

IT SERVICES - SERVICE LEVEL AGREEMENT

1. Service Level Guarantees

1.1. Neterra guarantees that in the event of of a partial or critical problem with the server or its applications, Neterra will start diagnosing the problem and eliminating the problem within the time limits specified under the parameters “Response time in case of a partial problem” and “Response time in case of a critical problem”.

1.2. In the event that Neterra fails to comply with the time limits specified, Neterra shall owe penalties to the Client according to the table of penalties in item 5.

2. Trouble tickets

2.1. Upon detection of a problem, the Client is required to submit a trouble ticket or inform Neterra immediately.

2.2. In the event of activities performed under a trouble ticket, the employee on duty of Neterra shall provide the following information:

- a) time of receipt of the trouble ticket if it is submitted by phone;
- b) nature of the problem, description of the actions performed and any other information related to the request/problem;
- c) hours of work.

2.3. To be most effective in the detection and elimination of the problems, employees of Neterra may require active assistance from the technical staff of the Client, i.e. monitoring and reporting results from events, performing test configurations, etc. The Client is obliged to provide such assistance.

3. Escalation Procedure

If a problem has not been resolved in a quality manner and in due time, the Client may contact and request assistance from a senior management level within Neterra’s corporate structure, i.e.:

Level	Problem	Level of Responsibility	Contacts at the time of signing the contract
1	Critical, major, partial or warning problems, as well as all other types of requests	Engineers on duty	24-hour line: +359 (0) 700 42 300 itservices(at)neterra.net
2	Critical or major problems, that cannot be resolved by the engineer on duty	Manager ITSOC	Cell phone: +359 889 348 956 manageritsoc(at)neterra.net
3	Critical problems, that cannot be resolved by the Manager of ITSOC	Head of Technical Department	Cell phone: +359 88 2 793 986 headofoperations(at)neterra.net
4	Critical problem, that cannot be resolved by the Head of Technical Department	Managing Director	working hours: +359 2 9751616 mdirector(at)neterra.net

4. Access to information

The Client shall have the right to be informed (in a direct call or electronically) of the progress of the work on elimination of his or her problem.

5. Table of penalties

Penalties in case of a partial problem as a percentage of the monthly fee of the affected server.

Penalties in case of a partial problem as a percentage of the monthly fee of the affected server.	
Response time	Penalties
Response later than the time limit specified in the parameter "Response time in case of a partial problem"	Proportionally 5% for every two hours of delay up to a maximum of 100% of the monthly fee of the affected server.
Penalties in case of a critical problem as a percentage of the monthly fee of the affected server. In case of critical problems no penalties shall be paid for partial problems.	
Response time	Penalties
Response later than the time limit specified in the parameter "Response time in case of a partial problem"	Proportionally 5% for every two hours of delay up to a maximum of 100% of the monthly fee of the affected server.

6. Other provisions

6.1. Neterra shall not be responsible in the event of degradation in the quality of service due to problems in the networks of third party operators, including of the global Internet providers (Tier-1) or of the Client.

6.2. Neterra shall not be responsible for problems occurred as a result of actions of the Client and problems caused by the access to and/or use of the content on managed servers by the Client or third parties.

6.3. Neterra shall not be responsible in case of a remote management of servers located in other data centers and problems with them which don't allow a reaction within the committed time limits.

6.4. Neterra shall not be responsible for problems occurred as a result of computer viruses, worms, Trojans, any other form of malware, hacker attacks and other malicious acts by third parties.