ACCESSREAL
SERVICE LEVEL AGREEMENT ("AccessReal SLA")

EFFECTIVE AS OF 1 June 2018

During the term of the subscription period, the AccessReal web admin interface and web services for both Web and Mobile Clients, AccessReal Services will be operational and available to the Companies at least 99.90% of the time in any calendar month during the service window. Upon request, we, i-Sprint Innovations Pte Ltd ("i-Sprint), will provide service report to the Companies on a monthly basis to indicate our Service uptime.

Definitions The following definitions shall apply to the AccessReal SLA.

- "Companies" means our Platform Partners or organizations that have signed a Purchase Agreement with i-Sprint for the AccessReal Services.
- "Downtime" means when there is more than a five percent user error rate across all of a Company's Users. Downtime is measured based on server side error rate.
- "Service" means the subscribed AccessReal Services as stated in the Purchase Agreement which may include Product Authentication, Anti-countering, Track and Trace, Direct Management, Customer Engagement (Loyalty Program, Warranty Management, Product Recommendation).
- "Monthly Uptime Percentage" means total number of minutes in a calendar month minus the number of minutes of Downtime suffered in a calendar month, divided by the total number of minutes in a calendar month excluding the scheduled downtime.
- "Scheduled Downtime" means the periods of Downtime relating to network, hardware, or service maintenance or upgrades. i-Sprint will use reasonable commercial endeavors to provide written notice to the Company prior to the commencement of Scheduled Downtime.

i-Sprint AccessReal SLA **Exclusions**:
The AccessReal SLA does not apply to any services that expressly exclude this AccessReal SLA including scheduled downtime or any performance issues: (i) caused by "Force Majeure" or (ii) that resulted from one or more of the Company's equipment or third party equipment not within the primary control of i-Sprint.

i-Sprint reserves the right to modify this AccessReal SLA *at any time by updating the terms on this site. This AccessReal SLA is subject to all other applicable documentation including AccessReal Service Terms and Conditions.*

SERVICE COVERAGE

For our standard contract, the following security and operations aspects are covered:

Systems Operations and Security Implementations

1. Infrastructure
2. System Administration and Monitoring
3. Backup and Recovery
4. Penetration Testing
5. ISMS and Quality Management

Application Services and Security Implementations

6. Application and User Security
7. Application Access Control
8. Communication Security
9. Data Security
10. Cryptography and Cryptographic keys

Systems Operations and Security Implementations

Aspect	Service Scope	Optional Services
1. Infrastructure	• AccessReal infrastructure components are configured to provide **high-availability to deliver maximum uptime**. All critical systems in scope of the application have a redundant set-up across at least **two geographically separated data centers.**	
	• AccessReal Services are hosted in a **firewall protected network** segment together with other services that have similar protection requirements only.	
	• A **DDOS prevention infrastructure** has been implemented to prevent denial of services attacks.	
	• A **DMZ infrastructure** is in place for AccessReal Services. Internet connections are terminated in the DMZ and	

	then forwarded to backend systems.	
	• All our AccessReal infrastructure components (virtualisation platform, operating systems on web-, application- and database servers) **are hardened** following current best practices.	
	• AccessReal is delivered on a shared infrastructure.	• As an optional service, a **dedicated service infrastructure is available** (not shared with other Companies).
2. System Administration and Monitoring	• **Privileged Account Activity Management system** has been implemented to control and monitor privileged access and system administration activities to ensure accountabilities. All system administration activities and session logging is recorded.	
	• **Availability and Load Balance of AccessReal Services are monitored**, as well as security events. Alerts will be sent out if any critical events have been detected. • The retention period for the Audit Log is 30 days.	• Optional service is available to maintain a longer retention period.
3. Backup and Recovery	• **Secure Daily backup** is provided. All data is replicated and kept updated to **at least two data centers.** Backup replicas are kept at least at two distinct locations for 30 days.	Optional service is available to maintain a longer retention period.
	• **Regular disaster recovery drills** based on our established protocols are conducted to validate the recoverability of the AccessReal infrastructure.	
4. Regular Penetration Testing	• All systems that are needed for the service delivery have undergone **regular penetration testing and vulnerability scanning**. Penetration includes the application/service and not	

	be limited to infrastructure components.	
5. ISMS and Quality Management	• i-Sprint is an **ISO27001 certified** organization. Our Information Security Management System (ISMS) is in lines with the ISO27001 standards.	• Other than performing regular self-assessments, we provide optional services for the Company Audits carried out by The Company or a third party Auditor
	• i-Sprint has achieved **ISO9001 certification** for our qualify certification. This signifies our process is based on a documented and auditable process.	

Application Services and Security Implementations

Aspect	Service Scope	Optional Services
6. Application and User Security	• Depending on the services subscribed and customization services requested by the Company, **AccessReal Services provide the Web Admin Portal with Dash Board, Web Services, AccessReal Mobile App and Wechat Micro App** to delivery the Brand Protection, Anti-Counterfeiting, Track-and-Trace, Customer Engagement and Marketing Services to the Company and their users.	• Realtime App Self Protection (RASP) service to protect app integrity and malware attacks for customized apps are available as an optional service
	• Username/password Authentication is required for users to access the AccessReal Services. AccessReal provides comprehensive and complex password policies such as password length, complexity, password expiry, etc. which can meet some of stringent security requirements. The implemented password policies can easily comply with the security policy of the Company	• AccessReal provides Multi-Factor Authentication for user authentication as an optional service. • AccessReal supports SAML, OAuth and OpenID Connect authentication protocols. If required, we can provide integration services to integrate AccessReal Authentication process with the Company's Federated Authentication

		infrastructure to achieve seamless single-sign-on.
	• AccessReal's development, test and production environments are separated from each other. A defined transport procedure between the environments is in place. All updates and patches are tested in the test environment before transport into the production environment.	
7. Application Access Control	• AccessReal has implemented **Role Based Access Control system (RBAC)** to control the user access to application features and it can fulfill all necessary requirements for implementing a least privilege/need-to-know access policy.	• AccessReal provides technical provisioning APIs for the automated control of all relevant identity attributes and all authorization elements of the application/the service via the Company IAM infrastructure. This is an optional service for integration.
	• AccessReal supports the **least privilege principle and there is no super user in the system**. The effective revocation of access rights is implemented whenever users (including privileged users) leave the company, change roles. If there is an emergency the possibility of immediate access deactivation can be given.	
8. Communication Security	• Other then securing communication of internal and external clients with the service via encrypted connection using HTTPS and SSL/TLS, AccessReal also provides an additional encryption layer using **E2E Encryption on top of SSL to secure communication using application level encryption**	
9. Data Security	• **Personal/Customer Data is always kept encrypted** at rest	

	and in-transit. All sensitive personal data is encrypted at the database level.	
	• AccessReal complies with the "**privacy by default**" principle. AccessReal provides the privacy protection which certain information has been encrypted during storage and the user information can only be assessed by the user himself only. With only the clear text information, no one can derivate the actual user identity.	
	• AccessReal provides the user profile screen for users to perform "right of access to personal data": 1. The right to be informed 2. The right of access 3. The right to rectification 4. The right to erasure	
10. Cryptography and cryptographic keys	• AccessReal uses current BSI recommended cryptography algorithms and key-sizes e.g. AES256, RSA2048 and SHA2 for all cryptography operations.	
	• All private and symmetric cryptographic keys, including the Company-dedicated keys, authentication credentials and keys that are accessed by system components are kept in an encrypted store. Only authorized staff can access the credential store to generate or replace credentials. • AccessReal also supports automatic key roller to enable encryption keys to be changed on a regular basis automatically.	For higher security requirements, AccessReal can store encryption keys inside a HSM as an optional service.