UK BIM Alliance - Security Guidance
BIM Execution Plan (BEP) Content

Title of guidance:	*Basic Security Considerations for the BIM Execution Plan*
Author:	*Javed Edahtally*
Company:	*Metropolitan Police Service*
Email:	*Javed.edahtally@met.police.uk*
Objective of guidance:	*To provide guidance as to how access to data could be considered, the questions to ask and how best to action.*

Abbreviations/acronyms	**Full name**
BEP	*BIM Execution Plan*
CDE	*Common data environment*
EIRs	*Employer Information Requirements*
PESTEL	*Political, Environmental, Social, Technological, Economic, Legislative*

Relevant/referenced sources	
PAS 1192-2:2013	*Specification for information management for the capital/delivery phase of construction projects using building information modelling*
PAS1192-5: 2015	*Specification for security-minded building information modelling, digital built environments and smart asset management*
CPIx BIM Execution Plan	*http://www.cpic.org.uk/cpix/cpix-bim-execution-plan/*
Cyber Essentials Scheme	*https://www.cyberaware.gov.uk/cyberessentials/*

Keywords:	*Base line Security, BEP, BIM Execution Plan, Cyber Essentials*

Briefing note text

The BIM Execution Plan (BEP) is a technical response developed by the project delivery team. It addresses the requirements set out in the Employers Information Requirements (EIRs) and confirms the supply chain's capabilities - how and when project information is to be prepared, by whom, and using what standards/rules.

It is defined as a "*plan prepared by the suppliers to explain how the information modelling aspects of a project will be carried out*" in PAS 1192-2:2013. The structure of a BEP will usually be based an established template ie. CPIx. It is typically submitted in two stages: initially to confirm approach and capability (referred to as a 'pre-contract BEP' and offering a means of supplier evaluation). The 'post contract BEP' will then be developed in detail once appointment/building contract has been awarded.

Every project is different and therefore the associated data protection and information management requirements adopted will need to reflect this.

Nonetheless there are some basic steps that can help reduce data and information risks. It is suggested that in the absence of appropriate security considerations within the clients EIRs , the BEP considers baseline security measures for the project. These measures can be broadly categorised into 4 key areas:

- Personnel
- Process
- Physical
- Technical

Personnel details: Personnel details including contact names, organisations, telephone numbers and email addresses of the project delivery team including the supply chain and client are likely to be identified in BEP and within other project files. As a result this data may be covered under the Data Protection Act and new data protection legislation published in 2018.

It is therefore important to ensure that this information is managed accordingly and is not unnecessarily published (for example, on-line). The BEP may contain guidance on acceptable sharing of this information.

Process details: Where the common data environment (CDE) is administered by a member of the project delivery team the BEP may consider how access to the CDE and permissions relating to the files held within the CDE are to be managed.

Where the CDE is administered independently the BEP may confirm guidance around permissible download of files and communication and distribution of files by email and portable media.

Physical details: Even if a project is not deemed sensitive in accordance with PAS 1192-5 there may be sensitivities around aspects of it for commercial, political and/or safety reasons.

Similarly certain spaces and/or functions within or around the built asset may be sensitive. The BEP might therefore consider how space usage and project identifications and activities are stated in project files and remain appropriate. For example, spaces might be alphanumerically referenced instead of naming the spaces according to activities within them on a per project basis.

Equally there is a collective duty to ensure due consideration is afforded to neighbouring built assets to reduce any exposure to them by limiting publication of data in relation to them.

Technical details: The BEP might detail security related standards (such as the Cyber Essentials Scheme) that the project delivery team will be working in accordance with.