Damar Services Technology Policy

Policy Statement

This policy defines acceptable methods for planning, preparedness, management and mitigation of IT systems and services at Damar Services, Inc.

Entities Affected By This Policy

Damar Services, Damar Charter Academy, and Damar Specialized Services

- Responsible Executives: Chief Operations Officer Jennifer Maggard
- Responsible Department: Information Technology Committee
- Contact: Information Technology Committee

Reason for Policy

The standards in this policy provide a systematic approach for safeguarding the vital technology and data managed by the Information Technology Committee. This policy provides a framework for the management, development, and implementation and maintenance of a disaster recovery program for the systems and services managed by Damar Services.

Document Conventions

To assist in the usage of this policy document, the Appendix Section below contains a summary of all the DR Timeline deliverables plus a DR glossary. Please check the DR glossary in the Official Policy for the definition of DR terms.

Principles

Planning is a program that has a continuous lifecycle. Detailed requirements for each of these steps are below. The high-level process for DR Lifecycle is as follows:

- **Governance**

    1. All managed systems must comply with Damar's disaster recovery policies and requirements.
    2. Resultant is responsible for IT DR program coordination and project management: including reporting status of IT DR planning, testing, and auditing activity to Information Technology Committee on a regular basis; at least twice per year.

3. Information Technology Committee is responsible for ensuring sufficient financial, personnel and other resources are available as needed.
4. Information Technology Committee will review and update the DR Policy as necessary at least every other year.

- **Program Development**

1. The Damar Disaster Recovery Program (DDRP) addresses the protection and recovery of IT services so that critical operations and services are recovered in a timeframe that ensures the survivability of Damar and is commensurate with customer obligations, business necessities, industry practices, and regulatory requirements.
2. Plans must be developed, tested, and maintained to support the objectives of the Program, and those plans should include relevant IT infrastructure, computer systems, network elements, and applications. At minimum, annual updating is required.
3. Information Technology Committee is responsible for conducting Business Impact Analyses (BIA) to identify the critical business processes, determine standard recovery timeframes, and establish the criticality ratings for each; at least every other year.
4. Information Technology Committee is responsible for conducting Capability Analyses (CA) to determine Damar's capacity to recover critical IT services that support defined critical business processes and recovery objectives; at least every other years.
5. Information Technology Committee is responsible for maintaining the Recovery Tier Chart , which defines the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of all managed systems. The Service managers are required to prioritize their IT processes and associated assets based upon the potential detrimental impacts to the defined critical business processes.
6. Resultant is required to create disaster recovery plans for the IT portion - including services, systems, and assets - of critical business processes. These IT services, systems, and assets must be inventoried and correlated according to the technical service catalog , prioritized based upon results of the Business Impact Analysis, and ranked according to their Recovery Time Objectives and Recovery Point Objectives.
7. A Risk Assessment must be conducted at least every other year to determine threats to disaster recovery and their likelihood of impacting the IT infrastructure.
8. For each risk or vulnerability identified in the Capability Review and Risk Assessment, a mitigation or preventive solution must be identified.
9. The IT DR program must include a change management and quality assurance process.

10. Above Program Development statements will be progressively fulfilled via Disaster Recovery Manager, Departmental and/or other resources.

- **Emergency Management**

    1. The Information Technology Committee is responsible for overseeing IT DR activities in the event of an emergency -i.e., an unplanned outage where RTO is in jeopardy.
    2. Information Technology Committee should be part of the representation within the institution's Emergency Management Team .
    3. Each department must develop and maintain a documented emergency plan including notification procedures.
    4. Each department shall account for its associates when a building evacuation is ordered. Supervisory personnel are responsible to account for the associates they supervise.
    5. The Information Technology Committee is required to complete a post-mortem report documenting outages and recovery responses within 45 days after the occurrence of a disaster recovery event.

- **Budgeting**

    1. IT DR budgeting must be informed annually by requirements gathered in the BIA and CA as well as the budgeting process.
    2. Information Technology Committee is responsible for tracking and reporting on planned and unplanned outage spending related to the recovery and restoration effort. During an outage, vendors may incur special recovery and restoration costs that are unbudgeted. For a small outage, these costs would be immaterial; but for a longer outage, these costs could be significant.

- **Plan Objective**

    1. IT DR plans must provide information on Business Impact Analysis, Data Backup, Recovery, Business Resumption, Administration, Organization Responsibilities, Emergency Response & Operations, Training and Awareness and Testing.
    2. Plans must contain Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
    3. Technological solutions for data availability, data protection, and application recovery must be considered by data gathered by the BIA and CA.

- **Vital Records**

    1. Damar must maintain a single, comprehensive electronic inventory of all servers, network equipment, relevant configuration, and model information, and the applications they support. This inventory should be aligned with the service catalog and the technical service catalog.
    2. All backup data must be labeled and logged, and are available for use during an emergency within stated recovery time objectives. A documented decision making process will be used to determine what subset of backup data will be additionally encrypted, and stored off-site in a secured location outside of the geographical area of the system they are backups of.
    3. DR plans must be stored in a single, comprehensive database.
    4. DR plans owners need to be able to access a copy of emergency and recovery plan(s) independent of ITS services and/or network.
    5. Upon completion or update, DR plans must be sent to the Disaster Recovery Manager and ITS Change Manager for review.
    6. Plan information must be reviewed and updated as warranted by business and/or information systems environment changes, at least annually.

- **Plan Attributes**

    1. Plans must address an outage that could potentially last for a period of up to six weeks.
    2. Plans must identify risk exposure and either accept the risk or propose mitigation solution(s).
    3. Backup strategies must comply with predefined businesses continuity requirements, including defined recovery time and point objectives. Backup strategies must be reviewed at least every other year.
    4. Recovery strategies must meet recovery objectives defined in the DR tier chart.
    5. Approved recovery strategies must be tested to ensure they meet required recovery time and recovery point objectives.
    6. Recovery strategies must be implemented within a previously agreed upon period of time, generally not more than 180 days after management approval.
    7. The Information Technology Committee is required to provide DR training and awareness activities at least twice per year.

- **Maintenance**

    1. Plans must contain current and accurate information.
    2. Planning must be integrated into all phases of the IT system life cycle.

3. IT DR tests that demonstrate recoverability commensurate with documented IT DR plans must be conducted regularly; as well as when warranted by changes in the business and/or information systems environment.
4. Backup media supporting critical business processes must be tested semi-annually. Reviews are required within 60 days after a test to correct exposed deficiencies.
5. Plan revisions must be completed within 60 days after a DR test is completed.
6. The following maintenance activities must be conducted annually:
    1. Updating the documented DR plan
    2. Reviewing the DR objectives and strategy
    3. Updating the internal and external contacts lists
    4. Conducting a simulation/desktop exercise
    5. Conducting a telecommunication exercise
    6. Conducting an application recovery test
    7. Verifying the alternate site technology
    8. Verifying the hardware platform requirements
    9. Submitting the DR Status and Recoverability Report
    10. Information Technology Committee is responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.