The AET

Business Continuity and Disaster Recovery Plan

Purpose and Scope

This Business Continuity and Disaster Recovery Plan guides The AET in the event of a significant business disaster or other disruption to normal service. The AET must respond to business disasters and disruption by safeguarding employees' lives and company assets, making a financial and operational assessment, securing data, and quickly recovering operations.

This plan applies to all The AET assets utilized by employees and contractors acting on behalf of The AET or accessing its applications, infrastructure, systems, or data. All employees and contractors are required to read, accept, and follow all The AET policies and plans.

Scope for Mission Critical Services

Mission critical services and systems are those required for the functioning of the The AET product(s). Mission Critical services and systems include critical production systems required for immediate recovery, services affecting the engineering team's ability to support production operations and product development, and the ability to support The AET customers.

All essential data is typically stored remotely using commercial cloud providers with proper backup and redundancy processes in place. This approach is subject to change and designed to minimize any disruption from physical incidents or disasters.

System Outages

Planned Outage

From time to time, The AET may distribute a service update to all affected users prior to planned downtime.

Unplanned Outage

All unplanned outages should be treated as an incident; and the executive team should be immediately emailed and notified of any unplanned outage.

Expectations

Alternate Physical Location(s) of Employees

In the event of an internal disaster that affects a The AET office location, all team members will be moved from such affected offices to each member's respective home or an alternate location to work remotely.

Reliance on Third-Party Services

The AET utilizes and relies on mission critical third-party cloud services. In the event of a significant business disaster, The AET will quickly work to establish alternative arrangements if a mission critical vendor can no longer provide the needed services or goods.

Mission critical third-party vendors include:

This plan depends on the likelihood that:

1. Remote work can continue to take place in the event of a disaster; and
2. Mission critical vendor services, and essential The AET services, systems, and data can still be made available or alternative solutions can be implemented (including backups and services provided by such third-party vendors)

Priorities

In the event of a disaster affecting The AET essential systems or its team members, Roger Hanagriff will oversee and respond in accordance with this Plan and will initiate specific actions for recovery.

The priorities during a business disaster are to:

1. Secure the safety of team members and visitors;
2. Mitigate threats or limit the damage that threats can cause to The AET, its team, and its customers; and
3. Ensure that essential business functions can continue or determine what is required to restart essential business functions

Backup and Retention

All vital data that would be affected by disruption are maintained and controlled by the data's applicable teams.

In the event of a facility disruption, critical records located in such a facility may be destroyed or inaccessible. The number of critical records, which would have to be reconstructed, will depend on when the last transfer of critical records to the cloud storage location occurred.

Backup Requirements

1. Database backups must be performed
2. Backups must be retained for at least 30 days
3. The maximum allowable retention period for a database backup should be determined base on regulatory and contractual requirements
4. Backups are periodically tested to ensure that backups are sufficient and reliable in accordance with this plan
5. Backup systems and media protect the availability of stored data

Alternate Communication

The organization may communicate using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.

In the event of a significant business disaster, an assessment will be conducted to determine which means of communication are still available. These means of communication will then be utilized to communicate with personnel, customers, partners and other third-parties.

Testing

Testing the plan is critical to ensuring the plan is effective and practical. Any gaps in the plan that are discovered during the testing phase will be addressed by Roger Hanagriff and any designee. All tests must be thoroughly documented.

Testing of this plan may be performed using the following methods noted in the subsections below.

Walkthroughs

Team members must walk through the steps documented in this plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This walkthrough provides the opportunity to review the plan with all relevant stakeholders and familiarize them with procedures, equipment, offsite facilities, and recovery efforts in preparation of a business disaster or disruption.

Table Top Exercises

Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test.

Personnel involved with business continuity must utilize validated checklists to provide a reasonable level of assurance for many disaster scenarios. These personnel must analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Business Continuity and Disaster Recovery Stages

This Plan divides recovery into three stages: Disaster, Response, and Recovery.

Declaring a disaster is the responsibility of senior management. Since it is almost impossible to predict when and how a disaster might occur, The AET and its team members must be prepared to monitor and signal a disaster to management from:

- First hand observation
- Security applications
- Network monitoring and logging tools
- Environmental and security alarms
- Team members
- Customers
- Partners
- Vendors
- Media

Disaster Stage

If a disaster has been declared, this Plan and any related responses would go into effect.

The disaster stage may include the following processes:

1. Senior management declares the disaster, and

2. Notifies management and appropriate team members to create the appropriate Disaster Recovery Team (DRT),
3. DRT initiates internal and external communication lines, and communicate to the following parties as appropriate:
4. General Counsel
5. Authorities
6. Personnel
7. Customers
8. Vendors, third-parties, and other applicable stakeholders
9. DRT determines appropriate emergency response measures

Response Stage

In this phase, the team determines what team members, facilities and customer deployments are affected by the disaster scenario and in what way they are affected by performing an impact assessment.

This stage continues until an alternate facility location and/or essential business and production functions are established and services restored. If non-essential functions are affected, essential functions may be prioritized during a disaster event.

The response stage may include the following processes:

1. Execution of a business impact assessment,
2. Relocation to an alternative facility or establish work from home requirements,
3. Verification and/or backing up of affected data and systems, and
4. Restoration of essential The AET services

Recovery Stage

Recovery begins with the activities necessary to return to business as usual including re-establishing the primary facility. For engineering, this stage begins with the restoration of The AET services in an available commercial cloud provider’s region. Recovery time objectives (RTOs) and recovery point objectives (RPOs) are to be defined when relevant for applicable systems.

Recovery time objective(s) (RTO): [RTO]

Recovery point objective(s) (RPO): [RPO]

Key Learning Stage

As soon as possible, The AET senior management must meet with the DRT and other stakeholders for a post-mortem review to better understand the disaster event that took place and how it and others may be prevented in the future.

The retrospective must be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

Lessons learned during the disaster must be captured within the post-mortem review and incorporated as updates into existing documentation.

Exceptions

The AET business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other The AET policy. If an exception is needed, The AET management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other The AET policy or procedure may result in disciplinary action, up to and including termination of employment. The AET reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. The AET does not consider conduct in violation of this policy to be within an employee’s or contractor’s course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of The AET as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

This Business Continuity and Disaster Recovery Plan is reviewed and tested at least annually. Ensuring that the plan reflects ongoing changes to resources is crucial. This task includes updating the plan, testing the updates with walkthroughs, tabletop exercises, and training necessary personnel. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

The AET reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually.

This development, maintenance, and testing of this plan are managed by Roger Hanagriff.

This plan was last updated on 01/29/2024.