SAMPLE STANDARDS AND REQUIREMENTS

Sample of the standards and requirements for a disaster recovery plan.

Standards and Requirements

Recovery of Servers and Software

When possible, the primary choice for recovery of any server and/or software will be a restore from the latest viable image backup. A manual rebuild is the solution of last resort.

Viability of the backup image will be determined by multiple factors including:

- Probable date of infection in the case of a malicious software attack
- Age of the backup image
- Number of updates to all software systems between current production and the backup image

The preferred image will be the latest image taken of the server to be recovered (or equivalent) by date.

Image recovery will be initiated by [redacted]

Location Viability

Viability of a location that has been previously used but has been affected by a disaster will be determined by multiple factors including:

- Safety concerns for staff at the facility
- Remaining facilities or speed of restoration of existing facilities
- Safety concerns in the general environment
- State of emergency in the city / province

Scenario Breakdown

Each scenario shares elements of the recovery process but differ in scope and urgency.

[redacted] *Down with the Loss of All Physical Data Centers (All Critical Hardware)*

This scenario follows the far-left path of the main process map (figure 1) - report/analysis stream. The priority for this scenario would be critical. This would primarily cover a physical disaster where all hardware in both data centers are lost and requires a full rebuild of one production environment. In the case where an original location is still viable, the requirement to identify a new location could be skipped. Rebuild of affected machines may happen in parallel to shorten turnaround time and may engage both the manual and image recovery processes in parallel.

[redacted] *Down with the Loss of Multiple Pieces of Critical Hardware and No Redundancy*

This scenario follows the left path of the main process map (figure 1) - report/analysis stream until the decision for ‘lost both datacenters’. The priority for this scenario would be critical. As the design of the architecture will not allow a loss of redundancy for one piece of critical hardware, it should be expected that the decision for hardware type may result in multiple flow paths in the hardware stream which is acceptable in this instance. Rebuild of affected machines may happen in parallel to shorten turnaround time and may engage both the manual and image recovery processes in parallel.

[redacted] *Up but No Redundancy Due to the Loss of One or More Pieces of Critical Hardware*

This scenario follows the right path of the main process map (figure 1) - report/analysis stream and flows into the hardware stream. Due to the risk of having no redundancy, though [redacted] is still

functional, the priority for this stream would be considered high. This scenario would also cover a situation like the loss of one data center.

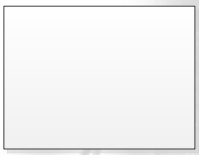
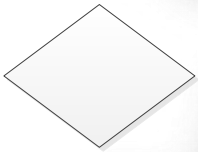
Malicious Software Attack

This scenario can evolve through either path of the main process map (figure 1) - report/analysis stream and flows into the software stream. This may have a priority of critical or high depending on if both datacenters are affected by the malicious software attack and if [redacted] is down or not. The degree of severity of the malicious software attack will dictate the response – ie: a known virus outbreak that can be mediated by port modifications to the firewall would not trigger a full rebuild of a server.

General

Process map legend

Symbols:

Symbol	Definition
	This symbol represents a process or procedure to be performed.
	This symbol represents a subprocess that is part of the larger process, but significant enough to be defined outside of the overall process.
	This symbol represents a decision to be made during the process. It may cause the process to branch off in another direction or may simply indicate a decision about the priority or need for another action.
	This symbol indicates a link to another process or flow diagram.
	This symbol indicates a link from another process or flow diagram.

Color coding within the process map indicates which group has responsibility for that piece of the process. Green represents [redacted] support, blue represents the [redacted] team and purple represents the [redacted] team. Symbols which are left white represent an automated process or a process where multiple teams may share responsibility for restoring services.

Documentation

Documentation of the event should be tracked via standard incident procedures (ie: tracked in Jira) when possible. For disaster recovery, the JIRA Tracker that should be used is [redacted]. If systems used in standard incident procedures are not available, then best effort to document the recovery process should be made via alternate measures (email chain, spreadsheet, etc).

Hardware Failure & Warranty Replacement / OEM Support Agreements

In cases where catastrophic hardware failure is the cause of [redacted] inoperability, then warranty /OEM support replacement of the hardware should be pursued. However, due to the criticality of the [redacted] system and delays that can sometimes be a part of a warranty /OEM support replacement – if [redacted] is down and no existing hardware is viable for restoration of production, the procurement of hardware should not be delayed until a warranty replacement becomes available. If [redacted] is up but with no redundancy, then a management decision to procure hardware outside the warranty replacement is necessary.