Introduction

This Information Security Policy (ISP) is intended to provide the Named Users of the Licensee with the details of how Accurri Pty Limited (referred to as Accurri, we, us, or our) addresses information security as part of its broader Information Security Management System (ISMS).

The document is intentionally brief in order to encourage readership and also to ensure a focus on the things that matter. Accordingly, and by way of example, readers will note the absence of reference to such things as 'on-site' security and this is due to the fact that Accurri does not have 'on-site' visits and all meetings are conducted online (whether via email or online meeting platforms). Further, we do not require, and will not accept, hard copy data and therefore have no need to secure this form of data.

A key element in the selection and on-going assessment of our hosting vendor Amazon Web Services (AWS) is the vendor's commitment to security. We understand that our Licensees expect and deserve the most rigorous security available and this is key in our decision to use AWS and by extension, leverage their security expertise and framework.

This policy should be read in conjunction with the Accurri End User Licence Agreement (EULA) and the Accurri Product DIsclosure Statement (PDS) both of which are available for download at: accurri.com/resources.

Sections

Cloud infrastructure

Accurri's cloud infrastructure is maintained by the industry leading cloud platform provider, Amazon Web Services (AWS), in multiple unmarked facilities within Australia, Ireland and Singapore.

The terms of agreement between Accurri and AWS, are here: aws.amazon.com/agreement. AWS are recognised as industry leaders in the area of cloud services certification and compliance and they are also acknowledged as having best practices in Information Security. For a full listing of AWS certification and compliance, please visit aws.amazon.com/compliance.

Security controls

Accurri is ISO 27001 certified and utilises multiple layers of security controls (software, physical and process based) to protect Licensee data. This includes, but is not limited to:

- Local and Network Firewalls
- Web Software Firewalls
- Intrusion Detection and Prevention Systems
- Anti-Virus and Anti-Malware
- DDoS Throttling Services
- Access Control Lists
- ITIL Framework (release/incident/change)
- Identity and Access Management
- Centralised Log Management
- Symmetric and Asymmetric Encryption Systems
- Secure Code Reviews
- Separation of Duties
- Vulnerability and Penetration Assessment
- Anomaly Detection
- Remote Monitoring and Alerting
- Endpoint Protection

Please note, Accurri will not release the details of its security control processes or test results as doing so creates a control weakness and presents what we consider to be an unacceptable risk.

Data encryption

The Accurri software is accessed via HTTPS using Transport Layer Security (TLS 1.2). TLS is a cryptographic protocol designed to protect information transmitted over the internet, against eavesdropping, tampering, and message forgery.

Once Licensee data reaches the Accurri AWS hosted environment, all information is encrypted at rest, using AES-256, military grade encryption and AWS key management services. This is done to protect Licensee information in the unlikely event of an Accurri server being compromised.

Employee vetting and confidentiality

All Accurri staff go through a vetting process, including police checks, and their employment agreement specifically addresses their obligations with regard to the security of Accurri and the Licensee data held within it.

The Accurri position with regard to confidentiality is that all Licensee data (regardless of form) held by Accurri on behalf of the Licensee, will be treated as confidential and will not be disclosed to anyone, except where:

- such disclosure is required by law
- the Licensee gives specific written permission authorising the disclosure

From time to time Accurri support team members may need to access Licensee data to provided training or investigate a scenario in which support has been requested by the Licensee's Named Users. All such access will be bound by the confidentiality statement above and the confidentiality clause within the employee's employment agreement.

Software availability

Licensee data is hosted in secure AWS facilities in the geographic location (Australia, Singapore or Ireland) specified by the Licensee at the time of the grant or renewal of the licence. In the event that Accurri was unavailable due to a disaster, alternate data centres can be commissioned to ensure minimal service interruption. Alternate data centres will always remain in the same geographic location specified by the Licensee at the time of the grant or renewal of the licence.

Licensee data

'Licensee data' means any data or materials provided by the Licensee to Accurri or input into the software by the Licensee's Named Users and all outputs generated using the software.

Licensee data ownership

The Licensee data is the property of the licensee.

Data retention - Licensee

Licensee data will be retained until:

1. The Licensee's Named Users delete it, or
2. The client provides Accurri with a written instruction to delete it, or
3. The licence was not renewed and six months have elapsed since the expiry date, or
4. The licence was cancelled within the first 120 days and at least six months has elapsed since the purchase date

Accurri will not provide confirmation of data destruction unless the Licensee specifically requests such confirmation.

In the event of the non-renewal of a licence, Accurri will allow the Licensee's Named Users a courtesy period of 14-days beyond the expiry date in order to allow for the retrieval or deletion of Licensee data.

Data retention - Trial entity

Data provided or input as part of a trial will be retained until:

1. The trialing entity's Named Users delete it, or
2. The trialing entity provides Accurri with a written instruction to delete it, or
3. At least six months has elapsed since the trial expiry date

Accurri will not provide confirmation of data destruction unless the trialing entity specifically requests such confirmation.

Backup policy

The Licensee acknowledges that it should make and retain copies of all data input into the software and all outputs derived from the software. It also acknowledges that such copies should be stored in a manner that will allow the Licensee's Named Users to access said inputs and outputs in the event that the software is inaccessible due to factors which are beyond the control of Accurri.

The Accurri database is backed up daily at approximately 2:00 am (local time at the relevant AWS data centre) however this is a total system backup and is not intended to restore an individual Licensee's data.

Monitoring

Accurri is monitored 24 hours a day, 7 days a week, 365 days a year.

Suspected data breach

If the Licensee believes Accurri information may have been compromised, the Licensee's Named User should contact Accurri as soon as possible by emailing support@accurri.com with as much information as possible.

Accurri takes its duty of care seriously and in the event that our security was breached (which has not occurred to date) we will notify all affected clients at the earliest opportunity and we will, as a matter of priority, take all necessary corrective action.

Deleted data is not recoverable

Once data has been deleted as per this policy, it cannot be recovered.