

ITWorks website security requirements

The following website ITWorks standards must be followed when developing websites. These standards will ensure that we are following the current industry standards to secure and protect the websites and the content from unauthorized users.

**Authentication**  
Authentication ensures that each entity involved in using a Web service—the requestor, the provider, and the broker (if there is one)—is what it actually claims to be. Authentication involves accepting credentials from the entity and validating them against an authority.

**IT Works recommended strategy**: Only allow registered user to access the restricted content

**Authorisation**  
Authorisation determines whether the service provider has granted access to the Web service to the requestor. Basically, authorization confirms the service requestor’s credentials. It determines if the service requestor is entitled to perform the operation, which can range from invoking the Web service to executing a certain part of its functionality.

**IT Works recommended strategy**: Limiting the access to the database using access levels

**Data Protection**Data protection ensures that the Web service request and response have not been tampered with en route. It requires securing both data integrity and privacy. It’s worth mentioning that data protection does not guarantee the message sender’s identity.

**IT Works recommended strategy**: Sensitive content such as user password are encrypted. Use of https to secure the communication between client and the web server.