



CONFIDENTIALITY, COPYRIGHT, DATA PROTECTION AND SECURITY

Protecting sensitive project data

Within the global architectural, engineering and construction (AEC) industry, as online collaboration systems become increasingly popular, potential customers are demanding reassurances about systems' provisions with respect to confidentiality, copyright, data protection and security.

Drawing on experiences gained in delivering thousands of projects, including sensitive schemes for financial institutions and defence agencies, BIW Technologies (BIW) has accumulated considerable expertise in protecting its customers' mission-critical information. It has created robust legal frameworks protecting confidentiality and copyright, and deployed state-of-the-art security measures. Little wonder, then, that it is trusted by its customers and users as a powerful and, above all, secure system.

Why you should read this paper

Within the global architectural, engineering and construction (AEC) industry, online collaboration systems are becoming increasingly popular. As design, construction and operation and maintenance information may have long-term security risks, potential customers - whether they are clients, contractors, consultants or others - are also demanding reassurances about systems' provisions with respect to confidentiality, copyright and security.

This paper focuses on these issues. In so doing, it augments other BIW papers and publications:

- 'Legal aspects of collaboration' focuses on various key areas of potential concern, including the legal status of electronic communications, the legal relationship with the technology provider, and issues relating to service interruption or unforeseen termination.
- 'Ownership of data and copyright' - from Wilkinson, P. (2005) *Construction Collaboration Technologies: The Extranet Evolution* (London: Taylor & Francis), pp. 120-121.¹
- 'Hosting collaboration' outlines the key minimum quality of service (QoS) requirements for hosting a collaboration system (a BIW technical paper entitled 'A lowest risk solution: the BIW hosting infrastructure' describes in detail the extensive physical and technological safeguards surrounding the BIW infrastructure).

Key elements of these documents are summarised in this paper (full versions of the original papers are available upon request from BIW Technologies - covered by a non-disclosure agreement, NDA, where necessary).

Contents

■ Why you should read this paper	2
■ Why you should read this paper	2
■ Contents	2
■ Confidentiality of information	3
Master Licence Agreement (MLA)	3
End User Licence Agreement (EULA)	4
Related documents	4
■ Copyright	5
■ Data Protection	6
■ Security of the collaboration platform	7
Minimum QoS requirements	7
Secure BIW infrastructure	8
Secure communications	8
Full audit trail security	9
Individual security	9
■ BIW: a proven secure system	9

¹ Paul Wilkinson is head of corporate communications at BIW Technologies, and has been called one of the UK's leading analysts on construction collaboration technologies.

Confidentiality of information

Entrusting the information created by a customer's project team to a collaboration system places some strong obligations on the technology provider. BIW always ensures appropriate legal arrangements are put in place to support its relationships - both with the ultimate customer (usually through its Master Licence Agreement, MLA), and then with the Licensee's selected end-users (via End User Licence Agreements, EULAs).

End-users are selected by the Licensee, and these third parties will have their own agreements, which will include treatment of confidential data and information.

BIW also urges its customers to create and support appropriate agreements between individual project team members stipulating use of the BIW technology (the core collaboration system has historically been branded as BIW Information Channel™, or the Channel) to communicate with each other. This may require amendments to consultant agreements and/or contracts with and between the main contractor and sub-contractors, suppliers, etc.

Master Licence Agreement (MLA)

The MLA covers the relationship between BIW and the ultimate customer (or its agent). Among other issues, the MLA includes provisions in respect of the confidentiality of project-related information, including security precautions with respect to user names, passwords, etc. Specifically:

[The Licensee will:]

- 4.3.2 *use and adhere to the user names, passwords, and any authentication codes or security procedures which we notify to you from time to time; and*
- 4.3.3 *establish reasonable security precautions, accuracy checks and back up procedures in respect of your data and operational procedures ("Safeguards") to guard against possible unauthorised access, inaccuracy, or loss of your data howsoever caused, in your use of the Services.*
- ...
- 7.6 *Both we and you undertake to the other not to disclose to any third party any information about the other, its business, and its methods or processes which is identified to the other as being confidential in nature, or a trade secret, and is not in the public domain (unless it enters the public domain through the breach of this provision by the other). However, you may make information concerning the Services available to your auditors or to tax, excise or similar authorities but only to the extent that is required by law.*

End User Licence Agreement (EULA)

The EULA covers the contractual relationship between BIW and a project's participants. In many key respects, including confidentiality of project-related information, it reflects conditions imposed in the MLA, but at a level specific to participants. For example:

3.3 You must establish reasonable security precautions, accuracy checks and back up procedures in respect of your data and operational procedures ("Safeguards") to guard against possible unauthorised access, inaccuracy, or loss of your data howsoever caused, in your use of the Channel.

...

6. Confidentiality & Privacy

6.1 In consideration of the End User Licence granted to you, you agree to exercise due care in order to keep confidential any trade secrets you may learn and all other confidential information concerning the Channel, including the usernames and passwords issued to you.

6.2 Information may be confidential to the Client, the Project, the Participants or to BIW. You agree to keep all Information you receive in the course of using the Channel in the strictest confidence, except for communicating the Information to Participants in the normal course of participating in a Project, or Information which is manifestly in the public domain or which cannot reasonably be regarded as being of a confidential nature.

6.3 You agree to ensure that all relevant employees, agents and sub-contractors are aware of the confidentiality provisions in this clause 6 relating to the Channel and to Information, and that they comply with them.

Related documents

Complementary information to the MLA and EULA may be contained in separate documents (but forming part of the contract), including schedules outlining agreed levels of BIW service delivery (service level agreements, SLAs), and project protocol documents.

If additional assurances in respect of confidentiality are required, BIW would suggest that the appropriate parties sign a non-disclosure agreement (NDA). BIW's standard format NDA can be provided on request.

Copyright

Sharing project information in an electronic environment can make some team members anxious about the use, and possible abuse, of the information they contribute. For example, depending on what project protocols have been agreed, architects and other designers may be required to submit CAD drawings in their native format (eg: Autocad files in DWG format), giving rise to concerns about unauthorised use of design drawings - and hence breach of copyright - based on a perception that an electronic system may be more prone to abuse than a paper-based one.

So far as internet-based construction collaboration technologies are concerned, there are no special rules relating to copyright. Protection of CAD drawings and other material is governed by copyright law.² As such, designers and others should follow normal procedures to protect their intellectual property; eg: RIBA, the professional body for UK architects recommends:

- Include a statement of permitted use on all drawings. For example: 'This [plan/drawing] has been produced for [client] for the [project] and is submitted as part of planning application [application number/relating to site name] and is not intended for use by any other person or for any other purpose.'
- Include the architect's name and logo on all drawings and make sure that all work carries a copyright statement, for example, '© [name of copyright owner] [date of creation]'
- Put a watermark through all drawings - this could be the architect's name or logo.

Client contracts with designers usually include provisions about copyright in the designer's designs. Typically, the designer retains ownership of the copyright but grants a licence to the client and other team members to use the design in relation to the specific project. The use of an electronic collaboration platform does not change this, though one can foresee instances where a design may have been developed collaboratively to such an extent that it no longer represents the intellectual output of one individual or firm but of a group, raising issues about co-ownership of the copyright in that design.

Should a breach of copyright be suspected, any construction collaboration technology that maintains a full audit trail will at least be able to catalogue every instance of a CAD file being accessed, viewed or downloaded, detailing who instigated the action and at what date and time. Subject to the normal court rules, this audit trail can be offered as evidence. This contrasts with the situation with paper-based information, CDs or email attachments where it can be difficult, if not impossible, to show who has had access to a particular drawing once it has left the designer's office.

² The UK's Copyright, Designs and Patents Act 1988 reflects similar legislation in the US and most industrialised nations, all covered by the Berne Convention and administered by WIPO, the World Intellectual Property Organisation.

Data Protection

Broadly, the Data Protection Act 1988 covers any information that relates to living individuals which is held on computer. For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified. The Act created eight principles to make sure that information is handled properly. These state that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than is necessary
- processed in line with your rights
- secure
- not transferred to countries without adequate protection.

By law data controllers have to keep to these principles. BIW is registered as a data controller on the Data Protection Register (number Z478751X).

One of the purposes for which BIW collects personal data is for 'accounts and records', defined as follows:

Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity.

BIW collects personal data about each user of its platform in order to identify them as users of the system, to ensure that the system is securely and correctly configured to reflect each user's role and responsibilities within a project, and to record their interactions with the service (including the creation of an audit trail, the compilation of reports on use of the system, etc).

The BIW master licence agreement, MLA, clearly states (clause 4.1.2) that users must not use BIW's services to 'publish, post, distribute or disseminate personal information on individuals prohibited under UK and EU data protection law';³ the MLA (clause 8.2.1) also specifically requires users to 'to fully comply with all laws, regulations, licences or binding codes or standards of practice relevant to personal data (including without limitation the Data Protection Act 1998)'.

³ A similar clause, 3.1(b), is included in the BIW end-user licence agreement, EULA.

Through the system end-user license agreement, users are also notified about the use of 'Cookies' within the BIW platform, as follows:

Cookies are small pieces of text information generated by our web servers that are stored on your computer. These are not a danger to your computer and do not spread viruses.

BIW uses two types of cookies:

- a session cookie - this holds information which identifies you as a valid user. This type of cookie only lasts for the duration of your login session and enables us to provide you with a continued level of secure access to BIW. If you set your Internet browser so that session cookies are not to be downloaded then you will not be able to use BIW.
- a persistent cookie - as the name suggests this lasts beyond the duration of your login session and holds details of the preferences you have made whilst using BIW, such as viewer choice. If you set your Internet browser so that persistent cookies are not to be downloaded then you will still be able to use BIW but your preferences will not be saved.

In neither case is personal data downloaded or stored on your computer.

Security of the collaboration platform⁴

Minimum QoS requirements

The BIW infrastructure meets or exceeds all basic quality of service (QoS) requirements, including high levels of system, data and application security:

- high levels of performance (eg: speed of access to data)
- constant availability of application and data, 24 hours a day, 365 days a year, coupled with low latency (ie: minimal delay between sending data and recipient receiving it)
- high reliability and resilience (eg: full redundancy - all primary network system components such as servers, power sources and telecommunication links have secondary back-ups in case they fail)
- high levels of security, both physical (preventing unauthorised access to servers) and technological (preventing hackers, viruses, denial of service attacks, etc), and

⁴ This section draws on information from a BIW technical paper entitled 'A lowest risk solution: the BIW hosting infrastructure'. This details the extensive physical and technological safeguards surrounding the BIW infrastructure, and is available - subject to a signed NDA - upon request from BIW.

- service management to recognised standards of best practice (eg: the UK government-created ITIL - increasingly adopted worldwide as the standard for best practice in IT service provision - and ISO/IEC27001:2005).

ISO/IEC27001:2005 certified

The BIW hosting provider is certified to the ISO/IEC27001:2005 standard for information management security. This requires, among other things, that it implements change control and business continuity plans, making websites more robust and protecting them from potential threats to availability.

Secure BIW infrastructure

The data centre was designed with security in mind. Mechanical rooms are physically segregated from the server farms to enhance secure access. Movement within and around the facility is monitored and constrained. Key-cards, electromechanical locks and biometric palm readers ensure that only those authorised to enter, and then authenticated, are allowed to gain access.

The BIW system is also constantly monitored 24 hours a day, 365 days per year. This monitoring covers all hardware and the BIW application, and includes virus protection and intruder detection.

BIW database servers are situated in a separate section of the network to ensure that they are not visible directly from the internet. In the unlikely event that a hacker was able to hack onto the web servers, they would have no access to client data. No client data is held on the web servers.

The firewall is also constantly monitored to check for unusual traffic patterns indicating 'denial of service attacks' or hacking attempts. In the event of a hacking/DOS attack discovery then the originating IP address will be blocked.

Penetration tested

At various times, the BIW system has been subjected to rigorous independent security audits (the latest undertaken by IT consultants from KPMG commissioned by Bovis Lend Lease) in which IT experts try to hack into the BIW system. To date, the system's safeguards have effectively prevented any intrusions.

Secure communications

Connections to the BIW platform can be secured using a secure server certificate (HTTPS), similar to that used when making online financial transactions. Such server certificates provide a website or web server with an electronic means of confirming both the identity of the website operator and ownership of the relevant domain name. It operates seamlessly, creating an encrypted link between the client's browser and the web server, which protects all the information that is sent during transactions. The benefits of secure server certificates include:

- reassurance to visitors of the authenticity of the organisation's websites
- enhanced security, as all data sent or received via the secure session is encrypted

128-bit encryption

New secure BIW channels use 128-bit encryption certificates - a 'High Security' level of encryption. With a possible 309,485,000,000,000,000,000,000 (309 septillion) different key combinations, this level of security has yet to be penetrated.

Full audit trail security

The BIW audit trail provides a complete and tamper-proof record of who did what and when. Individual users are required to enter a unique user name and password to use the BIW system. BIW's technology does not allow documents (or versions of them) to be deleted or over-written; all document and drawing versions and associated revisions are electronically time- and date-stamped, and the identity of the individuals involved in their production and amendment is also automatically recorded.

Individual security

The BIW platform is entirely database-driven. Any information an end-user sees is restricted to that authorised within the database security set-up. General access is controlled by a password so anyone trying to gain access will be unable to do so unless they have a current password. BIW is able to track who is accessing and from which IP address, so it would be possible to limit access quite tightly at this basic level.

BIW: a proven secure system

Since 1998, the BIW system has been deployed on thousands of projects by hundreds of customers. The range of projects includes many sensitive and mission-critical schemes, including:

- **financial institutions** - data centres, headquarters buildings and high street outlets for major financial institutions (eg: Royal Bank of Scotland, HBOS, Abbey - now part of Banco Santander, Barclays, Morgan Stanley)
- **airports** - buildings at several major international airports (eg: London Heathrow, London Gatwick, Manchester Airport, etc)
- **defence** - establishments (eg: Andover North, Colchester Garrison) for the UK's Ministry of Defence
- **justice** - eg: Manchester Criminal Justice Courts

- **medical research** - eg: clinical research laboratory, Cambridge

The BIW system has been used by over 90,000 registered users from more than 9,000 different organisations, and has managed literally millions of copies of drawings and documents and many more process-related items. Despite this massive volume of communications and the many millions of information transactions completed, the BIW system has never been called into question in litigation.

Employing state-of-the-art security measures supported by internationally-recognised information security management standards, the BIW platform is trusted by BIW customers and accepted and respected by its users as a powerful and, above all, secure system that will more than withstand robust scrutiny during any legal processes.