## Introduction

This Information Security Policy ('ISP') is intended to provide both clients and employees with the details of how Accurri Pty Limited (referred to as Accurri, we, us, or our) addresses information security.

The policy 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 'on-site' security and this is due to the fact that Accurri does not have 'on-site' visits as such and all client and vendor meetings are conducted online (whether via email or online meeting platforms). Further, we do not require, and will not accept, client 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 is the vendor's commitment to security. We understand that our clients expect and deserve the most rigorous security available and this is key in our decision to use Amazon Web Services (AWS) and by extension, leverage their security expertise and framework.

Further details relating to information security are available in 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



## Our guarantee

Accurri is used by many entities. It is used to prepare thousands of statutory reports/accounts for a broad cross section of public and private companies, professional services firms and government departments, each of which has specific information security requirements and expectations.

We work extremely hard to ensure that Accurri software (the software) is easy to use and it exceeds the needs, including information security, of our most discerning users. As a measure of our confidence in the software and our ability to support it, we offer a 120 day 'no strings attached' refund as follows:

- If the Licensee is dissatisfied, in any way, with Accurri they may cancel the licence. If the cancellation occurs within 120 days of the Commencement Date (i.e. the first 120 days) the full amount of all licence fees paid will be refunded within 14 days into a nominated bank account.

The Licensee is not required to provide a reason for cancellation (although for development purposes we like to know) they just have to advise us via email that they wish to cancel and provide details of the bank account into which they wish the refund to be paid.

## 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 utilises multiple layers of security controls (software, physical and process based) to protect our client 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

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). TLS is a cryptographic protocol designed to protect information transmitted over the internet, against eavesdropping, tampering, and message forgery.

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

## Employee vetting and confidentiality

All Accurri staff who have direct access to our cloud infrastructure go through a vetting process and their employment agreement specifically addresses their obligations with regard to the security of Accurri and the client data held within it.

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

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

From time to time Accurri support team members may need to log into a report to investigate or understand a scenario. Any such access will be bound by the confidentiality statement above and the confidentiality clause within the employee's employment agreement.

## Software availability

Accurri is designed to be easy to use and readily available. Accurri services are split over multiple AWS data centres including Australia, Ireland and Singapore. This ensures that client data is held in an appropriate geographic location and in the event of one data centre going offline in a disaster scenario, another centre will continue to serve data with minimal, if any, service interruption.

Accurri has substantial in-built redundant capacity that ensures there is no degradation of service during peak use times. Traffic loads, resource use and constantly monitored and assessed.

## Data ownership

The data contained in Accurri remains the property of the licensee.

In the event that a licensee does not renew their license with Accurri, there is a courtesy period of 14 days after the expiry date. Clients should ensure that they have taken copies of all required outputs prior to the end of the courtesy period. Data is retained for six months to cover to possibility of accidental non-renewal. After 6 months, all data will be deleted.

## 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 Users to access said inputs and outputs in the event that the software is inaccessible due to factors which are beyond the control of the Licensor.

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 individual user reports.

## Monitoring

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

## Suspected data breach

If you believe Accurri information may have been compromised, please contact us immediately at support@accurri.com

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.