

EMERGYS MANAGED INFRASTRUCTURE AND SERVICES

SUPPORT POLICY

This Support Policy is a part of an agreement for certain Emergys Managed Infrastructure and Services Agreement between Emergys and the Client. All capitalized terms not defined in this Policy shall have the same meaning as set forth in the Emergys Managed Infrastructure and Services, General Terms and Conditions.

1. SCOPE

Emergys will provide support for the following:

- 1.1 SEV 1: The Managed Infrastructure and Service is inaccessible to all or a majority of Client's users and Emergys's users through all Access Mechanisms detailed in Schedule I, for reasons other than Scheduled Maintenance.
- 1.2 SEV 2: The Managed Infrastructure and Service is inaccessible through a subset of Access Mechanisms detailed in Schedule I or is inaccessible to a significant subset of Client's users, for reasons other than Scheduled Maintenance.
- 1.3 SEV 3: Service is accessible, but Client reasonably believes that the Managed Infrastructure and Service operation is deviating from normal behavior in a repeatable and consistent way.
- 1.4 SEV 4: Client requests for service related to:
 - 1.4.1 System management
 - 1.4.2 Performance monitoring
 - 1.4.3 Remote Connectivity administration
 - 1.4.4 Changes to Infrastructure, including but not limited to adding servers, increasing storage, and adding VPN connectivity; which may incur additional Fees
 - 1.4.5 Installing, configuring and maintaining other third party software on the Infrastructure; which may incur additional Fees

2. SUPPORT REQUEST MECHANISM

Emergys shall enable the Client to request support through the following, whose details shall be provided on the Emergys's website:

- 2.1 Support Ticketing system
- 2.2 Support telephone number

3. SERVICE LEVEL AGREEMENT

The Emergys shall take reasonable and earnest measures as detailed in the Protection Mechanisms herein below to maintain security and availability of the Managed Infrastructure.

- 3.1 Emergys shall provide advance notice of Scheduled Maintenance to the Client by no less than twenty-four (24) hours. Scheduled Maintenance is the maintenance carried out by the Emergys to upgrade, replace, or maintain the Managed Infrastructure during a pre-announced window of time, which can require the Management Infrastructure to be shut down in part or in entirety. Maintenance includes server changes, new releases, application-based security patches, operating system patches (critical, hot fixes, and service packs).
- 3.2 Emergys shall take reasonable and earnest measures as detailed in the Protection Mechanisms of Schedule I to maintain 99% availability for the Managed Infrastructure and Service, measured each calendar month. The Managed Infrastructure Service is unavailable if the Managed Infrastructure and Service is inaccessible to all or a majority of Client's users and Emergys's users through all Access Mechanisms detailed in Schedule I, for reasons other than Scheduled Maintenance. Downtime shall be counted, 10 minutes after Emergys is notified by a phone call, till the time any Emergys or Client user is able to re-access the service.
- 3.3 Emergys will respond to Sev-1 notifications within 2 hour of notification of Managed Infrastructure and Service unavailability by phone, 24x7x365.
- 3.4 Emergys will respond to Sev-2 notifications within 4 hours of notification of Managed Infrastructure and Service unavailability by phone, subject to the Support Hours. For e.g., a ticket raised at 5 pm on a particular day shall not be expected to be responded by 9 pm on the same day. Therefore, a 5 pm ticket may be responded to by 12:30 pm the next day and this shall be construed as within the Support Hours.
- 3.5 Emergys will respond to Sev-3 notifications within One Business Day of notification of Managed Infrastructure and Service unavailability by phone.
- 3.6 Emergys will respond to Sev-4 notifications within Three Business Days of notification of Managed Infrastructure and Service unavailability by phone.

4. PROTECTION MECHANISMS

Emergys shall include the following Protection Mechanisms with the Infrastructure as security and availability measures:

- 4.1 Backup databases on a daily schedule.
- 4.2 Backup servers on a monthly schedule.
- 4.3 Private VLAN for all servers
- 4.4 Network firewall and policies restricting access to Infrastructure network ports and services.
- 4.5 Anti-virus protection for servers, as available for the Operating System installed on the servers.
- 4.6 Server recovery from backup
- 4.7 Replace failed Infrastructure server manually.