|  |  |
| --- | --- |
| **Document Name** | **Business Continuity Policy** |
| **Version** | **0.1** |
| **Last Updated by** | **Anjaly T A** |
| **Approved By** | **Mohammed Riaz, Inderjit Singh Bedi** |
| **Released on** | **25-08-2022** |

Table of Contents

[1 Introduction 5](#_Toc112683266)

[2 Objective 5](#_Toc112683267)

[3 Scope 6](#_Toc112683268)

[4 Reference 6](#_Toc112683269)

[5 Stakeholders 6](#_Toc112683270)

[6 Xtracap Business Location 7](#_Toc112683271)

[6.1 Primary Location 7](#_Toc112683272)

[6.2 Alternative Operational Plan 7](#_Toc112683273)

[7 Maintenance of Procedure 7](#_Toc112683274)

[8 Strategy for Continuity of Business Plan (CoBP) 7](#_Toc112683275)

[9 Overview of the Continuity of Business Plan (CoBP) 7](#_Toc112683276)

[10 Recovery Prioritization 10](#_Toc112683277)

[Category I 10](#_Toc112683278)

[Category II 10](#_Toc112683279)

[Category III 10](#_Toc112683280)

[Category IV 10](#_Toc112683281)

[Category V 10](#_Toc112683282)

[11 RPO and RTO Error! Bookmark not defined.](#_Toc112683283)

[12 Procedure 10](#_Toc112683284)

[12.1 Disaster Recovery Process Flow 11](#_Toc112683285)

[12.2 Disaster Recovery Preparation 12](#_Toc112683286)

[12.3 Initiation of the Natural Disaster Recovery Plan (DRP) 12](#_Toc112683287)

[**12.3.1** **Activities depending upon the nature of loss** 13](#_Toc112683288)

[**12.3.2** **Damage Assessment and Salvage** 14](#_Toc112683289)

[**12.3.3** **Salvage Operations** 14](#_Toc112683290)

[**12.3.4** **Security** 15](#_Toc112683291)

[**12.3.5** **Information Dissemination** 15](#_Toc112683292)

[**12.3.6** **Infrastructure and Telecommunications** 15](#_Toc112683293)

[12.4 Disaster Recovery Plan (DRP) & Strategy for IT Network 16](#_Toc112683294)

[12.5 Disaster Recovery Plan (DRP) & Strategy for IT Software Segment 17](#_Toc112683295)

[12.6 Disaster Recovery Plan (DRP) & Strategy for Active Directory (Domain Server) 19](#_Toc112683296)

[12.7 Emergency Incident Response Plan 23](#_Toc112683297)

[**12.7.1** **Incident Definition** 24](#_Toc112683298)

[**12.7.2** **Incident Classification** 25](#_Toc112683299)

[**12.7.3** **Incident Severity Level** 25](#_Toc112683300)

[**12.7.4** **Incident Response** 26](#_Toc112683301)

# Introduction

Business survival in the current competitive environment necessitates planning for every type of business disruption including - but by no means limited to - the categories of natural disasters; hardware and communications failures; internal or external sabotage or acts of terrorism; and the failures of supply chain and sales affiliate organizations. While some business disruptions, may give advance warning others, such as terrorism, flash floods, fire, etc., can strike without notice. The threats that we (and by extension our clients) face today are more numerous and complex than those we have faced in the past. In addition, this is not going to change - tomorrow's threat environment will be much worse than todays. These disruptions usually affect the normal operations of the business, with results ranging from insured losses of replaceable tangibles to uninsurable capital losses, customer dissatisfaction, and even possible desertion.

The situation gets more complex with the growth of e-commerce and other factors, having driven system availability expectations toward 24 X 7. The average organization’s requirement for recovery time from a major system outage now ranges between 2 and 24 hours.

Xtracap being a customer-oriented organization with the philosophy of growing together with customers is sensitive to the impact that any such break down would have on its customer’s business and commitments. This has led to the formulation of a holistic approach to Disaster Management and Business Process Continuity for Xtracap as the Continuity of Business Plan. The purpose of the plan is to equip Xtracap to be able to respond to any type of situation - including those that we have not identified as a threat. To put in place management controls to respond quickly and to a plan as situations unfold.

# Objective

The objectives of a Business Continuity Plan are (but not limited to):

* To minimize interruptions to normal operations.
* To limit the extent of disruption and damage.
* To establish alternative means of operation in advance.
* To provide immediate solution for smooth and rapid restoration of service.

# Scope

The scope of the disaster recovery plan for the Xtracap office covers high impact risks.

High impact risks:

* Loss of access to office facilities due to
* political unrest/disturbances – medium probability, high impact
* Loss of office facilities due to
* Fire – Low probability, high impact
* Floods- Low probability, high impact
* Landslips/Subsidence - medium probability, high impact
* Loss of network connectivity - low probability, high impact

Scope excludes: Client-owned information resources exclusively governed by client’s own Disaster recovery and Business Continuity procedure. Also, area level disasters are outside the scope of BCP, but best efforts will still be made.

# Reference

* ISO/IEC 27001:2013

# Stakeholders

|  |  |
| --- | --- |
| **Stakeholders** | **Roles & Responsibility** |
| Director | * Handle communications with Media and all relevant stakeholders, * Approve Business Continuity Plans (BCP) and monitor its implementation at the time of disaster to ensure timely resumption of essential operations. |
| Leadership Team/  Emergency Management Team | * Members: Inderjit Singh Bedi, Nitin Verma, Pulkit Dham * Establishing & Implementation of their related part of this procedure to ensure that the above-mentioned objective is accomplished to meet the prime objective of ISMS Policy. * Provides support during the emergency. Makes recommendations on changes to the normal control procedures necessitated by the recovery process. Coordinates risk reduction and avoidance activities and emergency response with the DRC. |
| Human Resource Department | * Provides support for human resources elements of recovery and staff notification. |
| Finance Department | * Provides liaison to insurance carriers and claims adjusters. |

# Xtracap Business Location

## Primary Location

Xtracap Fintech

5th Floor, The Circle - Huda City Centre, Sector 29, Gurugram, Haryana 122002

## Alternative Operational Plan

As because of our setup and arrangement, we may operate virtually from any location as most of our key employees have been given Laptop and Internet Data cards. During emergencies they can take current backup from their laptop or connect to client’s server to continue their tasks, where copy of original data is also available.

# Maintenance of Procedure

Ensuring that the procedure reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect the updates, testing the updated Plan and training personnel. This Plan undergoes a formal review, at least once in a year, to confirm the incorporation of all changes since the previous review and the task is done by CISO. Further testing of BCP is also done once a year by use of either of simulation testing, walk-through, and checklist-based testing, etc.

# Strategy for Continuity of Business Plan (CoBP)

The Plan is predicated on the validity of the following assumptions:

* The situation that causes the disaster is localized to the facility of Operations and Systems in the current office premises of Xtracap Fintech at Gurugram.
* It should be noted however, that the Plan would still be functional and effective even in an area-wide disaster. Even though the basic priorities for restoration of essential services to the surrounding affected areas will normally take precedence over the recovery of an individual organization. Xtracap's Continuity of Business Plan can still provide for a more expeditious restoration of our resources for supporting key functions.
* The continuity of business plan is based on the availability of the hot sites or the back-up resources, as described in this document. The accessibility of these, or equivalent back-up resources, is a critical requirement.

# Overview of the Continuity of Business Plan (CoBP)

Xtracap recognizes the low probability of severe damage to Data Processing, Telecommunication, or Support Services capabilities at both Xtracap and any of its preferred vendors. Nevertheless, a plan like the COBP is necessary to identify the potential impact of such an incident on the assets of Xtracap and its clients.

In the event of a disaster affecting any of the functional areas, the Disaster Recovery Team serves as liaison between the functional area(s) affected and other external organizations providing major services. For the BCP purpose, following roles and representatives are identified as Disaster Recovery Team (DRT): -

|  |  |  |
| --- | --- | --- |
| **Role** | **Primary** | **Alternate** |
| Disaster Recovery Manager | Inderjit Singh Bedi | Nitin Verma |
| IT Network - Representative | Inderjit Singh Bedi | Nitin Verma |
| Administration - Representative | Mohammed Riaz | Inderjit Singh Bedi |
| Security – Representative | Inderjit Singh Bedi | Nitin Verma |
| IT Software – Representative | Nitin Verma | Pulkit Dham |
| HR – Representative | Mohammed Riaz | Inderjit Singh Bedi |
| Finance – Representative | Mohammed Riaz | Inderjit Singh Bedi |

**KEY MANAGERIAL PERSONNEL**

The Designation & Contact Information of Key Managerial Personnel is mentioned below:

|  |  |  |
| --- | --- | --- |
| **Name** | **Designation** | **Number** |
| Inderjit Singh Bedi | Head, Infra | 9899106810 |
| Nitin Verma | Head, IT | 8800997950 |
| Pulkit Dham | Senior Software Developer | 9634161986 |

**IMPORTANT Partner INFORMATION**

The Contact Information of Partners & Service providers to be Contacted during a Disaster is given below: -

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Contact Person** | **Number** |
| **IIFL** | IIFL Finance Limited, 802, 8th Floor, Hubtown Solaris, N. S. Phadke Marg, Vijay Nagar, Andheri East, Mumbai –400069 | ROMIL WARADE | 9960837143 |
| **Nupay** | UNITECH COMMERCIAL TOWER, First Floor, Unit 102, 2, Arya Samaj Rd, Phase 2, Greenwood City, Sector 45, Gurugram, Haryana 122003 | Nishant Mahajan | 999970791 |
| **Finbit** | Brigade IRV Centre, No. 73/1, Nallurahalli Village Borewell Road, Whitefield, K.R. Puram, Hobli Bangalore Bangalore KA 560066 IN | Debashish Raut | 9971735959 |
| Equifax | Unit 932, 3rd Floor, Building No 9, Solitaire Corporate Park, Andheri Ghatkopar Link Road, Andheri East, Mumbai 4000093 | Pooja Sontakke | 8591312961 |
| Iris | Tower 2, 3rd Floor  International Infotech Park  Vashi, Navi Mumbai 400703 | Gautam Mahanti | 9833242464 |
| Gupshup | Mumbai. 101 Silver Metropolis,1st Floor, Western Express Highway, Goregaon (E), Mumbai - 400063 | Santhosh Jigalmadi | **9742172704** |

# Recovery Prioritization

## Category I

* Restoring the API connectivity between the Bank and NBFC so that the payments are collected & disbursed smoothly.

## Category II

* Restoring the connectivity between various integration partners so that customer onboarding & management can start.

## Category III

* Tools used by the software development people.
* Applications that are used by the accounts department.
* Applications that are used by the IT Network department
* Application that are used by the HR department

## Category IV

* Application used by Quality Department
* Application used by Admin department

## Category V

* All other left-out things

# Procedure

The business continuity plan essentially requires infrastructure, system, people, and process management to be mobilized in case of any kind of contingency to re-locate the Offshore projects to alternate site to have the minimal impact on the business and to avoid reputation loss. The following sections describe the process of recovery of systems, people, and processes in times of disaster.

Disaster may be classified into 3 categories depending on the area affected due to it:

* Local - affecting systems, infrastructure & people at a particular location or in a designated part of the organization.
* Zonal - affecting the entire building due to factors such as fire, bomb blasts, etc;
* Regional - affecting the building and surrounding areas due to factors like major terrorist attack, political turmoil, earthquakes, floods etc.

The Disaster Recovery Team (DRT) is formed of the employees by management or CISO from the various practices/ work groups of the company and is authorized to decide on:

* Identifying critical activities and projects in line with DR & BCP.
* Mobilization of manpower to re-locate the project depending on the type of contingency.

## Disaster Recovery Process Flow

Response





Evacuate or Shelter-in-Place



Notify Public Authorities,

as needed

i

.

.

Fire or Police



Notify Disaster Recovery team Team

Leader or Alternate

**Information Technology**



Activate DR Plan



Move to alternate recovery site



Recover critical servers and applications



Switch network traffic

**Business Units**



Activate business continuity plans



Move to alternate recovery site



Perform manual work around procedures until

To recover systems

**Crisis Management Team**



Activate plan



Move to alternate recovery site



Provide ongoing support activities for IT and

Business Units during event

Is the event life

Threatening? ?

Does it

Present a significant risk? to

Emergency Event



**Disaster Recovery Team Leader**



Briefed on situation



Determine appropriate

Management response





Situation contained,

Resolved and documented



Management and Team

Members updated as

NO

YES





Activate Command

Center location



Contact remaining Crisis

Management Team



Determine extent of

Disaster

**Declare Disaster?**

NO





Reassess situation and

Document follow-up items



Management and Team

Members updated as

needed



Document any lessons

Learnt. Revise DR Plan if needed

YES

Recovered

* Return to Primary Site
* Management and Team Members updated

## Disaster Recovery Preparation

The Disaster Recovery Team (DRT) led by the Disaster Recovery Manager will:

* Get ready the list of all personnel's name and their telephone numbers.
* Keep a list of Key Managerial Personnel for business continuity
* Have the bridge number handy to get on the conference call.
* Make all personnel aware of their tasks and responsibilities.
* Maintain a list of hardware resources and desktops required.
* Maintain a list of software required for business continuity.
* Provide CDs of the software required to respective Manager and to the critical resources identified by them.
* Identify critical services without which work may be hampered.
* Identify critical services that need to be restored on priority – Internet, email, Vendor Domain, and VPN connectivity.
* Identify DR site/s that will be used when a disaster occurs. Keep direction to the DR site readily available.
* Identify any additional item that would be needed at the DR site so that it can be transported when required.
* Keep a list of primary vendors for assistance at the time of emergency
* The IT Software Representatives of the DRT are required to take backup of important files.
* The IT Software Representatives of the DRT to ensure data is regularly backed up as per backup policy.
* The IT Software Representatives of the DRT to Test and evaluate the DR plan regularly.

## Initiation of the Natural Disaster Recovery Plan (DRP)

Initiation of the DRP & CoBP is the responsibility of the DRT Manager or Director.

* Activate the **Damage Assessment Team** (DAT), which is a nominated team comprising of DRT members.
* Update the Director to initiate damage control exercises with the clients considering the criticality matrix
* Respective Communication Manager will inform the domestic clients about the impact of the damages and the immediate plans

### **Activities depending upon the nature of loss**

**Case 1 – Loss of Access to Office Premises – Xtracap Remains Functional**

Office is functional; however, accessibility of people to reach office is restricted.

* Respective Manager will identify the criticality of project and its deliverables.
* Manager will identify critical people who need to resume work.
* Manager will intimate critical people to resume work immediately - those having system, internet, and access to requisite VPN connectivity.
* DRT Leader will take decision with the team whether to use the DR site
* If a decision is taken not to use the business center but have people work from home, Manager will be required to do the following: -
  + Intimate critical people to resume work immediately - those having system, internet, and access to requisite VPN connectivity.
  + Arrange data cards for internet connection for those not having it. Manager will get in touch with the identified vendors to supply the same.
  + Arrange systems for those who have no system. Manager will coordinate with the vendor to provide hardware and the data card.
  + CDs with the software required to resume work will be made available to critical project team through courier or by reaching out.
  + Manager will request IT-Support/onsite counterpart to provide VPN access to those not having it and are critical to the delivery.

**Case 2 – Loss of Access to Office Premises –Xtracap is non-Functional**

* Respective Manager will identify the criticality of project and its deliverables.
* Manager will identify critical people who need to resume work.
* Manager will intimate critical people to resume work immediately - those having system, internet, and access to requisite VPN connectivity.
* DRT Leader will take decision with the team whether to use the DR site. If a decision is taken not to use the business center but have people work from home, Manager will be required to do the following: -
  + Arrange data cards for internet connection for those not having it. Manager will get in touch with the identified vendors to supply the same.
  + Arrange systems for those who have no system. Manager will coordinate with the vendor to provide hardware and the data card.
  + CDs with the software required to resume work will be made available to critical project team through courier or by reaching out.
  + Manager will request IT-Support/onsite counterpart to provide VPN access to those not having it and are critical to the delivery.

### **Damage Assessment and Salvage**

This subsection contains instructions to Disaster Recovery Team for disaster response, disaster assessment and recovery efforts.

* **Plan of Action**
  1. Disaster Recovery Manager to notify team members, and vendors to report to the site for initial damage assessment and clean up.
  2. Disaster Recovery Manager to notify insurance representative, if any.
  3. Disaster Recovery Manager to issue work-orders and call appropriate personnel.
  4. Take a service representative from each of the appropriate vendors, the insurance claims representative and appropriate department personnel into the site.
  5. Disaster Recovery Team members to review and assess the damage to the facility. List all equipment and the extent of damage. List damage to all support systems (power, A/C, fire suppression, communications, etc.).
  6. Disaster Recovery Team members to notify the Disaster Recovery Manager (DRM) and Director, as to the severity of the damage and what can potentially be salvaged.
  7. Disaster Recovery Team members to notify the Disaster Recovery Manager if the area can be restored to the required level of operational capability in the required timeframe.

### **Salvage Operations**

* **Plan of Action**

1. Disaster Recovery Manager to initiate the Emergency Notification List and have all Disaster Recovery Team members report to the Staging Area.
2. Disaster Recovery Team Have the Manager Administration to determine which equipment and furniture can be salvaged. Photograph all damaged areas as soon as possible for potential insurance claims.
3. Disaster Recovery Team Important \*\* before performing any salvage operation contact Insurance Team to coordinate with possible insurance claims requirements and appraisals.
4. Have the staff start salvaging any furniture and equipment.
5. Based upon advice from Insurance Team and Infrastructure team, contact computer hardware refurbishes regarding reconditioning of damaged equipment
6. Disaster Recovery Manager to meet with the Director to provide status on salvage operations.

### **Security**

This subsection contains instructions to the Security for disaster response and recovery efforts.

* **Plan of Action**
  1. The Security personnel to ensure that all facets of security protection Staff are afforded, relative to entry/exit controls, transportation of information, etc. at both the damaged and backup sites.

### **Information Dissemination**

* **Plan of Action**
  1. In instances where media are notified immediately, due to fire department or police involvement, the Director or person nominated by him, will proceed to the scene at once to gather initial facts. Emphasis must be placed upon getting pertinent information to the news media as quickly as possible.
  2. When appropriate, prepare news releases on a periodic basis for distribution to the local media list.
  3. If employee injuries or fatalities are involved, notify HR to send appropriate management personnel to the homes of the involved families.
  4. HR notifies Disaster Recovery Manager and Director as soon as families have been informed. This will permit the release of names and addresses of victims so that families of those not involved can be relieved of anxiety.
  5. To contact the hospitals where injured have been taken to coordinate the release of information.
  6. Coordinate follow-up news releases after the immediate emergency has passed to present Xtracap in as positive light as possible. Possible topics could include:
     1. What has been done to help employees?
     2. What are plans for disaster recovery?
     3. What are plans for business continuity?
     4. What are plans for reconstruction?
     5. What has been done to express gratitude to the community for its help?
     6. What has been done to prevent recurrence of this type of emergency?

### **Infrastructure and Telecommunications**

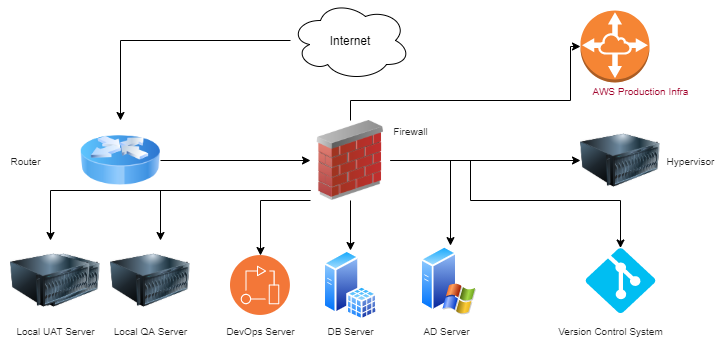
This subsection contains instructions to the Infrastructure and Telecommunications Systems team for disaster response and recovery efforts.

* **Plan of Action**

1. Receives report of disaster.
2. Oversees assessment of damage to infrastructure and telecommunications facilities. Directs contingency and recovery efforts. Provides updates to Disaster Recovery Team, Disaster Recovery Manager along with Top Management.
3. Arranges for telecommunications services to support critical functions. Procures stock to repair or replace damaged equipment. Restores full services in a timely manner.
4. Assists with restoration of cable and wire, as needed. Assists other departments with relocation and restoration of data facilities.

## Disaster Recovery Plan (DRP) & Strategy for IT Network

* **Network Diagram**



* **Monitoring & Alert : Yes**
* **Scenario: NETWORK DEVICE IS DOWN, SECONDARY BACKUP DEVICE AVAILABLE**
  + Action plan for network devices is as follows:

**Case 1 : Auto Transition Successful**

**Plan of Action :** There are two complete failure scenarios.

1. H/W Failure steps are as follows:-

1. Network team will decide whether complete hardware or only a part needs to be replaced.
2. Network team will coordinate the activity and will get the faulty H/W part replaced and if required will install software from location: File Location
3. After fixing the device Network team will test the device by accessing its URL, gateway, internet, and VPN.
4. Complete activity would take maximum 6 hours, which includes 4 hours SLA from vendor side and 2 hours for software installation.

2. S/W Failure

1. IOS can be reinstalled by using the dump kept at location: File Location
2. No configurations need to be done. This activity would take around 2 hours.

**Case 2 : Transition Unsuccessful**

**Plan of Action :** Steps are as follows: -

1. N/W team will manually make the device down.
2. Available Backup device will now route the traffic automatically otherwise manually change the route.
3. To recover faulty device, action will be as stated in CASE 1 above.

## Disaster Recovery Plan (DRP) & Strategy for IT Software Segment

* Xtracap employees have been given Laptop and Internet Data cards, hence during emergencies they can work from home and connect to VPN to continue their tasks.
* Containment strategy is also to be taken in the event of a disaster or service disruption to minimize the impact of any service disruption through a focus on keeping the operations running at the highest level of service possible.
* To smooth communication, it is imperative to have responsibilities clearly allocated, which is done as required and as follows: -

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Customer Account Manager (CAM) | * Single point of contact for customer during disaster or critical ticket. * Communication with customer during disaster or major incident, as required. (However, you may appoint someone as Communication SPOC). * Updates to Sr. Mgt after taking updates from BCP Lead. * Decision of invoking Plan B (Manual or alternative process) after taking inputs from BCP Lead and in consultation with customer. * Decision of reversal to Plan A from Plan B after taking inputs from BCP Lead and in consultation with customer. * Declare disaster and will invoke BCP team * Will appoint BCP Lead either from Application team or from IT team based on the disaster scenario. * Review and finalize RCA report after taking inputs from BCP Lead and submit to Sr. Mgt and Client. |
| BCP Lead | * Coordination with Application side and IT side BCP representatives; who further will take command in their respective areas. * Getting the BCP documentation created and tested before roll-out and its institutionalization. * Inputs and Updates to CAM & Service Desk during disaster or critical ticket. * Will help CAM take decision, whether to invoke Plan B if the resolution is uncertain or delayed. * Guide the client-side BCP coordinator how Plan B is to be executed and ensure progress. * Help CAM take decision during reversal of Plan A from Plan B. * Prepare RCA report after taking inputs from App and IT side coordinators and submit to CAM. |
| Application side  Coordinator | * Assist BCP Lead during disaster or critical ticket in context of Application and Database. * Working along with IT side Coordinator to identify the root cause and to take corrective measures. * Coordinate with application team members in order to identify the root cause and to take corrective measures or to activate Plan B. * Designing, documenting and validating BCP - from application side while coordinating with application team. |
| IT Side  Coordinator | * Assist BCP Lead during disaster or critical ticket in context of IT infra and connectivity related activities. * Working along with Application side Coordinator to identify the root cause and to take corrective measures. * Coordinate with ITISG team members in order to identify the root cause and to take corrective measures or to activate Plan B * External vendor Coordination, wherever required. * Designing, documenting and validating BCP - from IT side while coordinating with IT team. |
| Client side BCP Coordinator | * Activation of Plan B after Getting go-ahead from CAM. * Update BCP Lead on the progress. * Inputs / Assistance / Updates to CAM or BCP Lead for any validation to be done at customer-side. |

## Disaster Recovery Plan (DRP) & Strategy for Active Directory (Domain Server)

* **Scenario 1: OS corrupt, Hardware Failure and object deletion**
* Case 1: Operating System corrupted on DC1 server, System State Backup available.

STEPS:

1. Take Backup Active Directory DC1
2. Format the server DC1, & reinstall OS
3. Start server in DSRM mode.
4. Restore System State Backup on original Location (Non-Authoritative Restore), & restart in normal mode
5. Check DC health thru DCDIAG, NETDIAG, and replication through repadmin

STEP 1:

1. Open your command prompt by clicking Start and type "cmd" and hit enter.

1. In your command prompt type "wbadmin start systemstatebackup -backuptarget:e:" and press enter.
2. Note: You can use a different backup target of your choosing
3. Type "y" and press enter to start the backup process.
4. When the backup is finished running you should get a message that the backup completed successfully. If it did not complete properly you will need to troubleshoot.

STEP 2:

1. Now format the root drive C, and reinstall OS.
2. Reinstalled the OS to the same drive letter C as previously and with at least the same amount of physical drive space.

STEP 3:

1. Now restart the server, and after NetBIOS information press F8 key.
2. Now select the option Directory service restore Mode through arrow key, and press Enter key.
3. Now a Pop up Message will appear, click on OK.
4. When login prompt will appear enter administrator, in User Name box, and the password in Password box, click on OK.

STEP 4:

* + - * 1. To do this you will need to boot into DSRM (Directory Services Restore Mode) by restarting your server and pressing **F8** during the restart.
        2. Choose Directory Services Restore Mode from the Advanced Boot menu.
        3. Login to your server with your DSRM password you created during Active Directory installation.
        4. Once you're logged into your server and in DSRM safe mode, open a command prompt by clicking Start, type "cmd", and press enter.
        5. To make sure you restore the correct backup it's a good idea to use the "wbadmin get versions" command and write down the version you need to use.
        6. Now we need to perform a non-authoritative restore of Active Directory by typing "wbadmin start systemstaterecovery -version: “Date-time".

Note: The version of backup will vary depending on your situation. Type "y" and press enter to start the non-authoritative restore.

STEP 5:

1. Click on Start Run, and type cmd .
2. In command prompt type dcdiag /fix, and view the result.
3. Now type netdiag, and view the result.
4. To verify the replication type repadmin /showreps

* Case2: The server hardware damaged, restore domain controller on other server computer.

STEPS:

1. Take System State Backup of DC1
2. Install OS on second Server.
3. Restart server in DSRM mode.
4. Restore System State Backup on original Location (Non-Authoritative Restore).
5. Change the BURFLAG value to D2 to complete Non-Authoritative Restore.
6. Restart Computer/Repair OS.
7. Verify the existence of ClientProtocols key.
8. Verify the DNS record registration of this server through dcdiag & netdiag.

**STEP 1:**

1. Open your command prompt by clicking Start and type "cmd" and hit enter.

2. In your command prompt type "wbadmin start systemstatebackup -backuptarget:e:" and press enter.

1. You can use a different backup target of your choosing
2. Type "y" and press enter to start the backup process.
3. When the backup is finished running you should get a message that the backup completed successfully. If it did not complete properly you will need to troubleshoot.

**STEP 2:**

* 1. Reinstalled the OS to the same drive letter **C** as previously, with same installation folder, and with same physical amount.

**STEP 3:**

1. Now restart the server, and after ***BIOS*** information press ***F8*** key.
2. Now select the option ***Directory service restore Mode*** through arrow key, and press ***Enter*** key.
3. Now a Pop up Message will appear, click on ***OK.***
4. When login prompt will appear enter ***administrator,*** in ***User*** Name box, and the password in ***Password*** box, click on ***OK.***

**STEP 4:**

* + - 1. Once you're logged into your server and in DSRM safe mode, open a command prompt by clicking Start, type "cmd", and press enter.
  1. To make sure you restore the correct backup it's a good idea to use the "wbadmin get versions" command and write down the version you need to use.
  2. Now we need to perform a non-authoritative restore of Active Directory by typing "wbadmin start systemstaterecovery -version: “Date-time".
  3. Note: The version of backup will vary depending on your situation. Type "y" and press enter to start the non-authoritative restore.

**STEP 5:**

1. Click ***Start,*** and then click ***Run***
2. In the ***Open*** box, type ***regedit***, and then click ***OK.***
3. In the left pane expand ***My Computer.***
4. Expand ***HKEY\_LOCAL\_MACHINE***, and then expand ***SYSTEM*.**
5. Expand ***CurrentControlSet***, and then expand ***Services*.**
6. Expand ***NtFrs***, and then expand ***Parameters***
7. Expand ***Backup/Restore***, and then click ***Process at Startup***
8. In the right pane, right-click ***BurFlags***, and then click ***Modify***
9. In the ***Value data*** box, type ***d4***, and then click ***OK***

**STEP 6:**

1. Now restart the server in normal mode.
2. If server not restart in normal mode then an OS repair is required

**STEP 7:**

* 1. Click ***Start***, and then click ***Run***.
  2. In the ***Open*** box, type ***regedit***, and then click ***OK***.
  3. In the left pane, expand ***My Computer***.
  4. Expand ***HKEY\_LOCAL\_MACHINE***, and then expand ***SOFTWARE***.
  5. Expand ***Microsoft***, and then expand ***Rpc***
  6. Now verify the existence of key ***ClientProtocols***
  7. Now in right pane verify the existence of the following values:

Ncacn\_ip\_tcp REG\_SZ rpcrt4.dll

Ncacn\_nb\_tcp REG\_SZ rpcrt4.dll

Ncacn\_ip\_udp REG\_SZ rpcrt4.dll

Ncancn\_np REG\_SZ rpcrt4.dll

**STEP 8:**

1. Click on ***Start Run,*** and type ***cmd .***
2. In command prompt type ***dcdiag /fix***, and view the result.
3. Now type ***netdiag,*** and view the result.
4. To verify the replication type ***repadmin /showreps***

## Emergency Incident Response Plan

* This section of the document explains the importance of developing an incident response plan through a well-defined incident response framework. The framework comprises seven phases that ensure a consistent and systematic approach in handling such incidents. The details for each of the seven phases is summarized below:
  + **Phase 1 – Preparation:** In any incident response plan, it is essential to form an Incident Response Team (“IRT”) prior to other tasks. The role of the team is to promptly handle an incident so that it will have minimal impact to the business operation. The team is formed of members from various functional roles in your organisation. The process of setting up the team is explained in section 4.1.
  + **Phase 2 – Identification:** The occurrence of an incident is unpredictable. An anomaly in the system behaviour may indicate an incident or configuration errors. Hence, identifying an incident amidst routine daily operations is not an easy task. In section 4.2, some guidelines are provided to facilitate the process of positively identifying an intrusion incident.
  + **Phase 3 – Assessment:** After the identification phase, an initial assessment should be performed to confirm the existence of the incident. The assessment should include determining the scope, the impact of the incident, and the extent of the damage caused by the incident.
  + **Phase 4 – Containment:** Containment of the incident is necessary to minimise and isolate the damage incurred by your Company. In section 4.4, some guidelines are provided to help determine the appropriate course of action for limiting the extent of the incident.
  + **Phase 5 – Eradication:** In order to successfully eliminate the incident, the IRT need to determine the cause of the incident that resulted in the compromise of the system.
  + **Phase 6 – Recovery:** The recovery phase restores operations of the compromised system to facilitate the resumption of normal business operations. Prior to the resumption process, a validation check should be performed to ensure that the system is secured against any repeated incidents. Furthermore, the system should be placed under surveillance to ensure that if the perpetrator returns, unauthorised attempts may be detected early.
  + **Phase 7 – Follow-up:** As a follow-up, you should perform a post-mortem analysis of the compromised system to understand the weaknesses that resulted in the incident and other potential vulnerable areas. In the event that the Company is considering legal action against the perpetrator, it is recommended that forensic specialists and/or law enforcement agencies should be engaged to ensure that digital evidence are accumulated and preserved in a manner that is consistent with the legislative requirements.

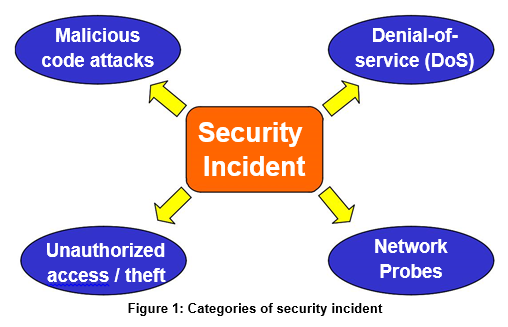
### **Incident Definition**

A security incident can be any of the following:

1. violation of an explicit or implied security policy
2. attempts to gain unauthorized access
3. unwanted denial of resources
4. unauthorized use of electronic resources
5. Modification without the owner’s knowledge, instruction, or consent.

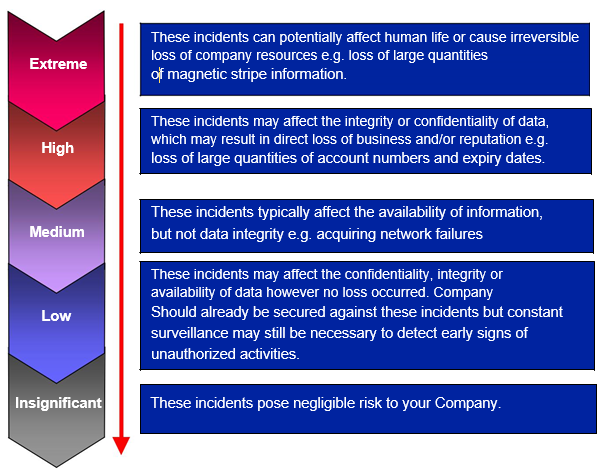
As an illustration, one of the security requirements in the Xtracap is to ensure that all vendor-supplied default system passwords should be changed. There are many websites that publish default passwords for many vendor products. One of the websites is http://www.astalavista.com. If an intruder compromises a router using its default password obtained from the above website, an incident has occurred. Using the compromised device, further exploits may be launched against other systems or network devices in the IT infrastructure.

### **Incident Classification**



### **Incident Severity Level**

Once classification of the incident has occurred, the severity level of the incident can be determined. The severity level of the incident will dictate the course of actions that should be performed to resolve the incident. The following five severity levels may be assigned to the incident:



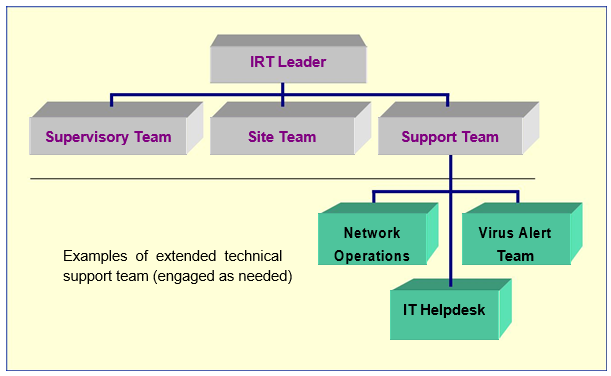
### **Incident Response**

The objective of an incident response is to provide a systematic approach in developing an incident response plan. A well-defined incident response plan will enable you to handle any incident efficiently and effectively with minimal impact to the business operations. When developing these plans, efforts must be made to anticipate scenarios before they happen, and to make the following decisions in advance:

1. Where did the incident happen?
2. Which areas of the business processes are affected?
3. Who should be notified?
4. What are the procedures/actions to be taken?
5. How should the procedures/actions be performed?

#### **Preparation**

An Incident Response Team (IRT) is made up of senior management and experienced people – these are immediately made, which are comprises of the stakeholders discussed above or as needed from the organization. The role of the IRT is to promptly handle an incident so that containment, investigation and recovery can quickly occur. The IRT should be empowered by the top management to have decision-making authority for facilitating the incident response process. The needs and resources of the company also play a part in the selection of the team members. Below picture illustrates an overview of the team structure in IRT:



* IRT Leader : Inderjit Singh Bedi
* Supervisory Team Leader : Nitin Verma
* Supervisory Team Member :Pulkit Dham

*Note: More people may be added as needed.*

The responsibility of the Supervisory Team includes:

1. Making decisions on, and reviewing steps taken to rectify matters
2. Communicating and translating technical information to senior management or board of directors
3. Supervising and reviewing test results based on the tests conducted to verify the feasibility and effectiveness of the incident response procedures
4. Cooperating with and supplying information to the support team so that their duties can be carried out
5. Coordinating resources, e.g. software and hardware acquisition, if required
6. Maintaining proper records of events and actions taken
7. Attending, establishing and conducting training for relevant personnel
8. Performing scenario planning and identifying corrective actions for each scenario; and
9. Supervising and reviewing the update, including lessons learnt, on the Incident Response Procedures.

The responsibility of the Site Team includes:

* 1. Surveying and securing the systems and environment
  2. Containing the incident
  3. Eradicating incident and performing recovery procedures
  4. Compiling “recovery kit”, e.g. recovery procedures, contact list, boot disks, software, tools, hard disk, and so on
  5. Attending and conducting training for relevant personnel and
  6. Updating and maintaining the Incident Response Procedures.

The responsibility of the Support Team includes:

1. Providing logistic and technical support to other IRT teams when required
2. Updating public and relevant authorities via commercial press, web sites, telephone and others, and
3. Coordinating communications for the company with various external parties, if required.

A leader will be appointed in the IRT as the point of contact in the event of an incident. When an incident is reported by the helpdesk, the leader will be responsible for contacting the relevant sub-teams to handle the incident.

When reporting the incident, communication should be made via the telephone, etc. This is to prevent interception of emails by the perpetrator if the computer used for sending the email has been compromised or by a “sniffer” program that has been planted on the network to capture information sent across the network. Should sensitive electronic media need to be passed to a third party (e.g. listings of account numbers that were leaked) this may be done via secure courier. However the media must be strongly encrypted.

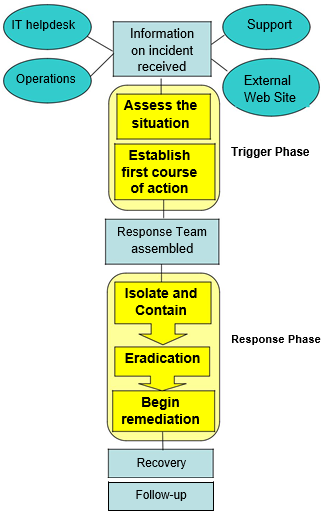
Depending on situation, support from other technical teams in the Company (e.g. the network operations, anti-virus team or IT helpdesk) may be required to assist in the incident handling process.

#### **Identification**

The cost of incident response and recovery can be high. When a staff member notices a suspicious anomaly in data, a system, or the network, the IRT must perform investigation and verification, which is time and resource consuming. This activity is at risk if the number of false reports exceeds the number of real incidents that occurred, as it diverts resources away from real incidents. To facilitate the task of identification, the following is a list of typical symptoms of security incidents, which include any or all the following:

* 1. A system alarm or similar indication from an intrusion detection tool
  2. Suspicious entries in system or network accounting (e.g. a UNIX user obtains root access without going through the normal sequence)
  3. Accounting discrepancies (e.g. an eighteen-minute gap in the accounting log with no entries)
  4. Repetitive unsuccessful logon attempts within a short time interval
  5. Unexplained new user accounts, new files or unfamiliar file names
  6. Phishing messages
  7. Unexplained modifications to file lengths and/or dates, especially in system executable files
  8. Unexplained attempts to write to system files or changes in system files
  9. Unexplained modification or deletion of data
  10. Denial/disruption of service or inability of one or more users to login to an account
  11. Ransomware attack
  12. Poor system performance of dedicated servers
  13. Operation of a program or sniffer device to capture network traffic
  14. Unusual time of usage (e.g. users login during non-working hours)
  15. An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user, and
  16. Unusual usage patterns (e.g. programs are being compiled in the account of a Finance user with no programming background).

Although no single symptom conclusively shows that a security incident is taking place, observing one or more of these symptoms prompts the observer to investigate events more closely. System administrators who encounter one or more of these symptoms should work with the IRT to determine the cause of the incident. Using the above-mentioned categories of incidents as reference, the IRT should validate security incidents on a per case basis before proceeding with the other phases in the framework. All details in the Identification phase should be documented in the Incident Reporting Form.



#### **Assessment**

The next step to be taken by the IRT is to assess the scope, the impact and the magnitude of the incident. As a note of precaution, never power off or reboot a compromised system immediately as this may result in the loss of data, information or evidence required for forensic investigation later. The following are some of the factors to consider during the assessment:

1. How many computers are affected by this incident?
2. Is sensitive information involved?
3. What is the entry point of the incident (e.g. network, phone dial)?
4. What is the potential damage caused by the incident?
5. What is the estimated time to recover from the incident?
6. What resources are required to manage the situation?
7. How should the assessment be performed effectively?

Depending on the severity of the situation, top management may have to be informed. Notification guidelines should be developed by the IRT during the preparation of the incident response plan. For “Extreme” and “High” risk incidents, the IRT should escalate them to Visa. The Incident Reporting Form can be used to document the information gathered from the assessment.

#### **Containment**

The objective of the containment phase is for the IRT to regain control of the situation by limiting the extent of the damage. The IRT may consider isolating the compromised system from the rest of the network systems. However, this may disrupt the business operation if the compromised system is critical or many systems were affected by the incident, as in the example of a virus outbreak. Hence, the IRT must evaluate with the management on a per case basis the risk of continuing operations versus regaining control of the compromised system. All attempts to contain the threat must consider every effort to minimize the impact to the business operations.

Furthermore, a backup should also be performed on the system to maintain the current state of the system to facilitate the post-mortem and forensic investigation later. The IRT may also consider changing the system passwords to prevent the possibility of Trojan programs being installed on the compromised system that allows the intruder from returning to the system via a backdoor.

#### **Eradication**

After the containment phase, further investigation should be performed to uncover the cause of the incident by analyzing system logs of various devices (e.g., firewall, router, host logs). It is important that the IRT uses a separate set of administrative tools for the investigation and not those in the compromised system. If the perpetrator has modified the system configuration, execution of any system tools may have dire consequences. For example, the intruder may have modified the DOS CMD.EXE application of the compromised system to delete all files in the system rather than to return a command shell.

A clean operating system should be reloaded into the compromised server after the investigation. Many off-the shelf operating systems are not developed with security in mind. Hence, to increase the security defence of the system, it must undergo a hardening process, which should include:

1. Applying all the latest patches
2. Disabling any unnecessary services
3. Installing anti-virus software, and
4. Applying the Company’s security policy to the system.

#### **Recovery**

Prior to restoring the system from a clean backup, it is recommended that the IRT validate that the eradication procedures have been properly performed. After installing the backup, the system should be monitored in a test environment to determine if it is functioning normally before it can be restored into the business operation.

#### **Documentation and Records**

All details related to the incident response process should be documented and filed for easy reference. This provides valuable information to unravel the course of events and can serve as evidence if prosecution of intruders is necessary. It is recommended that the following items be maintained:

* + 1. All system events (audit records)
    2. All actions taken (including the time that an action is performed), and
    3. All external conversations (including person with whom the discussion was held, the date and time and the content of the conversation).

Furthermore, an incident report documenting the following should be written by the IRT at the end of the exercise:

* + 1. A description of the exact sequence of events
    2. The method of discovery
    3. Preventive measure put in place, and
    4. Assessment to determine if the recovery step taken is sufficient and what other recommendations need to be considered

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learnt, to improve on the identified areas and used as reference for future incidents.