

MILES CITY DATA CENTER &
CLOUD DISASTER RECOVERY PLAN



STATE INFORMATION TECHNOLOGY SERVICES DIVISION | 2023

IMAGE FROM VISITMT.COM

INTRODUCTION

The State Information Technology Services Division (SITSD) is working to complete a transition out of the Miles City Data Center by the end of 2023 for most compute and storage solutions. This document is intended to provide details about this plan addressing Legislative Finance Committee questions, including:

- A description of moving disaster recovery from the Miles City Data Center to the cloud (including a timeline with significant milestones from the start of decision making to anticipated completion).
- An explanation of the problem being addressed by this change
- Alternative methods of addressing the problem
- Rationale for choosing to move disaster recovery to the cloud
- A projection of the costs of having disaster recover at the Miles City Data Center versus disaster recovery on the cloud for FY 2024 through FY 2029
- The rates state agencies currently pay for the Miles City Data Center in FY 2022 and FY 2023 and a projection of the rates state agencies will pay for disaster recovery on the cloud from FY 2024 through FY 2029
- Will there be any loss of revenue from outside entities using the Miles City Data Center? If so, what is the projected loss of revenue for FY 2024 through FY 2029?
- What is proposed to happen with the existing data center? If this facility is going to be repurposed, what will it be repurposed to do and what is the process for repurposing?

A DESCRIPTION OF MOVING DISASTER RECOVERY FROM THE MILES CITY DATA CENTER TO THE CLOUD (INCLUDING A TIMELINE WITH SIGNIFICANT MILESTONES FROM THE START OF DECISION MAKING TO ANTICIPATED COMPLETION OF THE TRANSITION)

In 2021, Governor Gianforte instructed the State CIO, Kevin Gilbertson, to transition as many applications as possible from being hosted in State-owned data centers to the cloud to provide greater availability, integrity, and security of State applications. Traditional on-premises data centers have served us well over the years, but they are not without their disadvantages, particularly in terms of disaster recovery. As technology continues to evolve, many organizations are now looking to the cloud as a viable and superior alternative. In general, the cloud offers numerous advantages including shifting from a capital expenditure (CapEx) model to an operational expenditure (OpEx) model to allow for predictable, scalable spending that aligns with actual usage and business growth. Other advantages include scalability, flexibility, and enhanced reliability. By shifting to cloud hosting, we can leverage these benefits to safeguard our data against a variety of disaster scenarios, ranging from natural catastrophes to cybersecurity incidents, therefore ensuring business continuity in an increasingly unpredictable world.

Disaster recovery (DR) was the first logical step in moving to the cloud because it allows us to test and validate the cloud environment before moving production workloads in the future. This is important because it helps to mitigate the risk of any unexpected issues that may arise during the migration process.

Additionally, DR in the cloud can provide a number of other benefits for state government IT teams, including:

- Improved scalability: Cloud-based DR solutions enable us to buy only what we use and shrink and expand resources as needed. This is because cloud providers have a large pool of resources that can be used to meet the needs of their customers, including the unique needs of government clients.
- Enhanced security: Cloud providers like AWS, Google, and Microsoft, due to their scale, have typically implemented a variety of security measures and will continue to update these measures to protect customer data. Additionally, they are not subject to the same hiring difficulties experienced at the State.
- Increased Resiliency: In the event of an actual disaster, the cloud enables the State to access resources from anywhere.

SIGNIFICANT MILESTONES

The following provides a high-level overview of the significant milestones we have completed and plan to complete in this transition.

- Key milestones in 2022:
 - Completed proof of concepts with multiple cloud providers.
- Key milestones first half 2023:
 - Setup direct network connections from Helena and Miles City to cloud provider.
 - Data migration of systems that don't contain protected data.
- Key milestones second half 2023:
 - Get approval to DR protected data to cloud.
 - Complete data migration for all state servers.

Introduction

- Move load balancing and web application firewall to cloud.
- Migrate some key systems to full cloud hosting.
- Key milestones first half 2024:
 - Complete DR drill to cloud.
 - Move public DNS to cloud.
 - Move key public web applications to full cloud hosting.

AN EXPLANATION OF THE PROBLEM BEING ADDRESSED BY THIS CHANGE

The primary problem being addressed by moving DR to the cloud from a State-owned data center is the limitation and risk associated with maintaining an on-premises disaster recovery solution. These risks include high equipment costs with ongoing maintenance (moving from CapEx to OpEx), complexity in management, limited scalability (the cloud allows scale without over purchasing to account for usage spikes), and a potentially longer recovery time in the event of a disaster affecting the main operations, if not geographically dispersed. By migrating to a cloud-based DR solution, the State can mitigate these risks, ensuring our data remains secure and accessible, irrespective of any disruptive event.

SITSD is transitioning to the cloud as we retire hardware. This has allowed us to offset some of the costs of the move by avoiding new hardware purchases.

ALTERNATIVE METHODS OF ADDRESSING THE PROBLEM

The alternatives to moving DR to the cloud are 1) business as usual or 2) co-location in a third-party data center. Neither of these solutions address all the problems stated above including scalability, geographic redundancy, complexity, resiliency, and the ability to only pay for actual usage.

RATIONALE FOR CHOOSING TO MOVE DISASTER RECOVERY TO THE CLOUD

Moving disaster recovery (DR) to the cloud can offer several benefits, including:

- Moving IT staff to higher priority activities to serve citizens. In the cloud, the backend infrastructure is maintained by the cloud provider, which can free up Montana IT staff to focus on other tasks.
- Scalability. Cloud-based DR solutions can be easily scaled up or down to meet the changing needs of the State.
- Compliance with regulations. Cloud providers can help organizations to comply with various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). This is because cloud providers have implemented a variety of security and compliance measures. In particular, we are working with vendors who are FedRAMP certified, meaning the federal government has verified their systems and controls.

Here are some specific reasons why SITSD chose to move DR to the cloud:

Introduction

- We are buying finished services (e.g., comes with 24x7x365 support). This means that we do not have to worry about the day-to-day maintenance of our DR infrastructure.
- This is IT best practice. Private sector companies are no longer supporting data centers as the norm. A multi-cloud approach enables organizations to run in several locations (both private and public cloud) for the most efficient and reliable service.
- It provides the ability to utilize more security expertise if an incident were to occur. Senior security resources are leaving the state for dramatic pay raises. Cloud providers have a large pool of security experts that can be used to help organizations respond to security incidents.
- We can continually choose the most cost-effective way to run our systems. Cloud providers offer a variety of pricing options that can be tailored to our needs.
- Eliminates short term skill shortage issues. As employees retire, we are losing key expertise that is hard to replace.

A PROJECTION OF THE COSTS OF HAVING DISASTER RECOVERY AT THE MILES CITY DATA CENTER VERSUS DISASTER RECOVERY ON THE CLOUD FOR FY 2024 THROUGH FY 2029

Overall, SITSD believes this move will be cost neutral across all IT spending. However, the short-term cost of moving to the cloud does increase for the State. This is, in part, due to the one-time cost of professional services needed to make the transition. Also, some equipment in Miles City will not be replaced in the next five years, which would cause a spike in following years. These estimates are:

- Estimated 5-year cost to host DR in Miles City: \$5,776,187
- Estimated 5-year cost to host DR in cloud: \$7,860,000

From a larger IT budget perspective, savings recognized elsewhere that are not included in the calculations above include the following:

- Staff for moving and managing key enterprise applications.
- Savings we will have in the Helena data center due to repurposing hardware.
- Reducing staff travel to support infrastructure.

Finally, it is important to remember that this transition was not undertaken as a cost-saving measure. We believe the advantages justify the cost of transition.

THE RATES STATE AGENCIES CURRENTLY PAY FOR THE MILES CITY DATA CENTER IN FY 2022 AND FY 2023 AND A PROJECTION OF THE RATES STATE AGENCIES WILL PAY FOR DISASTER RECOVERY ON THE CLOUD FROM FY 2024 THROUGH FY 2029

We will be buying disaster recovery in the cloud instead of buying, operating, and maintaining equipment in the MCDC. The rates that state agencies currently pay will be the same in 2024 and 2025 as they were budgeted. At this time, we also do not anticipate a significant increase in the future; however, additional years may increase due to inflation and other factors that would impact both the data center and the Cloud and cannot be predicted at this time.

WILL THERE BE ANY LOSS OF REVENUE FROM OUTSIDE ENTITIES USING THE MILES CITY DATA CENTER? IF SO, WHAT IS THE PROJECTED LOSS OF REVENUE FOR FY 2024 THROUGH FY 2029?

No. There is not currently any revenue being generated from outside entities at the Miles City Data Center.

WHAT IS PROPOSED TO HAPPEN WITH THE EXISTING DATA CENTER? IF THIS FACILITY IS GOING TO BE REPURPOSED, WHAT WILL IT BE REPURPOSED TO DO AND WHAT IS THE PROCESS FOR REPURPOSING?

The land on which this building stands is owned by the Department of Corrections. Once vacated, it will return to that agency. We have not had a significant conversation with Corrections about the future uses of the building.