Cyber Tree Systems

A Business IT Solution Company

POLICY NAME	**Future Network Design**		
DATE OF LAST REVISION:	9/4/2003	**VERSION NO.**	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

CTS Network Design – Future

The CIO understands the security implications of the current network setup and has allocated funds to upgrade and compartmentalize the network, so it performs better and more securely.

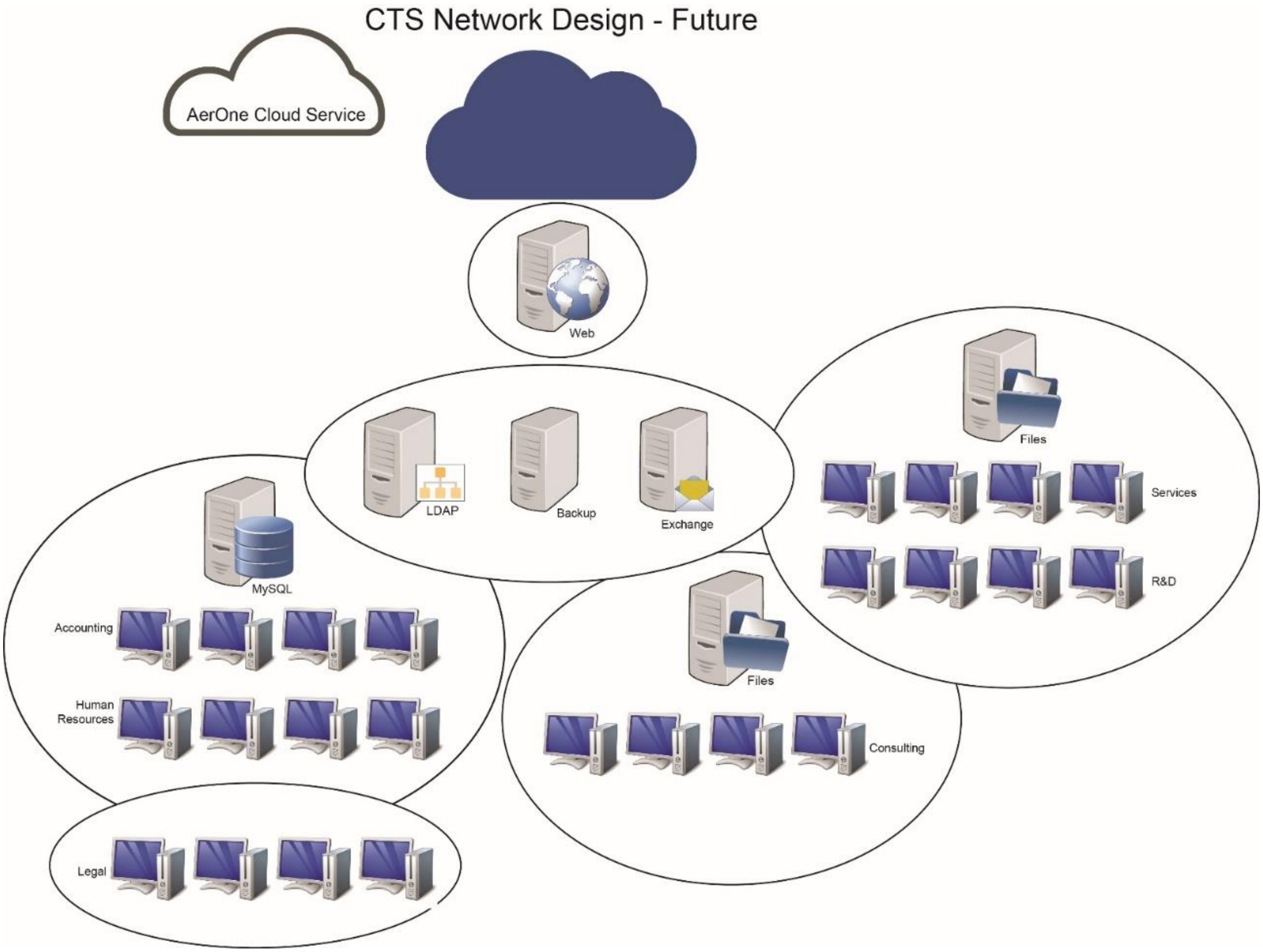
He has provided a logical diagram of how the assets should be divided up and secured.

1. All departments need access to the LDAP, Exchange, and Backup Cloud Service servers.
2. No departments need access to the Web servers. The Web servers should not be able to access anything other than the cloud. The Web server should be completely isolated from the internal network.
3. Accounting and HR both need access to the MySQL servers, AerOne Cloud, and the cloud.
4. Legal only needs access to the AerOne Cloud, and the cloud.
5. Services and R&D needs access to the File server, AerOne Cloud, and the cloud.
6. Consulting needs access to its File server, AerOne Cloud, and the cloud.
7. Each department should be independent and not able to access another department.

You have been given enough funds to purchase any combination of the following hardware:

- 2 firewalls
- 3 routers
- 6 switches

Configure the new network and explain what technical policies would be put in place to achieve the CIO’s vision. CTS uses a Cloud Service for customers and for CTS internal use and backups. Planned State assumes each server icon accounts for 2 servers and each workstation icon counts for 5 clients. CTS uses a Cloud Service for customers and forCTS internal use and backups.



Revision History

Revisions made 9/4/2023