UK BIM Alliance - Security Guidance
Drafting Information Requirements

Title of guidance:	*Drafting information requirements*
Author:	*Sarah Davidson*
Company:	*Gleeds*
Email:	*Sarah.davidson@gleeds.co.uk*
Objective of guidance:	*To provide guidance on things to think about when drafting content for operational, asset and project information requirements*

Abbreviations/acronyms	**Full name**
OIRs	*Operational information requirements*
AIRs	*Asset information requirements*
EIRs	*Employer's Information requirements*
BEP	*BIM Execution Plan*
AIM	*Asset information model*
CDE	*Common data environment*

Relevant/referenced sources	
PAS 1192-5:2015	*Specification for security-minded building information modelling, digital built environments and smart asset management*
PAS 1192-2:2013	*Specification for information management for the capital/delivery phase of construction projects using building information modelling*
PAS 1192-3: 2014	*Specification for information management for the operational phase of assets using building information modelling*
BS 1192-4: 2014	*Collaborative production of information Part 4: Fulfilling employer's information exchange requirements using COBie – Code of practice*
	The Cyber Essentials Scheme

Keywords:	*Confidentiality, non-disclosure, social media, common data environment, cyber essentials, compliance, resilience*

Briefing note text

There are typically three documents or elements of content that the Employer (or their representative) needs to think about for a construction project:

1. Operational information requirements (OIRs)
2. Asset information requirements (AIRs)
3. Employer's Information Requirements (EIRs)

CPNI has drafted EIRs content for projects adopting a security-minded approach – you can see this at CPNI.Gov.UK. For baseline requirements it is suggested that consideration is given to issues such as:

- ✓ The extent to which information can be publicised. The project or aspects of the Employer's business operation may be subject to confidentiality and non-disclosure agreements and the Employer may have security policies that should be adhered to. In addition the Employer may have some concern about the sharing of information via social media.

- ✓ Maximum permitted level of detail and information contained in design and construction models and other information. Does the Employer really want it to be apparent where an intruder alarm control panel is located, along with its detailed installation and operating instructions for example?

- ✓ The requirements for structured file naming; this both assists with file management but also helps to not over or unnecessarily disclose file content.

- ✓ Specific compliance requirements such as evidence of compliance with the Cyber Essentials scheme or Cyber Essentials Plus – a recommended minimum requirement within PAS 1192-5. This will help provide assurance that organisations working on the project have reasonably resilient and protected IT systems themselves.

- ✓ How project files should be transferred from a project Common Data Environment (CDE) to a CDE (or similar) supporting asset operation and management

- ✓ Any requirements for disposal of data and information about either the project, the operation and management of the completed asset or the Employer's organisation.

- ✓ Basic good house-keeping around the use of computer systems, portable media and mobile devices.

- ✓ Information that is to be withheld from a consolidated asset register/COBie file. Whilst this is less likely for baseline it is worth consideration.

- ✓ Specific management requirements to be detailed in the pre and post tender BIM execution plan (BEP) coupled with tender evaluation measures. Make sure that organisations appointed to a project understand and can work to the baseline requirements detailed.

The CDE will in theory, hold all of the files relating to the design and construction of the completed project. The Employer is unlikely to want the project to be exposed to any avoidable CDE downtime nor for the project files to be lost in cyber-space. CDEs also have the potential to give everyone working on the project access to everything. It is good practice then to make sure that the EIRs contains clear requirements around:

- The management of access to the CDE
- Permissions within the CDE
- Resilience of the CDE itself (where it is hosted via the project team)
- The continued or uninterrupted service of the CDE throughout the project's life (ditto)

Remember in drafting information requirements you are thinking about 'baseline' security management. You want to make sure that people take care over management of data and information and that there is a degree of systems resilience without it becoming an expensive or over-complicated matter.