[INSERT COMPANY NAME AND LOGO]	
Title: Applications and Data Criticality Analysis	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: To support the continuation of critical business processes, and to protect and secure sensitive and regulated data during emergency mode operations.

Scope: This policy is applicable to all Information Technology (IT) resources owned or operated by [Insert Company Name.] All users are responsible for adhering to this policy.

Policy: Assess the relative criticality of specific applications and data in support of other contingency plan components. The criticality analysis will serve as the basis for the recovery prioritization of sensitive and regulated data and systems during the disaster recovery plan.

Definitions:

1. Disaster (Information System): An event that makes the continuation of normal information system functions impossible; an event which would render the information system unusable or inaccessible for a prolonged time period (may be departmental or organization-wide).
2. Disaster Recovery Coordinator (DRC): Individual assigned the authority and responsibility for the implementation and coordination of IS disaster recovery operations.
3. Disaster Recovery Plan: The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
4. Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices; an adverse event whereby some aspect of computer security could be threatened. An IS Disaster would be considered a security incident.

Procedure:

1. Activities and Materials that are critical to daily business operations include:
    a. Network services (i.e. firewalls, switches, fiber optic lines, wireless)
    b. Servers (i.e. authentication server)
    c. Software
    d. Equipment (computers, printers)

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

    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

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.