zainTECH

SERVICE LEVEL AGREEMENT (SLA)

1. SERVICE LEVEL AGREEMENT

1.1. **Incident Priority:** Incidents are prioritized from Priority 1 to Priority 4, each priority is defined below:

- Priority 1 – System or Service failure with critical business impact;
- Priority 2 – System or Service failure with significant business impact;
- Priority 3 – System or Service impaired with no business impact; and
- Priority 4 – General questions/advice or planned maintenance activities

PRIORITY LEVEL	DESCRIPTION
P1	A large number of users cannot access the system.
	Critical functionality is not available.
	The system cannot continue because a vital feature is inoperable, data cannot be secured, backed up, etc.
P2	Internal system error, causing the system to fail, but restart or recovery is possible.
	Severely degraded performance.
	Some important functionality is unavailable, yet the system can continue to operate in a restricted fashion.
P3	A system error for which there is a Client acceptable workaround.
	Minimal performance degradation.
	System error requiring manual editing of configuration or script files around a problem.
P4	A system enhancement for which there is a Client acceptable workaround.
	Documentation error.

1.1.1. Incident Priority examples

PRIORITY	RESPONSE SLA	SPECIALIST REVIEW	ESCALATION MANAGER	ESCALATION DIRECTOR	EMAIL FREQUENCY	TARGET RESOLUTION
P1	15 Minutes	30 Minutes	1 Hour	2 Hours	30 Minutes	2 Hours
P2	30 Minutes	1 Hour	2 Hours	4 Hours	Hourly	4 Hours
P3	4 Hours	2 Hours	2 Days	Never	Daily	1 Day
P4	1 Day	2 Days	2 Days	Never	Daily	2 Days
RFC	1 Day	2 Days	2 Days	2 Days	Daily	2 Days
Emergency RFC	30 Minutes	1 Hour	2 Hours	2 Hours	Hourly	2 Hours

1.2. Incident Response, Escalation and Target Resolution

1.2.1. For an Incident, "Response" is the time from when the Customer first logs a request via telephone for assistance to the time that the Service Provider responds with a suitably qualified employee whether via an email, telephone call or in person. Support to provide a resolution shall be provided from the time of Response until such time as the Incident has been resolved.

DESCRIPTION	METHOD

Online	http://vision.zaintech.com
Telephone	+971 4 378 9088/+971 437 89000 (UAE) +962 793 334409 (Jordan) +965 222 61298 (Kuwait) +966 114 797399 (Saudi Arabia) +968 210 30744 (Oman) +973 166 09209 (Bahrain)

1.2.2. For an Incident, "Escalation" shall take place if a resolution to the Incident has not been achieved within the time frame set out in the table above, and will continue to be escalated until details of the Incident is given to the Technical Director.

The people listed below are our Escalation Contacts for this Agreement.

LEVEL	CONTACT	TITLE	EMAIL ADDRESS	MOBILE NO.
1	Service Desk	ZainTECH Support	zt-support@zaintech.com	Refer 1.2.1
2	Your Customer Success Manager			
3	Hassan Zohaib	Senior Manager – Managed Services	hassan.zohaib@zaintech.com	+971 52 569 7052
4	Ahmed Hassaan	Head of Managed Services	ahmed.hassaan@zaintech.com	+971 56 179 4356
5	Simmi Thomas	Director of Cloud Operations	simmi.thomas@zaintech.com	+971 50 384 8320

1.2.3. From the time of Response until resolution, updates shall be provided to the Named Contacts by email at such frequencies as set out in the table above.

1.2.4. Cases on hold will be automatically closed if the customer does not respond to requests from the case handlers for updates according to the priority of ticket SLA.

1.2.5. **Requests for Change (RFC) –** All RFC's will be treated as Priority 4 and therefore will be subject to the RFC SLA. Should the Customer require an urgent RFC to be undertaken, then an Urgent RFC can be requested. Acceptance of an Urgent RFC will be at the discretion of the Service Provider and will therefore be classified as Priority 2 subject to Priority 2 SLA. RFC can only be initiated by the Named Contacts.

1.2.6. **Emergency Requests for Change (eRFC) –** Emergency RFC's will be treated as Priority 1 on the contingency that they have been raised or approved by a named contact under this Agreement from the Customer.

1.2.7. **Disaster Recovery –** In case the Customer has opted for 'Disaster Recovery as a Service' (DRaaS), then Service Provider will deliver and manage a disaster recovery site, as part of the solution. As connectivity is a critical component for replication under the Disaster Recovery (DR) services and thus Customer is solely entrusted with the responsibility to connect to the data center through a direct connection based on bandwidth requirements. Customer production systems will be replicated to the disaster recovery site and automation for recovery will be provided as part of the solution, according to the following SLA defined for the service:

Category	Service Level Target	Maximum Service Level	Service Credit

Active Directory Replication	RPO ≤10 minute	RPO ≤ 30 minutes	10% of monthly fee if SLA not met
	RTO ≤ 30 minutes	RTO ≤ 90 minutes	
Database replication	RPO ≤ 30minutes	RPO ≤ 60 minutes	
	RTO ≤ 60 minutes	RTO ≤ 120 minutes	
Virtual machine replication	RPO ≤10 minutes	RPO ≤ 60 minutes	
	RTO ≤ 30 minutes	RTO ≤ 60 minutes	

1.3. **Service Credits:** Service Credits in the form specified in the table below will be applied (except to multi cloud services), in the form of discounts on the next available billing cycle should the target SLA not be met by the Service Provider.

CATEGORY	SERVICE LEVEL TARGET	MINIMUM SERVICE LEVEL	SERVICE CREDIT
P1 Incident Response	100% Incidents responded to within 30 minutes	90% Incidents responded to within 30 minutes	10% of monthly fee if SLA not met
P2 Incident Response	100% Incidents responded to within 1hour	90% Incidents responded to within 1 hour	10% of monthly fee if SLA not met
Downtime on Service Provider infrastructure*	99.9% uptime within a calendar month	95% uptime within a calendar month	15% of monthly fee if SLA not met

*defined as Service Provider resources including ISP line provided under this Agreement. Does not include issues with ISP, Operating System or Customer application. Further, it is subject to Customer maintaining resiliency and high availability of its environment throughout the contractual period.

1.4. **Limitations on Service Credits**

1.4.1. Notwithstanding anything in this Agreement to the contrary, the maximum total Service Credit for any calendar month for failure to meet the Service Level Agreement shall not exceed one hundred per cent (100%) of Customer's monthly recurring fee for the affected cloud Services. Service Credits that would be available but for any limitation on credits will not be carried forward to future months.

1.4.2. Customer is not entitled to a Service Credit under any Service Level Agreement for downtime or outages resulting from Maintenance. For purposes of the Agreement, Maintenance shall mean:

1.4.2.1. Scheduled maintenance – Repairs, modifications, or upgrades announced at least seventy-two (72) hours in advance;

1.4.2.2. Scheduled customer maintenance – Maintenance of Customer's configuration that Customer requests and that Service Provider schedules with Customer in advance (either on a case by case basis, or based on standing instructions), such as hardware or software upgrades;

1.4.2.3. Emergency maintenance – Critical unforeseen maintenance needed for the security or performance of Customer's configuration or Service Provider's network.

1.4.3. Customer is not entitled to a Service Credit under any Service Level Agreement for downtime or outages resulting from:

1.4.3.1. External factors or circumstances outside of Service Provider's control, including zero-day attacks, unknown vulnerabilities, denial of service attacks, virus attacks, hacking attempts and spikes in network traffic or application utilization;

1.4.3.2. A change which Customer effects or requests which results in downtime or outages or interferes with Service Provider's ability to provide the Services;

1.4.3.3. Deficiencies, bugs or errors in Customer's applications, application codes, data structures, system software, operating systems, or in any vendor supplied patches;

1.4.3.4. Any unsupported third-party products or third-party services (or their interaction with the Services) which were not provided or installed by the Service Provider.

1.4.4. Customer is not entitled to a Service Credit under any Service Level Agreement if Customer is in breach of the Agreement at the time of the occurrence of the event giving rise to the Service Credit until Customer has cured the breach. Customer is not entitled to a Service Credit if the event giving rise to the Service Credit would not have occurred but for Customer's breach of the Agreement with or Customer's misuse of the Services.

1.4.5. Customer must request a Service Credit via support ticket in the Service Provider portal within thirty (30) days following the occurrence of the event giving rise to the Service Credit. If the claim is approved, the Service Credit will be applied during the next billing cycle following approval. Customer must show that its use of the Service to which the applicable Service Level Agreement applies was adversely affected in some way as a result of the downtime or outage to be eligible for the Service Credit.

1.4.6. For the purpose of determining whether a Service Credit is due, time periods will be measured from the time stamp generated by Service Provider's ticket system, the time an interruption is recorded in Service Provider's monitoring system, until network availability is restored or the affected device is powered back on, as applicable. Customer may open a support ticket to document the start time for a support request or other Incident, or if Customer contacts the Service Provider by telephone to request support, Service Provider will open a support ticket. If Customer contacts Service Provider by phone, there may be a delay between the time of the call and the time Service Provider opens a support ticket.

1.4.7. Service Provider Assured is in place to ensure the Customer's environment is available, secure, maintained and governed up to industry best practices. The Service Level Objective (SLO) is defined as below:

1.4.7.1 Target uptime (i.e in IaaS) of 99.9% of infrastructure limited to:

a. Compute environment (server hardware and hypervisor),
b. Network (routers, firewalls, switches),
c. Storage systems (production and disaster recovery),
d. Backup infrastructure (hardware and software),
e. Operating system (windows and linux) and
f. Service Provider's management console.

1.4.8. SLO is not subject to ISP downtime, datacenter provider downtime or Service Credits.

1.4.9. Service specifications

1.4.9.1 The Services are subject to and governed by Service specifications applicable to Customer's order. Service specifications are defined as provisioning and management processes applicable to the Services (such as capacity planning), types and quantities of system resources (such as storage allocation or virtual machine resources), functional and technical aspects of the service, as well as any managed service deliverables.

1.4.9.2 Customer acknowledges that use of the Services in a manner not consistent with the Service specifications may adversely affect Services performance and/or may result in additional fees. If the Services permit Customer to exceed the ordered quantity (e.g., soft limits on counts for Users, sessions, storage, etc.), then Customer is responsible for promptly purchasing additional quantity to account for Customer's excess usage.

1.4.9.3 Service Provider may make changes or updates to the Services (such as infrastructure, security, technical configurations, application features, etc.) during the Services period, including to reflect changes in technology, industry practices, patterns of system use, and availability of third-party content.

1.4.9.4 The Service specifications are subject to change at Service Provider's discretion; however, Service Provider's changes to the Service specifications will not result in a material reduction in the level of performance or availability of the applicable Services provided to Customer for the duration of the Services period.

1.4.9.5 Customer accepts the responsibility for Multiprotocol Label Switching (MPLS) connectivity.

1.4.9.6 The RACI for the services RACI shall state the parties for the Responsible, Accountable, Consulted, and Informed role.

2. SECURITY OF HOSTED SYSTEM

2.1. Service Provider shall implement reasonable and appropriate technical and organizational measures to protect Customer's hosted system against unauthorized access. However, Service Provider cannot guarantee 100% security as this is unachievable in IT security arena. Service Provider's security obligations with respect to Customer data are limited to those obligations described in this clause. Service Provider makes no other representation regarding the security of Customer data. Service Provider is not responsible to Customer for unauthorized access to the Customer data or the unauthorized use of the Services that does not directly result from Service Provider's failure to meet its security obligations stated in the Agreement.

2.2. **Customer Data Privacy.** Customer warrants that it shall process any Personal Data in compliance with all applicable data protection or privacy law. Customer shall, or shall require its end user(s) to, implement those technical and organizational measures required by the applicable data protection and privacy laws relative to Customer's use of the Services and the nature and the volume of the Personal Data stored on the Hosted System or processed through Customer's use of the Services. Customer is responsible for providing any necessary notices to individuals and for obtaining any legally required consents from individuals in relation to Service Provider's provision of any Services to Customer or Customer processing of any Personal Data. Customer is solely responsible for any losses or other consequences arising from its failure to implement reasonable security measures as set forth in this Agreement.

2.3. **IP Addresses.** Upon expiration or termination of the Agreement, Customer must discontinue use of the Services and relinquish use of the IP addresses and server names assigned to Customer by Service Provider in connection with the Services, including pointing the DNS for Customer's domain name(s) away from Service Provider Services. Customer agrees that Service Provider may, as it reasonably determines necessary, make modifications to DNS records and zones on Service Provider managed or operated DNS servers and services.

2.4. **Services Management Agent.** Customer agrees that it will not interfere with any services management software agent(s) that Service Provider installs on the Services. Service Provider agrees that its agents will use only a minimal amount of computing resources, and will not interfere with Customer's use of the Services. Service Provider will use the agents to track system information so that it can more efficiently manage various Service issues. Service Provider may also use the agents to identify security vulnerabilities. The Services will become "Unsupported", as described below, if Customer disables or interferes with Service Provider's services management software agent(s). Customer agrees that Service Provider may access the Services to reinstall services management software agents if Customer disables them or interfere with their performance.

2.5. **Patch Management.** Customer agrees to automated patch roll out for Microsoft Security Updates on a weekly basis. Service Provider guarantees that patches have been pre-tested and authorized before patching production systems. Service Provider mandated patches will be applied to customer UAT and pre-production environments and assessed for impact prior to patching customer environment.

2.6. **Exit of Services**. Upon completion of Agreement term or notice of termination, Service Provider will make provisions for safely migrating Customer services away from Service Provider's environment to platform of Customer's choice subject to professional charges. Migration activities must be completed within 90 days' notice period. Contracted MRC (As per SOF) will be applied for each month that Customer is still consuming services beyond the notice period, if Customer fails to migrate off the Service Provider's platform during that time. Should the Customer wish to take possession of hard disks used to house Customer data during the Agreement period, then Customer will be liable to pay replacement fees for new disks for the Service Provider environment. Irrespective of the credit terms agreed upon, Customer shall be obligated to settle all the outstanding invoices,

including notice period invoices, before Provider can initiate the exit process. Customer agrees that payment terms as per SOF will not be applicable in this case and exit process will be initiated only upon full settlement of all outstanding invoices.

2.7. **Secure Deletion Procedures.**

Secure Deletion Procedures (IaaS, DRaaS). In case the Customer asks for full secure VM deletion or left the cloud, we use a secure deletion procedure that use Secure Deletion Utilities which is a hard disk secure deletion tool that implement secure deletion based on 24 worldwide standards to secure wipe any data resides on disks. The below is the procedure we use:

- Customer Confirm VM secure deletion.
- Provider Cloud stop the virtual machine.
- Boot from Secure Deletion Utilities and use the secure deletion command which overwrite the data with various methods to make sure everything wiped.
- Delete the VM from the Hypervisor which is a second deletion layer.

By the end of this procedure the disks will be overwritten then the VM will be deleted to achieve the maximum secure deletion for the data inside the VM.

Secure Deletion Procedures (BaaS). In case the Customer asks for full secure backup deletion or left the cloud, we use a secure deletion procedure that use Secure Deletion Utilities which is a disk secure deletion tool that implement secure deletion based on 24 worldwide standards to secure wipe any data resides on disks. The below is the procedure we use:

- Customer Confirm backup data secure deletion.
- Provider CLOUD disable the backup policies.
- Disk sanitizing is a process that involves writing byte sequence multiple passes on all disk blocks that contain sensitive data.

2.8. **Additional terms for elected additional services**.

2.8.1. *Cloud Server Images*. If Customer provisions a Service Provider Cloud Server or other Service using a non-standard or non-Service Provider image or installation (even if such image is made available to Customer by Service Provider during configuration, provided that it is identified as such), then Service Provider shall have no obligation to provide Support for that Service, and any Support provided shall be on an AS IS basis. Customer agrees that if it uses our Services to share or receive an image, then such image sharing or receipt is at Customer's sole risk.

2.8.2. *Domain Name Registration Services*. If Customer registers, renews or transfers a domain name through the Service Provider, Service Provider will submit the request to its domain name services provider (the "Registrar") on Customer's behalf. Service Provider's sole responsibility is to submit the request to the Registrar. Service Provider is not responsible for any errors, omissions or failures of the Registrar. Customer's use of domain name services is subject to the Registrar's applicable legal terms and conditions. Customer is responsible for closing any account with any prior reseller of or registrar for the requested domain name, and for responding to any enquiries sent to Customer by the Registrar.

2.8.3. *Role-Based Access Control*. Customer's designated account administrator is responsible for role administration. When making permission changes with role-based access control services, there may be a delay before the implementation of changes. Service Provider is not responsible for any loss that may occur due to the delayed implementation of changes.

2.8.4. *Unsupported Configuration Elements or Services*. If Customer asks Service Provider to implement a configuration element (hardware or software) or cloud-related service in a manner that is not customary in the market, or that is in "end of life" or "end of support" status Service Provider may designate the element or service as "unsupported", "non-standard", "best efforts", "reasonable endeavours", "reasonable" "endeavours", "one-off", "EOL", "End of Support", "as is", or with like term (referred to in this Clause as an "Unsupported Service"). Service Provider makes no representation or warranty whatsoever regarding the Unsupported Service, and Customer agrees that Service Provider shall not be liable to Customer for any loss or damage arising from the provision of the Unsupported Service. Service

Level Agreement shall not apply to the Unsupported Service, or to any other aspect of the Services that is adversely affected by the Unsupported Service. Customer acknowledges that Unsupported Services may not interoperate with Service Provider's other services, including backup or monitoring.

2.8.5. *Data Backup*. Although the Service may be used as a backup service, Customer agrees that it will maintain at least one (1) additional current copy of the Customer Data and programs stored on the Hosted System somewhere other than on the Hosted System. If Customer utilizes Service Provider's Cloud Backup Services then Customer is responsible for performing and testing restores as well as testing its systems and monitoring the integrity of its Customer Data. Customer has the option to create a snapshot or backup of its cloud servers or databases, respectively, however it is Customer's responsibility to initiate the snapshot backup and test it to determine the quality and success of the backups.

2.9. **Data Security Measures**. Service Provider will have in place appropriate technical and organizational measures to protect the customer Data and Sensitive Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

2.10. **Third Party Access**. Service Provider will have in place procedures so that any third party the Customer authorizes to have access to the Personal Data and Sensitive Personal Data, including processors, will respect and maintain the confidentiality and security of the Personal Data and Sensitive Personal Data. Any person acting under the authority of the Customer, including a data processor shall be obligated to process the Personal Data and Sensitive Personal Data only on instructions from the Customer. This provision does not apply to persons authorized or required by law or regulation to have access to the Personal Data and Sensitive Personal Data.

2.11. **Hosted system ownership**. Customer will not acquire any ownership interest in or right to possess the Hosted System, and Customer has no right of physical access to the Hosted System. Customer agrees that Service Provider may migrate the Hosted System or Customer Data within or between data centers, including if Service Provider determines in its reasonable judgment that migration is required to remediate service degradation or shared resource constraints. Service Provider will give Customer reasonable advance notice of at least thirty (30) days and shall ensure that Customer Data is only transferred in accordance with all applicable data protection laws.

2.12. Customer has (and any vendor/contractor authorized by the Customer has) the right to physically access the Customer Equipment at any time and for any reason, including but not limited to for the purpose of conducting maintenance and upgrade works on the Customer Equipment.

2.13. Subject to payment of any due amounts, Customer has the right to remove the Customer Equipment once the Agreement is terminated.

2.14. Service Provider does not have knowledge of the Customer Data that Customer, or Customer's end-user, store on the Hosted System, including the content, quantity, value or use of the data. Customer Data is and at all times shall remain Customer's exclusive property and Customer is solely responsible for:

2.14.1. Determining the suitability of the Services in light of the type of Customer Data stored by Customer or Customer's end-user(s) on the Hosted System or otherwise processed by Customer or Customer's end user(s) through Customer's use of the Services;

2.14.2. use of the Hosted System and the Services by any of Customer's employees, Affiliates, or other user(s) which Customer authorizes or who gains access to the Hosted System or Services as the result of Customer's failure to utilize reasonable security precautions in light of Customer's use of the Services;

2.14.3. Taking all reasonable steps to mitigate the risks inherent in transmitting Customer Data to and from and while stored on the Hosted System using the Services, including any Customer Data loss or corruption; and

2.14.4. Reasonable steps under Clause 2.13.3 shall include:

2.14.4.1. Encrypting, in accordance with applicable laws, any Personal Data; any "non-public personal information" "protected health information" and other regulated financial,

health or sensitive data, transmitted to and from and while stored on the Hosted System.

2.14.4.2. Designating authorized users under Customer account and limiting access of login credentials associated with Customer account.

2.14.5. Customer agree to immediately notify Service Provider of any unauthorized use of the Services or account or of any other breach of security. Customer also agrees to cooperate with Service Provider's reasonable investigation of security-related breaches.

2.15. Customer is responsible to obtain all required consents from third parties (including Customer's end-customers, partners, distributors, and employees) in whatever form necessary under the applicable privacy and data protection laws with regards to any personal data (including for PII - personally identifiable information) as defined by the applicable data protection laws. Upon which Service Provider shall process the data in accordance with the written instructions of the Customer and the terms of this Agreement.

2.16. In performing the activities contemplated under this agreement or the relevant PO, Service Provider and/or its subcontractors will comply with requirements of a processor applicable to it under data protection laws and Customer will comply with the requirements of a controller applicable to it under data protection laws. In case Service Provider incurs additional costs for such compliance related to any new laws issued in this respect, Service Provider shall advise Customer on the additional cost; this cost shall be settled by the Customer through issuing a PO to Service Provider covering such additional costs. Customer agrees to comply with all applicable laws relevant to the provision of the Services, including but not limited to all applicable data protection laws relevant to the storage or transfer of Customer data as envisaged by this Agreement.

2.17. Security is a shared responsibility. Service Provider has included reasonable measures in its security architecture, which logically separate and prevent Customer data (including PII data) from being exposed to or accessed by unauthorized persons. At physical level, Service Provider & its suppliers maintain appropriate physical entry controls, card-controlled entry points and surveillance cameras to protect against unauthorized entry into Service Provider managed facilities (data centers) used to host the Service Provider services with access limited by job role and subject to authorization.

2.18. Customer is responsible for implementing and managing security and privacy measures for components that Service Provider does not provide or manage within the Service Provider services. Examples of Customer responsibilities include:

2.18.1. Security of systems and applications built or deployed by the Customer upon an infrastructure as a service or such other 'as a service' offering or upon infrastructure, components or software that Service Provider manages for the Customer.

2.18.2. Customer end-user access control and application level security configuration.

2.19. For Service Provider cloud services with self-managed features, Customer can remove content at any time. Otherwise, Service Provider will return or remove content from Service Provider computing resources upon the expiration or cancellation of the Service Provider cloud services, or earlier upon Customer's request. Service Provider may charge for certain activities performed at Customer's request (such as delivering content in a specific format). Service Provider does not archive content; however, some content may remain in the Service Provider cloud services backup files until expiration of such files as governed by Service Providers' backup retention practices.

2.20. Service Provider shall notify the Customer of any actual or suspected personal data breaches (including those that require organizations to notify authorities, such as attacks on critical infrastructure and those that affect personal data) without undue delay and, where feasible, not later than 72 hours after becoming aware of it except in the following circumstances:

2.20.1. Service Provider believes that the act of performing a notification increases the risk to other Customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.

2.20.2. Other unusual or extreme circumstances vetted by Service Providers' technical department.