Information Engine™: Secure and reliable.

August 2021.

At D2K Information, we take security very seriously. We have developed a comprehensive set of practices and technologies to help ensure the reliability, security and protection of our systems and your data and all our products within Information Engine™, including AuditWatch™.

Our security protocols

Our information security policies and practices are based on ISO27001, the Australian Government Information Security Manual, the New Zealand Information Security Manual (NZISM), and ACSC cyber security principles and guidelines including the Essential Eight Model.

To meet Australian and NZ privacy legislation all data is stored in Australia and we adhere to the Australian Privacy Principles (APPs) and Privacy Act 1988 (Privacy Act) and the New Zealand Information Privacy Principles (IPPs).

1. You own your data

Your organisation owns the form response data and file upload data. D2K Information accesses data only at your request. To protect your data from unauthorised access, we have implemented suspicious activity alerts.

You can download your information or delete your information from our system at any time.

2. Password and authentication

All our Information Engine™ products enforce strong passwords, with user lockout after several failed log in attempts . Passwords have an eight-character minimum. We use the Open Source zxcvbn library from Dropbox which produces a score between 0 and 4 for how long it would take to crack/brute force the password (using dictionaries with common/simple passwords, brute force estimation, etc). An Enterprise can configure their minimum score required (currently set to 3 or above (Strong/Very Strong), this value is communicated to the user when changing their password by a password strength meter.

Enterprises are encouraged to have Information Engine™ products integrated with their corporate identity provider (e.g. AzureAD), and control password and 2FA policies at their end.

D2K Information Pty Ltd ABN 51 625 382 381
A: PO Box 1237 HAWKSBURN VIC 3142 Australia **T:** +61 409 359 155 **W:** d2kinformation.com

3. Physical security

All Information Engine™ products run entirely in AWS Fargate, which is a serverless compute engine. It is a PaaS (Platform as a Service) provided by AWS. We made a strategic choice to use the world's leading cloud IT infrastructure provider that provides a high performing, robust and secure infrastructure set to meet the needs of our users. We also follow the advice from New Zealand's National Cyber Security Centre on Securing Amazon's Web Services.

AWS manages the provision and management of servers and ensures application isolation by design.

All the servers and software that run D2K infrastructure, are monitored, patched, secured and restricted by AWS itself. AWS Fargate meets the standards for PCI DSS Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, and SOC 3.

Information Engine™ code lifecycle starts in Github where it is scanned for dependencies and vulnerabilities as soon as it created.

From here, containers are created and pushed to AWS ECR (Elastic Container Repository) where code is scanned again by AWS for vulnerabilities. These are the containers that will run in AWS Fargate.

4. Network security

Our network security helps protect your data against the most sophisticated electronic attacks. Network security practices include Firewalls and other boundary devices, TLS encrypted communication, intrusion detection/prevention systems, control and audit and virus scanning.

Data in transit is protected by TLS 1.2+ to provide end-to-end communication security.

5. Application security

Web Application Firewalls are in place to monitor and control web traffic at the application level. We employ only best practice coding and have constructed our products so that every account is isolated. We have safeguards in place to detect common attacks such as SQL injection, cross-site scripting, cross site request forgery and more.

We engage third parties to perform regular audits and penetration testing against our applications. These are run on an annual basis with frequency increased if there are significant changes.

6. Redundancy and business continuity

We have designed our systems and infrastructure with high availability and redundancy in mind. This includes backup, mitigation and handling in case of server failure, power failure, fire or other disaster.

Information Engine™ has a business continuity and disaster recovery plan that allows customers to continue to run our products in the unlikely event of an outage.

D2K Information Pty Ltd ABN 51 625 382 381
A: PO Box 1237 HAWKSBURN VIC 3142 Australia **T:** +61 409 359 155 **W:** d2kinformation.com

7. Data backup and replication

Daily snapshots are taken of our application database cluster. These daily backups are stored for at least 30 days.

Data backups are also encrypted using AES-256.

8. Security monitoring and testing

Our application is configured for appropriate logging of activities to enable detection of security incidents. These incidents are reviewed and identified anomalies are investigated for a possible compromise. All logged activities are sent to a centralised logging infrastructure for audit purposes.

Internal Vulnerability Scans are run constantly.

Penetration testing for our products, network, and segmentation are run on at least an annual basis by a third-party security vendor.

D2K Information has the flexibility to run security testing more frequently if required, e.g. as a result of significant changes.

9. Employee access

Access to IT assets is granted to D2K Information employees on the 'Need to Know' and 'Least Privilege' principles.

We will only access your data at your request. To protect your data from unauthorised access, we have logs with alerts set to notify us of suspicious activity.

Background checks are conducted for all personnel engaged in delivering service to customers. These include thorough police checks as well as specialised background checks where relevant.

10. Incident response and data breach response

D2K Information has documented Incident Response and Data Breach Response Plans which outline the processes to respond to security events and incidents, including breaches of personal or protected data.

D2K Information Pty Ltd ABN 51 625 382 381
A: PO Box 1237 HAWKSBURN VIC 3142 Australia **T:** +61 409 359 155 **W:** d2kinformation.com

11. Risk management

Our organisation addresses cyber security risks in our risk management processes to identify critical assets, threats, and vulnerabilities.

D2K Information performs risk-based due diligence on new and existing vendors to determine if the vendor is using appropriate technical controls and organisation measures to protect data.

12. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

As part of our High Availability setup we use multi availability zone data replication to provide additional resilience and support low RPO and RTO requirements.

13. Testing

We use a rigorous set of testing processes and tools to mitigate potential issues that can be introduced by human error or changes in external factors that are out of our control. These include functional testing, usability testing, compatibility testing, performance testing and security testing.

14. Privacy Policy

We respect your personal information and are committed to protecting it when providing products and services to you.

Our privacy policy has been developed in line with the Australian Privacy Principles, Privacy Act, the New Zealand Information Privacy Principles, EU's General Data Protection Regulations (GDPR), and the U.S. Privacy Shield.

Document History

Item	**Information**	
Document	Information Engine(TM) Security Summary Sheet	
Version	RevC	
Author/s	Sonia Garcia Gonzalez	Operations Manager
	Angel Abad Cedeira	Systems Architect
	James Lucas	Senior Coder
Date	7 August 2021	
Reviewed by	Annette Davison	R&D Manager
Approved by	Phil Krasnostein	CEO

D2K Information Pty Ltd ABN 51 625 382 381
A: PO Box 1237 HAWKSBURN VIC 3142 Australia **T:** +61 409 359 155 **W:** d2kinformation.com