ACCEDE

DATA SHEET

ACCEDE - Security, Privacy and Architecture

2018 Update

Cloud Hosting and Security

Anyone involved in managing multi-million-dollar capital projects or programs should demand the lowest-risk solution appropriate for their enterprise, and ACCEDE therefore sets very high minimum quality of service requirements for hosting its Cloud based SaaS systems. As this involves non-core skills and expertise (such as Cloud infrastructure architecture, design & deployment) that complement its own capabilities, ACCEDE leverages the Amazon Web Services (AWS) platform and has partnered with several AWS's certified providers to help design, engineer & manage the technical infrastructure needed to run its Cloud SaaS based solution & related data services.

ACCEDE prides itself with the following processes, methodology, architecture, and security guidelines that are engrained in our day-to-day operations, and new product & feature development, ensuring that all our customers have a seamless, safe Cloud experience:

Access to Infrastructure & Data Locations

ACCEDE controls access to the infrastructure that our platform utilises to process customer data submitted to our services. Firewalls and other boundary devices that are employed to enforce strict control of the system accessibility are solely controlled by ACCEDE. Security patches and system updates are regularly performed on all servers and other infrastructure equipment.

Customer Data is processed within Australia for all customers in APAC (including off-site infrastructure backups), and within the EU for customers who have specific GDPR requirements. (*Available upon written request to ACCEDE*).

User Encryption for External Connections

Customer access to ACCEDE's Cloud services is through the Internet, and only after the authorized end user is properly authenticated. TLS encryption technology is required for all ACCEDE Service access. TLS connections are negotiated for at least 256-bit encryption or stronger when using both our Apple/Android applications & browser application, and the private key used to generate the cipher key is at least 2048 bits.

In addition, it is recommended that the latest available browser be used when accessing the application over the web.

Network Access Control

ACCEDE operations teams access Customer environments through a segregated network connection, which is dedicated to environment access control and isolated from ACCEDE and related entities internal corporate network traffic. Authentication, authorization, and accounting are implemented through standard security mechanisms (mentioned above) designed to ensure that only approved operations and support engineers have access to systems where required. Remote access to all our environments are restricted to select operations staff and only available via two-factor authentication.

Emergency Management Procedures

ACCEDE leverages AWS's high availability capabilities by balancing the architecture components of our application between multiple Data Centres (known as Availability Zones) help to keep our platform online, even if one whole Data Centre goes offline.

System Hardening / Monitoring

ACCEDE employs standardized system hardening practices across ACCEDE devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging. Additionally, ACCEDE employs an Enterprise Class platform wide monitoring and management toolset to monitor and alert on any non-authorized changes or security configurations, and environment availability and uptime.

Customer Project Data

Data uploaded to the ACCEDE Cloud is stored securely and is made accessible only to authorised users of a given project, for the duration of the project.

Upon project completion, the customer has the option to request the project be marked as Archived. Archived project data is able to be accessed online on a "read-only" basis and continues to be available for cross-project analysis and reporting if required.

The number of archived projects does not count toward the number of active projects specified in ACCEDE customer licencing.

Scalability

ACCEDE services are designed to leverage the benefits of "Cloud Native Architecture" which includes the capability to scale compute, memory and network resources to meet the demands of our customers. ACCEDE uses AWS to maintain application availability and scale our capacity up or down according to our demand.

Anti-Virus / Anti-Malware Controls

ACCEDE leverages enterprise-class solutions employed on all servers to protect against virus and malware incidents. Signatures for anti-virus and anti-malware are updated in a near real-time process as soon as they are available from the applicable vendors.

Data Management / Protection

ACCEDE maintains security incident management policies and procedures. All ACCEDE systems used in the provision of our services, including AWS infrastructure components and operating systems, log information to their respective system log facility or a centralized Syslogging servers (for our network systems) to enable security reviews and analysis.

Upon termination of our services, all customer data will be disposed in a manner designed to ensure that such data cannot reasonably be accessed or read unless there is a legal obligation imposed on ACCEDE or our related entities preventing us from deleting all or part of the data.

Software Deployments & Updates

Development and testing of the ACCEDE application is managed from physically separate infrastructure to production running workloads, and new code releases are tested as part of our deployment lifecycle to ensure that such releases cause no security breaches in the system, and the integrity of our platform & all data associated with it. Additionally, ACCEDE seeks to notify users in advance of any planned maintenance, with any system upgrades timed for low usage periods to minimise end-user inconvenience.

Project-level Security

The core ACCEDE Cloud is database-driven, with any information accessed restricted to that authorised within the database security set-up.

General access is controlled by at minimum, password authentication, so that anyone trying to gain access to the system will be unable to do so unless such person has a current login and password.

Our customers must ensure internal procedures secure the confidentiality of these logins. It is the client’s responsibility to only authorise these logins to persons who require them and ensure that those receiving them are fully aware of the security requirements.

ACCEDE’s hosting and underlying infrastructure services have been architected from the ground-up by AWS certified engineers in-line with AWS’s security best practices and methodologies, ensuring that all ACCEDE customers run on an industry standard, Cloud-native system following AWS’s “Security by Design” principles.

Notable AWS & partner security key points employed by the ACCEDE platform

AWS and partners engaged by ACCEDE provide many security capabilities and services to increase privacy and control network access to the ACCEDE platform. This includes but is not limited to:

- **Network firewalls** built into the ACCEDE core architecture, and additional WAF (web application firewall) capabilities that can be enabled on a per-customer basis (Enabled upon request to ACCEDE).

- **Encryption in transit** with TLS across all communication between ACCEDE internal services, and public SaaS endpoints.

- **TLS encrypted private connections** for all management and data related tasks performed in ACCEDE’s Cloud environment.

- **Protection against DDoS** attacks is built into key services leveraged by ACCEDE to help implement a “defence-in-depth” strategy for automatic response against DDoS attacks, minimizing impact at both an Application, and DNS level.

- **Physical security** - All data centres running the ACCEDE SaaS are state-of-the-art, housed in nondescript facilities with physical access strictly controlled and subject to video surveillance, intrusion detection systems etc.

- **Encryption of all customer data** that is stored in the ACCEDE SaaS environment is enabled by default. ACCEDE leverages AWS’s HSM (Hardware security module), storing all encryption keys of volumes containing customer data which is encrypted at rest.

- **Logging of access to environment & infrastructure** - All access to ACCEDE’s Cloud Infrastructure is logged and audited through a range of tooling provided by both AWS and third party security vendors. This includes deep visibility into all API calls through the AWS IaaS platform, and visibility of individual server components of ACCEDE’s infrastructure through Trend Micro’s leading “Deep Security” product.

- **Australian IRAP Certifications** - ACCEDE only leverages AWS services that have been certified for use by the Information Security Registered Assessors Program (IRAP), an Australian security standard, ensuring that any government and customer data stored at rest within the ACCEDE platform will be covered by this certification.

AWS Architecture & Compliance

In addition to the key Australian IRAP certifications, AWS Compliance enables ACCEDE and our customers to understand the robust controls in place at AWS to maintain the overall security and protection of ACCEDE data in the Cloud. IT infrastructure provided by AWS helps ensure that ACDEDE's offering is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 *(formerly SAS 70)*
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

Additionally, the ACCEDE platform undergoes security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.