IT and Network Security Policy

Security is taken seriously here at Verztec, and we have developed a system of processes, technologies, and policies to help ensure that your account, and all the data within it, is secure.

Our security practices cover 5 different areas: Physical Security; Network Security; Server Security; People Security; and Redundancy and Business Continuity.

Physical Security

Our data centers are in secure facilities that are located in areas with no history of natural disasters such as earthquakes, fires, floods, etc.

- 7x24x365 Security. Our data centers (and your data) are guarded around-the-clock by private security guards.
- Video Monitoring. Each data center is monitored around-the-clock with security cameras.
- Controlled Entrance. Access to our data centers is restricted, and only pre-authorized personnel can enter.

Network Security

We protect your websites and data against sophisticated electronic attacks. The following is just an intentional partial, generic description of our full network security practices. If you require further details on our network security, please get in touch with us.

- Control and Audit: All processes are controlled and audited for compliance and quality.
- 128/256-bit SSL. Our products, where possible, support SSL to ensure that data communications are secured.
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS): High-performance and certified IDS/IPS protect our network and your data.

Server Security

As with our network security processes, our server security is tightly regulated. The following is not an exhaustive list of processes that we follow to ensure security on our servers.

- Virus Scanning. Viruses are scanned for and detected using daily updated virus-scanning protocols.
- Hardened OS: Operating systems are hardened for security as vulnerabilities are minimized.

People Security

We focus not just on the technology but on people as well. Policies about escalation, management, and daily operations are well-defined to manage security risks.

- Authorisation: Only employees with the required clearance have access to specific servers and racks in our datacenter
- Restriction: Only employees who need access to customers' data (such as for troubleshooting) are given passwords and keys. Any access is logged and passwords are strictly controlled.
- Auditing: Regular audits are conducted on our processes and reviewed by management.

Redundancy and Business Continuity

One of the core principles of our network and infrastructure design is redundancy, because we know that it is not a matter of if, but a matter of when, that hardware fail. As such, we have designed our network and servers with the following in mind:

- Virtualised Architecture: Verztec servers run on a virtualised architecture, meaning that any hardware that do fail, can and will be migrated instantaneously.
- Data Back-ups. Data is backed-up regularly across multiple servers, ensuring an up-to-date copy of data even with hardware failures or disasters.
- Internet Redundancy: Verztec's network is connected to the world through multiple Tier-1 ISPs, ensuring that we don't depend on any single one bandwidth provider.
- Power Redundancy: All of our servers come with power redundancy.
- Redundant Network Devices: Our network makes use of redundant network devices, i.e.switches, routers, gateways, to avoid any single point of failure on our network.
- Geographical Separation: Separate geographic locations for customers who require Disaster Recovery and Business Continuity is available on selected products.
- Fire Prevention: Verztec's datacenters are protected by industry-grade fire prevention and fire control systems.