



Security Overview

The security of your data is a primary concern at CrystalTech and we've invested millions in our infrastructure over the years to make sure your critical information is safe. This document provides a very brief and general overview of some of the security features, policies, and procedures we've implemented to address the everyday security concerns of customers, from the physical security of our datacenter, to our internal controls, and even our hiring practices. Please understand that we've purposely excluded sensitive information from this document (e.g., firewall makes and models) as this information could be used in malicious ways against our network or to our customers.

Network Availability

Network availability and uptime is a key attribute for any quality web hosting provider, and we've made it one of our top priorities. It is our policy to have at least two full tier 1 connectivity providers, utilized at levels far below their peak thresholds, to feed into our fully redundant network infrastructure. This multi-level approach to redundancy allows for a complete and immediate switchover if one of the providers becomes unavailable for any reason.

We also employ redundant power supplies to our network and datacenter operations to ensure your website and related services are available, even during a power outage. We use top-of-the-line uninterruptible power supply systems for protection against power spikes and outages, and our multiple 2 Mw Caterpillar diesel generators allow us to function at full capacity for an indefinite period of time.

Server Monitoring

We use a blend of third party products, in-house developed solutions, and 24/7/365 staff to monitor a multitude of performance related services, including CPU and memory usage, and other items within our shared hosting segment to ensure the stability and reliability of our network and to customer websites. These monitors run year round and are set to 5 second intervals to ensure any issues are detected immediately. We also offer similar monitoring services for dedicated customers. For more information about these options, please contact our Sales department.

In addition to monitoring, CrystalTech has implemented a detailed escalation policy for issues that go beyond that of general server or network issues. What this means is that we employ secondary and tertiary levels of escalation on all issues, regardless of scope. Support representatives, server operations, and network operations staff, as well as all levels of executive management, are available 24/7/365 to ensure that all issues are dealt with and resolved as quickly as possible.

Data Protection & Security

One of the best methods to protect your critical data is to be sure you always have reliable backups. All services on our shared hosting segment receive daily backups, including website, database, and email

data. Dedicated and VPS customers have the option to add a daily backups option as well – for VPS customers, this means full backups of the entire virtual environment, not simple “snapshots” as provided by other companies. We retain all backups for a two week period which consists of two full weekly backups and daily incremental backups of all new data added in between.

Virus protection for a network infrastructure is also essential. Therefore, CrystalTech runs real time scans for viruses on all files coming into the shared hosting segment, and runs continuous scans of all servers, regardless of server function. This level of virus scanning includes the scanning, quarantining, fixing and/or deleting emails that come into our network. In cases where emails are deleted or quarantined due to infection by a virus, an email is returned to the sender informing them of the infection.

While securing servers is one step to protecting the integrity of our network, stopping "bad" traffic from reaching the servers in the first place is even more important. CrystalTech utilizes firewalls and other security features throughout its network. We restrict common ports of attack at our firewall, and these are manual/static changes. Once traffic does get into the network, we implement a number of systems that watch for malicious activity without possibly delaying “good” traffic and thereby negatively impacting legitimate customer traffic. These systems include many custom-built applications and monitors that were developed in-house by our network and server operations teams. We know our network, our infrastructure, and our systems better than any third-party vendor, so we rely on that knowledge and experience when we select the systems that protect our customers.

CrystalTech also utilizes a third party to run security and vulnerability audits. These audits include, but are not limited to, port scans, server configuration audits, and other security and vulnerability checks that help ensure that the network and servers we manage are as secure as possible. These audits keep CrystalTech safe, secure, and PCI compliant. CrystalTech is also registered as a Safe Harbor with the U.S. Department of Commerce. What this means is that CrystalTech has met or exceeded certain guidelines for the adequate protection of private and confidential information as defined by the European Union’s Directive on Data Protection. More information on Safe Harbor can be found at www.export.gov/safeharbor.

Internal procedures and controls

CrystalTech takes great care to secure customer data, and that includes internally. CrystalTech employees only have access to the customer information that enables them to perform his or her job duties to their fullest extent. Using our custom WebControlCenter, we are able to limit access to customer data for all employees. For example, our Customer Service Department has access to billing information pertaining to clients, but they do not have access to the functionality that allows them to change customer site settings, or terminal into customer servers. Our Technical Support staff, on the other hand, has the ability to terminal into servers, but may not necessarily have access to customer billing information. Access to customer data is strictly determined by job role and position within the CrystalTech employee structure.

We’ve also implemented a change management policy and procedure to effectively manage and control all internal changes that may affect customers. This includes, for example, any internal request for access to our core systems and any changes to our website or WebControlCenter. The change management process is also employed by both our Server Operations and Network Operations Teams so that any modifications made to server settings, hardware changes, or even setting changes made at an application level, are properly tested and approved by a CrystalTech executive before they are deployed.

In terms of hiring practices, CrystalTech follows strict guidelines when it comes to hiring. These guidelines are addressed in the Employee Handbook and Non Disclosure Agreement that each employee receives, reads, and is required to sign off on as proof of reading and understanding all of CrystalTech's policies and procedures. Each prospective CrystalTech employee is phone screened by the Human Resources staff and then scheduled for in-person or phone interviews with the appropriate hiring manager. Hiring managers may elect to extend the hiring process based on the candidate pool and needs of the company and department. Any candidate who makes it through the interview process receives an extensive background check prior to any offer of employment. The President and Senior Vice President of Human Resources or CEO of the company must approve any request for new hires prior to an offer of employment.

Finally, CrystalTech has a strict policy for the release and dissemination of customer data that is addressed in both our Terms of Service Agreement and our Corporate Privacy Policy. CrystalTech does not release, for any reason, any information relating to customers without prior written permission from the customer or without proper authentication and verification of ownership of that data. This policy covers everything from billing and support issues as well as questions from prospective CrystalTech customers looking for information or references about existing customers (for example, if a prospective customer asks a member of our Sales or Technical Support staff to provide the name of an existing client as a point of reference, we would not provide that information; instead we would refer the inquiry to our public forum where existing customers may willingly provide their own information.)

Physical Security

Our investment in enterprise-level hardware, data security measures, and network redundancy would be meaningless if we did not have the proper physical security measures in place to protect our assets. Therefore, we have implemented several security measures to ensure the physical security of our infrastructure and customer data. At our corporate office, we employ keycard access to enter the building and to key areas within the building. This ensures that only CrystalTech employees, or those persons with proper authorization, are able to enter our corporate office. We also have 24/7/365 video surveillance systems in place, both internal pointing at key areas of the office as well as external that points at all exterior locations, so that the premises is monitored and recorded at all times.

The CrystalTech datacenter can only be accessed by authorized CrystalTech staff with proper keycard, touch pad, and retinal scanning clearance, and well as passage through a bullet-proof, weight sensitive man-trap booth, so that only those employees requiring access to our servers are granted access. We also utilize manned, third-party security staff at all times, 24/7/365, and a state-of-the-art video surveillance system.

Our datacenter is located in Scottsdale, Arizona, a geographical area that features a highly stable climate and is nearly free from all natural disaster threats, such as earthquakes, tornados, hurricanes, and landslides. Scottsdale also ranks low among large cities as a target of terrorist or malicious activity.

Conclusion

As we have illustrated, CrystalTech has implemented many ways to protect customer data, not only at the server level, but at the highest points of our network. All of our precautions, of course, do not ensure 100% protection, and our procedures are ever evolving. It is our goal to continually update our security procedures so that we can provide the most secure web hosting environment possible to our customers.