Property
Directorate

SECURITY ASPECTS LETTER

Property Directorate: Project Control Framework

STD/BIM/P001.6

Document Ref	SECURITY ASPECTS LETTER
Version	2.0
Classification	OFFICIAL
Issue Date	3 October 2024
Status	S4 – Suitable for Stage Approval
Produced by	[redacted]
Contact Details	[redacted]

Version Control			
Issue No	Issue Date	Issue Author	Reason for Issue
1.0	[redacted]	[redacted]	[redacted]
1.1	[redacted]	[redacted]	[redacted]
1.2	[redacted]	[redacted]	[redacted]
1.3	[redacted]	[redacted]	[redacted]
1.4	[redacted]	[redacted]	[redacted]
1.5	[redacted]	[redacted]	
1.6	[redacted]	[redacted]	[redacted]
1.7		[redacted]	
1.8	[redacted]	[redacted]	[redacted]
1.9	[redacted]	[redacted]	[redacted]
1.10	[redacted]	[redacted]	[redacted]
2.0	[redacted]	[redacted]	[redacted]

Contents

1.	Background	5
2.	Definitions	5
3.	Definitions of Environments	6
4.	Security Management Culture and Awareness	6
5.	Personal Security Screening and Vetting	7
6.	Provision of Information to Non-Contracted Third Parties	10
7.	ROTL	11
8.	Information Management	11
9.	Digital/ Cyber Security	14
10.	Remote Working	15
11.	Security Incident Management	15
12.	Physical Security Conditions	16
13.	Social Media	19
14.	Use of Information	19

1. Background

1.1 This document will form part of the Contract between all parties. If there is any conflict between the terms of that contract and this letter, then the terms of the contract shall prevail.

1.2 All MoJ Property projects will require appropriate security minded approach to proceed safely. This letter has been developed to set out some of the strategic intent of the Authority's requirements in relation to security for any Project undertaken by the MOJ and its contractors/service providers.

1.3 All Parties shall comply with all applicable laws in relation to this letter and the Project.

1.4 The following Acronyms will be used

MoJ	Ministry of Justice
BASM	Built Asset Security Manager
BASMP	Built Asset Security Management Plan
BASS	Built Asset Security Strategy
CDE	Common Data Environment
HMPPS	Her Majesty's Prison and Probation Service
HMCTS	Her Majesty's Courts and Tribunals Service
DHR	Data Handling Request
ROTL	Release on Temporary Licence
SMP	Security Management Plan
ISMP	Information Security Management Plan
FOCI	Foreign Ownership, Control or Influence

2. Definitions

2.1 The following terms will be used throughout this document:

Authority	This refers to the Ministry of Justice (MoJ).
Governor	A person who manages a Prison and other units such as Young Offenders Institutions. They are responsible for the security and the overall care, progress and rehabilitation of prisoners.
Manager	Managing agent or officer manager in charge of building operations.

3. Definitions of Environments

3.1 The following Environments will be referred to throughout this document:

Brownfield sites	This refers to any land that is within the existing perimeter of an MoJ site or any previously developed land that is not currently in use, whether contaminated or not.
Greenfield sites	This refers to areas of land, usually agricultural or amenity land which is being considered for development.
Other MoJ Establishments	This refers to Courts, Probation offices, other offices such as the Office of the Public Guardian

4. Security Management Culture and Awareness

4.1 Security is defined in accordance with business impact levels defined in the HMG Security Policy Framework December 2022 and Government Security Classifications July 2023.

4.2 Security is everyone's responsibility, and its effectiveness relies on processes, procedures and policies being in place to help people to behave in the right way. This is enabled through a clear understanding of what is required by all those on MoJ projects and allows for the detection of security threat, The development of an appropriate security culture is essential for all MoJ Projects.

4.3 To satisfy Government requirements, the contractor/service providers should have:

- Staff who are well trained to exercise good judgement, take responsibility and be accountable for the information they handle.
- Mechanisms and processes in place to ensure assets and information are properly classified and appropriately protected
- An auditable, centralised security management system and security controls that are effective so that systems and services can protect the information they carry.

4.4 The level of security will differ from project to project and a security working group will be established, which will include the Mace Security Manager; Project Manager and Project Sponsor as a minimum this will determine the most appropriate form of security.

4.5 For all virtual and built assets, specific security measures related to information exchange will be identified on a project specific basis and communicated to the supply chain accordingly. The Client will dictate those procurement packages that have been deemed OFFICIAL-SENSITIVE. This has been developed by the MoJ and is subject to review and revision as necessary.

4.6 The Information Delivery Plan will communicate the information requirements for construction, assembly and asset management. This will be developed in conjunction with the Main Contractor's BIM Team(s). The details of the Employer's security requirements as

derived from ISO 19650-5 (Security-minded approach to Information Management) compliant materials such as the Security Strategy and the Security Management Plan including the Security Information Requirements and Security Breach and Incident Management Plan. The Security Strategy is an internal MoJ document which will not be made generally available, the Security Management Plan is authorised for general release. Please see link for an introduction to ISO 19650-5 (and any other future policies as directed by the Authority).

4.7 The Construction Security Manager will be required to develop and submit a Security Management Plan which will include an Incident Management Plan which reflects the MoJ's policies. Within the Incident Management Plan a clear Communications Plan will detail the responsibilities and actions required by the Incident Control Officer in response to a physical or information breach. It will include the necessity to engage, at the earliest possibility, and collaborate with the MoJ's Built Asset Security Manager (BASM) to resolve the security breach until it has been suitably contained. This will involve liaising with other Security Stakeholders. In addition, it will be the responsibility of the contractor/service providers to undertake corrective action to safeguard against any future breaches of a similar nature.

4.8 The contractor's/service providers Security Manager will be required to produce reports which will be recorded and stored on the MoJ's CDE by exception within 24hrs of an incident occurring and will extend to the following areas:

Site	Site Incident Management.
Personnel	Not likely to be applicable prior to construction phase.
Data	IT departments will be required to provide specialist reports

Additionally, all security incidents should be reported to the MoJ or it's nominated Security representative who will instigate a security working group and if appropriate a security investigation will be conducted.

4.9 The contractor/service providers will assist in supporting auditing procedure to provide the MoJ with Assurance statements involving the MoJ Security Stakeholders.

5. Personnel Security Screening and Vetting

5.1 Security checks and vetting are to be completed as a priority prior to access to any MoJ data or information being granted, however, a Data Handling Request (DHR) form can be used (details of which can be found in section 6) **as a temporary measure** (the minimum BPSS checks must be completed no later than 3 months of personnel starting). All personnel working on MoJ projects must obtain, as a minimum, a successful Baseline Personal Security Standard (BPSS) check (UK Governmental Requirement). The responsibility of these checks (including cost) will belong to the contractor/service providers and may be audited at any time by the MoJ or it's nominated Security representative.

5.2 Those who work next to or within a live environment will be required to meet the security requirements of that Establishment. General conditions are set out in the Table 1 below.

5.3 For certain types of establishment or for access to certain types of information either CTC (CTC clearance may be required if access is required to information assessed to be of value to terrorists) or DV clearance may be required. This will be advised by the MoJ.

5.4 Please refer to the following CDE viewpoint area for access to HMPPS Security Conditions Document, HMCTS Conditions Document and Home Office and Border Force Conditions Document.

Note: All other Establishments will be covered by the general conditions.

Role and/or Working Area	Vetting Contact Point (VCP)	Minimum Level of Clearance Required
Professional Services (Client Representative, Technical Advisor, Cost Consultant, Principal Designer etc.) Access to information only	Contractor NSVC This requires List X Registration*	BPSS Check**
Other MoJ Establishments	Contractor NSVC This requires List X Registration*	BPSS Check**

Table 1 Security and Vetting Requirements

*For link to further information please see section 12

** CTC clearance may be required if access to a large aggregate of information is required

5.5 The approximate time frames to obtain checks/ clearance are set out in table 2 below.

	BPSS	Enhanced Level 1
Time to Process	5 working days to 3 months	1-6 months*
Expiry Time	10 years BPSS's don't generally expire. However, for best practice we will be renewing these every 10 years.	10 years (Expires if subject leaves site for more than 6 months)

Table 2. Guidance for Application Time Frames against Vetting Stipulation

*This period of risk is mitigated by the Data Handling Request

5.6 The contractor/service providers must make allowances for absences by your regular teams and therefore have the ability to fill gaps with already cleared personnel. In addition, you must have a strategy in place for managing the recruitment and attrition of staff over the duration of the project. These conditions are to ensure you have planned contingency into your base to minimise any effect on the project.

[redacted]

[redacted]

5.8 The contractor/service providers must provide details of starters as soon as they are known to ensure all relevant paperwork and checks can be competed in sufficient time. Details of leavers should be provided as soon as a leaving date is known and a data destruction form completed which is to be returned to the MoJ or it's security nominated representative. This is to ensure the removal of access to project information as soon as is reasonably practicable. The contractor/service providers must provide, on a monthly basis, a full list of all of those currently on a project to the Authority.

5.9 The contractor/service providers will have signed a Non-Disclosure Agreement (NDA) in order to review all documents involved in any MoJ tender or access to information on the Client's CDE. This NDA applies to your entire team so you must have appropriate NDAs in place with your supply chain. A record of which should be stored on the clients CDE. The MoJ or it's nominated security representative will conduct quarterly audits across the supply chain to ensure the NDAs are being implemented.

5.10 The security and vetting requirements may preclude ex-offenders automatically from working on sites. Therefore, a proposed strategy is being finalised to assess which offences might be acceptable in an ex-offender's history. This is separate to the conditions for those individuals on Release On Temporary Licence (ROTL)

5.11 The Security Working Group (SWG) involving the MoJ or it's nominated security representative and the Supply chain security manager will dictate which people with current and spent convictions will be allowed to operate or work on site. The minutes from the SWG will be shared with the client for any feedback.

The following guidance should inform these site-specific decisions:

- [redacted]

5.12 The Supply chain security manager, in liaison with the site operational team will determine the level of access to the site and information.

- [redacted]

HMPSS

5.13 The minimum baseline requirements for Individuals working on HMPPS sites and HMPPS staff is an Enhanced Level 1 check. This differs from the BPSS as it checks both spent and unspent criminal records in line with the criminal record filtering rules. Non-directly employed workers providing services to any HMPPS public or private organisations with prisoner contact and issued keys and where a risk assessment identifies no further vetting is required.

5.14 For further information on the criteria for working on HMPPS sites please refer to HMPPS conditions document on the Viewpoint security section.

6. Provision of Information to Non-Contracted Third Parties

6.1 Permission requests for access to information by non-contracted and/or non-security cleared personnel will be managed through the MoJ's DHR form (the document can be found on Viewpoint Security section).

6.2 The DHR is a time bound document (maximum 3 months from submission of DHR) and will not cover members of the team for the life of the project. This is not a replacement BPSS check. This is an interim document to allow access to information/Viewpoint and will prevent delay to the works. If a BPSS is not achieved within three months, access to information will be removed from the individual.

6.3 The DHR identifies the reason, role and the context of the request, as well as the responsible persons, storage and internal security of that information. The process of this request will be done by a Construction Security Manager, and the MoJ BASM within their responsibility will grant or escalate the access request.

6.4 There are currently two DHRs in use. The first being for non-security cleared Main contractors/service providers. The second is for non-security cleared sub-contractors. The exact process for the provision of information to non-security cleared contractors/service provider and Sub-Contractors is shown in Figure 1 below.

6.5 In granting access information, there will be a number of handling stipulations that will be dictated by the Security Manager / Information Assurance Officer. These will be recorded within the DHRs and then be referred to in the MoJ's Transmittal Note available via the Viewpoint Security Section.

6.6

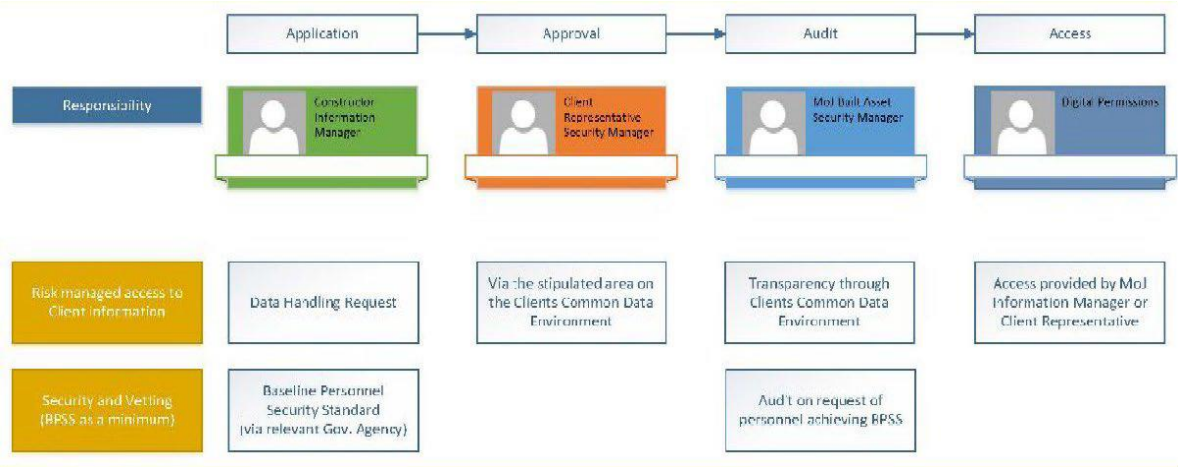

Figure 1. Provision of Information Process

6.7 The Information Transmittal Note will be a pre-condition to the final access to the information to the individual, thus communicating the handling conditions and transferring responsibility to the new user.

7. ROTL

7.1 ROTL facilitates the rehabilitation of those in custody by helping them to prepare for resettlement in the community once they are released.

7.2 Where a particular role is identified for an individual on ROTL, this role will be declared to the prison. The individual will then go through a detailed risk assessment process by the prison to establish their suitability for carrying out that specific role on site. They are approved for ROTL by job role and if this changes then a further risk assessment will be required however this will not be as in depth as the original risk assessment.

7.3 Guidance for the Security Working Group has been produced (please refer to the Viewpoint Security section for document), which sets out what is required by the contractor and the Project SWG to ensure the proper management of those individuals on ROTL.

7.4 The SWG will work alongside HMPPS and the MoJ to ensure that all the requirements set out in the Guidance are met.

8. Information Management

8.1 All documents used in the implementation of the programme for the MoJ constitute a security risk. Documents issued to contractors/service providers remain at all times the property of the MoJ and on completion of the contract shall either be returned to the MoJ in accordance with the conditions of contract or be certified by the Contactor as having been destroyed in a secure manner. A data destruction form is to be completed and returned to

the Mace Security team (the document can be found in the Viewpoint Security section) this shall be the responsibility of the contractor/service providers Security Manager.

8.2 The contractor/service providers is responsible at all times for the security of all information whether issued by the MoJ or copied, produced or obtained by the contractor/service providers or their agents. These security requirements have been incorporated in order to prevent information detrimental to the security of the MoJ coming into the possession of unauthorised persons and at the same time establish an audit trail of document movement.

8.3 In this context the term “documents” shall mean any and every drawing (including CAD), plan, schedule, specification standard presentation brochure, model, photograph, asset information and bill of quantities, whether in hard copy or electronic format.

8.4 Government Document Security Classification should be adopted, balancing the project specific needs of Confidentiality, Integrity and Accessibility with the consequences of any loss or unauthorised release of information.

8.5 The majority of MoJ project data sets will be typically categorised as OFFICIAL unless stated otherwise. However, although subsets of information may be OFFICIAL, if a large amount of OFFICIAL information is stored together the aggregated information may be treated under the same condition as though it were OFFICIAL – SENSITIVE. If OFFICIAL information is grouped with OFFICIAL- SENSITIVE data the classification will be raised to OFFICIAL- SENSITIVE. The security level will be decided by the Authority, please refer to Government Security Classifications - GOV.UK (www.gov.uk)

8.6 If, by exception and with the express authority of the client, OFFICIAL- SENSITIVE information needs to be sent via email it should be password protected. It should also include OFFICIAL- SENSITIVE markings in the email title. The password should be sent in a separate email. Sending documents via email will be avoided in all but essential circumstances.

Documents will be shared in one of two ways:
a) Via short codes from MoJ Viewpoint
b) Via links from the external document library on SharePoint

It is forbidden to send any private personal information without the subject’s specific approval and following 8.5 guidance.

8.7 The Contractor Security Manager will be on site for the duration of the project. This person is accountable for the control of all documents relating to the contract and in particular the whereabouts of each individual document. A document register should be created and maintained by the contractor Security Manager to monitor the physical movement of documents.

8.8 The contractor/service providers must notify all personnel handling documents of the requirements imposed by the MoJ and of the procedures for maintaining a security register.

8.9 Any security hierarchy is only as good as its weakest link. It is imperative therefore, that the contractor/service providers must include in all contracts with sub-contractors, suppliers

etc., where they will have access to sensitive information, similar but no less strict conditions of document security and shall be responsible for their compliance.

8.10 The Construction Security Manager is responsible for the issue of documents to site operatives including any subcontractors (whether nominated, approved, appointed or otherwise) to all others including suppliers and specialists and to representatives of the MoJ.

8.11 The contractor/service providers must provide, both at any relevant project location and at their offices, secure lockable, computers, cabinets and cupboards used for storing documents and these shall be kept locked at all times when not in use and secured at all times when the premises are unoccupied. In line with information management good practice no data should be left vulnerable to theft/loss.

8.12 At the completion of the works the contractor/service providers must obtain from all others having an interest in the contract, the return of all documents issued to and created by the other parties and shall remind them of the contractual obligations required by these security conditions.

8.13 The contractor/service providers must continue to safeguard and secure documents after completion of the works until such time as the contract has finally completed and the contractor/service providers has received all monies due from the MoJ. At that stage, and in agreement with the MOJ, the contractor/service providers shall confirm in writing what documents shall be returned, destroyed or kept and if kept shall continue to keep them secure as required above.

8.14 Classification of documents/Information Delivery references will be guided by a standard set of protocols to be detailed in the Information Delivery Plan; confirmed by the MoJ/ MoJ's Representative BASM.

8.15 The Construction Security Manager and Information Managers must ensure that all the relevant data protection legislation is adhered to. All procedures for management of a breach are incorporated and reported as part of the Incident Management Plan. Personnel data is to be stored and updated with the appropriate metadata on Viewpoint / client databases. The personnel data is to be held in a container with restricted permissions and in accordance with the BASM Plan.

8.16 **Data Protection Impact Assessment (DPIA)**

- The Security Working Group will be required to deal with information, which may result in a high risk to individuals rights and freedoms. In order to protect this information, the contractor will be required to complete a mandatory DPIA (please refer to the Viewpoint Security section) at the earliest opportunity via MoJ's One Trust tool.
- The DPIA is a tool for identifying and minimising risks around the collection, processing and disclosure of personal data and allows the Security Working Group to demonstrate compliance with the requirements of the law.
- A DPIA will allow the Security Working Group to systematically analyse, identify and minimise the data protection risks of a project.

8.17 **Data Retention Policy**

- The purpose of the Policy is to ensure only information relevant to support the work of Property Directorate is retained in compliance with the General Data Protection Regulation 2018 (GDPR), Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOI) and MoJ's Estates Records Retention and Disposition Schedule . All information no longer relevant or required is disposed of or destroyed correctly and in line with departmental guidance. Please refer to Information Wise — What to keep (publishing.service.gov.uk)

- The Policy will also ensure information is readily available in the event of requests arising from external audits, reviews etc. Where there is a need to keep electronic records permanently, these will need to be stored in the Property Directorate agreed filing system.

- A Records Retention and Disposal Schedule (RRDS) is required to manage MoJ's obligation to destroy records not selected for permanent preservation. This can be found in the policy.

9. Digital/Cyber Security

9.1 The handling of all information; shared, published or exchanged is to be secure in accordance with the HMG - Technology Code of Practice. Guidance is to comply with these standards can be found in ISO 19650-5 and Ministry of Justice publications. Furthermore, the Construction Partner shall comply with the HMG – Technology Code of Practice that are available on the Viewpoint for projects website.

9.2 MoJ Viewpoint will be the official Common Data Environments (CDE) for MoJ projects. Any software systems such as office 365, Viewpoint etc will need prior approval from the Authority before they can be used on any project. Contractors/service providers will be required to complete the Secure Data Impact Assessment Document (SDIA). Any such system must adhere to the principles of Accessibility, Auditability and Security and as such the system must be effectively managed by a suitably trained/experienced manager. All those with access to a software platform that contains any MoJ data must demonstrate that they have appropriate Security Clearance. Approved software via the SDIA process remains on an approved list for 18 months and okay to be used by suppliers unless there is a change (e.g., location) in which case a new SDIA needs to be raised for reassessment.

9.3 All information must be stored in a secure area within the CDE and must be restricted to a strictly "need to know" group of named individuals.

9.4 All data produced and collated on behalf of the MoJ in connection with the activity in question is the property of the MoJ. Therefore, the contractor/service providers must produce, upon request by the Authority, any and all information held within the CDE to be audited by the BASM or their delegated authority.

9.5 The contractor/service providers must notify all personnel, and the personnel of their supply chain handling information relating to the Project of these security requirements. The

contractor/service providers must include the requirements of this letter in all contracts with their supply chain and is responsible for ensuring compliance. They shall be responsible for the issue and return of all documents to its own personnel and the personnel of their supply chain.

9.6 The contractor/service providers must report immediately to the MoJ by the most expedient method, the loss of any document stating details of the loss and what the contractor/service providers is doing to secure its recovery.

9.7 Neither you nor any associated third parties or sub-contractors may put Official Assets or any Aspect of this requirement (including, where relevant, the sourcing of material and/or equipment) at risk without prior MoJ approval in the following circumstances:

i. in a Cloud environment (including the use of Software-as-a Service applications);
ii. at offshore risk[1];
iii. with any entities which are subject to Foreign Ownership, Control or Influence (FOCI)[2]: if your company, or any associated third party or sub-contractor, is or becomes subject to FOCI you must inform Mace/MoJ;
iv. any items subject to Trade and Export Controls; or
v. any work conducted under this requirement that involves or has a reliance on Artificial Intelligence and/or Machine Learning mechanisms.

[1] *Offshore risk covers the delivery of any part of this requirement (including access to Official Assets) by individuals or entities based outside the UK.*
[2] *An entity is considered to be subject to FOCI if MoJ reasonably considers that it is or may be owned or controlled by a Foreign National or a Foreign Interest; or if a Foreign National or Interest has a Significant Interest; or is in partnership with a Foreign National or Interest; or if any Foreign National/government/other entity has any ability to direct or decide matters affecting the management or operations of the entity including but not limited to acting in a manner which may result in unauthorised access to Official Assets or may otherwise adversely affect the performance of MoJ contracts or the interests of the United Kingdom. Further guidance is available from MoJ.*

10. Remote Working

10.1 Personal devices and personal online accounts should not be used for MoJ work.

10.2 Those working remotely or from home should be careful not to draw attention to the fact they are working on OFFICIAL information.

10.3 Any loss of information while working remotely should be reported immediately.

10.4 Avoid working in a public area where there is a risk of being overlooked.

10.5 No information above OFFICIAL should be viewed in a public area.

10.6 The MoJ policy is that people working on MoJ projects are not able to travel and work abroad, the MOJ policy on the ability to be able to work abroad applies to MOJ permanent

employees only. Contractors/service providers are not permitted to work remotely from abroad in any capacity.

11. Security Incident Management

11.1 It is the responsibility of every individual to ensure that they maintain the most appropriate levels of security. They can do this by complying with this document. Breaches of security not only cause embarrassment and reputational damage to the MoJ but can result in the compromise of the confidentiality, integrity, or availability of assets. In the most serious of cases the damage caused may impact on operations, prejudice national security, and endanger lives. All breaches, or suspected breaches of security, must be taken seriously and reported immediately.

11.2 Personnel should be in no doubt that if they deliberately or negligently breach security disciplinary/administrative action and, in serious cases, termination of employment/Service and/or criminal prosecution may follow. The MOJ have stipulated that security breaches and loss compromise of their assets including data, will not be tolerated.

11.3 All breaches of security will be notified to the MOJ and may be investigated further.

11.4. The Security breach management process can be found on the Viewpoint Security section along with the activity guides on reporting procedures.

12. Physical Security Conditions

12.1 If appointed to a MoJ project, the contractor/service providers will need to ensure that there is a designated 'on- call' Incident Control Officer identified to react to a breach in security.

12.2 The contractor must appoint at the earliest opportunity a Construction Security Manager from within their team who will be accountable for all Security matters during the Project within that contractor team. The contractor's project director will remain responsible for ensuring their teams comply with the security requirements as a basis for meeting their contractual requirements.

12.3 General Conditions:

12.3.1 The following conditions must be met by all contractors working on any MoJ Establishment:

12.3.2 Security precautions arise from the need for the establishments to continue to function during the works of the contract and from the paramount need to maintain appropriate security during the execution of the works. The contractor shall allow in their rate for the necessary flexibility in working hours and conditions commensurate with these needs.

12.3.3 Security requirements arise from the need for the Authority to control risk at all times and to prevent a breach or compromise of the security as a direct result of

the execution of the works. The contractor shall take appropriate measures for complying with such conditions in meeting these requirements.

12.3.4 A Security, Health and Safety and Access Requirements pre-start meeting is to be undertaken at the earliest opportunity; to review security requirements in line with this document; to include a record of further meetings; and to log bespoke security conditions that will be required for each site. These conditions must be logged in the SAL Response Document available through the Viewpoint Security Section. This will be led by the Construction Security Manager.

12.3.5 The appointment of the Construction Security Manager must be made at the earliest opportunity. Their responsibilities will be guided by the MoJ's Built Asset Security Management Strategy and Plan and will include managing site specific security procedures, training and checks.

12.3.6 All conditions set out below shall be strictly observed by the contractor /service providers, their employees, subcontractors and all others under their direction from the start to the completion of the works.

12.3.7 All plant, tools and vehicles, scaffolding, temporary accommodation etc. mentioned elsewhere in the document shall comply with these security conditions.

12.3.8 Nothing contained in this document shall relieve the contractor/service providers of his obligations to comply with the Health and Safety at Works Act, Local Authority Requirements and other similar obligations imposed under the contract.

12.3.9 The Construction Security Manager will ensure a comprehensive site security induction is carried out with all personnel. On completion of which all site employees are to sign and return a security disclaimer, which will be filed and recorded and maintained by the Construction Security Manager.

12.3.10 Security induction training will be refreshed every 6 months for personnel who are continually employed. Re-engagement of personnel will also require a new induction. In addition to which, updates in security procedure will be disseminated by the most expedient and effective method to all personnel on site within a week of the update. Personnel records shall show that the individual has received any such updates. The occurrence of this update and its dissemination to personnel shall be recorded and retained by the contractor.

12.3.11 The Construction Security Manager shall ensure the implementation of personnel site access controls (biometrics or equivalent assurance system). A robust procedure will be implemented to ensure that site access is only granted to those presenting the correct identification with the correct clearances. Furthermore, the digital security surrounding the storage must be addressed to provide appropriate assurance (backup, encryption and site servers).

12.3.12 All contractors/service providers must complete the General section within the SAL Response Document (this can be found in the Viewpoint Security section) to reflect how the conditions in this document are to be met. Depending on the type of establishment you are working in, there will be further conditions that need to be

addressed. Further details can be found in this section and the SAL Response Document. If working adjacent to or on a live site, the procedures are to reflect those held locally and be approved by that establishment, Access to the procedures will be supplied upon request.

12.3.13 The Construction Security Manager must implement the update of security measures required for the site, zones, floors or rooms as the lifecycle of the project progresses and develops. It will be the Construction Security Manager's responsibility to detail the sequencing of the security upgrades, communicating and coordinating the changes to ensure that as the build sequence continues, vulnerable points are not exposed in the site security management.

12.3.14 The Construction Security Manager will ensure that vehicular booking in/ out procedures are adhered to and passes shown on all vehicles at all times (note that security clearance will not be required for delivery drivers escorted within the establishment).

12.3.15 The Construction Security Manager will set the specific digital strategy which will include the use of any internet, radio and telecommunication devices. The use of any such device will not be permitted unless the Site Specific Security Risk Assessment; local operational Establishment procedures; or Health and Safety risk assessments dictate otherwise.

12.3.16 Unless expressly permitted to the contrary, no mobile phones will be allowed within the establishment. Nor will any photographic device.

12.3.17 If Unmanned Aerial Vehicles are to be used to record site progress, permission must be sought from the Authority and relevant establishment and obtained before use. Only certified and accredited Drone operators are to be used during the works with prior agreement from the MoJ. All footage from the drone should be immediately removed and transferred to the MoJ's CDE. In some circumstances it is an offence to fly a drone over certain prisons without specific authority.

12.3.18 Rubbish and surplus excavated material is not to be allowed to accumulate on the site unless authorised by the authority beforehand to the contrary (i.e. to be stored for later landscaping use). This accumulation of materials should never be close to an operational prison.

12.3.19 The Construction Security Manager must ensure the security of the site 24 hours a day, seven days a week for the duration of the contract.

12.3.20 Contractors/service providers must employ and support the MoJ Whistle Blowing Policy, whereby observed breaches of security protocol and procedure can be highlighted in the correct manner.

12.3.21 All plant, tools and materials must be accounted for during the course of the project. The contractor will be required to report and record the losses of any tools, taking loss statements and mapping approximate location of lost items is essential and must be done immediately upon discovery of the loss.

13. Social Media

13.1 The Ministry of Justice encourages responsible use of social media. When participating online you are accountable for your contributions and the correct handling of security marked documents.

13.2 The social media policy applies to permanent and temporary employees, probationers, agency workers and all others who may by representing the Department at various times.

13.3 For more information please refer to the Ministry of Justice Social Media Policy and Guidance Documents.

13.4 All project posts released on social media should only be done so with written approval from the MoJ Comms team.

13.5 The contractor/service providers should take reasonable steps to communicate to their teams about the risks of social media and how to protect themselves and project information.

14. Use of Information

14.1 No information provided by, or generated in connection with an MoJ project may be used, reproduced, transmitted or adapted for alternative use outside the project scope without prior express permission from the MoJ.