Portal Support Tickets SLA

1. Definitions

"Business Days" will mean Monday through Friday, other than U.S. federal holidays.

"Normal Business Hours" means Business Days, 0700 through 1900 CDT

"Technical Support Request" will mean a verbal, electronic, or written communication submitted to Support requesting assistance with respect to operating Portal. Technical Support Requests that allege a deficiency with Portal are categorized and processed as a Software Complaint.

"Software Complaint" will mean any written, electronic, or oral communication alleging deficiencies with Portal, its operation, usability, content, and/or capability.

"Available Time" will mean the number of hours in any given month less the amount of Downtime related to Force Majeure or Scheduled Downtime.

"Downtime" will mean all times in which the Portal fails to provide the usual agreed upon service within this Agreement.

"Uptime" will mean all times when the Portal is running in conformance with this Agreement and is available to be accessed by Portal end-users

Complaint Severity	**Definition**
Critical	Issue that is affecting all or most external and/or internal customers, on critical data or system access, system crash/unavailable, corruption, major functionality unavailable, or affects customer's clinical operations with no timely reasonable workaround available.
High	Issue which results in a function, feature, or subsystem of Portal to be not operating or being severely impaired that is affecting external and/or internal users but a timely reasonable workaround is available.
Medium	Issue in which external and/or internal users are interrupted but can continue with desired workflow. Full service is maintained with a workaround. Examples may include: • Non-critical service incident affecting a large group of users • Support service incident affecting small groups of users • Core business service affecting one user
Low	Issue is not affecting daily use for external and/or internal users. Workaround not required to proceed with desired workflow.

Support Services

1. Portal Support. VIDA will provide 24 hour "live" chat support (English only) between Sunday 19:00 CDT to Friday 19:00 CDT, excluding U.S. federal holidays, to assist with Technical Support Requests. Email support response will be offered during normal business hours of Monday 07:00 CDT to Friday 19:00 CDT, excluding U.S. federal holidays.

2. Software Complaint Priority and Resolution

2.1 Complaint Priority. VIDA will provide support for the Portal according to the severity of the complaint, and not necessarily in the order in which the issue was received.

2.2 Complaint Investigation and Resolution Time

Severity Level	**Investigation Time** **(Business Days)**	**Resolution Time** **(Business Days)**
Critical	Within 24 hours	Fix provided within 24 hours
High	Up to 3 days	Workaround provided within 3 days
Medium	Up to 5 days	Workaround provided within 5 days Fix may be included in upcoming Portal software release(s) as allowed
Low	Up to 20 days	Will be taken into consideration for future improvements to Portal software

3. Product Availability

3.1 All scheduled and emergency maintenance that may cause end user service interruption may occur from 0500-0900 CDT during any day of the week. VIDA reserves the right to perform maintenance outside of these times when deemed necessary.

3.2 VIDA will ensure that Uptime is ninety-nine and one half percent (99.5%) of all Available time, measured monthly, excluding schedule downtime maintenance

4. Security Maintenance and Management

VIDA shall maintain a security incident management program, which shall include monitoring its system and its procedures for suspicious (questionable) activity, security incidents and breaches and blocking unauthorized access to, and/or transfers of, Confidential Information. This includes suspicious external activity (including, without limitation, unauthorized probes, scans or break-in attempts) and suspicious internal activity (including, without limitation, unauthorized system administrator access, unauthorized changes to its system or network, system or network misuse or theft or mishandling). VIDA will take all commercially reasonable measures to regularly assess its system and remediate vulnerabilities that could

compromise data, systems or critical functioning of its systems and secure and defend its locations and equipment against “hackers” and others who may seek, without authorization, to modify or access VIDA systems or the information found therein. VIDA will (a) actively monitor industry resources for applicable security alerts and immediately notify appropriate entities and end-users upon the discovery of a critical vulnerability in its external-facing, internal, subcontractor or partner environments or in the products or services VIDA provides (each, a “Critical Vulnerability”); (b) respond in writing no later than 48 hours to an inquiry made about the impact of a known Critical Vulnerability, (c) no later than 72 hours of either (i) VIDA’s discovery of a Critical Vulnerability or (ii) receipt of an inquiry about a Critical Vulnerability, provide a written and detailed plan to appropriately and urgently remediate such Critical Vulnerability; and (d) provide a written confirmation as soon as each such Critical Vulnerability has been remediated.