THE RECOVERY PROCESS

1. Recovery of user DB with all data
2. Moving recovered user data to the new application
3. Configuration adaptation
4. Application launch

Business contingency processes, failover, and disaster recovery/business continuity processes

WorldAPP has daily, weekly, and monthly backups. This information is stored for 7 days, 4 weeks, and 12 months, respectively.

Several servers are available as failover servers in case of a complete primary server failure. Monitoring software notifies WorldAPP administrators immediately when a server stops responding for any reason.

Server downtime is usually less than 10 minutes for minor issues. Total server failure can be remedied and your site back up and running within 1/2 hour to 3 hours depending on the custom contingency plan purchased. 99% contractually guaranteed uptime.

Incident Response program in place

There are several IR procedures in place.

They vary depending on incident, but generally involve the following parts.

There is a team that deals with solving the current existing problem while another team deals with tracking down the cause.

When the cause has been identified and a solution implemented a review is performed to make sure we have procedures to cover these and similar situations in the future. Depending on the incident, IT may also initiate an outside security review of our processes.

Duration of time assumed for each type of failure scenario or outage

Our worst case scenario (server burnout) has our servers up and running within 12 hours. We are in the process of growing our platform architecture across multiple data centers in case of data center failure.

This would allow a maximum of 4 to 8 hours downtime. We actually expect 1 hour or less downtime in case of the loss of 1 datacenter.

Company's mean time to repair (MTTR)

WorldAPP's MTTR is approximately 10 minutes. We use both automated software to automatically repair servers as well as 24 hour on call system administrators to repair more serious system issues.

Network management and security monitoring tools/solutions in place

We use several tools to monitor security and network and server status.

These tools are monitored 24 hours a day, alerting admins to events that fall outside normal operating parameters.

Some of the tools we use are Rootkit hunter, JASS, Security Check, Modsecurity, Nagios, Cacti, Watchdog, et al.

Expected recovery time for critical business functions

The expected recovery time for our critical business functions is 4 to 8 hours.

Covering locations from which services are provided

All locations from which we provide our services are covered by our business continuity and IT disaster recovery plan.

Notifying the team of an incident and directing them through the recovery

Monitoring software notifies administrators immediately when a server stops responding for any reason.

Notifying customers of an outage

Clients are notified via a combination of telephone and email, depending on the severity and expected down-time of the outage. A notice can be placed on our home page as well.

Business continuity and IT disaster recovery plan testing

The plan is tested annually.

Suspicious behavior monitoring

There is a dedicated security team which is responsible for monitoring any suspicious behavior and if something is found, they have a set of protocols to deal with it.

Reviewing and responding to the IDs alerts

Security personnel track each alert to a root cause.

When a cause is identified the information is passed to an administrator who deals with the area where the cause originated.

A ticket is kept that tracks the research of this event until the cause has been identified as a nonthreat, or terminated as a threat.

Primary and alternate contact information for communication during an emergency

There is a number you can call in case of emergency:

888-708-8118 ext. 2001

You are also welcome to contact our support team,

(888) 708-8118 – 24/5 EST

(781) 560-4463 – 24/5 EST

+44(0)-8451-303345 – 4am – 12:30pm EST