SWiZ Technologies Pte Ltd
Break-Fix IT Support Service Agreement

This agreement outlines SWiZ Technologies Pte Ltd's approach to the provision of break-fix IT support services, maintenance, and related technical advisory to clients as part of a professional service engagement.

It applies to services provided to Clients based on the scope, conditions, and entitlements specified in the approved quotation or proposal issued by SWiZ Technologies. This document defines the standard service framework under which SWiZ Technologies operates in delivering support activities.

This agreement serves as a reference for Clients to understand the service boundaries, responsibilities, limitations, and operational practices governing the provision of support services.

SWiZ Technologies reserves the right to amend this Service Agreement from time to time without prior notice. The most current version shall apply to all ongoing and future service engagements unless otherwise agreed in writing.

Change Management

Version	Date	Change Description	Approved By

4.0	29 April 2025	Conversion from Master Service Agreement to Break-Fix Agreement	Andy Lim
4.1	29 April 2025	Update Section 4	Andy Lim
4.2	30 April 2025	Update new clause – General Provision	Andy Lim

Table of Contents

1. Scope of Support

This Service Agreement covers break-fix IT support services provided by SWiZ Technologies Pte Ltd ("SWiZ") on a reactive, call-up basis. Services are limited to specific devices identified in the approved quotation, proposal, or the Client's IT asset list, and are intended to support the operational stability of the Client's core infrastructure components.

Device types that may be supported under this Agreement include:

- Servers
- Network switches
- Firewalls
- Backup systems
- Endpoint devices (desktops, laptops)

The devices and systems supported under this Agreement shall be strictly limited to those expressly listed and agreed upon in the Client's approved quotation, proposal, or IT asset list. The examples provided above are for general reference only and do not imply coverage of any devices not expressly included.

Under this Agreement, SWiZ will perform:

- Diagnosis and rectification of hardware or system faults on the covered devices
- Application of minor firmware or software updates within the same major version family (for example, upgrading from version 6.4.x to 6.6.x)

Support services are initiated upon the Client's request and are subject to the Client providing the necessary access credentials or remote connectivity to the affected systems. If pre-arranged credentials are available, SWiZ will utilize them; otherwise, access will be coordinated at the point of service.

2. Out-of-Scope Activities

The following activities are expressly outside the scope of this Agreement:

- Major version upgrades, platform migrations, or system overhauls (for example, upgrading from version 6.x to 7.x)
- Cybersecurity services, including malware removal, security incident response, or vulnerability assessments
- Support for business or third-party application software (e.g., accounting systems, CRM platforms)
- Network redesigns, architectural planning, or infrastructure expansion projects

- New system installations or deployment of equipment not listed in the approved service scope or asset list
- Routine preventive maintenance, proactive monitoring, or scheduled health checks
- Data recovery services resulting from system failure, corruption, or cybersecurity attacks
- Devices not registered under the Client's approved IT asset list or not explicitly covered under the quotation or proposal

Requests for out-of-scope services may be addressed separately under a new quotation and are subject to SWiZ's prevailing service rates.

3. Service Hours and Response Commitment

Support services under this Agreement are available during SWiZ's standard business hours, unless otherwise specified in the Client's approved quotation or proposal. Standard business hours are Monday to Friday, 9:00 AM to 5:00 PM (Singapore time, excluding public holidays). Requests received outside of standard hours will be acknowledged and processed on the next business day unless otherwise arranged.

SWiZ categorises support activities into incidents, service requests, and change requests to manage prioritisation and service handling effectively. Estimated response times vary according to the severity and nature of the request as outlined below. All response timeframes are provided as non-binding targets for service management purposes and may vary depending on complexity, resource availability, and third-party vendor dependencies. These targets shall not constitute binding service level guarantees unless otherwise expressly contracted.

3.1 Incident Response

An "Incident" refers to an unplanned interruption to an IT service or a reduction in the quality of an IT service that requires restoration efforts. Estimated response times for incidents are as follows:

Incident Severity	Estimated Response Time
Crisis – Severe issue requiring immediate attention, significantly impacting business operations	Within 30 minutes
Site Down – Site- or branch-specific disruption, requiring swift resolution to prevent further disruption	Within 1 hour
Major – Moderate impact affecting some users, requiring resolution within a reasonable timeframe	Within 4 hours

Incident Severity	Estimated Response Time
Minor – Low-impact issue affecting few users, manageable without significant disruption	Within 1 working day
No Impact – No operational effect; general inquiry or cosmetic issue	Within 3 working days

3.2   Service Request Response

A "Service Request" refers to a formal request from a user for standard services such as software installations, access permissions, information queries, or other routine service needs. Estimated response times for service requests are as follows:

Service Request Severity	Estimated Response Time
Major – High-priority request impacting multiple users	Within 4 hours
Minor – Standard request impacting limited users	Within 1 working day
No Impact – Non-urgent or informational request	Within 3 working days

3.3   Change Request Response

A "Change Request" refers to the addition, modification, or removal of anything that could affect IT services, typically subject to formal change management processes. Estimated response times for change requests are as follows:

Change Request Severity	Estimated Response Time
Major – Critical change with significant business impact	Within 4 hours
Minor – Routine change with limited business impact	Within 1 working day
No Impact – Non-urgent change request without operational impact	Within 3 working days

3.4   Vendor Dependency

Where incident resolution, service fulfilment, or change implementation depends on third-party hardware or software vendors, SWiZ will coordinate with the relevant vendors and follow up in accordance with the estimated response times outlined above. However, SWiZ cannot

guarantee the response or resolution performance of third-party vendors and shall not be held liable for delays resulting from vendor dependencies.

3.5 Security and Risk Considerations

SWiZ reserves the right to delay immediate action on any reported incident, service request, or change request where it is necessary to evaluate and manage potential risks to system security, data integrity, or operational stability. In such cases, SWiZ will maintain prompt communication with the Client to assess the situation and determine the safest and most appropriate course of action.

The preservation of system security, data protection, and the minimisation of operational risks shall take precedence over any stated service response or resolution targets under this Agreement.

4. Additional Services and Billing

This Agreement is aligned to the services, devices, and deliverables specified in the approved quotation or proposal issued by SWiZ.

Services, activities, or requests that are not explicitly covered in the quotation or proposal, or which fall outside the described scope, shall be treated as additional services. Such additional services will be subject to separate billing, based on SWiZ's prevailing service rates or as otherwise agreed.

Where an additional service, item, or subscription has already been presented in the quotation or proposal, SWiZ reserves the right to bill for such service or item upon activation, deployment, or usage by the Client, without the need for a further quotation or separate written agreement.

By proceeding with the activation, deployment, or use of any such service or item, the Client acknowledges and accepts the corresponding charges as outlined in the original quotation or proposal.

In the event that a new requirement arises that was not previously included in the quotation or proposal, SWiZ will provide a separate quotation for the Client's review and approval prior to the commencement of any related work.

All additional service charges are subject to the payment terms stated in the original quotation or as otherwise communicated by SWiZ.

5. General Service Conditions

SWiZ operates under a reactive engagement model, where services are provided upon the Client's notification of an issue. No proactive system monitoring or scheduled maintenance activities are included under this Agreement unless otherwise specified in a supplementary service annex.

Where applicable, on-site support will be provided in accordance with the entitlements and conditions stated in the Client's approved quotation or proposal. On-site scheduling and service durations are subject to these commercial terms.

It is the Client's responsibility to ensure timely provision of administrative access and system credentials to facilitate effective troubleshooting and resolution. SWiZ shall not be held responsible for delays arising from lack of access or incomplete system information.

The Client is also responsible for maintaining valid manufacturer warranties or hardware maintenance contracts for all supported devices, in order to facilitate hardware replacements and repairs when necessary. SWiZ does not perform physical hardware repairs and shall not be responsible for sourcing, procuring, or replacing defective hardware components.

Similarly, the Client is recommended to maintain active software support or maintenance subscriptions with original vendors to enable access to necessary patches, updates, and technical support services. SWiZ's ability to perform software updates, upgrades, or apply vendor-released fixes may be limited if the Client does not maintain such vendor relationships.

From time to time, SWiZ may inform the Client of known vulnerabilities, patches, or security advisories relevant to supported systems. Notification will be provided on a best-effort basis as a courtesy, and the decision to proceed with any patching, upgrading, or other remediation measures rests solely with the Client.

6. General Provisions

6.1 Indemnity

The Client shall indemnify and hold harmless SWiZ, its officers, employees, and authorised subcontractors, from and against any and all claims, losses, liabilities, damages, costs, and expenses (including reasonable legal fees) arising out of or in connection with:

- the Client's breach of this Agreement;
- misuse of the services provided by SWiZ;
- the Client's failure to comply with applicable laws and regulations; or
- any third-party claims resulting from data, materials, or instructions provided by the Client.

6.2 Force Majeure

SWiZ shall not be held liable for any failure or delay in the performance of its obligations under this Agreement due to events beyond its reasonable control, including but not limited to acts of God, natural disasters, war, terrorism, riots, governmental actions, pandemics, power outages, telecommunications failures, or delays caused by third-party vendors. In such events, SWiZ will make reasonable efforts to resume affected services as soon as practicable.

6.3 Dispute Resolution

In the event of any dispute or disagreement arising out of or in connection with this Agreement, the parties shall first attempt to resolve the matter in good faith through informal discussions. If the dispute remains unresolved within thirty (30) days, the parties agree to refer the matter to mediation in Singapore before pursuing any formal legal action. Nothing in this clause prevents either party from seeking urgent interim relief where appropriate.

6.4 Entire Agreement

This Agreement, together with the approved quotation or proposal referenced herein, constitutes the entire agreement between the parties relating to the subject matter and supersedes all prior discussions, negotiations, or communications, whether written or oral. No amendment or variation shall be effective unless agreed in writing by both parties.

6.5 Severability

If any provision of this Agreement is found to be invalid, unlawful, or unenforceable under applicable law, such provision shall be severed from this Agreement, and the remaining provisions shall remain in full force and effect.

7. Responsibilities and Limitations

7.1 SWiZ Responsibilities

SWiZ shall exercise reasonable care, skill, and professionalism in the delivery of support services described under this Agreement. Support services will be delivered according to the scope and conditions set out in the approved quotation or proposal.

SWiZ's responsibilities under this Agreement include:

- Responding to incidents, service requests, and change requests in accordance with the response guidelines outlined in Section 3
- Providing technical guidance related to fault resolution, system recovery, and the maintenance of supported systems, within the agreed service scope

- Escalating incidents to relevant third-party vendors or suppliers when necessary, and following up based on the agreed service level guidelines
- Informing the Client of known vulnerabilities, security advisories, or recommended patches that may affect supported systems, where such information becomes known to SWiZ in the course of operations
- Maintaining the confidentiality of Client information accessed or handled during the delivery of services, in accordance with SWiZ's internal data protection policies
- Documenting key actions taken during service incidents where necessary, and providing reasonable updates to the Client throughout the support process

Support services shall be provided on a best-effort basis within the agreed frameworks, but SWiZ does not guarantee uninterrupted services, absolute resolution of every reported issue, or outcomes where dependencies outside SWiZ's control exist (such as third-party product performance, environmental limitations, or access restrictions).

7.2 Client Responsibilities

The Client is responsible for maintaining a stable and supported IT environment, and for ensuring that the following conditions are met:

- Granting SWiZ timely access (remote or on-site) to systems, accounts, and relevant infrastructure for the purposes of support
- Ensuring all devices to be supported are declared and listed in the approved asset inventory or quotation
- Maintaining reliable system and data backups; SWiZ does not hold responsibility for backup failures or data restoration unless explicitly engaged for managed backup services
- Maintaining valid manufacturer warranties or hardware maintenance contracts for all supported devices, to facilitate necessary hardware replacements and repairs
- Maintaining active software support or maintenance subscriptions with original vendors to ensure access to necessary patches, updates, and technical support services
- Informing SWiZ of any changes to the supported environment, including system upgrades, replacements, or reconfigurations
- Ensuring that actions taken by SWiZ are authorised by designated contacts or decision-makers within the Client's organisation

Where any of the above responsibilities are not fulfilled, SWiZ shall not be held accountable for any resulting delays, service limitations, data loss, or operational impact.

7.3 Limitation of Liability

To the fullest extent permitted by law, SWiZ shall not be liable for:

- Any indirect, incidental, special, punitive, or consequential damages, including but not limited to loss of profits, loss of revenue, business interruption, or loss of data
- Delays or failures arising from circumstances beyond SWiZ's reasonable control, including but not limited to those described under the Force Majeure clause (Section 6.2)
- Any loss of data or inability to recover data, unless SWiZ has been specifically engaged and contracted to provide managed backup services for the affected systems
- Security breaches, data losses, or system vulnerabilities resulting from the Client's decision not to apply recommended patches, upgrades, or security measures
- Any adverse impact resulting from the Client's non-adoption of SWiZ's technical recommendations or advice

In all cases, SWiZ's total cumulative liability for any and all claims arising out of or relating to this Agreement shall not exceed the total amount paid by the Client for services rendered in the preceding three (3) months before the claim arose.

Nothing in this Agreement shall limit liability for death, personal injury, or other matters which cannot be excluded under applicable law.

8. Cybersecurity Services (Where Applicable)

This section applies only where cybersecurity services have been expressly included in the approved quotation or proposal provided by SWiZ.

Where cybersecurity services are engaged, the specific scope, deliverables, and service commitments are as detailed in the corresponding quotation or proposal. No services beyond those explicitly listed shall be implied under this Agreement.

8.1 Risk and Threat Management

SWiZ will provide cybersecurity services with reasonable care, skill, and professionalism, supporting the Client in identifying, managing, and responding to cybersecurity risks and threats as defined in the agreed scope of services.

While no security service can guarantee absolute prevention of cybersecurity incidents, SWiZ will work alongside the Client to manage and mitigate risks to the best of its capabilities. In the event of a security incident, SWiZ will assist in investigation, containment, mitigation, and recovery efforts, maintaining a collaborative partnership with the Client throughout the process.

Residual risk remains an inherent aspect of cybersecurity, and ultimate risk ownership remains with the Client. SWiZ will, where applicable, assist the Client in evaluating cybersecurity risks related to supported systems and services.

8.2 Cybersecurity Awareness and Best Practices

Where included as part of the engaged services, SWiZ may provide cybersecurity awareness advisory to the Client's designated personnel, covering topics such as cyber hygiene, common security threats, and recommended practices for maintaining a secure environment.

SWiZ may also share best practice guidelines relating to patch management, system configuration, access controls, and other basic cyber hygiene measures to support the Client's internal security posture.

Formal cybersecurity training programs or employee certification initiatives are outside the scope of this Agreement unless otherwise stated in the quotation or proposal.

8.3 Security Incident Response

Where security incident response services are engaged, SWiZ will assist the Client in identifying, containing, and mitigating cybersecurity incidents in accordance with internal structured response processes.

Should an incident exceed the engagement's operational scope (e.g., complex forensic investigation, legal proceedings), SWiZ may recommend escalation to specialised third-party providers. Such services, if engaged, will be separately arranged and billed.

SWiZ's assistance does not extend to legal, regulatory, or financial liabilities resulting from cybersecurity incidents.

8.4 Client Responsibilities for Cybersecurity

The Client agrees to:

- Cooperate fully during cybersecurity assessments, incident response, and remediation activities
- Maintain up-to-date system backups, endpoint protections, patching, and user access control practices
- Act promptly on critical security advisories and risk mitigation recommendations provided by SWiZ
- Notify SWiZ immediately upon detection of suspected security incidents, vulnerabilities, or abnormal activities
- Designate internal contacts responsible for cybersecurity matters and communications with SWiZ

Failure to fulfill these responsibilities may impact the effectiveness of cybersecurity services and limit SWiZ's ability to respond to incidents.

8.5   Limitations of Cybersecurity Services

Cybersecurity services provided under this Agreement are limited strictly to the systems, devices, and service areas explicitly listed in the approved quotation or proposal.

SWiZ shall not be liable for:

- Undetected threats, breaches, or vulnerabilities originating from systems, environments, or devices not covered under the service scope
- Security incidents or impacts resulting from the Client's failure to implement recommended security measures or hygiene practices
- Losses or damages arising from Client-side misconfigurations, outdated systems, unmanaged third-party solutions, or refusal to act on critical advisories

Cybersecurity services provided by SWiZ are intended to supplement the Client's internal risk management, compliance, and governance processes. Responsibility for overall cybersecurity strategy, regulatory compliance, and risk acceptance decisions remains with the Client.

Where requested, SWiZ may participate in periodic cybersecurity service reviews to support continuous improvement; however, such reviews are advisory in nature and non-binding unless separately agreed.

9. Agreement Acknowledgement

This Agreement is intended to be read in conjunction with the approved quotation or proposal provided to the Client.

By accepting the quotation or proposal, requesting services, or utilising services provided by SWiZ, the Client acknowledges and agrees to the terms and conditions outlined in this Agreement.

SWiZ reserves the right to amend or update the terms of this Agreement from time to time with reasonable notice to the Client. The most current version of the Agreement will apply to all ongoing and future services unless otherwise agreed in writing.