UK BIM Alliance - Security Guidance
Common Data Environment (CDE) Principles

Title of guidance:	*CDE Principles*
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**
CAD	*Computer Aided Design*
CDE	*Common Data Environment*
FM	*Facilities Management*
PLQ	*Plain Language Questions*

Relevant/referenced sources	
PAS 1192-5:2015	*Specification for security-minded building information modelling, digital built environments and smart asset management*
ISO 27001: 2013	*Information technology – Security techniques – Information security management systems - Requirements*

Keywords:	*Access, Permission, Administration, Control, CDE, Baseline, security, BIM,*

General notes to support the text/publication on the UK BIM Alliance website
[Baseline Security Guidance for Project Data, use of a Common Data Environment]

Briefing note text

A common data environment (CDE) is a collaborative information area that allows the client and project delivery team to engage and interact with design, construction information and operational data and information. It is important to ensure that the CDE chosen meet the needs of the project and is acceptable to the client.

The CDE may be procured by a member of the project delivery team (for example the principal contractor) as part of their usual offering. Alternatively and perhaps more appropriately, the CDE may be owned/purchased and managed by the client. In some cases there will be both with the client operating their own CDE for internal or asset management purposes.

Data and information present within a CDE will be in the form of documents, data and graphical data in the form of 2D CAD plans and 3D models. A CDE can be anything from a basic setup of a series of folders on a networked hard drive on an internal network - to a dedicated, off the shelf cloud based application designed to facilitate regular interaction of complex data with audited files. The choice of CDE might be driven by budget and/or how accessible the information needs to be. Cloud based systems are not restricted to the confines of an organisation's network but can allow data to be exchanged across the globe. Dedicated CDE's also have integrated functions such as search tools, document management, visualisation and performance reporting.

For a number of reasons, it is important to limit and protect this information aided by appropriate document control and information security even where a project is not considered especially sensitive (as defined by PAS 1192-5). Project files, such as 3D models are likely to hold vast amounts of

information, including in some cases, personal information which would come under the Data Protection Act. It is therefore a legal obligation to ensure this information is suitably protected.

CDE baseline security measures might include:

- Establishing what standards the CDE is in compliance with in terms of both data hosting and CDE administration (for example ISO 27001)
- Ensuring managed/controlled access to (plus denial of access to) the CDE
- Ensuring managed and controlled activity permissions relating to CDE files
- Establishing that the CDE is hosted on a secure server with appropriate backups and resilience measures so that any failure of the servers will not compromise the project
- Ensuring that adequate training (covering security breaches and implications) is considered for people who will be using the CDE
- Requiring that uploaded data is appropriate to the project

Refer to the CDE process map for a suggested CDE procurement/use process

Practical Baseline Plain language Questions (PLQ's) to consider when implementing a CDE are suggested as follows:

In terms of CDE access:

- How is access to the project data controlled? e.g. username and password
- Who controls/monitors access: Information Manager/Document Controller/Administrator, etc.?
- When are access controls reviewed: New organisations/team member joining a project/ Removal of access for people and organisations no longer involved in the project etc.?
- How are unauthorised access attempts recorded?

In terms of CDE file, data and functionality permissions:

- How does the CDE allow for user permissions to be applied? (e.g. read only, read only and mark up, edit, upload/download or do these limit the scope of data a user can access – only part of a model, level of detail etc.)
- How will permissions be allocated? i.e. by role?
- Who is/how many individuals are responsible for administrating permissions?
- How are administrator privileges controlled?

Implementation and Review

Once security measures are in place it is important to review:

- If access controls have/are being applied as intended via appointed responsible owner(s)
- Who has requested permissions, what those permissions are (i.e. read, write, edit, mark-up) and for how long they need to be available for;
- Any additional access needs to be provided for future activities – i.e. in preparation for handover to FM?
- Use of the CDM for file transfer. Where possible, it is suggested that it is best practice to transfer files between all parties through a CDE environment.