isolation

The DIP Service Provider shall isolate security functions from non-security functions by means of:

1. Partitions
2. Domains
3. Control access and integrity to the security functions of:
   1. Cloud resources
   2. Software
   3. Firmware
4. Separate execution domain (e.g., address space) for each executing process.
5. Segmenting the network based on the label or classification level of the information stored on the servers.
6. Locate all sensitive information on separated Virtual Local Area Networks (VLANs) or micro-segmentation.

### Resource-Priority

The DIP Service Provider shall limit the use of resources by priority.

### Unauthorised Connections

The DIP Service Provider shall ensure;

The solution is capable of detecting any unauthorised connection that has been made to them, and any unauthorised attempt to connect to them, by any other System; and

That the connection is terminated or the attempted connection prevented (as the case may be).

### Unauthorised Network Services

The DIP Service Provider shall ensure that the solution:

1. Identifies any unauthorised or unnecessary network port, protocol, communication, application or network service;
2. Causes or permits to be open at any time only those network ports, and allows only those protocols, which are required at that time for the effective operation of that system, and blocks all network ports and protocols which are not so required; and
3. Causes or permits at any time only the making of such communications and the provision of such applications and network services as are required at that time for the effective operation of that system.

### Boundary Protection

The DIP Service Provider shall monitor and control communications at the external boundary of the DIP and at key internal boundaries within the system. Physically allocate publicly accessible systems components (e.g., public web servers) to separate subnetworks with separate, virtual network interfaces.

The DIP Service Provider shall ensure:

1. The Systems are capable of detecting and where necessary preventing any unauthorised connection that has been made to them, and any unauthorised attempt to connect to them, by any other System
2. It has capacity to detect and prevent a DOS (Denial of Service) or DDOS (Distributed denial of Service) attack
3. It has the means to inspect traffic for malware
4. All network traffic to or from the Internet passes through an authenticated application layer device that is configured to filter unauthorised connections.
5. Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organisation. This filtering shall be enforced for each of the DIPs systems.
6. All network connections shall be separated from the internet

The DIP service provider shall ensure boundary protection devices must be context-aware (also known as attribute-based access controls or ABAC) and use situational information, such as identity, geolocation, time of day, or type of endpoint device.

### Transmission Integrity

The DIP Service Provider shall protect the integrity of transmitted information.

1. Employ cryptographic systems to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

The DIP Service Provider shall ensure that data in transit over a public network is secured:

1. Using TLS version 1.2 or later
2. Using encryption algorithms that are aligned to NCSC guidance

### Transmission Confidentiality

The DIP Service Provider shall protect the confidentiality of transmitted information.

1. Employ cryptographic mechanisms to prevent unauthorised disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).

### Network Disconnect

The DIP Service Provider shall terminate a network connection at the end of a session or after a time specified in the DIP ISMS.

### Cryptography

The DIP Service Provider shall enforce Cryptographic Key Establishment and Management:

1. Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management for Cloud resources in the DIP
2. Use Of Validated Cryptography:
3. When cryptography is employed within the DIP, perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules, operating in approved modes of operation.
4. Use separate certificates and keys in each environment.

### Message signing

The DIP Service Provider shall ensure that where it provides Message Signing capability, that capability is provided so that it can be confirmed, on receipt by the entity to whom it is provided, as:

1. Having been provided by the sender; and
2. Being authentic, such that any tampering to the data would be apparent.
3. Using hashing algorithms that are aligned to NCSC guidance

### Public Access Protections

The DIP service provider shall ensure for publicly available systems they protect the integrity of the information and applications.

### Collaborative Computing

The DIP Service Provider shall prohibit remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provide an explicit indication of use to the local users (e.g., use of camera or microphone).

## Contingency Planning

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update Contingency Planning policies, procedures, and practices that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Coordination among Market participants
* Compliance

The DIP Service Provider shall document Contingency Planning policies, practices, and processes and their associated Contingency Planning controls for all systems within the DIP.

### Contingency Plan

The DIP Service Provider shall develop and implement a contingency plan for the DIP addressing:

1. Contingency roles
2. Responsibilities
3. Assigned individuals with contact information
4. Activities associated with restoring the system after a disruption or failure.
5. Designated officials must review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

### Training

The DIP Service Provider shall ensure personnel having roles relating to contingency planning must be trained in their contingency roles and responsibilities and must be provide refresher training, at a minimum, on an annual basis. This training must:

1. Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.
2. Use of automated mechanisms is recommended to provide a more thorough and realistic training environment.

### Testing

The DIP Service Provider shall test the contingency plan, at a minimum, on an annual basis, using unit-defined tests and exercises to determine the plan’s effectiveness and the Service Providers readiness to execute the plan.

1. Appropriate officials within the DIP service provider will review the contingency plan test results and initiate corrective actions.

The DIP Service Provider is responsible for:

1. Related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan).
2. Test the contingency plan for the DIP to evaluate the capabilities required to support contingency operations.
3. The use of automated mechanisms to more thoroughly and effectively test the contingency plan is recommended.

### Plan Updates

The DIP Service Provider shall review their contingency plan, at a minimum, on an annual basis and revise the plan to address:

1. System/organisational changes
2. Problems encountered during plan implementation
3. Execution
4. Testing

### Alternate Sites

The DIP Service Provider shall ensure an alternate storage site is used for the storage of the DIP systems backup information.

The DIP Service Provider shall ensure an Alternate processing site is available and can initiate the necessary agreements to permit the resumption of the DIP in a timely manner, as specified by the DIP Service Provider when the primary processing capabilities are unavailable.

### ISP Services

DIP Service Provider to ensure fully resilient internet services are configured and failover of services is in-line with the service description and SLAs.

### Backup, Recovery, and Reconstitution

The DIP Service Provider shall ensure:

That: Backups are carried out and that the Data which is backed up is:

1. protected in accordance with the Information Classification Scheme, including when being transmitted for the purposes of backup; and
2. Located in secure facilities, at least one of which facilities must be in a different location.
3. Test backup information for the DIP, at a minimum, on an annual basis to ensure media reliability and information integrity.

That: for the DIP systems

1. Selective use of backup information in the restoration of system functions as part of contingency plan testing.
2. Backup data is protected in accordance with the Information Classification Scheme, including when being transmitted for the purposes of Backup; and
3. Backup data is stored on media that are located in physically secure facilities, at least one of which facilities must be in a different location.

Conduct System Recovery and Reconstitution:

1. Employ mechanisms with supporting procedures to allow the system to be recovered and reconstituted to the system’s original state after a disruption or failure.
   1. Include a full recovery and reconstitution of the DIP as part of contingency plan testing.

### Failure scenarios

The DIP Service Provider shall identify and document in the ISMS the failure scenarios covered by the solution including but not limited to:

a) Failure Type

b) Description

c) Service Impact (RTO)

d) Action required

e) Mitigation in Place

An example can be found in Appendix C – Failure scenarios

## Maintenance

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update Maintenance policies, procedures, and practices that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Coordination among Market participants
* Compliance

### Periodic Maintenance

The DIP Service Provider shall Schedule, perform, and document routine preventative and regular maintenance on the security components of the DIP in accordance with manufacturer or vendor specifications and/or operating unit requirements and;

Maintain a maintenance log for the DIP that includes:

1. Date and time of maintenance
2. Name of the individual performing the maintenance
3. Name of escort, if necessary
4. Description of the maintenance performed
5. List of equipment removed or replaced (including identification numbers, if applicable).

Employ automated mechanisms to ensure that periodic maintenance of the DIP is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

### Remote Maintenance

The DIP Service Provider shall approve, control, and monitor remotely executed maintenance and diagnostic activities.

1. Audit all remote maintenance sessions, and appropriate organisational personnel review the audit logs of the remote sessions.
2. Address the installation and use of remote diagnostic links in the ISMS.
3. Remote diagnostic or maintenance services are acceptable if performed by the DIP Service Provider and its own systems meet the same level of security as that implemented in the DIP being serviced.
4. Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighbouring systems, through technologies such as Private VLANs or micro-segmentation.

### Maintenance Personnel

The DIP Service Provider shall ensure only authorized personnel are permitted to perform maintenance on the DIP.

1. A list of personnel authorized to perform maintenance on the system should be maintained and kept up to date and

### Timely Maintenance

The DIP Service Provider shall ensure maintenance support is in place for all components of the DIP within agreed time frame (SLA) following a failure and

## Personnel Security

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, disseminate, and periodically review and update Personnel Security policies, procedures, and practices that address:

* Purpose
* Scope
* Roles
* Responsibilities
* Management commitment
* Compliance

The DIP Service Provider shall document Personnel Security policies, practices, and processes and their associated Personnel Security controls for all systems within the DIP.

### Position Categorisation

The DIP Service Provider shall assign a risk designation to all positions and establish screening criteria for individuals filling those positions.

1. On an annual basis the DIP Service Provider will review and revise position risk designations on a sampling basis.

### Service Personnel

The DIP Service Provider ensure that

1. a) Each member of the provider personnel who is authorised to access data held on the provider solution has only the appropriate privileges required to the role performed by that individual and to the data to which he/she is authorised to access; and
2. b) They review annually the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the data to which he or she is authorised to access.

### Personnel Screening

The DIP Service Provider shall require that all personnel, where applicable, be subject to the screening process prior to being permitted permanent access to the DIP.

1. Screening must be performed for operating unit employees, contractors, and any “guests” prior to their being given access to the DIP.
2. A risk-based, cost-effective approach must be followed to determine the risk of harm to the system in comparison to the opportunity for personnel performing the following functions:
3. Personnel with security authority, “root” access to systems, or access to software source code who have opportunity to bypass system security control settings – for example, Cloud engineer/system administrator,
4. System developer, and security program positions (such as ISOs and security managers).
5. User with privileged access to systems who may modify core data stores, users with authority to electronically approve financial transactions, or users with access to personal/Privacy Act/other protected data (e.g., GDPR, other sensitive data etc.) other than their own.

### Changes in Personnel

The DIP Service Provider must ensure the following for all personnel:

When employment is terminated the following actions must occur according to the ISMS:

1. Terminate user system access
2. Conduct exit interviews
3. Ensure they return all assets in a timely manner.
4. Appropriate personnel are to be granted access to all official records created by the terminated employee.
5. Personnel Transfer:
6. Review systems/access authorisations when individuals are reassigned or transferred to other positions and initiates appropriate actions (e.g., closing old accounts and establishing new accounts; and changing system access authorisations).

### Access Agreements

The DIP Service Provider shall complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behaviour, conflict-of-interest agreements) for all individuals requiring access to the DIP before authorising access.

### Third-Party Personnel

The DIP Service Provider shall comply with the personnel security requirements for third-party providers (e.g. contractors, and other organisations providing system development, technology services, outsourced applications, network and security management) and monitor provider compliance to ensure adequate security.

### Personnel Sanctions

The DIP Service Provider shall comply with the formal sanctions process for personnel failing to comply with established security policies and procedures established by the Service Provider.

## Certification and Accreditation

### ISO27001

The DIP Service Provider shall be ISO27001 certified prior to operational running and for the lifetime of the contract.

### Policy and Procedures

The DIP Service Provider shall develop, and document within its ISMS, the security assessment, certification and accreditation policies, practices, and processes for all systems within the DIP.

### Security Assessments

The DIP Service Provider shall perform an assessment, of the security controls within the DIP to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the DIP. The assessment should take place at least annually / after significant changes.

### NCSC CHECK Assessments (Penetration Testing)

The DIP Service Provider shall ensure that an organisation which is a NCSC CHECK service provider carries out assessments that are designed to identify any vulnerability of the systems to compromise:

1. In respect of each System, on at least an annual basis;
2. In respect of each new or materially changed component or functionality of the Systems, prior to that component or functionality becoming operational; and
3. On the occurrence of any Major Security Incident in relation to the Systems.
4. Prior to operational running of the DIP

#### External Penetration Test

The DIP service provider shall ensure the scope of any external penetration test incorporates the exposed external perimeter of the DIP and critical systems connected or accessible to public network infrastructures. The penetration test should assess any unique access to the scope from the public networks, including services that have access restricted to individual external IP addresses. Testing must include both application-layer and network-layer assessments. External penetration tests also include remote access vectors such as dial-up and VPN connections.

#### Internal Penetration Test

The DIP service provider shall ensure the scope of internal penetration tests incorporates the internal perimeter of the DIP and critical systems from the perspective of the internal network. Testing must include both application-layer and network-layer assessments.

Testing activities to include attempting to bypass internal access controls intended to prevent unauthorised access or use of systems that store, process, or transmit sensitive data from those that do not. In cases where there is an internal DIP perimeter, the scope of testing will need to consider the DIP perimeter as well as critical systems within and outside of the DIP.

When access to the DIP is obtained as a result of the testing, the scope of the penetration test may allow the tester to continue exploring inside the network and further the attack against other systems within the DIP, and may also include testing any data-exfiltration prevention (data-loss prevention) controls that are in place.

In all cases, the scope of internal testing should consider the specific environment and the DIPs risk assessment.

### Vulnerability Assessments

The DIP Service Provider shall ensure that it carries out assessments that are designed to identify any vulnerability of the Systems to Compromise:

in respect of each System, on at least a 3 monthly basis;

in respect of each new or materially changed component or functionality of the CSS Systems, prior to that component or functionality becoming operational; and

On the occurrence of any Major Security Incident in relation to the Systems.

#### External Vulnerability Assessments

The DIP service provider shall run external vulnerability scans to identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system

#### Internal Vulnerability Assessments

The DIP service provider shall run internal ‘authenticated’ vulnerability scans to identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system

#### Frequency

The DP Service provider shall run scans at least quarterly and where possible continuous scanning.

Vulnerability assessments should aligned to the NCSC guidance

* <https://www.ncsc.gov.uk/guidance/vulnerability-management>

### Security Patching

The DIP Service Provider shall ensure, updates to devices or software to improve security and/or enhance functionality are aligned to a recognised framework such as NIST.

* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>

### Connectivity to the DIP

The DIP Service Provider shall explicitly authorise all connections to the DIP and monitor/control the interconnections of the DIP on an ongoing basis.

### Certification and Accreditation

The DIP Service Provider shall perform an assessment of the security controls within the DIP to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the DIP.

1. The assessment should take place at least annually Or
2. After significant changes.

### Plan of Action (POA)

The DIP Service Provider shall develop and update, according to the frequency specified in the ISMS, a plan of action (POA) that documents the planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

### Continuous Monitoring

The DIP Service Provider shall ensure the DIP is continuously monitored for effectiveness and adequacy of system controls as documented in the DIP Service Provider ISMS.

## Awareness and Training

### Policy and Procedures

The DIP Service Provider shall ensure they develop, disseminate, periodically review, and update:

1. Security awareness and training policies that address purpose, scope, roles, responsibilities and compliance
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls for the DIP.

### Security Awareness Training

The DIP Service Provider will provide all users, both employees and contractors, basic security awareness instruction within 30 days of appointment and before granting permanent access to the DIP and

1. Provide all users, both employees and contractors, security awareness instruction on an annual basis.
2. Security training will present a core set of generic security terms and concepts for all personnel.
3. Update Awareness Content Frequently

### Security Training and Records

The DIP Service Provider shall identify personnel with significant security roles and responsibilities, document those roles and responsibilities, and provide appropriate security training before authorising access to the DIP and

1. Establish, and, at least bi-annually, execute training plans for these personnel covering the training topics.
2. Document and monitor individual security training activities, including basic security awareness training and specific security training such as.

* Secure Authentication
* Identifying Social Engineering Attacks
* Sensitive Data Handling
* Causes of Unintentional Data Exposure
* Identifying and Reporting Incidents

### Lessons Learned

The DIP Service Provider Shall ensure, where an incident does occur that, lessons are learned as to why it happened and, where appropriate, takes steps to prevent the issue from reoccurring.

1. The aim should be to address the root cause or to identify systemic problems, rather than to fix a very narrow issue.
2. For example, to address the organisation's overall patch management process, rather than to just apply a single missing patch.

# Reports, Dashboards and KPIs

The security requirements regarding reports, dashboards and KPI’s cannot be defined at this time and will be deferred until the ESO is on-board to help define these requirements.

1. End to end security requirements



1. PKI Certificate Services.



1. Failure scenarios (Examples)



1. OFGEM DPIA

***OFGEM – MHHS DPIA v2***



***OFGEM - Addendum to MHHS DPIA v2***

