Predikt-r Security Policy

Effective date: 01 July 2018

1. Overview

At Predikt-r, we know that our customers rely on us as an important part of their business processes. We take this responsibility to our customers very seriously, and the security and reliability of the software, systems and data that make up the Predikt-r suite of products are always our priority.

All Predikt-r products are hosted in Amazon Web Services (AWS) in *Sydney, Australia*. The infrastructure for databases and application servers are managed and maintained by the cloud service providers. At Predikt-r, we take a multifaceted approach to application security, to ensure everything from engineering to deployment, including architecture and quality assurance processes complies with industry and best practice standards of security.

2. Infrastructure Security

The Predikt-r application is hosted and managed within the AWS cloud computing infrastructure. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. AWS inherently protects from threats by applying security controls at every layer – from physical to application – isolating applications and data, whilst rapidly deploying security updates without service interruption. As a result, the Predikt-r application is afforded all the benefits of being hosted on the AWS infrastructure, including:

- Regular security assessments and compliance auditing
- Scheduled penetration testing and vulnerability assessments
- Real-time antimalware and antivirus protection for file systems, memory, processes and registry database
- Rolling updates and security patching with zero downtime
- Environmental safeguards
- Network security safeguards
- Data security safeguards
- System security safeguards
- Vulnerability management
- Backups and disaster recovery
- Privacy
- Restricted access to customer data
- Employee screening and policies
- Dedicated security staff

Additionally, AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards, allowing Predikt-r to meet specific government, industry, and company security standards and regulations. For more information, please see the AWS Security page.

3. Application security

The Predikt-r web application adopts the Open Web Application Security Project (OWASP) *OWASP Top Ten* as a means of ensuring application code is free from flaws and security vulnerabilities. The *OWASP Top Ten* is a set of powerful awareness document for web and mobile application security. The *OWASP Top Ten* represents a broad consensus about what the most critical web and mobile application security flaws are. Project members include security experts from around the world who have shared their expertise to produce a list of the top ten security vulnerabilities affecting web and mobile applications. Adopting the *OWASP Top Ten* strengthens Predikt-r's security posture against:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

For more information, please see the OWASP website.

3.1 Application Architecture

The application is initially protected by AWS's firewall which is equipped to counter regular DDoS attacks and other network related intrusions. The second layer of protection is industry leading third-party application firewall which monitors against offending IPs, users and spam. While the application can be accessed only by users with valid credentials, it should be noted that security in cloud-based products is a shared responsibility between the company and the businesses who own those accounts on the cloud.

Our products also come with features aimed at securing business data on the cloud:

- All account passwords that are stored in the application are one-way hashed and salted.
- Access to the application by the Predikt-r development team is also controlled, managed and audited. Access to the application and the infrastructure are logged for subsequent audits.
- The in-line email attachment URLs for the product are public by design, to enable us to embed links within the email for end-user ease. This can be made private on customer request.

3.2 Application Engineering and Development

All Predikt-r employees and contractors are equipped with secure laptop computers with antivirus software centrally installed, configured and managed. Technical staff undergo training on relevant security matters that pertain to their job.

Our engineers are trained in industry-leading secure coding standards and guidelines to ensure our products are developed with security considerations from the ground-up. A security review is a mandatory part of application engineering (development and deployment) process at Predikt-r. The security review leverages code analysis tools, in addition to manual reviews, to ensure adherence to good practice and standards.

4. Network Security

All Predikt-r products are hosted and security managed by Amazon who monitor the infrastructure 24x7 for stability, intrusions and spam using a dedicated alert system. Periodically, end-to-end vulnerability assessments and penetration tests are performed by an independent third-party.

5. Quality Assurance

Besides functional validation and verification, the quality assurance process at Predikt-r also subjects application updates to a thorough security validation. The validation process is performed by an independent third-party security team with ethical hackers whose goal is to discover and demonstrate vulnerabilities in the application. An update to the application does not get the stamp of approval from the quality assurance team if vulnerabilities (that can compromise either the application or data) are identified.

6. Deployment & Post Deployment

Deployments to production servers are performed only by trusted and authorised engineers. Only select few pre-authorised engineers have access to Predikt-r production environment. In order to view and inspect access logs, engineers need to go through a committee of authorised employees, who will then deliver the logs to them after validating their purpose.

An independent information security team carries out periodic comprehensive application audits. The tests are performed with the help of static analysis tools and aided by manual analysis.

Network penetration tests and other black box tests are performed to help identify security vulnerabilities in the application. The independent information security team stays vigilant about common vulnerabilities and exposures and stays on top of updates to the published list of information security vulnerabilities and exposures.

7. Vulnerability Management and Penetration Testing

Predikt-r undergoes periodic vulnerability assessments conducted by an independent third party, with all high and critical vulnerabilities being addressed immediately.

8. Data Security

Predikt-r takes the protection and security of its customers' data very seriously. Predikt-r manages the security of its application and customers' data. However, provisioning and access management of individual accounts is at the discretion of individual business owners.

The Predikt-r development team has no access to data on production servers. Changes to the application, infrastructure, web content and deployment processes are documented as part of an internal change control process.

Predikt-r takes the integrity and protection of customers' data very seriously. Data at rest is encrypted using AES-256 bit standards with the keys being managed by AWS Key Management Service. All data in transit uses standard encryption over secure sockets layer (SSL) connection for all accounts hosted on predikt-r.com.au.

Application logs are maintained for a duration of one (1) year.

Predikt-r uses Amazon RDS which provides two different methods for backing up and restoring DB instance(s) automated backups and database snapshots (DB Snapshots). Customers' data is backed up using a snapshots backup - maintained by AWS in different datacentres to support a system failover if it were to occur in the primary datacentre. Should an unlikely catastrophe occur in one of the datacentres, businesses would lose only one hour of data.

Data is backed up to persistent storage every day and retained for the last seven days.

Different environments are in use for development and testing purposes, access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification, with Segregation of Duties built in, and reviewed on a quarterly basis.

8.1 Data Deletion

The primary purpose we collect your personal information is to:

(a) carry out our obligations arising from any contracts entered into between you and us and to provide you with the information, products and Services that you request from us and billing you for the Services provided;

(b) to provide you with information about further Assessments, reports and Services we offer that are similar to those that you have already purchased or enquired about;

(c) verify your identity;

(d) to optimise and personalise our Website and deliver content to you;

(e) conduct Assessments and provide to Customers information, feedback and reports generated by us based on your input to Assessments ("Predikt-r Results");

(f) develop new features, products and services;

(g) provide you with information about our products and services; and

(h) conduct research for our own internal purposes.

When an account is deleted or disabled, all associated candidate data is kept by Predikt-r for the aforementioned purposes. You may request deletion of your data by e-mailing support@predikt-r.com.au.

For more information regarding your data refer to our Privacy Policy.

9. Operational Security

Predikt-r understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. Predikt-r has clear change management processes, logging and monitoring procedures, and fall-back mechanisms which have been set up as part of its operational security directives.

Operational security starts right from recruiting an engineer to training and auditing their work products. The recruitment process includes standard background verification checks (including verification of academic records) on all new recruits.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organisational security policies. Security incidents (breaches and potential vulnerabilities) can be reported via email: support@predikt-r.com.au.

Only authorised and licensed software products are installed by employees. The third parties or contractors managing the software as well as the outsourced development activity are authorised by the management team before they are carried out.

10. Regulatory Compliance

All formal processes and security standards at Predikt-r are designed to meet regulations at the industry, state and national levels. As the processors of personal information on behalf of our customers, we implement industry standard security, technical, physical and administrative measures against unauthorised processing of such information and against loss, destruction of, or damage to, personal information as more fully described in Predikt-r Privacy Policy.

For more information regarding Privacy Shield please refer to our Privacy Policy.

11. Reporting issues and threats

At Predikt-r we take the protection of our customer's data very seriously. If you have found any issues or flaws impacting the data security or privacy of Predikt-r users, please write to support@predikt-r.com.au with the relevant information so we can get working on it right away.

We ask that you do not share or publicise an unresolved vulnerability with/to third parties. If you submit a vulnerability report, the Predikt-r security team and associated development teams will use reasonable efforts to:

- Respond in a timely manner, acknowledging receipt of your vulnerability report
- Investigate the reported issue and provide an estimated time frame for addressing the vulnerability report. We might also ask for your guidance in identifying or replicating the issue(s) in order to understand any means to resolving the threat right away
- Notify you when the vulnerability has been fixed.

Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing flaws in Predikt-r and will acknowledge your contribution once the threat is resolved.

12. Get in touch with us

If you have any questions or doubts, feel free to get in touch with us at support@predikt-r.com.au and we'll get back to you right away.