



DISASTER RECOVERY

END-TO-END PROTECTION OF YOUR DIGITAL EXPERIENCES

Ensuring you have a plan for how your technology infrastructure will fare in the event of a natural or human-induced disaster is important given the vital business systems and functions tied to your websites. Different types of companies need different levels of a disaster recovery plan that ensures their digital experiences are minimally disrupted.

Crownpeak offers both **Standard Disaster Recovery**, which is included with every Digital Experience Management subscription, and a **Premium Inter-Regional Disaster Recovery** plan, which can be added to your package.

Overview

Crownpeak is proud to offer Amazon Web Services (AWS) for companies who choose to have their hosting managed and administered by Crownpeak. Through an in-depth vetting process, AWS was chosen for its exceptional track record hosting high-traffic enterprise websites, its multiple and highly secure data centers across the world, high levels of availability, scalability, and performance.

Included with every Crownpeak platform subscription is one AWS Web Hosting Pod, which includes Standard Disaster Recovery. Additional hosting pods may be purchased.

Standard Disaster Recovery for Web Hosting

All websites hosted by Crownpeak are replicated on two AWS servers located

in different geographical regions within the US, managed by a load balancer. Additionally, a second set of servers reside in a secure UK location, should both US locations become unavailable.

Inter-Regional Disaster Recovery for Web Hosting

Crownpeak offers Inter-Regional Disaster Recovery as an additional service. In this configuration, redundant web hosting infrastructure is maintained in two *separate* AWS Regions, with content replicated between the sites in real-time. In the event of a customer-declared disaster, traffic can be redirected to the secondary AWS Region by Crownpeak IT Operations Staff.

How It Works

Regardless of which option you choose, the process is the same. When you declare a disaster via our 24-hour reporting channel, we initiate the disaster recovery process. Almost immediately, your website traffic will be routed to one of the back-up sites on another set of servers, outside the disaster area. Once Crownpeak has determined there is no longer a threat and verified that the compromised server is safely back up and running, traffic is rerouted back based on the original configuration.

