Lectora Disaster Recovery Plan

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	10/28/2014	Christopher Hord	Lectora DR Plan
1.1	10/01/2015	John Blackmon	

Table of Contents

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and data. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

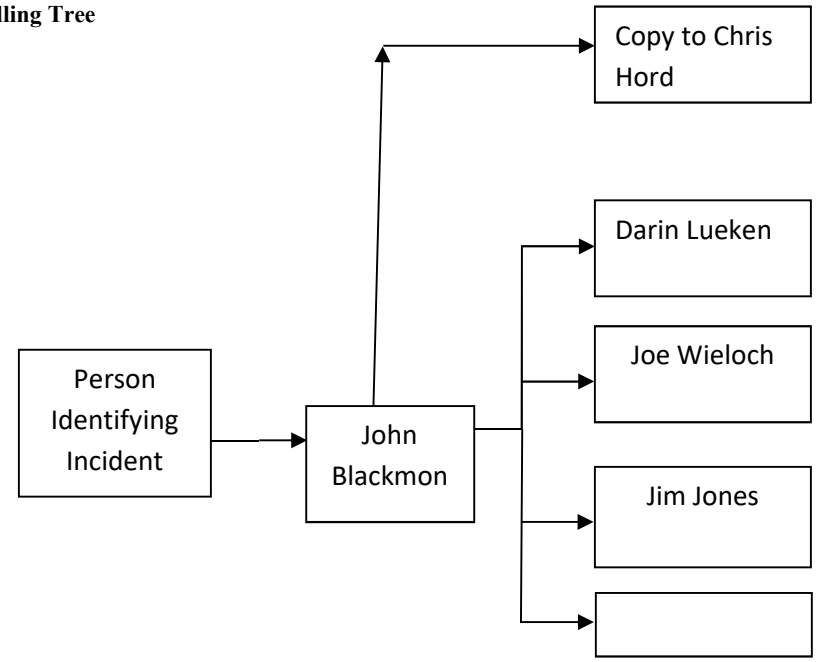
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications for both Trivantis and CourseMill hosted customers.
- Disaster recovery capabilities as applicable to customers, vendors and others.

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
Christopher Hord, CFO	Work	513.929.0188
	Alternate	513.929.0188 x144
	Mobile	513.238.2480
	Email Address	chris.hord@trivantis.com
	Alternate Email	
John Blackmon, CTO	Work	561-257-0127
	Alternate	513.929.0188 x301
	Mobile	561-306-1976
	Email Address	John.blackmon@trivantis.com
	Alternate Email	
Darin Lueken, Director of Development - Lectora	Work	561-293-2774
	Alternate	513.929.0188 x304
	Mobile	561-289-2542
	Email Address	Darin.lueken@trivantis.com
	Alternate Email	
Joseph Wieloch, Director of Development – Lectora Online	Work	561-293-2782
	Alternate	513-929-0188 x315
	Mobile	954-857-6210
	Email Address	Joe.wieloch@trivantis.com
	Alternate Email	
Jim Jones, Director of Development - ReviewLink	Work	561-293-2771
	Alternate	513-929-0188 x313
	Mobile	954-899-6938
	Email Address	Jim.jones@trivantis.com

Notification Calling Tree



External Contacts

Name, Title	Contact Option	Contact Number
	Contact:	
	Work	
	Mobile	
	Home	
	Email Address	
DR Facility		
	Contact:	
	Work	
	Mobile	
	Home	
	Email Address	
Server Supplier		
	Contact:	
	Work	
	Mobile	
	Fax	
	Email Address	
Workstation Supplier		
	Contact:	
	Work	
	Mobile	
	Home	
	Email Address	
Insurance – Name		
	Contact	Marcus Gilmore
	Work	1.901.766.5990
	Mobile	
	Home	
	Email Address	Marcus.gilmore@usi.com
Off-Site Storage 1		
	Contact	
	Work	
	Mobile	
	Home	
	Email Address	
Other –		
	Contact	
	Work	
	Mobile	
	Home	
	Email Address	

1 Plan Overview

1.1 Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the CTO

1.2 Plan Documentation Storage

Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the Trivantis. Each member of Disaster Recovery management team will be issued a CD and hard copy of this plan to be filed at home. A master protected copy will be stored on specific resources established for this purpose on Google Docs..

1.3 Backup Strategy

Key business processes and the agreed backup strategy is use of AWS off-site storage process. AWS will supply full product back-up to Trivantis

KEY BUSINESS PROCESS	BACKUP STRATEGY
Nightly Product backup	

1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	5	4	All critical equipment is located above the 100 year flood plain
Fire	4	3	Hallon suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5	2	
Electrical storms	5	4	
Hurricane	3	3	
Act of terrorism	5	3	
Act of sabotage	5		
Electrical power failure	3	3	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	3	Two diversely routed T3 trunks into building. WAN redundancy, voice network resilience

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

2 Emergency Response

2.1 Alert, escalation and plan invocation

- **2.1.1 Plan Triggering Events**

Key trigger issues at Amazon headquarters that would lead to activation of the DRP are:
- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Fire on the premises
- Loss of the building

- **2.1.2 Assembly Points**

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:
- Determine by Amazon
- Trivantis employees will assemble in Cincinnati Support Center and Boca Raton Development Center.

- **2.1.3 Activation of Emergency Response Team**

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees noted above will be notified via the calling trees. Responsibilities of the ERT are to:

- Immediately assess the extent of the disaster and its impact on the data center and customer.
- Determine which, if any, elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to:
    - Implement process to restore primary vital services
    - Implement process to return to normal operation;
- Ensure customers and ERT are notified and allocate responsibilities and activities as required.

2.2 Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include (depending on the severity of the incident):
- Establish facilities for an emergency level of service within 8.0 business hours;
- Restore key services within 24 business hours of the incident (Administrator access);
- Recover to business as usual within 48 to 72 hours after the incident (Instructor, Reporter and User access);
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team and customer communications or other issues

2.3 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

- **2.3.1 Emergency Alert**

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team - Trivantis
- John Blackmon: Office phone first, then Cell number if off Office hours
- Chris Hord: Contacted by John Blackmon, Office phone first, then Cell number if off Office hours

Note: If John Blackmon is not available follow the order, above, to notify Trivantis ERT.

Emergency Response Team - Customer

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the customer's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble (physically or virtually) and will involve sufficient information to have this request effectively communicated.

- **2.3.2 DR Communication with Customer**

The Customer will be contacted at the time the DRT is activated and every four hours thereafter until Primary service has been restored. Once Primary service has been restored the Customer will be updated every eight hours, or less, on restoration of full service.

- **2.3.3 DR Contact with Employees**

Trivantis DRT will serve as the focal points for internal departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

- **2.3.4 Backup Staff**

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

- **2.3.7 Alternate Recovery Facilities / Hot Site**

If necessary, the hot site in the Amazon Cloud will be activated as an alternate hosting facility. Hot site staffing will consist of members of the disaster recovery team only for the first 24 hours, with other staff members joining at the hot site as necessary.

4 Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, directors & officers liability, general liability, and business interruption insurance.

If insurance-related assistance is required following an emergency out of normal business hours, please contact: Christopher Hord 513-238-2480

Policy Name	Coverage Type	Coverage Period	Amount Of Coverage	Person Responsible For Coverage	Next Renewal Date
Package Plan	**General Liability**	**12/03/13-12/03/14**	**$1 mil each occurrence, $2 mil aggregate**	**Christopher Hord**	**12/03/2014**
E&O	**E&O**	**07/30/14 – 07/30/15**	**$2 mil aggregate**	**Christopher Hord**	**07/30/2015**
Technology Protection	**Same**	**07/30/14 – 07/30/15**	**$2 mil aggregate**	**Christopher Hord**	**07/30/2015**

5 Financial and Legal Issues

5.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of training time
- Loss of compliance or licensure
- Loss of new staff training
- Loss of administrative reporting

5.3 Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the hosting company for contract violations, etc.

6 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Appendix A – Technology Disaster Recovery Plan Templates

All Recovery plans are kept in Google Drive

List of all servers are in:
Trivantis/Development/Lectora/Lectora Online/Amazon/ Lectora Online Amazon Server Maintenance

List of all Recovery instructions are kept in:

Trivantis/Development/Lectora/Lectora Online/Amazon/ Lectora Online Amazon Server Maintenance Instructions

Appendix B

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

Management of DR Activities Form

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

Disaster Recovery Event Recording Form

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:

Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Disaster Recovery Team's Work Completed: <Date>
Event Log <Date>

Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

Mobilizing the Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
- The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

Description of Emergency:
Date Occurred:
Date Work of Disaster Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader.
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead.
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.