Annexure 8: Warranty, Support and Maintenance (including Exit Requirements)

1. Purpose

This Annexure defines the requirements and procedures for warranty support, defect management, incident handling, corrective actions, and minor changes during the warranty period for the Building Blocks delivered under this Contract, as defined in the BRD and ToR Section 5.2 (Deliverable–Gate–Timeline–Payment Matrix). It also sets the service levels (SLAs) for Production support from Go-Live, the Hypercare requirements, and the exit and transition requirements referred to in ToR Sections 7.2.4 and 14.

The requirements in this Annexure shall be read together with ToR Section 14 – Warranty, Support and Maintenance, the approved Business Requirements Document (BRD), Non-Functional Requirements (NFR), the reporting and KPI provisions of Annexure 3, and other applicable provisions of the ToR.

2. Warranty Period and Support Before Final Acceptance

- The Vendor shall provide a warranty period of twelve (12) months for each Lot, starting on Final Acceptance of the Lot (ToR Section 14.1). Final Acceptance is the date of the Deliverable Acceptance Certificate for D5 (Lots 1 and 2) or D6 (Lot 3).
- Building Blocks that go live before Final Acceptance shall be supported by the Vendor from their Go-Live until Final Acceptance, on the same terms as this Annexure and at no additional cost, as part of the implementation obligations (ToR Section 14.1).
- Where the Building Blocks are migrated to GovCloud during the Warranty Period, the warranty continues to apply in GovCloud, and defects arising from the migration are warranty defects.

3. Warranty Coverage

During the warranty period, the Vendor shall provide all necessary support and corrective actions at no additional cost to the PA. Warranty coverage shall include, but not be limited to:

- correction of software defects, bugs, errors, and failures;
- correction of performance and availability issues;

- correction of integration and interoperability issues;
- correction of defects related to APIs and interfaces;
- remediation of security vulnerabilities and security-related deficiencies attributable to the delivered Building Blocks;
- implementation of necessary patches, updates, fixes, and configuration changes, and keeping third-party components patched and supported (ToR Section 14.1);
- correction of data-related issues attributable to the delivered Building Blocks;
- maintenance of compliance with the approved BRD, NFR, technical specifications, and applicable GovStack Building Block specifications, APIs, and standards, irrespective of the underlying solution architecture;
- necessary support for GovStack Building Block integration and interoperability within the approved scope;
- necessary troubleshooting, technical support, and corrective actions; and
- minor modifications covered under the warranty change allowance in Section 10.

If the delivered Building Blocks fail to meet any approved requirement during the warranty period, the issue shall be treated as a defect or non-conformity and shall be rectified by the Vendor within the resolution times in Section 5, at no additional cost to the PA.

4. Defect and Incident Classification

The following severity levels shall be used for reporting and managing defects and incidents in Production. They correspond to the Critical, High, Medium and Low levels in Annexure 3, Section 1.7.

Severity	Description	Example
Critical (P1)	Complete system failure or a major failure that prevents a Building Block or a critical function from being used in production.	Complete service outage, critical security incident, loss of critical functionality, major data corruption

High (P2)	Significant failure that affects important functionality or a large number of users, but the system remains partially operational.	Major integration failure, significant performance degradation, failure of an important API or service
Medium (P3)	Issue affecting limited functionality or users where a reasonable workaround is available.	Non-critical functional defect, minor integration issue, limited performance issue
Low (P4)	Minor issue with limited operational impact and no significant effect on system availability or core functionality.	Minor UI issue, formatting issue, minor documentation issue

The PA may determine or revise the severity level based on the actual impact of the incident.

5. Service Levels (SLA)

5.1 Support Model

- **L1** support (first contact and triage) is provided by the PA or GovTech helpdesk, through UCS once it is live. The Vendor provides **L2 and L3** support (diagnosis, workaround, fix) for its Lot.
- Incidents are logged in UCS or in the ticketing tool agreed at Inception. Response and resolution times are measured from the time the ticket is logged.
- **Support hours:** P1 incidents, 24 hours a day, 7 days a week. P2 to P4, working hours (09:00–17:00 Bhutan time, Monday to Friday, excluding Government holidays).
- Support may be given remotely. Where the PA requests, the Vendor shall attend on-site in Thimphu within one (1) working day.

5.2 Response and Resolution Times

Severity	Response (acknowledge and assign)	Status updates	Workaround or service restored	Permanent fix
Critical (P1)	30 minutes	Every 2 hours	Within the block's resilience-tier RTO (Annexure 2, CP-REL-02), and not later than 4 hours	2 days
High (P2)	2 working hours	Daily	1 working day	5 working days
Medium (P3)	1 working day	Weekly	5 working days	15 working days
Low (P4)	2 working days	Weekly	Not required	Next scheduled release

These times are the single source for Production incident SLAs (Annexure 2, Section 1.10).

- **Availability:** as specified in Annexure 2, and not less than 99.5% per month, excluding maintenance windows approved in advance by the PA (Annexure 3, Section 2.1).
- **Security vulnerabilities:** Critical within 7 days and High within 15 days of identification (Annexure 3, Section 2.1). Security incidents shall be reported to the PA within 24 hours of discovery (ToR Section 10).
- Time spent waiting for action by the PA, a GA system or a national platform is excluded, where the Vendor records it in the ticket.
- SLA performance is measured as KPIs under Annexure 3. Breaches are addressed through the Notice to Correct and Formal Performance Review procedure (Annexure 3, Section 3) and count towards the Project Success Rate that decides AMC eligibility (ToR Section 14.2).

5.3 Incident Handling

The Vendor shall:

- acknowledge the reported incident within the applicable response time;
- assess the impact and severity of the incident;
- provide regular status updates until resolution;
- implement appropriate corrective actions;
- restore the affected service as soon as reasonably possible and within the times in Section 5.2;
- provide a workaround where immediate permanent resolution is not possible;
- confirm the resolution with the PA; and
- close the incident only after the PA has confirmed that the issue has been satisfactorily resolved or in accordance with the agreed incident closure procedure.

6. Hypercare

During the thirty (30) day Hypercare period after Go-Live of the integrated Ready Services (ToR Definitions and Section 5.1), the Vendor shall, in addition to Section 5:

- assign named L2/L3 engineers, available on-site in Thimphu or online during working hours, and on call for P1 incidents;
- hold a daily review of incidents and service health with the PA;
- resolve P1 and P2 incidents within the times in Section 5.2, with no P1 or P2 incident open at the end of Hypercare (ToR Section 5.4); and
- submit the Hypercare and Warranty SLA Report (R7, Annexure 3) weekly.

7. Root Cause Analysis

For all Critical incidents and recurring High severity incidents, the Vendor shall conduct a Root Cause Analysis (RCA). The RCA shall include, at a minimum:

- description of the incident;
- date and time of occurrence;

- affected Building Block, component, service, or integration;
- impact of the incident;
- identified root cause;
- corrective action taken;
- preventive action proposed to avoid recurrence; and
- relevant supporting evidence, where applicable.

The Vendor shall submit the RCA within five (5) working days of service restoration for a Critical incident, and ten (10) working days for a recurring High incident, unless the PA agrees otherwise.

8. Testing and Verification of Fixes

The Vendor shall conduct appropriate testing before deploying any warranty-related fix, patch, update, configuration change, or modification into the production environment. Testing shall include, as applicable:

- functional testing (unit, integration, system, smoke and sanity, regression and user acceptance testing);
- non-functional testing (performance, load and stress, security, usability, compatibility, reliability and recovery testing);
- CI/CD pipeline checks (SAST, DAST and SCA); and
- penetration testing, where the change affects security controls.

The Vendor shall ensure that warranty-related changes do not adversely affect existing functionality, integrations, security, performance, data integrity, or other GovStack Building Blocks.

All fixes shall be committed to the PA repository and deployed through the CI/CD pipeline, via the QA and Staging environments, with the PA's approval before each Production deployment. An emergency fix for a P1 incident may be deployed with the PA Project Manager's verbal approval, confirmed in writing within one (1) working day and followed by full testing.

The Vendor shall provide relevant test results or evidence to the PA upon request.

9. Changes and Change Management

For the avoidance of doubt:

- Correction of defects, bugs, security vulnerabilities, performance deficiencies, integration failures, and non-conformities against approved requirements shall be treated as warranty obligations and shall not be considered Change Requests.
- New functionality, major enhancements, or requirements that are outside the approved BRD baseline — including GA System-side changes approved after Final Acceptance — shall be managed in accordance with ToR Section 13 – Change Management, Annexure 4 and ToR Section 14.1, and shall not be treated as warranty obligations.
- No change that requires additional payment shall be implemented without prior written approval from the PA in accordance with ToR Section 13.

10. Warranty Change Allowance

- The Vendor shall provide, within the Contract Price, an allowance of two (2) person-months (forty (40) person-days) per Lot during the Warranty Period for minor modifications requested by the PA.
- Minor modifications are small changes to configuration, forms, reports, workflows, content or user interface that do not add a new Building Block capability, do not change an approved Interface Specification, and can each be completed within five (5) person-days.
- The PA shall request each use of the allowance in writing. The Vendor shall estimate the effort before starting, and the PA shall approve the estimate.
- Effort used shall be recorded in the Warranty Issue Register and reported in each warranty report. Unused allowance lapses at the end of the Warranty Period and has no cash value.
- Work beyond the allowance, or outside the definition above, is a Change Request under ToR Section 13 and Annexure 4.

11. Security and Vulnerability Remediation

The Vendor shall:

- address vulnerabilities identified through security testing, monitoring, audits, or incident investigations within the times in Section 5.2;
- apply required security patches and updates;
- keep the SBOM and CBOM current and monitor components for newly disclosed vulnerabilities;
- support investigation and resolution of security incidents;
- implement corrective measures to prevent recurrence; and
- provide relevant remediation evidence upon request.

Security vulnerabilities and security deficiencies attributable to the delivered Building Blocks shall be corrected at no additional cost to the PA.

12. Data Integrity and Recovery

Where a data loss, corruption, inconsistency, or processing error is attributable to the delivered Building Blocks or the Vendor's services, the Vendor shall:

- investigate the cause;
- take immediate corrective action;
- support recovery or restoration of affected data, where technically possible;
- identify and address the underlying cause; and
- implement preventive measures to avoid recurrence.

The Vendor shall coordinate with the PA and relevant Government technical teams for any required data recovery or restoration activities, keeping all data within Bhutan (ToR Section 10.1).

13. Documentation Updates

The Vendor shall update relevant documentation affected by warranty-related changes, fixes, patches, or modifications. This may include:

- technical documentation;
- architecture and design documentation;
- API and integration documentation;
- configuration documentation;
- operational and troubleshooting documentation;
- security documentation; and
- release notes.

All updated documentation shall be provided in the format required by ToR Section 16.3, version-controlled in the PA repository, and maintained throughout the warranty period.

14. Proactive Monitoring and Support

The Vendor shall provide proactive technical support during the warranty period to identify potential issues before they materially affect system operations, using the national Observability platform.

Where monitoring information identifies potential defects, performance degradation, security vulnerabilities, availability issues, or integration problems, the Vendor shall assess the issue and take appropriate corrective action.

The Vendor shall coordinate with the PA and relevant technical teams for issues involving Government infrastructure, network, cloud, or other dependent services.

15. Warranty Issue Tracking

The Vendor shall maintain a Warranty Issue Register throughout the warranty period. The register shall include, at a minimum:

Field	Description
Issue ID	Unique reference number (UCS or ticketing tool reference)
Date Reported	Date and time issue was reported
Building Block	Affected Building Block

Issue Description	Description of the issue
Severity	P1, P2, P3, or P4
Impact	Business/technical impact
Response and resolution times	Times achieved, and whether the SLA in Section 5.2 was met
Root Cause	Identified cause, where applicable
Corrective Action	Action taken to resolve the issue
Status	Open / In Progress / Resolved / Closed
Date Resolved	Date corrective action was completed
Verification	Confirmation of successful resolution
Related CR	Change Request reference, where applicable
Allowance used	Person-days charged to the warranty change allowance (Section 10), where applicable
Remarks	Additional information

The Vendor shall provide the Warranty Issue Register to the PA upon request and as part of the periodic warranty reporting.

16. Warranty Reporting

The Vendor shall provide the Hypercare and Warranty SLA Report (R7) in the frequency set in Annexure 3: weekly during Hypercare and monthly from Go-Live until the end of the Warranty Period. The report shall include:

- number and status of reported incidents;
- incidents by severity;
- response and resolution performance against the SLAs in Section 5.2, and availability achieved;

- outstanding issues;
- Critical and High severity incidents;
- Root Cause Analysis reports;
- security vulnerabilities and remediation status;
- patches and updates implemented;
- warranty-related changes implemented;
- utilization of the warranty change allowance (Section 10);
- recurring issues and preventive actions; and
- any risks or issues requiring the attention of the PA.

17. Outstanding Critical and High Severity Defects

Any Critical or High severity defect reported during the warranty period that remains unresolved at the expiry of the warranty period shall continue to be addressed by the Vendor at no additional cost until the defect is fully resolved and the affected Building Block is restored to the required operational condition.

The completion of the warranty period shall not release the Vendor from its obligation to resolve such outstanding defects.

18. Warranty Completion and Exit Review

At least thirty (30) days before the end of the warranty period, the Vendor shall prepare and submit a Warranty Completion Report (the Warranty Completion deliverable: D7 for Lots 1 and 2; D8 for Lot 3; ToR Section 5.2). The report shall include:

- summary of warranty activities;
- list of all incidents and defects reported during the warranty period;
- status of all reported issues;
- details of Critical and High severity incidents;
- security incidents and vulnerabilities addressed;
- patches, updates, and fixes implemented;
- Root Cause Analysis reports;

- warranty-related changes implemented;
- utilization of the warranty change allowance (Section 10);
- SLA performance for the full Warranty Period and the Project Success Rate for the Warranty Period (Annexure 3, Section 2.2);
- outstanding issues, if any; and
- confirmation of compliance with the warranty requirements.

A Warranty Exit Review shall be conducted by the PA to confirm satisfactory completion of the warranty obligations. The warranty shall be considered satisfactorily completed only when:

- all warranty obligations have been fulfilled;
- all warranty defects are closed, or transferred with the PA's written agreement (ToR Section 5.4);
- required documentation has been updated;
- all agreed warranty reports and records have been submitted and SLA reports for the full Warranty Period accepted;
- the exit requirements in Section 20 have been met, to the extent they apply at the end of the Warranty Period; and
- the PA has completed the Warranty Exit Review.

Acceptance is recorded on the Deliverable Acceptance Certificate (Annexure 5).

19. Transition to Post-Warranty Support and Maintenance

Where post-warranty support and maintenance are required — including under an Annual Maintenance Contract (AMC) per ToR Section 14.2 — the Vendor shall provide reasonable transition support to ensure continuity of service from the warranty period to the post-warranty arrangement. The transition shall include, where applicable:

- outstanding issue status;
- system health and operational status;
- pending fixes and planned updates;
- configuration and deployment information;
- relevant documentation; and

- other information required by the PA for continued operation and maintenance of the Building Blocks.

Post-warranty support and maintenance shall be governed by the AMC entered into under ToR Section 14.2, including its scope, term, pricing, and SLA carry-over provisions, and shall not affect the Vendor's obligation to resolve outstanding warranty defects as specified in this Annexure. The SLAs in Section 5 carry over to the AMC unless the AMC's own SLA schedule revises them (ToR Section 14.2).

20. Exit and Transition Requirements

This Section applies on expiry of the Warranty Period where no AMC follows, on expiry or non-renewal of an AMC, and on termination of the Contract for any reason (ToR Section 7.2.4).

- **Exit Plan.** The Vendor shall submit an Exit Plan with the Source Code, Documentation, Training and Knowledge Transfer deliverable, and update it at least sixty (60) days before the end of the Warranty Period, or within ten (10) working days of a notice of termination. The Exit Plan shall list the artefacts, activities, responsibilities and dates for handover.
- **Handover of artefacts.** The Vendor shall hand over all artefacts listed in Annexure 3, Section 5, including source code, build and deployment scripts, Infrastructure as Code, documentation, SBOM and CBOM, data and configurations, and escrow details for any COTS component (ToR Section 12.7).
- **Access and credentials.** The Vendor shall transfer all administrator accounts, credentials, certificates and keys to the PA, and the PA shall revoke all Vendor access on the exit date.
- **Continuity of service.** Until the exit date, the Vendor shall continue to meet the SLAs in Section 5, and shall not reduce resources or service quality.
- **Knowledge transfer.** The Vendor shall provide reasonable knowledge-transfer and transition support to the PA or its nominated successor for up to sixty (60) days (ToR Section 7.2.4), including joint working sessions and answering technical questions.
- **Data.** The Vendor shall return all PA data, securely destroy any copies it holds, and provide a certificate of destruction (ToR Section 10.1).

- **Licences.** Any licences for COTS or third-party components remain valid for the RGoB's continued use after exit, as provided in ToR Section 12.7.
- **Exit confirmation.** Exit is complete when the PA confirms in writing that the Exit Plan has been carried out.