Data Security Information | Australia

Updated: November 2019

Wonde provides a service for transmitting school information in a private and secure manner between authorised third party applications. Wonde gives schools the ability to take control of their school data, protect its distribution and further comply with their data protection obligations.

Software Security

Wonde is hosted on Amazon Web Services (AWS) facilities in Australia. AWS computing environments are continuously audited, with certifications from accreditation bodies across the world, including ISO 27001, FedRAMP, DoD CSM, and PCI DSS.

AWS is also fully compliant with applicable Privacy Act laws, and the Australian Notifiable Data Breaches (ANDB) Addendum incorporates the Australian notifiable data breaches (NDB) scheme.

Further details about the considerable measures Amazon take in securing their facilities and services can be found here:
https://aws.amazon.com/security/https://aws.amazon.com/compliance/

Encryption

All data exchanged with Wonde's application and API is always transmitted via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

Availability

Wonde's application and API are hosted in multiple availability zones this provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

Stored Data

All data is encrypted at rest and during transit. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process.

Authenticated API Calls

Wonde requires that all API calls are authenticated with a secure API token and transmitted on a secure SSL connection.

Data Access

No information will be transmitted to a third party application (Data Processor) without approval from a school (the Data Controller). Third party applications are only permitted and able to request access of school data if they have a signed or agreed contract in place.

Two-Factor Authentication

Two-Factor authentication is used for any account that has access to privileged permissions which prevents unauthorised access in event of a password being compromised. Third party applications and schools that use Wonde to provision school data also have the ability to turn on Two-Factor Authentication upon request.

More information can be found here: https://en.wikipedia.org/wiki/Two-factor_authentication

Security Testing and Code Review

Passwords are an important aspect of security and as poorly chosen password may result in unauthorised access and/or exploitation, Wonde enforces a strong password policy to include the following:

- the use of both upper-case and lower-case letters (case sensitivity);
- inclusion of one or more numerical digits;
- a minimum password length of 8 (eight) characters;
- inclusion of special characters, such as @, #, $;

Any student passwords that may included picture passwords will undertake an alternative strong password policy.

Security Testing and Code Review

Wonde engages with external suppliers to ensure the security of its code-base and infrastructure, and works with them to resolve potential issues as they arise.

Further information

For more information on our security procedures, or if you have any questions regarding the above, please contact Wonde on (02) 8310 4489 or hello@wonde.com.