

## DATASHEET

To enable true collaborative team working practices online, BIW Technologies (BIW) places a very high priority on security. Accordingly, even the minimum levels of secure access to BIW's systems are set at a high level. This ensures, first, that only authorised individuals can access, view, exchange and work upon the information stored. Second, it ensures that nothing can be deleted from the system, whether accidentally or maliciously, while all other interactions are logged in the system's audit trail. Security can also be finely controlled by varying individual's rights to access certain types of data.

The BIW collaboration platform has been designed to allow customers and their project teams to specify the levels of security and information transparency that are appropriate for their needs. For example, some clients or other team members may require strict controls on who can access particular types of information. In other scenarios - eg: projects or programmes of work undertaken as part of a partnering framework with high levels of trust and openness - few restrictions may be placed on access to information.

### Secure access

For each implementation of BIW, a specific web address (or URL: uniform resource locator) is created. This URL does not have the 'www' prefix and is not submitted to search engines, so web-surfers are unlikely to find the project by accident.

As an option, BIW can offer customers secure connections using HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL). This enhanced level of security - typically used in online banking, for example - means all exchanges between the user and the web server are encrypted (the URL starts with 'https' instead of the usual 'http' and a padlock symbol appears in the bottom right hand corner of the web browser).

From the login page, access to the system is controlled by the user's entry of a valid user name and password. Passwords must be at least eight characters and a combination of letters and numbers. Clearly, each user is responsible for safeguarding their login details; they should also be aware that they may be blamed for any changes, etc, made within the system by a third party using their login details. Changing passwords regularly is good practice; BIW prompts individuals to change their passwords at regular intervals, normally every 30 days - though shorter intervals can also be specified.

If a user leaves the BIW system open but is inactive for a period, the system will 'time-out'. The default time-out allowance is 40

minutes (it can, of course, be set for shorter intervals if required), allowing users to undertake work in a different application and then resume interaction with BIW, but it also limits the time that the system might be left open inadvertently. Once 'timed-out', users will be prompted to login again.



If a user enters the wrong login or password three times, the BIW platform is locked, and the user will need assistance from his/her nominated company administrator to reset the system.

### Security roles and access rights

Maintaining its highly secure approach, the BIW platform is entirely database-driven. The project(s), registers, files and other information users can see are limited to those authorised for their role within the database security set-up. After logging in, each user is normally presented with a 'headlines' page containing their details and configured with information registers (see overleaf for more information) and tools appropriate to their role and responsibilities. For example, a specially trained team member - the Project Information Co-ordinator (PIC) - will have access rights to most documents and will have administrative tools to control other team members' access settings, while basic users will usually have access to more limited ranges of documents and processes and will only be able to configure their own user settings.

### Audit trail

Every user interaction with the BIW system is recorded, keeping a time- and date-stamped record of who did what and when. Perhaps most importantly from a security perspective, **drawings, documents and other information cannot be deleted from the system, nor can they be over-written.**

## Information access

In the BIW system documents are not assigned a URL and so cannot be exposed to anyone other than users interacting with the system through the database.

The default configuration ensures that all published information is available to every user with access to that project or programme. This is appropriate for many implementations, and can help promote particularly high levels of collaboration, but this level of access may not always be appropriate. Where projects require access to be controlled, typically, as already mentioned, a PIC is given overall responsibility to administer and maintain the system's security settings, though some lower level security provisions may be delegated to 'company information coordinators'.

Access to project information can be restricted in four different ways:

- by marking individual documents or processes 'private'
- by only allowing access to those project members on the original issue list
- by only allowing access if the document's status permits it
- by restricting access to particular document registers

### 1. 'Private' documents or processes

When a document is published privately, it is issued to a particular selection of users for their information or action, and although all users can see the document exists, only those users on the notification list can view or comment on it. For example, a design team's meeting minutes might be marked as private so that users from, say, tenants or subcontractors, cannot view them (note: this setting is applied to individual documents, and it would not therefore be appropriate to use it when publishing large numbers of files). On the process side, particular discussion threads could also be restricted to defined groups of users.

### 2. Restrict by issue list ('received view only')

When individual users are added to a project, their user profile can be set up so that they only see information that is published to them (ie: they can only view drawings, documents and other information they receive). There are three levels of access:

- received view - users can only see information which has been issued to them
- received view company - users can only see information that has been issued to someone in their company
- tender recipient - users have a very restricted view of a project. They can see only information that has been issued to them as part of a tender process and they cannot see other confidential information such as who else a document has been issued to.

### 3. Restricting access by status

Items which are under review can be published with access restricted to certain users until they reach a defined status - at which point the restriction is automatically removed. For example, a design team may wish to restrict access to work in progress by ascribing a drawing the status of 'For Review'; when the lead reviewer changes the status to 'Approved' or 'Status A' the drawing then becomes available to all team members.

### 4. Restricting access by register

In the BIW system, documents, drawings, etc, are published to particular registers. Access to different registers can be restricted according to the user's role (eg: design team, client, etc), according to the user's company, or at an individual level. There are essentially three levels of register access:

- Full - access is unrestricted
- Read Only - users can view, but not publish, to that register
- No Access - users cannot see the register name, or any documents within that register

Information access can be controlled by using all four methods simultaneously, but high levels of access control - particularly at the register level - may increase the administrative burden.

## Legal admissability

The ability to show that an electronic information system is managed in accordance with internationally recognised and audited codes of practice or standards - such as ISO/IEC 27001 (formerly BS7799/ISO 17799) - will be persuasive to a court of law. The wider-ranging and more exacting international standard, ISO/IEC27001, was introduced on 15 October 2005.

BIW's hosting partner Attenda was one of the first companies to

be certified by BSI as compliant with the new standard (on 10 January 2006).

**With all BIW users' interactions with its collaboration system being completely managed via Attenda's infrastructure, this means BIW's collaboration platform was the first 'extranet' system managed on a system certified to ISO/IEC27001:2005.**

## BIW Technologies Limited

21-25 Church Street West, Woking, Surrey GU21 6DJ

T 0845 1300 800 Int +44 (0)1483 712620

F 0845 1300 900 Int +44 (0)1483 756325

E [info@biwtech.com](mailto:info@biwtech.com)

[www.biwtech.com](http://www.biwtech.com)