Inteum Company LLC

Disaster Recovery Plan (DRP) for Inteum

Plan and related Business Processes

Business Process	Feature	Relevant Technical Components
Information Systems	Web Hosting, Email, DNS	Server, email software, Web software, user data base
Information Systems	Customer Database	Hardware, User Database, COTs software
Information Systems	Customer Support	User Database, Server hardware,
Software Engineering	Code repository	Server Hardware, Code repository, file server
Accounting	Accounts receivable, Account payable	Server Hardware, Accounting Software, Business partner databases, Customer database

January 10, 2025

Table of Contents

1. Purpose and Objective

Inteum Company LLC (Inteum) developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to the features listed in the table above. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope

The scope of this DRP document addresses technical recovery only in the event of a significant disruption. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the Business Continuity Plan and/or the Corporate Incident Response plans Inteum has in place.

This disaster recovery plan provides:

- Guidelines for determining plan activation;
- Technical response flow and recovery strategy;
- Guidelines for recovery procedures;
- References to key Business Resumption Plans and technical dependencies;
- Rollback procedures that will be implemented to return to standard operating state;
- Checklists outlining considerations for escalation, incident management, and plan activation.

The specific objectives of this disaster recovery plan are to:

- Immediately mobilize a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage the restoration of operations to full processing capabilities;
- Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team.

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside Inteum. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

2. Dependencies

This section outlines the dependencies made during the development of this disaster recovery plan. If and when needed the DR TEAM will coordinate with their partner groups as needed to enable recovery.

Dependency	Assumptions
User Interface / Rendering Presentation components	• Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application). • Infrastructure and back-end services are still assumed to be active/running.
Business Intelligence / Reporting Processing components	• The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). • Standard backup processes (e.g. tape backups) are not impacted, but the active / passive or mirrored processes are not functioning. • Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.
Network Layers Infrastructure components	• Connectivity to network resources is compromised and/or significant latency issues in the network exists that result in lowered performance in other layers. • Assumption is that terminal connections, serially attached devices and inputs are still functional.
Storage Layer Infrastructure components	• Loss of SAN, local area storage, or other storage component.
Database Layer Database storage components	• Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable
Hardware/Host Layer Hardware components	• Physical components are unavailable or affected by a given event
Virtualizations (VM's) Virtual Layer	• Virtual components are unavailable • Hardware and hosting services are accessible
Administration Infrastructure Layer	• Support functions are disabled such as management services, backup services, and log transfer functions. • Other services are presumed functional
Internal/External Dependencies	• Interfaces and intersystem communications corrupt or compromised

3. Disaster Recovery Strategies

The overall DR strategy of Inteum is summarized in the table below and documented in more detail in the supporting sections. These scenarios and strategies are consistent across the technical layers (user interface, reporting, etc.)

Data Center Disruption	Significant Dependency (Internal or External) Disruption	Significant network or other issues
Failover to alternate Data Center	Reroute core functions to backup / alternate provider	Reroute operations to backup processing unit / service (load balancing, caching)
Reroute core processes to another Data Center (without full failover)	Participate in recovery strategies as available	Wait for service to be restored, communicate with core stakholders as needed
Operate at a deprecated service level	Wait for the restoration of service, provide communication as needed to stakeholders	
Take no action		

4. Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration.

Response Phase: The immediate actions following a significant event.

- On call personnel paged
- Decision made around recovery strategies to be taken
- Full recovery team identified

Resumption Phase: Activities necessary to resume services after team has been notified.

- Recovery procedures implemented
- Coordination with other departments executed as needed

Restoration Phase: Tasks taken to restore service to previous levels.

- Rollback procedures implemented
- Operations restored

Response Phase

The following are the activities, parties and items necessary for a DR response in this phase. Please note these procedures are the same regardless of the triggering event (e.g. whether caused by a Data Center disruption or other scenario).

Per FedRAMP/StateRAMP guidelines the Inteum Compliance and Incident Response teams have defined and planned for a Recovery Time Objective (RTO) of 1 hour and a Recovery Point Objective (RPO) as defined below. Please note that the steps taken to enable recovery will vary based on the type of issue.

Response Phase Recovery Procedures – All DR Event Scenarios

Step	Owner	Duration	Components
Identify issue, page on call / Designated Responsible Individual (DR TEAM)	DR TEAM	30 minutes	• Issue communicated / escalated • Priority set
Identify the team members needed for recovery	DR TEAM	30 minutes	Selection of core team members required for restoration phase from among the following groups: • Operations • Network • DBA
Establish a conference line for a bridge call to coordinate next steps	DR TEAM or Ops	10 minutes	Bridge line: **470-808-3150** Alternate / backup communication tools: email, communicator
Communicate the specific recovery roles and determine which recovery strategy will be pursued.	DR TEAM	30 minutes	• Documentation / tracking of timelines and next decisions • Creation of disaster recovery event command center / "war room" as needed

This information is also summarized by feature in Appendix A: Disaster Recovery Contacts - Admin Contact List.

Resumption Phase

During the resumption phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

Data Center Recovery

Full Data Center Failover

Step	Owner	Duration	Components
Initiate Failover	DR TEAM	TBD	• Restoration procedures identified • Risks assessed for each procedure • Coordination points between groups defined • Issue communication process and triage efforts established
Complete Failover	DR TEAM	TBD	• Recovery steps executed, including handoffs between key dependencies
Test Recovery	DR TEAM	TBD	• Tests assigned and performed • Results summarized and communicated to group
Failover deemed successful	DR TEAM	TBD	•

Reroute critical processes to alternate Data Center

Step	Owner	Duration	Components
Change DNS Configuration	IT	30 min	• Backup DNS • Modify DNS records to point to new location
Test changes to DNS	IT	30 min	•

Take no action – monitor for Data Center recovery

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the Data Center is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	Communications	As needed	•
Send out frequent updates to core stakeholders with the status.	ERT	As needed	

Restoration Phase

During the restoration phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

Data Center Recovery

Full Data Center Restoration

Step	Owner	Duration	Components
Determine whether failback to original Data Center will be pursued	DR TEAM	TBD	• Restoration procedures determined
Original data center restored	DR TEAM	TBD	• Server Farm level recovery
Complete Failback	DR Team	TBD	• Failback steps executed, including handoffs between key dependencies
Test Failback	DR Team	TBD	• Tests assigned and performed • Results summarized and communicated to group • Issues (if any) communicated to group
Determine whether failback was successful	DR TEAM	TBD	• Declaration of successful failback and communication to stakeholder group. • Disaster recovery procedures closed. • Results summarized, post mortem performed, and DRP updated (as needed).

Appendix A: Disaster Recovery Contacts - Admin Contact List

The critical DR TEAM members who would be involved in recovery procedures for feature sets are summarized below.

Feature Name	Contact Lists
Web Hosting, Email, DNS	IT, Communications
Customer Database	IT, Communications
Customer Support	IT, Communications
Code Repository	IT, Communications
Accounts receivable, Account Payable	Finance, IT, HR

For the key internal and external dependencies identified, the following are the primary contacts.

Emergency Response Team
The Emergency Response Team (ERT) is managed and control by the Crisis Management Team (CMT) the CMT will is responsible for activating all required team and managing those teams during a crisis. CMT team consists of upper management this would include the CEO, CIO, CFO, and President. These individuals will be responsible also for assisting emergency response teams like the fire and police if necessary and identifying a alternate location if necessary.
ERT is consists of the following organizations within the company:

Gannon Mikesell: Communication
Rob Sloman: CMT,
Ruth Benson:HR and Legal
Tim Hollobon: IT
Matt Campbell: IT and Security

Communications: These individuals consist of public relations and individuals that are needed for communication between all the other ER Team within the company. They are responsible for relaying vital information and any orders from the CMT.

Human Resources: These individuals are responsible for making sure the needs of the employees are met during a crisis this could me making sure that there is staff available to meet vital resource needs. They are also responsible for emergency medical insurance in case there is a need to go out of network from the current plan. They will also field employee concerns and make sure employees are getting paid and dealing with any other employee needs.

Legal: Is responsible for making sure that the company is compliant with any laws and regulations. They could also be needed to make sure that when the company has had a disaster that the company is protected from criminal or civil actions from the employees or the public.

IT: is responsible for bringing systems back online and that there is as minimal disruption within the company as possible. They would also be responsible handling all computer incidents that include malicious code, denial of service, data proliferation, inappropriate use, etc and will be able to respond and remove threats and return the data systems back to organizations as soon as possible.

Business Units: will have members assigned to work with each of the above mentioned groups in order to return the business unit back to regular operations. These units will coordinate the needs of the group to the appropriate groups. The following people will work directly with a specific group to make sure the needs of the business group are met.

Dependency Name	Contact Information
Matt Campbell	425-814-8212
Tim Hollobon	425-823-1780
Gannon Mikesell	970-237-1791
Ruth Benson	425-820-8415
Preet Mood (QA)	781-534-5833

Appendix B: Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

Inteum has defined **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** metrics to ensure disaster recovery and business continuity for systems categorized as **Moderate Impact Level** under **StateRAMP**. These metrics reflect operational priorities and comply with the requirements of StateRAMP Moderate. It is important to note that each situation is different, and the indicated times may vary depending on the severity and complexity of the issue at hand.

Recovery Time Objective (RTO)

RTO specifies the maximum allowable downtime for systems and services to avoid unacceptable impacts on business operations. For StateRAMP Moderate systems:

- **Moderate Impact Systems:** Restoration is targeted within **24 hours**, ensuring continuity of essential functions while minimizing disruption.

Recovery Point Objective (RPO)

RPO defines the maximum amount of data loss acceptable during an incident and drives the frequency of backups. For StateRAMP Moderate systems:

- **Moderate Impact Systems:** Backups are performed to achieve an RPO of **a few hours to a day**, ensuring the preservation of critical data.

Implementation of RTO and RPO for StateRAMP Moderate Systems

To meet these objectives, Inteum implements the following measures:

1. **Business Needs Assessment:** Systems are categorized by criticality and operational impact, reflecting the Moderate Impact Level.
2. **Risk Analysis:** Potential downtime and data loss impacts are analyzed to prioritize recovery and backup strategies.
3. **System Dependencies:** Dependencies between systems and services are mapped to define recovery order.
4. **Backup and Redundancy:**
    - Backups occur at least every **4–12 hours**, ensuring compliance with Moderate RPO objectives.
    - Redundant storage and infrastructure ensure data recovery within defined RTO targets.
5. **Recovery Infrastructure:** Inteum leverages **AWS GovCloud**, **redundant virtual servers**, and **automated recovery processes** to ensure timely restoration of services.

6. **Monitoring and Testing:** Disaster recovery processes are tested annually to verify compliance, and adjustments are made as business or technological needs evolve.

Data Retention and System Decommissioning

In the event of system or customer environment termination, Inteum follows a structured process:

1. Data is backed up and returned to customers in a secure format (e.g., CSV).
2. Access to the customer's environment is disabled on the agreed termination date.
3. The environment is retained temporarily until the customer confirms successful data restoration.
4. Upon confirmation, the environment is fully decommissioned, and all related system components are securely removed from the inventory.

Alignment with StateRAMP Moderate Standards

Inteum's RTO and RPO objectives are explicitly aligned with **StateRAMP Moderate Impact Level** requirements:

- Restoration of services occurs within **24 hours** of a disaster (RTO).
- Backups are performed every **4–12 hours**, minimizing data loss (RPO).

This approach ensures that disaster recovery and business continuity processes meet StateRAMP compliance standards and provide resilience for critical operations.

Testing and Validation

Inteum regularly validates the effectiveness of recovery processes through:

- **Annually Testing:** Disaster recovery and backup processes are tested to ensure compliance with RTO and RPO metrics.
- **Monitoring and Alerts:** Automated alerts track backup completion and recovery operations, escalating issues to the Compliance and IT Teams.
- **Continuous Improvement:** Recovery metrics are reviewed and adjusted as operational requirements evolve.

Appendix C: Glossary/Terms

Standard Operating State: Production state where services are functioning at standard state levels. In contrast to recovery state operating levels, this can support business functions at minimum but deprecated levels.

Presentation Layer: Layer which users interact with. This typically encompasses systems that support the UI, manage rendering, and captures user interactions. User responses are parsed and system requests are passed for processing and data retrieval to the appropriate layer.

Processing Layer: System layer which processes and synthesizes user input, data output, and transactional operations within an application stack. Typically this layer processes data from the other layers. Typically these services are folded into the presentation and database layer, however for intensive applications; this is usually broken out into its own layer.

Database Layer: The database layer is where data typically resides in an application stack. Typically data is stored in a relational database such as SQL Server, Microsoft Access, or Oracle, but it can be stored as XML, raw data, or tables. This layer typically is optimized for data querying, processing and retrieval.

Network Layer: The network layer is responsible for directing and managing traffic between physical hosts. It is typically an infrastructure layer and is usually outside the purview of most business units. This layer usually supports load balancing, geo-redundancy, and clustering.

Storage Layer: This is typically an infrastructure layer and provides data storage and access. In most environments this is usually regarded as SAN or NAS storage.

Hardware/Host Layer: This layer refers to the physical machines that all other layers are reliant upon. Depending on the organization, management of the physical layer can be performed by the stack owner or the purview of an infrastructure support group.

Virtualization Layer: In some environments virtual machines (VM's) are used to partition/encapsulate a machine's resources to behave as separate distinct hosts. The virtualization layer refers to these virtual machines.

Administrative Layer: The administrative layer encompasses the supporting technology components which provide access, administration, backups, and monitoring of the other layers.

RTO: Recovery Time Objective

RPO: Recovery Point Objective

Appendix D: Document Maintenance Responsibilities and Revision History

This section identifies the individuals and their roles and responsibilities for maintaining this Disaster Recovery Plan.

Primary Disaster Recovery Plan document owner is:

Primary Designee: Preet Mood

Alternate Designee: Matt Campbell

Name of Person Updating Document	Date	Update Description	Version #	Approved By
Justin Adair	10/10/2016	Initial draft	1.0	Rob Sloman
Preet Mood	2/5/2018	Added Preet Mood in Contacts	1.1	Justin Adair
Preet Mood	1/23/2019	Review document to see if any changes needed. No changes are needed to the current document.	1.2	Justin Adair
Preet Mood	12/3/2019	Review document to see if any changes needed. No changes are needed to the current document.	1.3	Justin Adair
Preet Mood	1/12/2021	Review document to see if any changes needed. No changes are needed to the current document.	1.4	Justin Adair
Preet Mood	1/4/2022	Review document to see if any changes needed. No changes are needed to the current document.	1.5	Justin Adair
Preet Mood	1/13/2023	Reviewed document to see if any changes needed. No changes are needed to the current document.	1.6	Matt Campbell
Yavuz Alparslan	6/6/2024	Remove versioning from file name. Add Recovery Time Objective (RTO) and Recovery Point Objective (RPO) per FedRAMP/StateRAMP.	1.7	Preet Mood
Yavuz Alparslan	1/9/2025	Moved Glossary up to Appendix C. Added StateRAMP related RTO & RPO as Appendix B. Moved Revision History to Appendix D.	1.8	Preet Mood