|  |
| --- |
| Hexagonal background with blue neon lights |
| <Project Name>  Last Updated: <date> |
| |  |  |  | | --- | --- | --- | |  |  |  | |

Contents

[**Introduction** 2](#_Toc97717787)

[**Type of System** 2](#_Toc97717788)

[**Definition of a Disaster for this DRP** 2](#_Toc97717789)

[**Purpose** 2](#_Toc97717790)

[**Scope** 3](#_Toc97717791)

[**Version Information or Changes** 3](#_Toc97717792)

[**Mandates, Policies, Obligations and References** 3](#_Toc97717793)

[**Disaster Recovery Teams & Responsibilities** 4](#_Toc97717794)

[**Disaster Recovery Lead(s)** 4](#_Toc97717795)

[**Disaster Management Team** 5](#_Toc97717796)

[**Network Team** 5](#_Toc97717797)

[**Server Team** 6](#_Toc97717798)

[**Applications Team** 7](#_Toc97717799)

[**Vendor Team** 8](#_Toc97717800)

[<business area name> **Senior Management Team** 8](#_Toc97717801)

[**Data and Backups** 9](#_Toc97717802)

[**Restoring IT Functionality** 9](#_Toc97717803)

[**Current System Architecture** 9](#_Toc97717804)

[**IT Systems** 10](#_Toc97717805)

[**Impacts of Risks** 10](#_Toc97717806)

[**Plan Testing & Maintenance** 10](#_Toc97717807)

[**Maintenance** 11](#_Toc97717808)

[**Testing** 11](#_Toc97717809)

[**Appendix A: Scenarios** 11](#_Toc97717810)

**<name of project or solution here>**

# **Introduction**

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the IT information that describes <business area name> ability to withstand a disaster as well as the processes that must be followed to achieve IT disaster recovery as it relates to the <application or solution name>. **NOTE:** This disaster plan will only focus on IT Disaster Recovery and is a compliment to <business area name> standard Business Continuity Plan (BCP). All items not IT related have been removed.

**Type of System:** <indicate criticality of the system i.e., mission critical | this information can be found in your STRA>

# **Definition of a Disaster for this DRP**

Disasters for this DRP are defined two ways:

1. Any event that manifests as a creeping operational problem, that exceeds SLAs and OLAs, is deemed “likely”, and could result in “Significant”, “Major”, or “Severe/Catastrophic” impacts to BC Prosecution Services IT infrastructure and our ability to delivery services, may trigger a disaster declaration.
2. If a provincial level disaster is declared by Emergency Management BC, the Provincial Emergency Coordination Centre (PECC) is activated.  In turn, the IT Operations Centre within our ministry is activated to support the PECC.  <business area name> awareness of a provincial disaster declaration will, at minimum, trigger assessment of the threat and impact on our IT infrastructure and our ability to deliver <business area name> services. If potential or known impacts to IT infrastructure exceed SLAs and OLAs, are deemed “likely”, and could result in “Significant”, “Major”, or “Severe/Catastrophic”, a disaster declaration by <business area name> staff with the authority to do so may be triggered. The IT Operations Centre in a provincial emergency is our conduit to the PECC.

# **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. Note that in the event of a disaster the first priority of <business area name> is to prevent the loss of life. Before any secondary measures are undertaken, <business area name> will ensure that all employees, and any other individuals on the organization’s premises, are safe and secure.

After all individuals have been brought to safety, the next goal of <business area name> in partnership with Ministry of Attorney General (AG) Information Systems Branch (ISB) 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 <name of solution> Solution DRP takes all of the following areas into consideration:

* Network Infrastructure
* Servers Infrastructure
* Data Storage and Backup Systems
* Data Output Devices
* Organizational Software Systems
* Database Systems
* IT Documentation

This DRP does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters.

# **Version Information or 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, <business area name> 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** |
|  |  |  | *1.0* | *Initial version of DR Plan* |
|  |  |  |  |  |
|  |  |  |  |  |

# **Mandates, Policies, Obligations and References**

* [BC Government Information on Business Continuity and Disaster Recovery Plan](https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-directives/business-continuity-and-disaster-recovery-plan)
* [Emergency Management BC](https://www2.gov.bc.ca/gov/content/safety/emergency-management/emergency-management)

**Policies**

* **Risk Rating Table:** <http://gww.fin.gov.bc.ca/gws/pt/rmb/ref/RMB_ERM_Guideline.pdf>
* [CPPM Policy Chapter 16: Business Continuity Management](https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/policies/business-continuity-management)

**Legal Obligations**

* <add information here or indicate n/a>

# **Disaster Recovery 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 employees of <business area name>. The different groups and their responsibilities are as follows:

* Disaster Recovery Lead(s)
* Disaster Management Team
* Network Team
* Server Team
* Applications Team
* Vendor Team
* Management Team
* Note - All other roles will be contained in <business area name> Business Continuity Plan (BCP)

The lists of roles and responsibilities in this section have been created by <business area name> 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(s)**

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 <business area name> 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 <business area name>.

**Role and Responsibilities – ISB Client Services Manager**

* Advise <business area name> that 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.

**Role and Responsibilities –** <business area name>

Consult with the ISB Client Services Manager and provide authorization that the DRP should be triggered.

**Contact Information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **Disaster Management Team**

The Disaster Management Team that will oversee the entire disaster recovery process. They will be the first team that will need to take action in the event of a disaster. This team will evaluate the disaster and will determine what steps need to be taken to get the organization back to business as usual.

**Role & Responsibilities**

* Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
* Determine the magnitude and class of the disaster
* Determine what systems and processes have been affected by the disaster
* Communicate the disaster to the other disaster recovery teams
* Determine what first steps need to be taken by the disaster recovery teams
* Keep the disaster recovery teams on track with pre-determined expectations and goals
* Keep a record of money spent during the disaster recovery process
* Ensure that all decisions made abide by the DRP and policies set by <business area name> and Ministry of Attorney General (AG) Information Services Branch
* Get the secondary site ready to restore business operations
* Ensure that the secondary site is fully functional and secure
* Create a detailed report of all the steps undertaken in the disaster recovery process
* Notify the relevant parties once the disaster is over and normal business functionality has been restored
* After <business area 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** | **Email** | **Mobile Phone Number** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **Network Team**

Both AG Information Systems Branch (ISB) and OCIO provides server support and should be contacted via AG Service Desk at 250-356-0545. They will direct whether OCIO needs to be contacted at 250-387-7700. The ISB Client Services Manager will initiate the process.

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network 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 network services are not functioning at the primary facility
* If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.
* If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.
* In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility
* Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order: o
  + All members of the DR Teams
  + All executive employees
  + All IT employees
  + All remaining employees
  1. • Install and implement any tools, hardware, software, and systems required in the standby facility
  2. • Install and implement any tools, hardware, software, and systems required in the primary facility
  3. • After <business area name> is back to business as usual, this team will be summarizing 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** | **Email** | **Mobile Phone Number** |
| AG Service Desk | Service Desk for the Justice and Public Safety Sector | 250-356-0545 | [jag.sd@gov.bc.ca](mailto:jag.sd@gov.bc.ca) | n/a |
|  | ISB Client Services Manager |  |  |  |

## **Server Team**

Both AG Information Systems Branch (ISB) and OCIO provides server support and should be contacted via AG Service Desk at 250-356-0545. They will direct whether OCIO needs to be contacted at 250-387-7700. The ISB Client Services Manager will initiate the process.

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 <business area name>’s 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 <business area name> is back to business as usual, this team will be summarizing 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** | **Email** | **Mobile Phone Number** |
| AG Service Desk | Service Desk for the Justice and Public Safety Sector | 250-356-0545 | [jag.sd@gov.bc.ca](mailto:jag.sd@gov.bc.ca) | n/a |
|  | ISB Client Services Manager |  |  |  |

## **Applications Team**

AG Information Systems Branch (ISB) and NTT Data (Vendor Team) provides application support and should be contacted via AG Service Desk at 250-356-0545. ISB Client Services Manager will initiate the process.

The Applications Team will be responsible for ensuring that all enterprise applications operate 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 facilities, the team will determine which applications are not functioning at the primary facility
* 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 <business area name> is back to business as usual, this team will be summarizing 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** | **Email** | **Mobile Phone Number** |
| AG Service Desk | Service Desk for the Justice and Public Safety Sector | 250-356-0545 | [jag.sd@gov.bc.ca](mailto:jag.sd@gov.bc.ca) | n/a |
|  | ISB Client Services Manager |  |  |  |

## **Vendor Team**

The Vendor Team will be responsible for working with ISB, <business area name> and any other resources that will aid in the recovery of the solution.

**Contact Information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Email** | **Mobile Phone Number** |
|  |  |  |  |  |
|  |  |  |  |  |

## <business area name> **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 make by the Senior Management Team. The Disaster Recovery Lead will ultimately report to this team.

**Role & Responsibilities**

* Ensure that the Disaster Recovery Team Lead is help accountable for his/her role
* 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 the primary facilities
  + Rebuilding of data centers
  + Significant hardware and software investments and upgrades
  + Other financial and business decisions

**Contact Information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Email** | **Mobile Phone Number** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **Data and Backups**

In this section it is important to explain where the organization’s data resides. Discuss the location of all the organization’s servers, backups and offsite backups and list what information is stored on each of these.

**Data in Order of Criticality**

Please list all of the data **used in this IT solution** in order of their criticality. Add or delete rows as needed to the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rank** | **Data** | **Data Type** | **Back-up Frequency** | **Backup Location(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **Restoring IT Functionality**

Should a disaster actually occur and <business area name> need 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 <business area name> information system will be recovered.

This section will contain all of the information needed for the organization to get back to its regular functionality after a disaster has occurred. It is important to include all Standard Operating Procedures documents, run-books, network diagrams, software format information etc. in this section.

## **Current System Architecture**

In this section, include a detailed system architecture diagram. Ensure that all of the organization’s systems and their locations are clearly indicated.

<add architecture or solution design here>

## **IT Systems**

Please list all of the IT components of the Solution that will need to be brought back online in the event of a disaster. Add or delete rows as needed to the table below.

**Authentication (Multi-Factor Authentication, Certificates, iKey etc.)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IT System Components** | **System Components** | **Key Contact** | **Maximum Allowable Outage Time** | **List information about the component** | **What is the process to restore?** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Infrastructure Scenarios (Network Zones, Database’s, Backup’s etc.)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IT System Components** | **System Components** | **Indicate**  **Manual Workaround** | **Maximum Allowable Outage Time** | **List information about the component** | **What is the process to restore?** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **Impacts of Risks**

Document the known risks that could cause disruptions to IT services, applications, and processes. For example, a server room that does not have a backup source of power will mean that services will not be available during a power outage. Specify the implications if the risk occurs and whether or not a strategy needs to be developed to address the risk.

**See Appendix A.**

# **Plan Testing & Maintenance**

While efforts will be made initially to construct this DRP is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

## **Maintenance**

The DRP will be updated any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

* Edit this list as required
* Ensuring that call trees are up to date
* Ensuring that all team lists are up to date
* Reviewing the plan to ensure that all of the instructions are still relevant to the organization
* Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals
* Ensuring that the plan meets any requirements specified in new laws
* Other organizational specific maintenance goals

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

## **Testing**

<business area name> is committed to ensuring that this DRP is functional. The DRP should be tested every <<indicate frequency>> in order to ensure that it is still effective. Testing the plan will be carried out as follows:

**Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).

Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

# **Appendix A: Scenarios**

| **Scenario** | **Likelihood**  **(1-5)** | **Level of Impact**  **(1-5)** | **Risk Rating**  **(Low, Med, High, Extreme)** | **Known Risk** | **Impact of Risk** | **Dependent Parties** | **Prevention Strategy** | **Recovery**  **Strategy** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |