



## Barrington Corporation Internal Data Security

All critical systems at Barrington/Intercept are redundant, resulting in minimal downtime. The following outlines our redundancy in critical systems.

1. Dual internet service providers. We have one path coming in on a T1 and another on a high speed wireless connection. These are connected to our routers and balanced using the BGP protocol.
2. We have a failover router scenario so that in the case that a router would failover all traffic would be routed through the other.
3. We have a failover firewall, so that in the case that our primary firewall fails, the failover would take over.
4. We have multiple switches, all on a redundant power supply, so that in the event of failure, we can move traffic from one switch to another until the failed switch is replaced.
5. All web servers and intermediary servers, accessing data, are redundant on load balancing. In the event one server would go down, the others would take over for the failed server until the server could be put back online.
6. All servers consist of dual hard drives in a RAID-1 disk array.
7. We take nightly backups of all of our data and file servers that are stored offsite.
8. All servers and PC's in our organization are protected by surge protectors and UPS. We also have a generator that will start in the event of power failure.