    e. Automated processes that support critical services or operations
    f. Network services (i.e. firewalls, switches, T1 lines, wireless)
2. Security and Privacy officers, as well as the DRC (Criticality Team) will meet with key department representatives and ask them about the applications and data they use. Also, meet with members of IT staff to find out what computer systems support those applications and data—those are the systems you must bring up first if a disaster or emergency occurs.
3. The criterion for identifying critical components is whether rendering a component unusable or unavailable would significantly disrupt [Insert company name] ongoing operation.
    a. To determine criticality, the Criticality Team will assess the options for replacing the affected components. The analysis must identify components that must be quickly replaced or restored to operating condition during an emergency. It must also identify the longest potential time period that those critical components can be unavailable and the most cost-effective method for restoring function within the critical time period.
4. Power outages disrupting network services, servers, and other applications can only be tolerated for 24 hours.
5. If servers are destroyed, a new server would be purchased and put in the most secure and reliable location. Data would be restored as described in the Data Backup Plan and Contingency Plan policies.
6. Document the organization's criticality ratings for systems and data, as well as recovery processes by criticality rating.
7. Re-visit these ratings regularly (yearly) or as changes in the information security environment change significantly.

Attachments: None

Related Policies:

- Data Backup Plan
- Disaster Recovery Plan
- Contingency Plan/Business Continuity Plan
- Cyber Incident Response Plan