SCHEDULE 2:

DIGITAL

Version number	Issue Date	Comment
1.0	28 November 2025	Execution Version

CONTENTS

1. Introduction

1.1 The Authority considers ICT and Information Assurance to be key to the effective delivery of the Services with consideration given to operational effectiveness, business continuity, the security of people and data, compliance with Legislation (including but not limited to the Data Protection Legislation), and to the performance of specific functions of the Services.

1.2 While providing scope for innovation through the use of technology, the high-level objective of this Schedule is to ensure appropriate ICT capability is delivered by the Contractor to the Authority and vice versa to enable the Contractor to operate the Prison as an integral part of the national prison service. Achieving continuity of care between prisons and between prisons and probation services is integral to this Contract.

1.3 Without prejudice to the obligations set out in **Part III (ICT)** of the Contract, the Contractor shall comply with all requirements set out in this Schedule and any others it identifies as necessary for the Contractor to achieve the effective outcomes identified in **paragraph 1.1 (Introduction)**.

1.4 The Contractor shall set out those requirements in addition to this Schedule it identifies as necessary for the delivery of the outcomes identified in **paragraph 1.1 (Introduction)** in the Operating Manual maintained and updated pursuant to **clause 25 (Operating Manual).**

1.5 This Schedule sets out the Authority's requirements for ICT (in particular, the requirements for the Contractor's ICT System and the Authority's ICT System) and the Information Assurance requirements relating to the Prison and the delivery of the Services.

1.6 In order to achieve this aim, the Authority requires the Contractor to interact with existing Authority Software Applications and ICT Systems, and any replacement Authority Software Applications and ICT Systems, that support the UK's criminal justice system. This will be through the use of APIs, a virtual desktop such as AVD (Azure Virtual Desktop) or directly by applications being directly available to the Contractor through the Contractor's ICT System over a Web Browser or, in limited circumstances, Authority-provided ICT Equipment subject to **paragraph 1.7 below (Introduction)**.

1.7 The Contractor shall meet all costs incurred in the provision of Authority ICT Equipment, within thirty (30) Business Days of invoice, wherever this is required by the Contractor to fulfil their requirements under this Schedule and **Part 1 (Custodial Services)** of **Schedule 1 (Authority's Custodial Service Requirements**).

1.8 Where the Contractor provides an alternative User Interface to the UI provided by the Authority, the Contractor will ensure that all available Authority APIs are integrated with, to ensure that the Authority's Single Source of Data remains updated in real time**.** The Contractor shall update or replace its systems during the lifetime of the Contract in order to keep abreast of technology

changes or enable new ways of working (e.g. mobile first/native applications). Such updates or replacements should not require any change to the Authority APIs, but, if required, API changes and new API development can be explored by the Parties and agreed between them. For the avoidance of doubt, such changes shall not be required to be agreed through **Schedule 16 (Change Protocol)**.

1.9 The Contractor shall utilise the Mandated Applications and/or mandated data sources to deliver the relevant aspects of the Custodial Service.

2. **Scope**

2.1 The following is within scope of the Authority's ICT specification:

2.1.1 the Contractor's use of Authority's ICT Systems or Authority Software Applications for the Contractor's management of the Prison or the Authority's management of the Prison;

2.1.2 the Contractor's provision and use of the Contractor's ICT Systems for the management of the Prison and/or management of their own systems and staff;

2.1.3 provision and use of the ICT Systems for use by Prisoners including the required risk assessment of Prisoners; and

2.1.4 the data which shall be supplied by the Contractor to the Authority using the ICT Systems.

2.2 This Schedule does not describe the ICT requirements for activities of Relevant Organisations on the Site or services provided by Third Parties including any Healthcare Provider, Social Care Service Provider or Probation Provider.

3. **Governance and Assurance**

3.1 The Contractor shall ensure it has available for the purposes of this Contract an Information Security Management System compliant to ISO/IEC 27001, as amended and updated from time to time, to cover the Information Assurance objectives set out in this Contract throughout the Contract Period, and will develop a plan of work to meet ISO/IEC 27001 certification within twelve (12) Months of the Services Commencement Date. This plan to ensure compliance with ISO/IEC 27001, as amended and updated from time to time, shall include the scope, statement of applicability, risk management plans, risk treatment plans and other artefacts all of which shall be agreed with the Authority.

3.2 The Contractor shall provide, no later than ninety (90) Days before the Services Commencement Date, the name and contact details of the Digital and ICT Security Lead.

3.3 The Contractor shall provide the Authority with such access to and information on the Contractor's ICT Systems as the Authority requires in order to audit and assess technical, personnel, procedural and physical security controls at the Prison and any other sites used for the purpose of meeting the Contractor's obligations under this Contract.

3.4 The Contractor shall ensure that cyber security is embedded in all service management (in compliance with ISO/IEC 20000, as amended and updated from time to time), including, but not limited to:

3.4.1 Change management;

3.4.2 incident management; and

3.4.3 other service management artefacts aligned with ISO/IEC 20000.

3.5 The Contractor shall ensure that all development and test environments in Contractor's ICT Systems shall have assured separation from the live/production systems, and shall not use live/production information without prior written Authority approval.

3.6 The Contractor shall ensure that the Contractor's ICT System shall be compliant with Legislation and Authority Policies, as amended from time to time, including but not limited to the:

3.6.1 Malware Policy;

3.6.2 Patching Policy;

3.6.3 Password Standards;

3.6.4 Information Handling Policy; and

3.6.5 Security Monitoring Policy.

3.7 The Contractor shall ensure that the Contractor's ICT System, including source code, shall be developed and reviewed against good commercial practices and in accordance with Good Industry Practice, taking into account the Prison environment in which it will be situated. The Contractor shall undertake regular review of the Contractor's ICT System to include security and cyber threat testing of the infrastructure and applications, and outcomes will be shared with the Authority, in line with HMG Standards and Guidance including an annual ICT health check in line with Good Industry Practice. The results of all reviews or health checks must be provided to the Authority as soon as practicable upon completion, along with the ICT health check remediation plan and timelines for completion.

3.8 The Contractor shall ensure that the Contractor's ICT System regularly notifies the users of the Contractor's ICT System to read and accept the terms and conditions of use, at least annually.

3.9 Without prejudice to its other obligations in relation to protecting Authority Data, the Contractor shall adequately protect all information processed or retained on Contractor's ICT systems (including personal information) and ensure that their systems deliver security management of all HMPPS Data in accordance with the Government Classification Scheme at 'OFFICIAL'.

3.10 The Contractor shall provide to the Authority the Contractor's plans to deliver appropriate cyber security engagement at least four (4) weeks prior to the Services Commencement Date.

3.11 The Contractor shall ensure that the Contractor's ICT System's design and operation follows Authority Policy and Good Industry Practice for cyber security, minimising access to those with a need to know, minimising the data that is held, and which is security tested (at a minimum thirty (30) Day vulnerability scans and more in depth security testing based on how any changes affect risk posture) for robustness against vulnerabilities.

3.12 The Contractor shall comply to the extent within its control with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the Contractor's ICT System.

4. **Access, Authorisation and Authentication**

4.1 The Contractor shall ensure that the Contractor's ICT System and locations shall have auditable authorisation, authentication and access control based on least privilege, and aligned appropriately to the business requirement.

5. **Risk Assessment**

5.1 The Contractor shall carry out a risk assessment of the entirety of the Contractor's ICT System (from network connectivity, security controls at the application level, codebase, and data in transit and at rest), throughout development and into live service, and supporting processes in line with their Information Security Management System and Authority Policies, and including when system changes are made. The Authority retains the right to review the results of such risk assessment and the Repeatable Methodology used for risk assessments.

6. **Risk Management**

6.1 The Contractor shall seek authorisation from the Authority with regards to managing all security-related risks in both the Authority's ICT Systems and Contractor's ICT Systems to ensure they are within risk appetite/tolerances of the Authority or there is a risk exception acceptance, in writing from the Authority pursuant to **clause 9.7 (Responsibility for Security of Authority ICT Systems).**

6.2 The Contractor must inform the Authority if there is reasonable suspicion and/or confirmation of a negative security event (including a Cyber Security Incident) or data breach (including a

Data Loss Event) that directly or indirectly accesses or processes Authority Data or the Authority's ICT Systems within one (1) hour of awareness as defined in the relevant Authority Policy.

7. **ICT for Relevant Organisations**

7.1 The Contractor shall ensure that all ICT deployed by the Contractor or any Sub-Contractor for the purposes of enabling Relevant Organisations or Third Parties is compliant with the Information Assurance requirements described in this Schedule.

8. **Infrastructure**

8.1 To deliver Services using Contractor's ICT Systems, the Contractor shall provide and maintain ICT networks, WiFi, ICT Equipment, applications, licences, user agreements and services to ensure:

8.1.1 the secure and effective management of; and

8.1.2 the exchange of information required in order to deliver the Services.

9. **Prisoner Information**

9.1 The Contractor shall ensure that all Prisoner data is either transferred (via an Authority approved API) or entered directly into the Authority's ICT System by the Contractor in real time, is accurate and complete in order to meet the Authority's Requirements pursuant to **Part 1 (Custodial Services)** of **Schedule 1 (Authority's Custodial Service Requirements**) and the requirements detailed in the Authority Policies, including (in relation to each Prisoner):

9.1.1 personal information;

9.1.2 sentencing details;

9.1.3 risk information including to others, self and in relation to offending behaviour;

9.1.4 offending and personal needs;

9.1.5 sentence progression work (such as offending behaviour work completed and engagement in purposeful activity etc.);

9.1.6 finance information;

9.1.7 booked visits;

9.1.8 activities;

9.1.9 discharge; and

9.1.10 any changes to any of the above.

9.2 The Contractor shall, on the request of the Authority, provide the Authority with unlimited read-only access to all Contractor's ICT System data relating to the management of Prisoners. This data shall include Prisoner monies, expenditures and booked visits, and shall be provided in a format as reasonably required by the Authority.

9.3 The Contractor shall ensure that all data provided to the Authority in accordance with **paragraph 9.2 (Prisoner Information)** is accurate and complete.

10. **Architecture**

10.1 The Contractor shall upon the Authority's request provide to the Authority comprehensive and detailed documentation explaining the Contractor's ICT System including its architecture, infrastructure, applications, functionality, licences, hardware, service management, sub-contractors, data storage, security, business continuity and risk management processes.

11. **Authority's ICT System**

11.1 The Contractor shall enter data into the Authority's Software Applications as required by the Authority under this Contract using one of the following means:

11.1.1 directly onto the Authority's Software Applications, using end-user devices provided by the Authority at the cost of the Contractor in accordance with **paragraph 1.6 (Introduction)**;

11.1.2 directly onto the Authority's Software Applications accessed via a Web Browser, using end-user devices provided by and at the cost of the Contractor in accordance with **paragraph 1.6 (Introduction)**, and can be via an Authority User Interface or Contractor User Interface; or

11.1.3 indirectly on to the Authority's Software Applications via available APIs.

11.2 The Contractor shall identify its requirements in relation to Authority provided ICT Equipment including but not limited to a specified number of terminals and printers connected to the Authority's ICT System in writing and provide this to the Authority ninety (90) Days prior to Services Commencement Date.

11.3 **Paragraph 11.2 (Authority's ICT System)** applies where the Contractor requires access to the Authority's Software Applications on the Authority's ICT System only via Authority provided ICT Equipment for the purposes of meeting the Authorities Requirements pursuant to **Part 1 (Custodial Services)** of **Schedule 1 (Authority's Custodial Service Requirements**).

11.4 All costs relating to the provision of the Authority provided ICT Equipment to the Contractor will be met by the Contractor within thirty (30) Days of invoice.

11.5 The Contractor shall be responsible for the appropriate usage of the Authority's Software Applications including replacement systems (as amended from time to time) by the Contractor's Staff (including for the avoidance of doubt those sub-contracted by the Contractor for the purposes of meeting the Custodial Services and the Property and Facilities Management Services), including the following applications:-

11.5.1 OASys – sentence and risk management planning;

11.5.2 ViSOR – public protection information sharing system to support MAPPA process;

11.5.3 NOMIS, Digital Prison Services (DPS) or any Authority-specified replacement system;

11.5.4 Performance Hub – record of performance against set targets;

11.5.5 Mercury – security and intelligence reporting;

11.5.6 PNC;

11.5.7 Data Exchange;

11.5.8 Virtual Campus and Curious – for Education Services;

11.5.9 EQuiP;

11.5.10 Digital use of force reporting;

11.5.11 Digital PER;

11.5.12 Video conferencing; and

11.5.13 Prisoner PIN phone services.

11.6 The Contractor shall deliver all appropriate data, as defined in the relevant Authority Policies, operational guidance or in the application itself, and any data as may be required by the Authority into the risk assessment systems (OASys) and any Authority-specified replacement system (as amended from time to time) in a timely and accurate manner.

11.7 The Contractor shall deliver all appropriate data, as defined in the relevant Authority Policies, operational guidance or in the application itself, and any data as may be required by the Authority into ViSOR, or any Authority-specified replacement system, and as required by the

HMPPS Mandatory use of ViSOR (24/01/2023) (available at: hmpps-mandatory-use-visor-pf.pdf (as amended from time to time)) in a timely and accurate manner.

11.8 The Contractor shall deliver all appropriate data, as defined in the relevant Authority Policies, operational guidance or in the application itself, and any data as may be required by the Authority into the case management systems, NOMIS, DPS, or any Authority-specified replacement system, in a timely and accurate manner. The Contractor shall meet the NOMIS requirements as set out within the relevant Authority Policies as amended from time to time.

11.9 The Contractor shall deliver all appropriate data, as defined in the relevant Authority Policies, operational guidance or in the application itself, and any data as may be required by the Authority into the performance management reporting tool, Performance Hub, or any Authority-specified replacement system, in a timely and accurate manner. The Contractor shall report Monthly on the metrics in the Performance Hub.

11.10 The Contractor shall comply at all times with the requirements of the HMPPS Performance Hub as set out in the guidance contained within the Performance Hub internet site as may be amended from time to time.

11.11 The Contractor shall deliver all necessary data and any data as may be required by the Authority from time to time into Mercury, or any Authority-specified replacement system in a timely and accurate manner.

11.12 The Contractor shall meet the requirements of Mercury.

11.13 Not Used.

11.14 If a PNC device is available within the Prison, the Contractor shall meet the requirements for access in order to use the PNC, as defined within the Use of the Police National Computer in Prisons Policy Framework (06/06/2023) (available at: https://www.gov.uk/government/publications/use-of-the-police-national-computer-in-prisons-policy-framework (as updated from time to time)) and police standards regarding Reporting as per PNC use in place from time to time.

11.15 If a PNC device is provided, the Contractor shall provide PNC data (Prison report) to other prisons upon request free of charge within two (2) Business Days of the request.

11.16 If the Authority requires the Contractor to exchange data between the Contractor's ICT System and the Authority's ICT System (or vice versa), the Contractor shall do so only by a method approved in writing by the Authority. Such method may include an automated system-to-system exchange or a manual exchange (such as data entry via a user terminal).

11.17 If a VIPER device is available within the Prison, the Contractor shall meet the requirements for access in order to use VIPER.

11.18 The Contractor shall deliver to the Authority all data relevant to Education Services in accordance with **Part 2 (Prisoner Education Services)** of **Schedule 1 (Authority's Custodial Service Requirements)** and **Schedule 15 (Performance Mechanism)**, and any additional data as may be required by the Authority into Virtual Campus, and any Authority-specified replacement system (as amended from time to time) in a timely and accurate manner.

12. Communications

12.1 General Telephony

12.1.1 The Contractor shall provide general telephony to the whole of the Prison, including for the use of other Custodial Service Providers to meet the day-to-day requirements of the Prison and ensure delivery of all Services.

12.1.2 Without prejudice to the Contractor's obligations under **clause 8.12 (Business Continuity and Disaster Recovery at the Site)**, the Contractor's telephony solution shall be sufficiently resilient to ensure availability and continuity of the telephony service in the event that local external communication lines are disrupted.

12.1.3 If the Contractor implements an Internet Protocol Telephony ("IPT") solution that integrates with the Authority's IPT solution at any time during the Contract term then it must do so on terms agreed in advance in writing with the Authority.

12.2 Other Communications

12.2.1 On request from the Authority, the Contractor shall make available to the Authority an electronic staff directory containing contact details of the Contractor's Staff within three (3) Business Days of request.

12.2.2 The Contractor will keep this directory up-to-date and ensure that the Authority is provided a copy of, or access to, the up-to-date information within three (3) Business Days of a request of any update.

12.2.3 The Contractor may use the HMPPS Intranet via a Web Browser or Authority Provided ICT. The Authority may limit the Contractor's access to only certain pages of the HMPPS Intranet.

12.2.4 The Contractor shall provide and maintain an email application that meets the security and standards contained in this Schedule and is accredited/authorised for the transmission of information marked "Official" under the Government Classification System.

12.2.5 The Contractor shall implement and maintain any functional email addresses identified by the Contractor and/or the Authority as necessary or desirable to ensure

timely, consistent and robust processes for managing Prisoners through the Prison and on release into the community.

12.2.6 The Contractor shall provide and maintain secure social video calling at the Prison in accordance with the "Secure Social Calling (Interim) Policy Framework" document and using one of the provider(s) nominated by the Authority as listed in the relevant Authority online portal / electronic data room or as may be notified by the Authority from time to time.

13. **Prisoner access to ICT**

13.1 The Contractor shall provide auditable access to ICT for Prisoners. Before any access to ICT is provided to Prisoners, the relevant ICT will need to be assessed and authorised by the Authority's cyber-security team, or those which they have delegated the task of assessment to.

13.2 The Contractor must provide the Authority with an incident report following remediation of any Cyber Security Incident demonstrating timescales of events from detection through to recovery as per the Authority Policies. This incident report should be included in the Operational Briefing Sheet in accordance with **Part 1 (Custodial Services)** of **Schedule 1 (Authority's Custodial Service Requirements)**.

13.3 This incident report includes but is not limited to, the Contractor's undertakings in relation to Relevant Organisations (such as any obligations to provide ICT for Healthcare Providers).

13.4 The Contractor shall provide Prisoners with opportunities to acquire relevant ICT skills.

13.5 The Contractor shall limit Prisoner access to on-line services to a list of Authority approved websites and services, which the Contractor shall develop and maintain. This approach for limiting access will be submitted to, and approved in writing by, the Authority's cyber security team.

13.6 The Contractor shall provide Prisoners with up-to-date in-cell technology, including devices through which Prisoners can access services and content. In-cell technology shall provide Prisoners with access to services that will support ongoing learning, resettlement and rehabilitation. The Contractor shall ensure that the in-cell technology is maintained, updated, upgraded, and replaced in order to keep such technology abreast of technological changes and ensure that any in-cell device is monitored from a security point of view.

13.7 The Contractor shall provide Prisoners with opportunities to apply for, engage with and undertake activities using ICT systems for the purpose of improving their resettlement and rehabilitative outcomes as detailed in **Schedule 7 (Contractor's Proposal).**

13.8 Without prejudice to the Authority's right to assess and authorise any Prisoner ICT access pursuant to **paragraph 13.1 (Prisoner access to ICT)**, the Contractor shall:

13.8.1 first assess the risk in allowing Prisoners to access ICT;

13.8.2 subject to a satisfactory risk assessment finding, require the Prisoners to accept the terms of use in respect of the ICT; and

13.8.3 in the event that there is any intentional destruction or damage to Prisoner ICT, ensure that the relevant Prisoner(s) will be subject to appropriate disciplinary procedures.