**IT Business Continuity Plan**

Developed and maintained by

The Information Technology Department

Table of Contents

**Introduction3**

Objectives3

Precedence3

Future Changes3

Layout & Use3

**Company Contacts4**

**Vendor Contacts4**

**RISKS4**

Active Directory4

Anti-virus5

Backup6

Database7

FTP8

**INTRODUCTION**

**Objectives**

The objectives of this plan are:

* To ensure that maximum possible service levels are maintained
* To ensure that we recover from interruptions as quickly as possible
* To minimize the likelihood and impact (risk) of interruptions

**Precedence**

*The Company’s general, security and IT procedures override these instructions if there are any conflicts.*

**Future Changes**

These plans will change in response to new business and client needs and new technology. Please refer all requests for changes to the IT department.

**Layout & Use**

* *Risk* – the application or equipment failure
* *Impact* – will the impact on our business be high, medium or low?
* *Functions Affected* – what document-related functions the problem impacts
* *Maximum tolerable outage* – Maximum time that this service can be down
* *Decision to invoke DR* – the time taken to implement DR so as to resume services.
* *DR Configuration* – the DR configuration in place for that particular service.
* *Data Recovery Point* – in case of data loss, the latest available data recovery.
* *Action* – Various actions to be undertaken for resume of service.
* *Responsibilities* – who takes what actions
* *Resources* – the implications for costs, staffing, facilities etc
* *Contact Details* – of support staff involved in enabling of DR.

**Company Contacts**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Department | Telephone | Email ID |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**RISKS**

|  |  |
| --- | --- |
| **Application at Risk** | **Active Directory** |
| **Impact** | High |
| **Functions affected** | All users |
| **Maximum Tolerable Outage (MTO)** | 2 hours |
| **Decision to invoke DR** | NA |
| **DR configuration** | **Application:**  The Active Directory (AD) domain Grant Investrade Ltd. (GIL) users is ‘grant-hits. Local’ which is child Domain of the AD forest where root is ‘hindujamedia.net’. Domain controllers, their roles and locations as follows:   1. **Media.** 2. **Mumbai.** 3. *GRANTHITSDC*   Roles:   1. RID Master 2. PDC Master 3. Infrastructure Master 4. Global Catalog 5. *GIL-ADC-BC-01*   Roles:   1. Global Catalog 2. **Noida.** 3. *GIL-ADC-BC-02*   Roles:   1. Global Catalog   Daily Differential, Weekly, Monthly & Quarterly full backup taken. Weekly, Monthly and Quarterly backup tape kept in Locker |
| **Data Recovery Point** | Latest. |
| **Action** | **Application failure:**  The above configuration, by default is redundant. In case of failure of one server, AD can be restored by running dcpromo and the specific AD FSMO role can be transferred or seized using NTDSUTIL.  **Database failure:**  Active Directory data is regularly replicated between the DC. In case of major failure restore Data from the latest Daily Incremental, Weekly, Monthly & Quarterly full backup, Daily off-site backup taken.  **Server Hardware failure:**  Run DCPROMO onto a temporary desktop and replicate data or restore server from the latest available BSR copy.  **LAN access failure:**  Users can not connect via VPN; local LAN failure has to be rectified.  **Datacenter failure:**  The above configuration, by default is redundant. In case of failure of one server, AD can be restored by running DC promo and the specific AD FSMO role can be transferred or seized using NTDSUTIL. |
| **Responsibilities** | IT Team |
| **Resources** | BSR Boot CD – \\172.21.10.24\Backup1\BESR\Symantec Boot CD.iso  BSR Data –\\172.21.10.24\Backup1\GHITS AD.  Symantec Backup Job: File backup on tape (Weekly, monthly, daily) |
|  |  |

|  |  |
| --- | --- |
| **Application at Risk** | **Antivirus** |
| **Impact** | High |
| **Functions affected** | Backup of Data |
| **Maximum Tolerable Outage (MTO)** | 12 hours |
| **Decision to invoke DR** | 1 hour |
| **DR configuration** | **Application:**  The application is installed on server GI-M-KI-AV001 - (192.168.188.6) in stand-alone mode. Server BSR is taken every month.  **Database:**  The SQL database is installed on server GI-M-KI-AV001 – with ePO\_GI-M-KI-AV001 DB name. |
| **Data Recovery Point** | EPD – End of previous day. |
| **Action** | **Application failure:**  Call McAfee support for troubleshooting. If the application is not recoverably, use the latest copy of BSR and restore on the server, apply the latest patches of the application.  **Database failure:**  Restore Data from the latest Daily Incremental, Weekly & Monthly full backup taken.  **Server Hardware failure:**  Restore the earliest BSR server copy onto a temporary server.  **Datacenter failure:**  Restore the earliest BSR server copy onto a temporary server. Restore data from the latest available backup set; Change the DNS settings to reflect the new IP address. Check whether the clients can connect to the server for updates. |
| **Responsibilities** | IT Team, McAfee. |
| **Resources** | BSR Boot CD – \\172.21.10.24\Backup1\BESR\Symantec Boot CD.iso  BSR Data CD – \\172.21.10.24\Backup1\BESR\GI-M-KI-AV001  SYMANTEC Backup Job: Database backup (Weekly, monthly, daily) |

|  |  |
| --- | --- |
| **Application at Risk** | **Backup Server** |
| **Impact** | High |
| **Functions affected** | Backup of Data |
| **Maximum Tolerable Outage (MTO)** | 12 hours |
| **Decision to invoke DR** | 1 hour |
| **DR configuration** | **Application:**  The application is installed on server GIL-BKP01 - (172.21.30.35) in stand-alone mode.  **Database:**  The HPDP Internal database is installed locally on the same server. Daily Incremental, Weekly & Monthly full backup taken. Monthly backup tape. |
| **Data Recovery Point** | EoD – End of previous day. |
| **Action** | **Application failure:**  Call HPDP support for troubleshooting. If the application is not recoverably, use the latest copy of BSR and restore on the server, apply the latest patches of the application.  **Database failure:**  Restore Data from the latest Daily Incremental, Weekly & Monthly full backup taken.  **Server Hardware failure:**  Restore the earliest BSR server copy onto a temporary server with sufficient disk space. |
| **Responsibilities** | IT Team, Symantec |
| **Resources** | BSR Boot CD – \\172.21.10.24\Backup1\BESR\Symantec Boot CD.iso  BSR Data CD – \\172.21.10.24\Backup1\BESR\GIL-BKP01  SYMANTEC Backup Job: Database backup (Weekly, monthly, daily) |

|  |  |
| --- | --- |
| **Application at Risk** | **Database** |
| **Impact** | High |
| **Functions affected** | All users – |
| **Maximum Tolerable Outage (MTO)** | 1 hour |
| **Decision to invoke DR** | 30 Minutes |
| **DR configuration** | **Application:**  The Database server is installed on server’s gildbadm01 - (172.21.50.201) & gildbadm02 - (172.21.50.202) in a two Cluster node (active/active). There are two instances installed on these servers; GILPROD and IMCLMQPROD.  Daily Incremental, Weekly, Monthly & Quarterly full backup taken. Monthly backup tape sent to Locker.  The applications connecting to the Database servers are as follows:  ICC SMS and MQ SMS |
| **Data Recovery Point** | EoD – End of previous day. |
| **Action** | **Application failure:**  Since reinstalling the SQL server is an elaborate process, restore the server using the latest available BSR copy.  **Database failure:**  Restore Data from the latest Daily Incremental, Weekly, Monthly & Quarterly full backup.  **Server Hardware failure:**  Restore server from the latest available BSR copy.  **LAN access failure:**  LAN failure needs to be rectified.  **Datacenter failure:**  One a temporary computer, install the SQL server enterprise edition software and Restore Data from the latest Daily Incremental, Weekly, Monthly & Quarterly full backup. |
| **Responsibilities** | IT Team, Oracle |
| **Resources** | – \\172.21.10.24\Backup4.  SYMANTEC Backup Job: Database backup (Weekly, monthly, daily) |

|  |  |
| --- | --- |
| **Application at Risk** | **FTP** |
| **Impact** | High |
| **Functions affected** | All users –. |
| **Maximum Tolerable Outage (MTO)** | 1 hour |
| **Decision to invoke DR** | 30 Minutes |
| **DR configuration** | **Application:**  The FTP application is installed on server GIL-KI-FS01- (192.168.188.8) and NAT to public IP 0.0.0.0. Daily backup of the FTP directories is taken. This includes the FTP data, system state, shadow copy components and Inetpub directory (this will include IIS configuration, registry entries and IIS files). Server BSR taken once in a month.  **Remote Connectivity for users:**  All users can access the FTP via internet at address <ftp://nxtftp.nxtdigital.in/> |
| **Data Recovery Point** | Last One hour |
| **Action** | **Application failure:**  Reinstall IIS; restore the system state, shadow copy components and the Inetpub directory.  **Database failure:**  Restore data from the latest hourly FTP backup  **Server Hardware failure:**  Restore server from the latest available BSR copy.  **LAN access failure:**  Laptop users can use data cards to connect the FTP server.  **Datacenter failure:**  At an alternative location, restore server from the latest available BSR copy, restore data from the latest hourly FTP backup. NAT the local IP to an available public IP and change the DNS settings to the new public IP. |
| **Responsibilities** | IT Team |
| **Resources** | BSR Boot CD – \\172.21.10.24\Backup1\BESR\Symantec Boot CD.iso  BSR Data CD – [\\172.21.10.24\Backup1\FTP Data Backup\WindowsImageBackup\GI-M-KI-FS001](file:///\\172.21.10.24\Backup1\FTP%20Data%20Backup\WindowsImageBackup\GI-M-KI-FS001)  BSR Data CD - \\172.21.10.24\Backup1\BESR\FTP\_BACKUP\D Drive\GI-M-KI-FS001\File Backup Data |

|  |  |
| --- | --- |
| **Application at Risk** | LCO Portal |
| **Impact** | High |
| **Functions affected** | All users –. |
| **Maximum Tolerable Outage (MTO)** | 1 hour |
| **Decision to invoke DR** | 30 Minutes |

|  |  |
| --- | --- |
| **DR configuration** | Application  The LCO Portal installed on GIL-WEBH6-LCO01 (172.21.60.73) ,GIL-WEBH7-LCO02 (172.21.60.74), IMCL-SMSH1-LCO03(172.21.60.93) , IMCL-SMSH2-LCO04 (172.21.60.94), GIL-WEBH6-CP03(172.21.60.77), GIL-WEBH7-CP04 (172.21.60.78) and IMCL-EMRF (172.21.60.40) & Backup of All Portals is taken. This includes Whole OS on Tape drivers. Backup taken every Week, Month & Quarterly.  **Remote Connectivity for users:**  All users can access the LCO Portal via internet at address <https://lcoportal.nxtdigital.in/login.php>  <https://lcoportal2.nxtdigital.in/login.php>  <https://lcoportal3.nxtdigital.in/login.php>  <https://lcoportal40.nxtdigital.in/login.php>  <https://172.21.60.78/login.php?exp=1>  <https://172.21.60.77/login.php?exp=1>  <http://172.21.60.40/INCABLE/> |
| **Data Recovery Point** | Last One hour |
| **Action** | **Application failure:**  Restore the system state, restart httpd service |
| **Responsibilities** | IT Team |
| **Resources** | LTO Tape |