UK BIM Alliance - Security Guidance

Managing Access and Permissions

Title of guidance:	*Managing access, permissions, denial - CDE and internal drives*
Author:	*Rachel Heywood*
Company:	*Gleeds*
Email:	*rachel.heywood@gleeds.co.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**
CDE	*Common Data Environment*
FM	*Facilities Management*

Relevant/referenced sources	

Keywords:	*Access, Permission, Administration, Control*

General notes to support the text/publication on the UK BIM Alliance website
[insert as applicable]

Briefing note text

Data and information have intrinsic value and should be protected even for baseline requirements. Protection can be aided by appropriate document control and information security.

Information security should consider the control of *access* to information in terms of who, what and how. It is also useful to understand not only what is able to be accessed but control how it can be amended via a series of *permissions*.

Such controls can apply equally to a common data environment (CDE) as to an internal drive or electronic document management system.

Plan

A simple set of questions can be asked to help inform a strategy to maintain baseline information security:

Access

- How is access to the CDE/drive to be controlled? e.g. username and password
- Who controls access?
- Are access controls reviewed for:
  New organisations joining a project
  New members of the team joining a project
  Removal of access for people and organisations no longer involved in the project
- Can access be monitored? (if required)
- Are denial records / unauthorised access attempts recorded?

Permissions

- Does the CDE/drive allow for permissions to be applied?
- What are those permissions? E.g. read only, read only and mark up, edit, upload/download
- How will permissions be allocated? Who needs to see and action what to fulfil their role?
- Who is responsible for administrating permissions?
- How are administrator privileges controlled?

Implement and Review

Once the controls are in place it is important to think about whether the strategy is working as it should.

- Are agreed access controls being applied?
- Is access being monitored?
- Do changes need to be made to access control?
- Have the requested permissions been applied?
- What are those permissions? E.g. read only, read only and mark up, edit, upload/download
- How have permissions been allocated?
- Do changes need to be made to permissions?
- Is the CDE being administered effectively in terms of access?
- Can the strategy look ahead? Does additional access need to be provided in preparation for handover to FM teams?