Texas A&M University
Enterprise Operations
Unified Window Device Management

Disaster Recovery Plan for Admin By Request

TEXAS A&M UNIVERSITY

Table of Contents

Introduction

- **Purpose**: The DRP is created to ensure the rapid recovery of ABR services in case of a disaster. It aims to minimize downtime and maintain communication with stakeholders
- **Scope**: This DRP covers the cloud hosted instance of ABR

Objectives

- **Description**: The primary goals of the DRP are to ensure rapid recovery, minimize downtime, and maintain communication.

Disaster Recovery Team

Name	Position	Contact Information	Department
Garrett Yamada	Associate Director	garrettyamada@tamu.edu +1 (619) 770-8134	Security
Jon Griffey	IT Director for Enpoint Management	Griffy@tamu.edu +1 (979) 862-9200	Unified Endpoint Management
Andrew Nelson	System Administrator II	Ajn@tamu.edu +1 (979) 845-8300	Unified Endpoint Management
Austin Akers	Account Executive	AustinA@fasttracksoftwareus.com +1 (262) 299-4600 ext. 1002	Admin By Request
Ryan Akers	Territory Director Americas & Australia	rak@fasttracksoftware.com +1 (262) 299-4600	Admin By Request
Lars Sneftrup	CEO	lsp@fasttracksoftware.com	Admin By Request

Disaster Recovery Team Roles and Responsibilities

Security

1. **Shem Miller, Identity Security Engineer**
    a. **Role**: Lead the security team and act as the product owner for Admin By Request during disaster recovery efforts.
    b. **Responsibilities**:
        i. Ensure the integrity and security of Admin By Request systems during recovery.
        ii. Coordinate with other teams to address security vulnerabilities and threats.
        iii. Monitor security systems and respond to incidents during recovery.
        iv. Communicate security status and updates to stakeholders.
        v. Oversee the overall recovery efforts for Admin By Request.
        vi. Contact: shem@tamu.edu
2. **Garrett Yamada, Associate Director, Identity Security**
    a. **Role**: Assist the Identity Security Engineer in security recovery efforts.
    b. **Responsibilities**:

i. Verify the integrity of identity systems and restore data as needed.
ii. Troubleshoot and resolve security-related issues during recovery.
iii. Document security recovery steps and outcomes for future reference.
iv. Contact: garrettyamada@tamu.edu, +1 619-770-8134

Unified Endpoint Management

1. **Jon Griffey, IT Director for Endpoint Management**
    a. **Role**: Lead the unified endpoint management team in supporting the recovery efforts of Admin By Request.
    b. **Responsibilities**:
        i. Coordinate with the Security team to ensure endpoint devices and management systems are restored efficiently.
        ii. Provide necessary resources and support to facilitate the recovery of Admin By Request.
        iii. Monitor endpoint performance and address any issues that may impact the recovery process.
        iv. Communicate recovery progress to stakeholders and ensure alignment with overall DRP objectives.
        v. Contact: griffey@tamu.edu, +1 979 862 9200
2. **Eli Billette, IT Manager II**
    a. **Role**: Assist the IT Director in supporting the recovery efforts of Admin By Request.
    b. **Responsibilities**:
        i. Implement recovery procedures for endpoint devices and management systems in coordination with the Security team.
        ii. Troubleshoot and resolve endpoint-related issues that may impact the recovery of Admin By Request.
        iii. Document recovery steps and outcomes for future reference and continuous improvement.
        iv. Contact: eli173@tamu.edu, +1 979-458-5427
3. **Andrew Nelson, Systems Administrator II**
    a. **Role**: Support the IT Manager in assisting the recovery efforts of Admin By Request.
    b. **Responsibilities**:
        i. Execute recovery procedures for endpoint devices and management systems in coordination with the Security team.
        ii. Monitor device performance and address any issues that may impact the recovery process.
        iii. Document recovery steps and outcomes for future reference and continuous improvement.
        iv. Contact: ajn@tamu.edu, +1 979 845 8300

Admin By Request

1. **Support Request**
    a. **Role**: Provide support for Admin By Request during disaster recovery.
    b. **Responsibilities**:
        i. Address any issues related to Admin By Request during recovery.
        ii. Provide guidance and assistance to ensure the service is restored efficiently.
        iii. Communicate with stakeholders to provide updates on recovery progress.
2. **Austin Akers, Account Executive**
    a. **Role**: Assist in coordinating recovery efforts for Admin By Request.
    b. **Responsibilities**:

i. Provide necessary resources and support for Admin By Request recovery.
ii. Communicate with stakeholders to provide updates on recovery progress.
iii. Address any issues related to Admin By Request during recovery.
iv. Contact: AustinA@fasttracksoftwareus.com, +1 262.299.4600 x 1002

3. **Ryan Akers, Territory Director Americas & Australia**
    a. **Role**: Lead the recovery efforts for Admin By Request in the Americas and Australia.
    b. **Responsibilities**:
        i. Coordinate recovery efforts for Admin By Request in the designated regions.
        ii. Provide necessary resources and support for Admin By Request recovery.
        iii. Communicate with stakeholders to provide updates on recovery progress.
        iv. Address any issues related to Admin By Request during recovery.
        v. Contact: rak@fasttracksoftware.com, +1 262-299-4600
4. **Lars Sneftrup Pedersen, CEO**
    a. **Role**: Oversee the overall recovery efforts for Admin By Request.
    b. **Responsibilities**:
        i. Ensure the recovery efforts for Admin By Request are aligned with company objectives.
        ii. Provide necessary resources and support for Admin By Request recovery.
        iii. Communicate with stakeholders to provide updates on recovery progress.
        iv. Address any issues related to Admin By Request during recovery.
        v. Contact: lsp@fasttracksoftware.com

Risk Assessment and Impact Analysis

Risk Assessment

1. Service Outage

a. Scenario 1: Worst-case All Systems Non-Functional – Short or Extended Period of Time
    i. Description: The entire Admin By Request service is non-functional for what is considered an acceptable or unacceptable period of time including website, APIs and mobile app.
    ii. Result: Users function normally from their end as their requests do not need to wait for approval. The current settings at the time of the service outage are maintained throughout, however editing of settings is unavailable. Any uploads are queued on the endpoint and will upload when the service is functioning again. Once all endpoints have offloaded their upload queue, the Auditlog will appear as if the service was never down.
    iii. Business Impact Rating: LOW
b. Scenario 2: Worst-Case All Systems Non-Functional – Short / Acceptable Period
    i. Description: The entire Admin By Request service is non-functional for an acceptable period of time, including website, APIs and mobile app.

   ii. Result: Users cannot get approval of requests, which sit on endpoints until the service is up again. When this happens, requests are updated from the endpoint to the API. User experience is that response time is longer than usual. Administrators cannot access Auditlog or other pages during the incident.
   iii. Business Impact Rating: MEDIUM
   iv. Remedial Actions: None
c. Scenario 3: Worst-Case All Systems Non-Functional – Extended / Unacceptable Period
   i. Description: The entire Admin By Request service is non-functional for an unacceptable period of time, including website, APIs and mobile app.
   ii. Result: Users cannot get approval of requests, which sit on endpoints until the service is up again. When this happens, requests are updated from the endpoint to the API. User experience is that response time is considerably longer than usual. Administrators cannot access Auditlog or other pages during the incident.
   iii. Business Impact Rating: HIGH
   iv. Remedial Actions: For Windows, set the AutoApprove registry key to temporarily allow elevations without approval:
      1. Open the Group Policy Management Editor from the Windows search bar (Edit group policy in menu) 2. Go to Computer Configuration > Preferences > Windows Settings > Registry 3. Policies are set under the registry key HKEY_LOCAL_MACHINE\Software\FastTrack Software\Admin By Request\Policies. KeyPath must be "Software\FastTrack Software\Admin By Request\Policies" 4. Set the AutoApprove registry key to 1.
d. Scenario 4: Service Ceases to Operate
   i. Description: The entire Admin By Request service ceases to operate indefinitely or permanently, including the website, APIs and mobile app. NOTE: This scenario is unrealistic because you pay a subscription for the Admin By Request service. Therefore, you would be made aware if our service were to cease operating.
   ii. Result: Users cannot get approval of requests, which sit on endpoints until the service is up again. When or if the service is up, requests are queued, and the user experience is an exceptionally long approval time.
   iii. Business Impact Rating: CRITICAL
   iv. Remedial Actions: Option 1: As a temporary solution while planning a replacement, set the AutoApprove and RequireApproval registry keys to temporarily allow elevations without approval. See Remedial Actions in the above scenario, section 4.1 Service Outage Scenarios > Customers using Require FastTrack Software Scenario 2: Worst-Case

All Systems Non-Functional – Extended / Unacceptable Period.
Option 2: Uninstall Admin By Request on endpoints and install a replacement solution.

2. **Software Failure**
    a. Scenario 1: Website is Down
        i. Description: The Admin By Request website is entirely non-functional for a short / extended period of time.
        ii. Result: IT administrators are not able to use the website for any function, including approving requests, viewing the Auditlog and configuring settings. Users may have to wait longer than usual for requests to be approved.
        iii. Business Impact Rating: LOW
        iv. Remedial Actions: Perform all functions using the Admin By Request mobile application on any iPhone, iPad or Android device, apart from change settings, which is unavailable via the app.
    b. Scenario 2: Mobile Application is Down
        i. Description: The Admin By Request mobile application is entirely non-functional for a short / extended period of time.
        ii. Result: IT administrators are not able to use the mobile app for any function, including approving requests and viewing the Auditlog. Administrators out of the office will not be able to approve requests on the move via the mobile app. Users may have to wait longer than usual for requests to be approved.
        iii. Business Impact Rating: LOW
        iv. Remedial Actions: To use Admin By Request on a mobile device, log in to the website user portal from the internet browser of a mobile device.
    c. Scenario 3: Support Assist Feature is Unavailable
        i. Description: The Admin By Request Support Assist feature is non-functional for a short or extended period of time.
        ii. Result: End users who are not able to self-service (either due to lacking IT skills or having Run as Admin and Admin Session disabled) cannot use the Support Assist feature to gain elevation.
        iii. Business Impact Rating: LOW
        iv. Remedial Actions: Log out the user who is unable to self-service or use Support Assist and log the Help Desk person in to perform the task that requires elevation.

Impact Analysis

1. **Service Disruption**
    a. **Impact**: Inability for a user to elevate on endpoint device
    b. **Severity**: Low, ABR is not required to operate it is a privilege.
2. **Data Loss**
    a. **Impact**: No data loss impact

   b. **Severity**: NA
3. **Financial Loss**
   a. **Impact**: Unknown
   b. **Severity**: Unknown
4. **Reputation Damage**
   a. **Impact**: Loss of trust from stakeholders, including university staff and students.
   b. **Severity**: Medium - Reputation damage can affect future collaborations and funding opportunities.
5. **Operational Downtime**
   a. **Impact**: Extended periods of reduced or halted operations, affecting productivity and service delivery.
   b. **Severity**: High - Operational downtime can have a significant impact on the university's ability to function effectively.

Backup and Recovery Procedures

- Backup services for cloud-provided solutions are handled by the vendor.

Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO)

- Recovery services are cloud-provided solutions that are handled by the vendor.

Communication Plan

Internal Communications Plan

1. **Notification of Disaster**
   - **Immediate Notification**: Notify key personnel and stakeholders immediately after a disaster is identified.
   - **Key Personnel**:
     - Ed Pierson, Vice President for Information Technology and Chief Information Officer (epierson@tamu.edu)
     - Ed Evans, Associate Vice President for IT Enterprise Operations (edevans@tamu.edu)
     - Dan Schmiedt, Associate Vice President for Enterprise Networks (willys@tamu.edu)
     - Lacey Baze, Assistant Vice President of Product Management (lacey-baze@tamu.edu)
     - Kris Guye, Assistant Vice President of Strategic Partnerships & Alliances (kguye@tamu.edu)
     - Mitch Wittneben, Assistant Vice President for IT Academic Operations (mwittneben@tamu.edu)
     - Chrissie Cordray, Assistant Chief Information Officer of Operations (chrissiec@tamu.edu)

    - Sharon Mainka, Chief of Staff to the Vice President for IT and CIO (smainka@tamu.edu)

2. **Regular Updates**
    - **Frequency**: Provide regular updates on recovery progress to all key personnel and stakeholders.
    - **Channels**: Use email, Teams messages, and scheduled meetings to communicate updates.
    - **Content**: Include information on recovery status, any issues encountered, and expected timelines for resolution.
3. **Coordination Meetings**
    - **Schedule**: Hold coordination meetings with key personnel to discuss recovery efforts and ensure alignment with overall DRP objectives.
    - **Participants**: Include representatives from Server Operations, Architecture and Engineering, and Unified Endpoint Management teams.

External Communications Plan

1. **Notification of Service Disruption**
    - **Immediate Notification**: Inform university staff and students about service disruptions as soon as a disaster is identified.
    - **Channels**: Use university-wide email notifications, website announcements, and social media posts to communicate the disruption.
    - **Content**: Provide details on the nature of the disruption, affected services, and expected recovery times.
2. **Regular Updates**
    - **Frequency**: Provide regular updates on recovery progress to university staff and students.
    - **Channels**: Use email notifications, website updates, and social media posts to keep everyone informed.
    - **Content**: Include information on recovery status, any issues encountered, and expected timelines for resolution.
3. **Stakeholder Engagement**
    - **Meetings**: Hold meetings with key external stakeholders to discuss recovery efforts and address any concerns.
    - **Participants**: Include representatives from university administration, faculty, and student organizations.

Testing & Maintenance

Regular Testing

1. **Testing Schedule**

a. **Frequency**: Conduct DRP tests quarterly to ensure readiness.
b. **Types of Tests**:
    i. **Full-Scale DRP Drills**: Simulate a complete disaster scenario to test the entire recovery process.
    ii. **Component-Specific Tests**: Focus on specific components such as database recovery, server restoration, and endpoint management.
    iii. **Tabletop Exercises**: Conduct discussion-based exercises to review recovery procedures and identify potential improvements.

2. **Testing Procedures**
    a. **Preparation**: Notify all key personnel and stakeholders about the upcoming DRP test and provide detailed instructions.
    b. **Execution**: Follow the step-by-step recovery procedures outlined in the DRP. Ensure all team members perform their assigned roles and responsibilities.
    c. **Monitoring**: Monitor the recovery process to identify any issues or bottlenecks. Document the performance of each component and team member.
    d. **Evaluation**: Evaluate the results of the DRP test to determine the effectiveness of the recovery procedures. Identify areas for improvement and update the DRP accordingly.
3. **Documentation**
    a. **Test Results**: Document the results of each DRP test, including any issues encountered and the steps taken to resolve them.
    b. **Lessons Learned**: Record lessons learned from each test to improve future recovery efforts.
    c. **Updates**: Update the DRP based on the test results and lessons learned to ensure it remains current and effective.

Plan Maintenance

1. **Regular Review**
    a. **Frequency**: Review the DRP annually to ensure it remains up-to-date and effective.
    b. **Review Process**:
        i. **Assessment**: Assess the current state of ABR systems, services, and infrastructure to identify any changes or new risks.
        ii. **Updates**: Update the DRP to reflect any changes in the ABR environment, including new systems, services, or personnel.
        iii. **Approval**: Obtain approval from key stakeholders for any updates to the DRP.
2. **Continuous Improvement**
    a. **Feedback**: Gather feedback from team members and stakeholders on the effectiveness of the DRP and recovery procedures.
    b. **Improvements**: Implement improvements based on feedback and lessons learned from DRP tests.

c. **Training**: Provide regular training to team members on updated recovery procedures and best practices.

3. **Documentation**
   a. **Version Control**: Maintain version control of the DRP to track changes and updates.
   b. **Accessibility**: Ensure the DRP is easily accessible to all key personnel and stakeholders.
   c. **Compliance**: Ensure the DRP complies with university policies and industry standards.

Appendices

Appendix A: Contact List

1. **Ed Pierson, Vice President for Information Technology and Chief Information Officer**
   a. **Email**: epierson@tamu.edu
   b. **Phone**: +1 979 458 9788
2. **Ed Evans, Associate Vice President for IT Enterprise Operations**
   a. **Email**: edevans@tamu.edu
   b. **Phone**: +1 979 458 9788
3. **Dan Schmiedt, Associate Vice President for Enterprise Networks**
   a. **Email**: willys@tamu.edu
   b. **Phone**: +1 979 458 9788
4. **Lacey Baze, Assistant Vice President of Product Management**
   a. **Email**: lacey-baze@tamu.edu
   b. **Phone**: +1 979 458 9788
5. **Kris Guye, Assistant Vice President of Strategic Partnerships & Alliances**
   a. **Email**: kguye@tamu.edu
   b. **Phone**: +1 979 458 9788
6. **Mitch Wittneben, Assistant Vice President for IT Academic Operations**
   a. **Email**: mwittneben@tamu.edu
   b. **Phone**: +1 979 458 9788
7. **Chrissie Cordray, Assistant Chief Information Officer of Operations**
   a. **Email**: chrissiec@tamu.edu
   b. **Phone**: +1 979 458 9788
8. **Sharon Mainka, Chief of Staff to the Vice President for IT and CIO**
   a. **Email**: smainka@tamu.edu
   b. **Phone**: +1 979 458 9788
9. **Roger Whitaker, Director Information Technology**
   - **Email**: roger@tamu.edu
   - **Phone**: +1 979 458 9788
10. **Michael Hafercamp, Senior IT Professional II**
    - **Email**: haferka@tamu.edu

11. **Megan Southerland, Associate Director**
    - **Email**: meghanmary@tamu.edu
    - **Phone**: +1 979 458 7738
12. **Nicholas Swanzy, Site Reliability Engineer III**
    - **Email**: nswanzy@tamu.edu
13. **Jon Griffey, IT Director for Endpoint Management**
    - **Email**: griffey@tamu.edu
    - **Phone**: +1 979 862 9200
14. **Jesus Perez, Senior Windows Device Management Professional**
    - **Email**: japerez@tamu.edu
    - **Phone**: +1 979 458 7512

- **Detailed Recovery Procedures**
    - TBD by Server OPS and A&E
- **Backup Schedules and Locations**
    - TBD by Server OPS and A&E
- **DRP Test Schedule and Results**
    - TBD by Server OPS and A&E

Revision History

Version	Date	Description of Change	Author
1.0	03/21/2025	Initial release	Danielle Narita
1.1	[Date]	[Description]	[Author Name]