Supporting instructions for access to secure web pages

Overview

1. AACA has established secure web pages to support the following groups:
   - Architect Registration Boards: for staff and Board member access
   - AACA Board of Directors
   - Various other AACA Committees and Panels, including all Accreditation Review Panels.
2. The intent is that all relevant papers (terms of reference, meeting minutes, reference documents, reports) and important information will be accessible via the dedicated secure webpage.
3. Links on secure web pages will initiate one of the following actions:
   a. Open a PDF document.
   b. Download a Word, Excel or PowerPoint document.
   c. Open a Dropbox Link (such as to a folder where multiple documents may be located)
   d. Open a separate URL to a different web page. This different web page may be either a public or secure page.

Usernames and passwords

4. To access a secure webpage a person requires a username and password.
5. The AACA Office is responsible for creating and maintaining a register of all usernames and passwords, and for issuing these details to authorised users.
6. *For architect registration board member access* – Usernames and passwords for architect registration board members are issued by the AACA to the relevant ARB Office. The ARB Office is responsible for the issue of a username and password to individual board members in their jurisdiction, and for the maintenance of their own records of which username and password has been issued to individual board members.
7. Authorised users do not have permission to change their allocated username or password. The creation and editing of usernames and passwords is managed solely by the AACA.
8. Where an individual may be on multiple Boards or Committees, a single username and password can be arranged, allowing access to all authorised secure pages.

Accessing a secure webpage

9. All secure webpages appear as “https://www.aaca.org.au/xxxx”, with the relevant details of the “xxxx” representing the dedicated secure webpage.
10. Authorised users should take note of the URL for the secure webpage that is sent to them. The secure webpages are not listed or linked anywhere on the AACA public pages.
11. On an authorised user’s normal home and/or work computer or device, the URL can be saved as a ‘favourites’ or can be typed in to the browser window as required.

12. When an authorised user attempts to log-in to a secure webpage for the first time, they can opt to select the '*Remember Me*' box so that they will be automatically logged-in when they open this page again from the same device.

Security

13. All secure webpages established by AACA are clearly indicated at the top of the page as a secure page.

14. Authorised users of the secure web pages are not permitted to share their access details with other people.

15. Authorised users should record their assigned username and password in a secure location.

16. When a person leaves a Board, Committee or Panel, AACA will either remove access to the relevant page from their username, delete the user name, or issue a new password to the relevant architect registration board. When an Accreditation Review Panel has completed their panel commitment after the Site Visit, user names and passwords will be deleted or access removed.

17. If an authorised user believes that their log-in details have been compromised, they should advise AACA (or the relevant ARB Office) and a new password can be issued.

Troubleshooting

18. If an authorised user forgets how to access the page or cant find/remember their username and/or password, they should contact AACA via email mail@aaca.org.au and access information will be re-sent. (Unless the user is an architect registration board member – this will require liaison with the relevant ARB Office).

19. If a user copies the text of their allocated username and/or password from the email or wherever these details were stored, *be careful not to include an excess space before or after* the username or password. If this occurs, access the secure webpage will be denied as the username and/or password will not be recognised.

20. If a user enters an incorrect username and/or password, a message will appear indicating that an incorrect username or an incorrect password, or possibly both, has been entered.

21. *If an authorised user enters an incorrect username or password more than three times, all access to the secure webpage log-in will be automatically blocked by the AACA website firewall*, and further access from the IP address associated with the user's computer / device will be denied. The user will need to contact AACA (Unless the user is an architect registration board member – this will require liaison with the relevant ARB Office) and advise of the IP address that access was denied to; AACA will facilitate having the advised IP Address 'whitelisted' by the AACA website developer. This may take 1-2 working days to complete.