Computer Information Development, LLC

Disaster Recovery Policy

Revision: 2.0

Table of Contents

Introduction

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes CID's ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery.

Definition of a Disaster

A disaster can be caused by man or nature and results in CID's IT department not being able to perform all or some of their regular roles and responsibilities for a period of time. CID defines disasters as the following:

- One or more vital systems are non-functional

Purpose

The purpose of this DRP document is twofold: first to capture all of the information relevant to the enterprise's ability to withstand a disaster, and second to document the steps that the enterprise will follow if a disaster occurs.

After assessing the scope of disaster the goal of CID will be to enact the steps outlined in this DRP to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- Preventing the loss of the organization's resources such as hardware, data and physical IT assets
- Minimizing downtime related to IT
- Keeping the business running in the event of a disaster

This DRP document will also detail how this document is to be maintained and tested.

Scope

The CID DRP takes all of the following areas into consideration:

- Servers Infrastructure
- Database Systems
- IT Documentation

This DRP does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters. For any disasters that are not addressed in this document, please refer to the business continuity plan created by.

Version Information & Changes

Any changes, edits and updates made to the DRP will be recorded in here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the DRP are up to date. Whenever there is an update to the DRP, CID requires that the version number be updated to indicate this.

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
IT Director	Technical Lead	10/2011	1.0	Initial policy adoption
IT Director	Technical Lead	10/2018	2.0	Completed new version of disaster recovery plan.

Disaster Recover y Teams & Responsibilities

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the clients of CID. The different groups and their responsibilities are as follows:

- Disaster Recovery Lead
- Network & Server Infrastructure Team
- Applications Team
- Operations Team

The lists of roles and responsibilities in this section have been created by CID and reflect the likely tasks that team members will have to perform. Disaster Recovery Team members will be responsible for performing all of the tasks below. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.

Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at CID regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in CID.

Role and Responsibilities

- Make the determination that a disaster has occurred and trigger the DRP and related processes.
- Initiate the DR Call Tree.
- Be the single point of contact for and oversee all of the DR Teams.
- Organize and chair regular meetings of the DR Team leads throughout the disaster.
- Present to the Management Team on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage all DRP test and author all DRP updates.

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Lou Perez	Primary Disaster Lead			*224-545-2548*

Network & Server Infrastructure Team

The Server Team will be responsible for providing the physical server infrastructure required for the enterprise to run its IT operations and applications in the event of and during a disaster. They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

Role & Responsibilities

- In the event of a disaster that does not require migration to standby facilities; the team will determine which servers are not functioning at the primary facility
- If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:
  - Assess the damage to any servers
  - Restart and refresh servers if necessary
- Ensure that secondary servers located in standby facilities are kept up-to-date with system patches Ensure
- that secondary servers located in standby facilities are kept up-to-date with application patches Ensure that
- secondary servers located in standby facilities are kept up-to-date with data copies
- Ensure that the secondary servers located in the standby facility are backed up appropriately
- Ensure that all of the servers in the standby facility abide by CID server policy
- Install and implement any tools, hardware, and systems required in the standby facility
- Install and implement any tools, hardware, and systems required in the primary facility
- After CID is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Name	Role/Title	Primary Number	Email
Lou Perez	CID Technical Lead	*224-545-2548*	*lou@idvalidation.net*
Microsoft Azure Support	Infrastructure Manager	www.windowsazure.com/support (for latest contact info / option)	

Applications Team

The Applications Team will be responsible for ensuring that all enterprise applications operates as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

Role & Responsibilities

- In the event of a disaster that does not require migration to standby servers, the team will determine which applications are not functioning on the primary server infrastructure.
- If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:
    - Assess the impact to application processes
    - Restart applications as required
    - Patch, recode or rewrite applications as required
- Ensure that secondary servers located in standby facilities are kept up-to-date with application patches
- Ensure that secondary servers located in standby facilities are kept up-to-date with data copies
- Install and implement any tools, software and patches required in the standby facility
- Install and implement any tools, software and patches required in the primary facility
- After CID is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Name	Role/Title	Primary Number	Email
Lou Perez	*IT Technical Lead*	*224-545-2548*	*lou@idvalidation.net*

Operations Team

This team's primary goal will be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They will need to provision all CID employees with the tools that their specific role requires.

Role & Responsibilities

- Maintain lists of all essential supplies that will be required in the event of a disaster
- Ensure that these supplies are provisioned appropriately in the event of a disaster
- Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster
- Ensure that spare computers and laptops have the required software and patches
- Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster
- Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe
- If insufficient computers/laptops or related supplies are not available the team will prioritize distribution in the manner and order that has the least business impact
- This team will be required to maintain a log of where all of the supplies and equipment were used
- After <<Organization Name>> is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Name	Role/Title	Work Phone Number	Mobile Phone Number
Nancy Palma	Director of Client Services	626-254-0000	*(562) 208-5912*
Lou Perez	*IT Technical Lead*		*(224) 545-2548*

Senior Management Team

The Senior Management Team will make any business decisions that are out of scope for the Disaster Recovery Lead. Decisions such as constructing a new data center, relocating the primary site etc., should be made by the Senior Management Team. The Disaster Recovery Lead will ultimately report to this team.

Role & Responsibilities

- Assist the Disaster Recovery Team Lead in his/her role as required
- Make decisions that will impact the company. This can include decisions concerning:
  - Rebuilding of data centers
  - Significant hardware and software investments and upgrades
  - Other financial and business decisions

Contact Information

Name	Role/Title	Work Phone Number	Mobile Phone Number
Paul Campoine	CEO	626-254-0000	(626) 255-1776

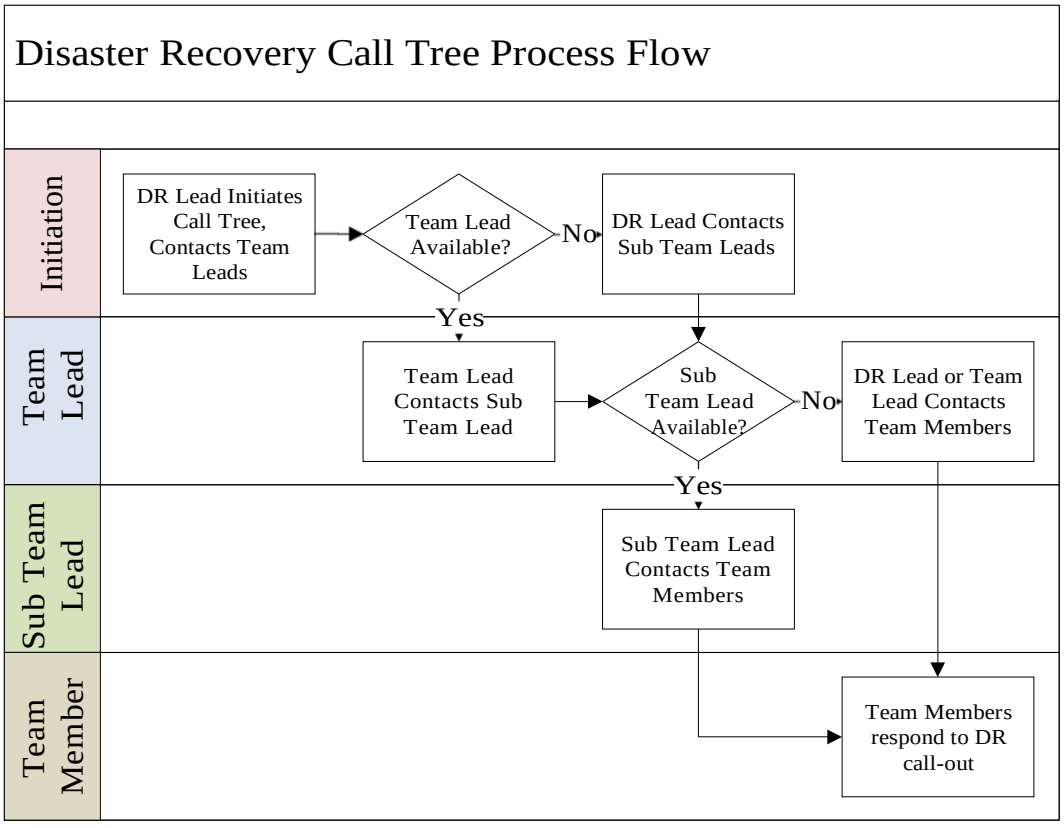
Disaster Recover y Call Tr ee

In a disaster recovery or business continuity emergency, time is of the essence so will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

- The Disaster Recovery Team Lead calls all Level 1 Members (Blue cells)
- Level 1 members call all Level 2 team members over whom they are responsible (Green cells)
- Level 1 members call all Level 3 team members over whom they are directly responsible (Beige cells)
- Level 2 Members call all Level 3 team members over whom they are responsible (Beige cells)
- In the event a team member is unavailable, the initial caller assumes responsibility for subsequent calls (i.e. if a Level 2 team member is inaccessible, the Level 1 team member directly contacts Level 3 team members).

Contact	Office	Mobile	Home
DR Lead *Lou Perez*		*224-545-2548*	

DR Management Team Lead		626-254-0000	
DR Management Team 1		*626-254-0000*	
Server Team Lead		562-208-5912	
Server Type 1 Team Lead Microsoft		www.windowsazure.c om/support	
Applications Team Lead		888-438-8330	
App 1 Team Lead		626-254-8507	
Management Team Lead		626-254-8507	
Management Team 1 Paul Campoine			



Data and Backups

Computer Information Development, LLC

This section explains where all of the organization's data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

Data in Order of Criticality

Rank	Data	Data Type	Back-up Frequency	Backup Location(s)
1	Production Website Portal Data	Application Data	Daily	Windows Azure > Highly GEO Redundant Cloud Storage https://manage.windowsazure.com
2	Production Website Documents	Documents	Daily	Windows Azure > Secured Highly Redundant Cloud Storage https://manage.windowsazure.com
3	Source Code for all applications	Code	Constantly	Unlimisoft.visualstudio.com / TFS
4	Application Assets	API's Tool	Daily	Highly Redundant Cloud Storage

Communicating with Clients

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing clients of the disaster and the impact that it will have on the following:

- Anticipated impact on service offerings
- Anticipated impact on delivery schedules
- Anticipated impact on security of client information
- Anticipated timelines

Crucial clients will be made aware of the disaster situation first. Crucial clients will be E-mailed first then called after to ensure that the message has been delivered. All other clients will be contacted only after all crucial clients have been contacted.

Dealing with a Disaster

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

1) Disaster identification and declaration
2) DRP activation
3) Communicating the disaster
4) Assessment of current and prevention of further damage
5) Establish IT operations

Disaster Identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, CID must be prepared to find out about disasters from a variety of possible avenues. These can include:

- First hand observation
- System Alarms and Network Monitors
- End users
- 3rd Party Vendors

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially declare that the company is in an official state of disaster.

DRP Activation

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- That a disaster has occurred
- The nature of the disaster (if known)
- The initial estimation of the magnitude of the disaster (if known)
- The initial estimation of the impact of the disaster (if known)
- The initial estimation of the expected duration of the disaster (if known)
- Actions that have been taken to this point
- Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads
- Scheduled meeting place for the meeting of Disaster Recovery Team Leads
- Scheduled meeting time for the meeting of Disaster Recovery Team Leads
- Any other pertinent information

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead

Communicating the Disaster

Refer to the "Communicating During a Disaster" section of this document.

Assessment of Current and Prevention of Further Damage

All teams will be required to create an initial report on the damage and provide this to the Disaster Recovery Lead within 2 hrs. of the initial disaster.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect CID's assets. Any necessary repairs or preventative measures must be taken to protect the infrastructure; these costs must first be approved by the Disaster Recovery Team Lead.

Restoring IT Functionality

Should a disaster actually occur and CID needs to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which CID <information system will be recovered.

IT Systems

Rank	IT System	System Components (In order of importance)
1	IDValidation.us Portal	Server Instance (Virtual Machine). Operating System, SQL Server, X509 and SSL Certificates, IIS, Secure Document Repo, Application
2		
3		

Cr iticality Rank -One System

System Name	IDValidation.us Portal
Component Name	Windows 2012 with SQL 2012 Virtual Machine Image
Vendor Name	Microsoft
Recovery Time Objective	24 hours

Title: Standard Operating Procedures for IDValidation.us

Security Level: RESTRICTED - SYSTEM ADMINSTRATOR

SOP Author/Owner: **Paul Campione**

a) Purpose

This SOP outlines the steps required to restore operations of IDValidation.us Portal

b) Scope

This SOP applies to the following components of the IDValidation.us Portal

- Web server
- Web server software
- Application server
- Application server storage system
- Application server software
- Application server backup
- Database server
- Database server storage system
- Database server software
- Database server backup

c) Responsibilities

The following individuals are responsible for this SOP and for all aspects of the system to which this SOP pertains:

- SOP Process: Paul Campione
- Network Connectivity: Microsoft
- Server Hardware: Microsoft
- Server Software: Paul Campione

For details of the actual tasks associated with these responsibilities, refer to section h) of this SOP.

d) Changes Since Last Revision

e) Documents/Resources Needed for this SOP

The following documents are required for this SOP:

- Administrator Access to windows azure account (COO and Systems Administrator are kept informed of access codes)
- Access to DNS server Name.com

f) Procedure

The following are the steps associated with bringing IDValidation.us Portal back online in the event of a disaster or system failure. The procedure assumes that the system is not accessible and needs to be restored completely.

Step	Action	Responsibility
1	Access Microsoft Windows Azure Management Portal using administrator credentials.	System Administrator
2	Create a new Virtual Machine Instance. Select Windows 2012 with SQL Server 2012 as the image.	System Administrator
3	Access Virtual Machine Server instance using Remote Desktop	System Administrator
4	Insure the following services are setup and running. IIS 8.0, SQL Server. Ensure HTTP and HTTPS ports are open on the firewall (this may have to be done via azure portal)	System Administrator
5	Obtain IP address of server and setup a notification (Saying services will be restored shortly) html page on the webserver root. Log into DNS server (Name.com) and point idvalidation.us to IP address. Anyone navigating to www.idvalidation.us will now get the notification page.	System Administrator
6	Restore Backup – Access redundant cloud storage via the Azure Portal and locate the VHD (Virtual Hard Disk). Detach disk if it is attached to server that is no longer accessible. Attach VHD to new instance via the Azure Portal – this will be added as another drive when you log in.	System Administrator
7	Locate SQL Server database and log files and copy to the new server. Attach to server.	System Administrator
8	Add a windows system user idvalidation_dbus er. Add user to Production_Live database User should have select / insert / update permissions on the database. Test to make sure access works. Note password for web configuration step.	System Administrator
9	SSL > Import Comodo Certificate from exported back up of cert on VHD. If backup is unavailable or expired a new certificate will need to be obtained from COMODO or another CA Authority.	System Administrator

10	X509 Certicate needs to be imported / installed from backup on VHD. Password for certificate can be obtained from COO or system administrator. IMPORTANT: The code the does he request signing with this certificate is looking for a friendly name of ComputerInformationDevelopment – so make sure the cert is name correctly. Permission to the private key need to be given to the idvalidation_dbUser and IIS_USR. If this step is not correctly completed the SSA's CBSV service will not function.	System Administrator
11	Restore application code to a new IIS Server app folder. Ensure asp.net worker process has read / write / execute permissions. Open up web configuration and make sure the password for idvalidation_db is set correctly.	System Administrator
12	Folder Permissions. Create a "Uploaded Files" folder on the root of the main drive – make sure IDvalidation_dbUser has write access – this is where the uploaded SSA89s will be placed. There is also a "Charts" folder that needs write permission under the Agent Portal folder.	System Administrator
13	Restore SSA89s to Uploaded Files folder from VHD Backup.	System Administrator
14	Test all system are operational	System Administrator
15	Remove "Maintenance / Notification" page and notify COO that site is now operational.	System Administrator

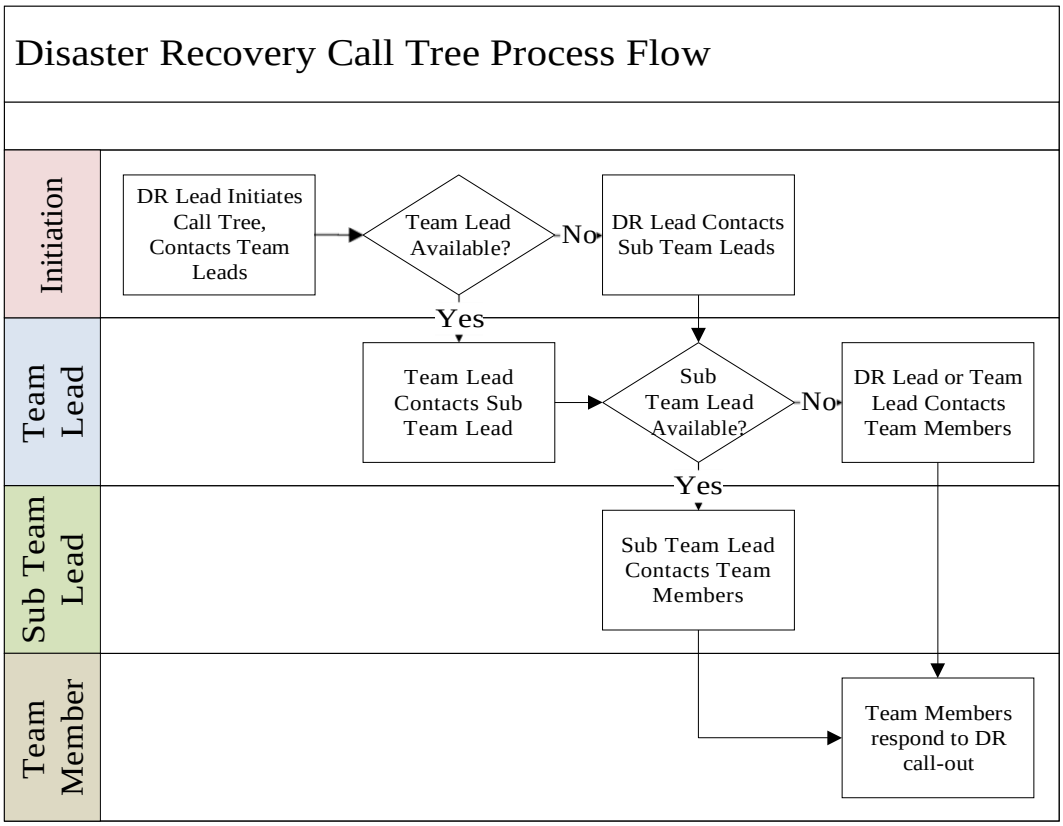
Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

- The Disaster Recovery Team Lead calls all Level 1 Members (Blue cells)
- Level 1 members call all Level 2 team members over whom they are responsible (Green cells)
- Level 1 members call all Level 3 team members over whom they are directly responsible (Beige cells)
- Level 2 Members call all Level 3 team members over whom they are responsible (Beige cells)
- In the event a team member is unavailable, the initial caller assumes responsibility for subsequent calls (i.e. if a Level 2 team member is inaccessible, the Level 1 team member directly contacts Level 3 team members).

Contact	Office	Mobile	Home
DR Lead *Lou Perez*			
DR Management Team Lead			
DR Management Team 1			
Server Team Lead			
Server Type 1 Team Lead		www.windowsazure.c	

Microsoft		om/support	
Applications Team Lead			
App 1 Team Lead			
Management Team Lead			
Management Team 1 Paul Campoine			



Data and Backups

This section explains where all of the organization's data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

Data in Order of Criticality

Rank	Data	Data Type	Back-up Frequency	Backup Location(s)
1	Production Website Portal Data	Application Data	Daily	Windows Azure > Highly GEO Redundant Cloud Storage https://manage.windowsazure.com
2	Production Website Documents	Documents	Daily	Windows Azure > Secured Highly Redundant Cloud Storage https://manage.windowsazure.com

3	Source Code for all applications	Code	Constantly	Unlimisoft.visualstudio.com / TFS
4	Application Assets	API's Tool	Daily	Highly Redundant Cloud Storage
5				
6				
7				
8				
9				
10				

Communicating with Clients

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing clients of the disaster and the impact that it will have on the following:

- Anticipated impact on service offerings
- Anticipated impact on delivery schedules
- Anticipated impact on security of client information
- Anticipated timelines

Crucial clients will be made aware of the disaster situation first. Crucial clients will be E-mailed first then called after to ensure that the message has been delivered. All other clients will be contacted only after all crucial clients have been contacted.

Dealing with a Disaster

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

6) Disaster identification and declaration
7) DRP activation
8) Communicating the disaster
9) Assessment of current and prevention of further damage
10) Establish IT operations

Disaster Identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, CID must be prepared to find out about disasters from a variety of possible avenues. These can include:

- First hand observation
- System Alarms and Network Monitors

- End users
- 3rd Party Vendors

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially declare that the company is in an official state of disaster. DRP Activation

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- That a disaster has occurred
- The nature of the disaster (if known)
- The initial estimation of the magnitude of the disaster (if known)
- The initial estimation of the impact of the disaster (if known)
- The initial estimation of the expected duration of the disaster (if known)
- Actions that have been taken to this point
- Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads
- Scheduled meeting place for the meeting of Disaster Recovery Team Leads
- Scheduled meeting time for the meeting of Disaster Recovery Team Leads
- Any other pertinent information

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead

Communicating the Disaster

Refer to the "Communicating During a Disaster" section of this document.

Assessment of Current and Prevention of Further Damage

All teams will be required to create an initial report on the damage and provide this to the Disaster Recovery Lead within 2 hrs of the initial disaster.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect CID's assets. Any necessary repairs or preventative measures must be taken to protect the infrastructure; these costs must first be approved by the Disaster Recovery Team Lead.

Restoring IT Functionality

Should a disaster actually occur and CID needs to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which CID <information system will be recovered.

IT Systems

Rank	IT System	System Components (In order of importance)
1	IDValidation.us Portal	Server Instance (Virtual Machine). Operating System, SQL Server, X509 and SSL Certificates, IIS, Secure Document Repo, Application
2		
3		

4		
5		
6		
7		
8		
9		

Criticality Rank -One System

System Name	IDValidation.us Portal
Component Name	Windows 2012 with SQL 2012 Virtual Machine Image
Vendor Name	Microsoft
Recovery Time Objective	24 hours

Title: Standard Operating Procedures for IDValidation.us

Security Level: RESTRICTED - SYSTEM ADMINSTRATOR

SOP Author/Owner: **Paul Campione**

g) Purpose

This SOP outlines the steps required to restore operations of IDValidation.us Portal

h) Scope

This SOP applies to the following components of the IDValidation.us Portal

- Web server
- Web server software
- Application server
- Application server storage system
- Application server software
- Application server backup
- Database server
- Database server storage system
- Database server software
- Database server backup

i) Responsibilities

The following individuals are responsible for this SOP and for all aspects of the system to which this SOP pertains:

- SOP Process: Paul Campione
- Network Connectivity: Microsoft
- Server Hardware: Microsoft
- Server Software: Paul Campione

For details of the actual tasks associated with these responsibilities, refer to section h) of this SOP. Changes Since Last Revision

j) Documents/Resources Needed for this SOP

The following documents are required for this SOP:

- Administrator Access to windows azure account (Systems Administrator are kept informed of access codes)
- Access to DNS server Name.com

k) Procedure

The following are the steps associated with bringing IDValidation.us Portal back online in the event of a disaster or system failure. The procedure assumes that the system is not accessible and needs to be restored completely.

Step	Action	Responsibility
1	Access Microsoft Windows Azure Management Portal using administrator credentials.	System Administrator
2	Create a new Virtual Machine Instance. Select Windows 2012 with SQL Server 2012 as the image.	System Administrator
3	Access Virtual Machine Server instance using Remote Desktop	System Administrator
4	Insure the following services are setup and running. IIS 8.0, SQL Server. Ensure HTTP and HTTPS ports are open on the firewall (this may have to be done via azure portal)	System Administrator
5	Obtain IP address of server and setup a notification (Saying services will be restored shortly) html page on the webserver root. Log into DNS server (Name.com) and point idvalidation.us to IP address. Anyone navigating to idvalidation.us will now get the notification page.	System Administrator
6	Restore Backup – Access redundant cloud storage via the Azure Portal and locate the VHD (Virtual Hard Disk). Detach disk if it is attached to server that is no longer accessible. Attach VHD to new instance via the Azure Portal – this will be added as another drive when you log in.	System Administrator
7	Locate SQL Server database and log files and copy to the new server. Attach to server.	System Administrator
8	Add a windows system user idvalidation_dbus er. Add user to Production_Live database User should have select / insert / update permissions on the database. Test to make sure access works. Note password for web configuration step.	System Administrator
9	SSL > Import Comodo Certificate from exported back up of cert on VHD. If backup is unavailable or expired a new certificate will need to be obtained from COMODO or another CA Authority.	System Administrator

10	X509 Certicate needs to be imported / installed from backup on VHD. Password for certificate can be obtained from COO or system administrator. IMPORTANT: The code the does he request signing with this certificate is looking for a friendly name of ComputerInformationDevelopment – so make sure the cert is name correctly. Permission to the private key need to be given to the idvalidation_dbUser and IIS_USR. If this step is not correctly completed the SSA's CBSV service will not function.	System Administrator
11	Restore application code to a new IIS Server app folder. Ensure asp.net worker process has read / write / execute permissions. Open up web configuration and make sure the password for idvalidation_db is set correctly.	System Administrator
12	Folder Permissions. Create a "Uploaded Files" folder on the root of the main drive – make sure IDvalidation_dbUser has write access – this is where the uploaded SSA89s will be placed. There is also a "Charts" folder that needs write permission under the Agent Portal folder.	System Administrator
13	Restore SSA89s to Uploaded Files folder from VHD Backup.	System Administrator
14	Test all system are operational	System Administrator
15	Remove "Maintenance / Notification" page and notify COO that site is now operational.	System Administrator