# THE FUTURE PROOF

## DECOMMISSION

OceanTech is committed to providing robust, secure, and environmentally conscious strategies for data center decommissioning.

We are equipped to handle the complexities of shutdowns while delivering value and peace of mind to our clients.

If your organization is facing the **need to decommission a data center, contact us to leverage our expertise and ensure a future-proof decommission.**

In an era of rapid technological advancement, the decommissioning of data centers is a critical operation that requires a comprehensive and strategic approach.

This whitepaper presents the methodology and strategies for an efficient and secure shutdown of data centers, ensuring that all activities, from planning to final disposition, are conducted with the utmost attention to simplicity, security, and sustainability.

By adopting these strategies, organizations can mitigate risks, optimize costs, and fulfill their environmental responsibilities.

## Introduction

The need to shut down data centers can arise from various factors like technological advancements, business restructuring, or shifting to cloud services. These shutdowns, if not managed properly, can lead to significant data breaches, financial losses, and environmental harm. OceanTech's future-proof strategies for data center decommissioning are designed to address these challenges with a proactive and systematic process that ensures the secure, compliant, and environmentally sound dismantling of IT infrastructure.

The purpose of this guide is to provide a comprehensive framework for both experienced and inexperienced data center managers to successfully decommission a data center. Proper decommissioning ensures the secure and environmentally responsible disposal of IT assets, compliance with legal requirements, and effective project management. This guide covers the entire decommissioning process from planning and preparation to post-decommissioning activities.

## Redundancy and Migration

Before decommissioning, it is crucial to establish systems that will take over the functions of the outgoing data center. This may involve setting up redundancies or migrating data and services to other locations or the cloud. A seamless transition is vital to maintain business continuity and minimize downtime. OceanTech provides guidance in developing a migration strategy that aligns with the client's operational objectives and technical capabilities.

## Cross-Functional Collaboration

A holistic approach to data center decommissioning necessitates the involvement of cross-functional teams. This collaborative effort between IT, facilities management, finance, and legal departments ensures that all perspectives are considered, and that the shutdown process aligns with broader organizational goals. OceanTech facilitates these collaborations to streamline decision-making and execution.

# The Decommissioning Process



## Planning and Preparation

Effective decommissioning starts with a detailed plan that encompasses all aspects of the shutdown. This plan should outline the scope of work, identify all assets and dependencies, and create a timeline for each stage of the process. It is crucial to conduct an audit of the physical and logical assets to understand the configuration and interdependencies of systems that will be affected. The audit will also reveal opportunities for asset recovery, be it through resale or recycling, thereby providing potential financial return and minimizing environmental impact.

## 01
### Assessing the Need for Decommissioning

Decommissioning a data center can be driven by technological upgrades, data center consolidation, relocation, cost reduction, and compliance with regulatory changes. Understanding these reasons aids in planning and justifying the process. Additionally, a cost-benefit analysis is crucial, comparing ongoing maintenance costs with decommissioning expenses, potential energy savings, and the value recovered from asset disposition.

## 02
### Project Management for Stakeholders

A successful project requires a dedicated team with relevant expertise, including IT staff, facility managers, security personnel, and external vendors, overseen by a project manager to ensure coordination. Clearly defined roles and responsibilities are crucial for accountability and efficiency, preventing confusion and delays. Identifying all stakeholders, both internal and external, and developing a communication plan keeps everyone informed, and ensures transparency throughout the process.

## 03
### Compliance Considerations

Data center decommissioning must comply with various legal and environmental regulations, including laws related to environmental protection, data privacy, and workplace safety, to avoid legal liabilities and penalties. Compliance with data privacy and security regulations, such as GDPR and HIPAA, is critical due to the sensitive information handled by data centers. Proper handling and destruction of data are essential for maintaining compliance and protecting against data breaches.

## 04
### Inventory Documentation

Creating a detailed inventory of all physical and virtual assets, including servers, storage devices, networking equipment, and software licenses, is the first step in the decommissioning process. Asset management software can help maintain accuracy and efficiency. Identifying and prioritizing systems with sensitive or critical data ensures proper backup, migration, or secure destruction. Mapping data dependencies helps understand the impact of decommissioning specific systems.

## 05
### Assessing Asset Condition

Conducting physical inspections and reviewing performance logs and maintenance records helps assess the condition of equipment, determining whether assets can be reused, resold, or recycled. Categorizing assets based on their condition and potential value is essential. Functional assets with resale value can be sold, while obsolete or damaged items should be responsibly recycled. Partnering with certified recyclers or resellers ensures proper handling of these assets.

## 06
### Risk Assessment

Analyzing potential risks such as security breaches, data loss, and operational disruptions helps in preparing for challenges that may arise during the decommissioning process. Developing and implementing risk mitigation plans, including redundancy measures and contingency plans, ensures these risks are effectively managed, minimizing their impact on the decommissioning project.

# Data Security and Compliance

Data centers house sensitive information that must be handled with the utmost care. It is imperative to follow strict data sanitization protocols to ensure all data is irrecoverably destroyed and to maintain compliance with industry and legal standards.



This involves using certified data destruction methods and providing documentation that verifies the integrity of the sanitization process. OceanTech emphasizes a security-first approach, ensuring that data breaches are prevented during the decommissioning process.

## Data Backup and Migration

Before decommissioning any systems, it is crucial to ensure the integrity and availability of data through comprehensive backup procedures. Verifying the completeness and integrity of backups safeguards against data loss and supports seamless migration to new systems or locations, thereby maintaining business continuity. Selecting reliable software and hardware solutions for backup and migration is essential. Testing these tools beforehand ensures they perform as expected and identifies any potential issues early in the migration process.

## Data Destruction

Secure data destruction is vital to protect sensitive information during decommissioning. Methods include using software-based erasure tools that overwrite data multiple times and employing physical destruction techniques like degaussing or shredding, ensuring data cannot be recovered from decommissioned equipment.

Obtaining certificates of data destruction from vendors provides proof of secure erasure, essential for compliance audits and demonstrating adherence to data privacy and security regulations.

## Compliance with Data Regulations

Adherence to GDPR, HIPAA, and other relevant data protection regulations is critical throughout the decommissioning process. This involves securely erasing or migrating data in accordance with legal requirements, documenting procedures, and maintaining compliance records. Ensuring all data handling practices comply with regulatory standards helps mitigate legal risks and ensures responsible data management practices.

## data wiping standards

| Standard | Passes |
|---|---|
| NIST 800-88r1 Clear | 1- Pass |
| Secure Erase | 1-Pass |
| U.S. Air Force System Security Instruction 5020 | 3-Pass |
| Gutmann All | 35-Pass |
| Russian GOST-R 50739-95 | 2-Pass |
| Pfitzner Algorithm | 33-Pass |
| AR 380-19 | 3-Pass |
| Gutmann MFM | 18-Pass |
| British HMG Infosec Standard 5 | 3-Pass |
| Canada RCMP TSSIT OPS-II | 7-Pass |
| U.S. Department of Defense 5220.22-M | 3-Pass |
| Gutmann RLL 1.7 | 26-Pass |
| Schneier's Algorithm | 7-Pass |
| U.S. Department of Defense 5220.28-STD | 7-Pass |
| Gutmann RLL 2.7 | 23-Pass |
| Pfitzner Algorithm | 7-Pass |
| Germany VSITR | 7-Pass |

# Physical Decommissioning
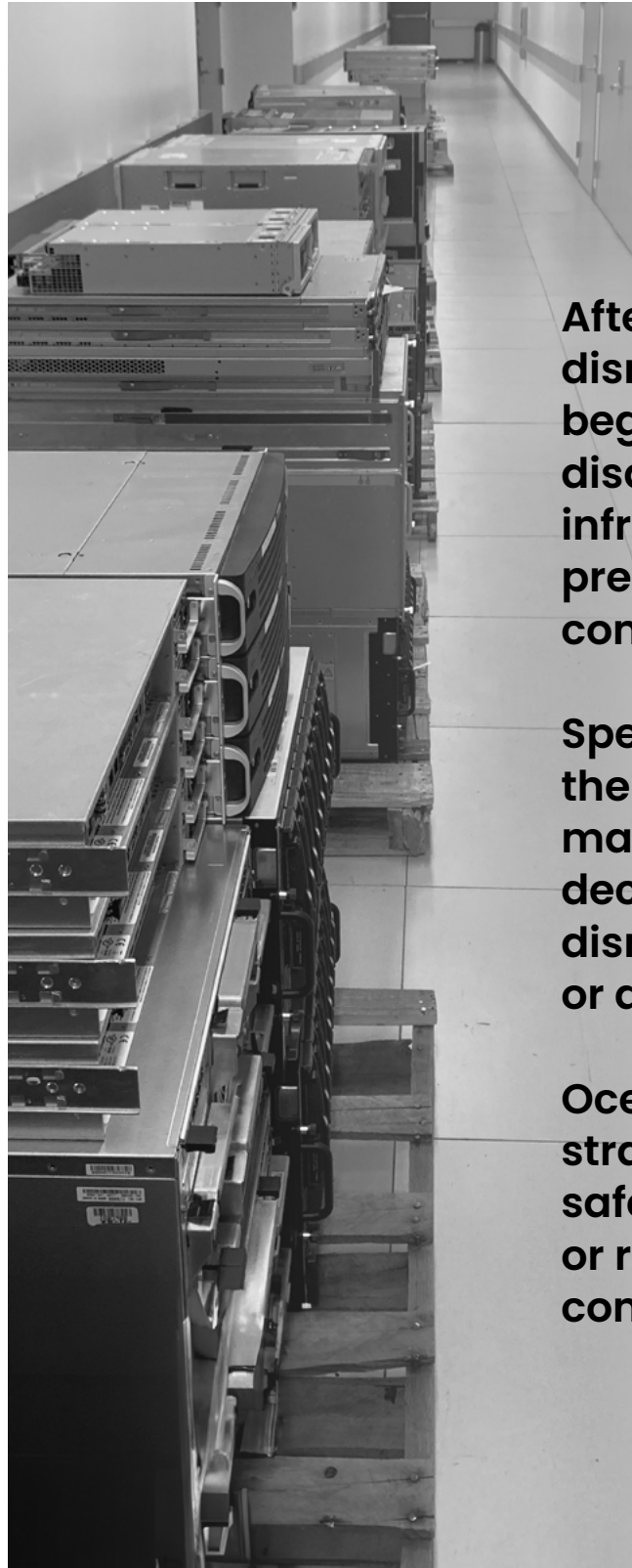


After data sanitization, the physical dismantling of the data center begins. This involves the careful disassembly of hardware and infrastructure in a manner that prevents damage to reusable components.

Special attention must be paid to the safe handling of hazardous materials and to ensuring that decommissioning activities do not disrupt ongoing operations within or adjacent to the data center.

OceanTech advocates for strategies that prioritize worker safety and maximize the resale or recycling value of hardware components.

## 1. Disconnecting and Removing Equipment

- **Safe Shutdown Procedures:** Following manufacturer guidelines for shutting down equipment ensures that systems are safely powered down without causing damage or data loss. This includes properly closing applications, disconnecting power sources, and confirming that backups are complete.

- **Disconnecting Power and Network Connections:** Safely disconnecting power and network connections is crucial to avoid electrical hazards and network issues. Properly labeling cables and connections helps in ensuring that the right components are disconnected and removed.

## 2. Physical Security Measures

- **Ensuring Secure Access During Decommissioning:** Controlling access to the decommissioning site prevents unauthorized personnel from interfering with the process. Implementing security measures such as access control systems, surveillance cameras, and security personnel helps in maintaining site security.

- **Preventing Unauthorized Access:** Using physical barriers, locks, and monitoring systems helps in preventing unauthorized access to sensitive areas and equipment. Regular security checks ensure that the site remains secure during the decommissioning process.

## 3. Transportation and Logistics

- **Coordinating the Removal of Equipment:** Scheduling the transportation of decommissioned equipment with trusted logistics partners ensures that assets are securely handled and transported to their destination. Coordinating with transportation partners helps in managing timelines and avoiding delays.

- **Selecting Transportation Partners:** Vetting transportation vendors for reliability and compliance ensures that they follow best practices for handling and transporting IT assets. Ensuring that vendors have proper insurance coverage protects against potential losses or damages during transit.

# Asset Disposition and Recovery

Decommissioning provides an opportunity to recoup investments through the sale, recycling, or re-purposing of hardware assets. Developing a hierarchy of disposition avenues—resale, donation, recycling—can help maximize returns and support corporate social responsibility efforts.

The R2v3 standard is essential for responsible electronics recycling and IT asset disposition, setting the best practices in environmental and data security. It emphasizes sustainable recycling methods to minimize environmental impact and requires certified vendors to implement robust data destruction techniques to protect sensitive information.

By following the R2v3 standard, organizations show their commitment to ethical management of electronic assets, regulatory compliance, and corporate social responsibility, making it a crucial certification for any ITAD vendor.

## Partnering with Certified Vendors

Choosing ITAD vendors with proper certifications, such as R2v3, ensures that assets are disposed of responsibly and in compliance with environmental and data security regulations. Reviewing vendor policies and procedures helps in selecting the right partner.

## Tracking and Documenting The Disposal Process

Maintaining detailed records of all disposed assets, including their condition and disposal method, ensures transparency and accountability. Using asset tracking software helps in managing this documentation and providing audit trails.

By partnering with specialized vendors or leveraging industry marketplaces, **OceanTech assists clients in achieving the best possible outcomes** for their decommissioned assets.

# Environmental Responsibility

Responsible e-waste management is a cornerstone of OceanTech's decommissioning process. By adhering to best practices for recycling and waste management, we ensure minimal environmental impact. This involves working with certified recyclers and waste management providers to dispose of non-recoverable assets in a manner that complies with all environmental regulations and ethical standards.

### E-Waste Recycling Best Practices

Following environmentally responsible recycling practices involves ensuring that all electronic waste is properly handled and recycled. This includes safely disposing of hazardous materials, such as batteries and chemicals, and promoting the reuse or refurbishment of functional equipment.

### Reducing Environmental Impact

Minimizing the environmental impact of decommissioning involves reducing landfill contributions by recycling and reusing as much equipment as possible. Implementing sustainable practices and partnering with certified recyclers help in achieving this goal.

### Compliance with Regulations

Adhering to local and international e-waste regulations is essential for responsible asset disposition. Conducting environmental impact assessments and following regulatory guidelines helps in maintaining compliance and avoiding legal issues.

### Obtaining Disposal and Recycling Certifications

Working with ITAD vendors to obtain necessary certifications for disposal and recycling demonstrates compliance with environmental regulations. Displaying these certifications provides proof of responsible practices and can be used in environmental audits.

---

**Post-decommissioning is a critical phase that encompasses thorough site cleanup, final audits, and continuous improvement.**

**By dismantling and removing all cabling and infrastructure, we ensure the site is left pristine and ready for its next use, adhering to environmental compliance standards.**

### Cleaning and Restoring the Site.

Performing a thorough cleaning of the site, including floors, walls, and ceilings, ensures that it is restored to its original condition or prepared for new occupants. This may involve hiring professional cleaning services and conducting final inspections.

### Final Audits and Reporting

Conducting final audits ensures that all decommissioning activities are reviewed for compliance with legal and internal standards, confirming secure asset disposal and complete documentation. Compiling comprehensive reports on the decommissioning process provides detailed records of activities and outcomes, crucial for demonstrating compliance and transparency to stakeholders and regulatory bodies.

### Lessons Learned and Continuous Improvement

Analyzing what went well and areas for improvement during the decommissioning process helps in identifying best practices and lessons learned. Documenting these insights ensures that future projects benefit from this knowledge.

Updating decommissioning procedures based on feedback from post-mortem reviews helps in continuously improving the process. Training staff on new protocols and best practices ensures that future decommissioning projects are more efficient and effective.

---

### CERTIFICATE OF DATA DESTRUCTION

This document certifies that OceanTech, a division of Ocean Enterprises LLC, has received 78,061 lbs of electronic equipment from Company on 01/04/2024

We hereby certify that all electronic scrap will be managed and recycled according to applicable EPA, MPCA, and Hennepin County waste management rules. And that all data on all storage devices from the above equipment has been destroyed to standards of NIST SP 800-88r1 Clear (National Institue of Standards and Technology Standard 800-88r1) and in compliance with the following laws and regulations:

- HIPAA (Health Insurance Portability and Accountability Act)
- Sarbanes-Oxley Act
- Gramm-Leach-Bliley Act (GLBA)
- Bank Secrecy Act
- Patriot Act of 2002
- Identify Theft and Assumption Deterrence Act
- FDA Security Regulations (21 C.F.R. part 11)
- All Applicable State Laws

---

EPA number: MNS 000 153 460
Hennepin Co. Operation ID: 1747405309028

### AUDIT REPORT

| # | Make and Model | Serial Number |
|---|---|---|
| 1 | X5-2, 1U Database Server, EXADATA X5 | 152INMI10E |
| 2 | X5-2, 1U Database Server, EXADATA X5 | 152INMI07T |
| 3 | X5-2L, 2U, High Capacity Server, EXADATA X5 | 152INMI07T |
| 4 | X5-2L, 2U, High Capacity Server, EXADATA X5 | 152INM714R |
| 5 | X5-2L, 2U, High Capacity Server, EXADATA X5 | 152INM70AR |
| 6 | X5-2, 1U Database Server, EXADATA X5 | 1514NMI072 |
| 7 | X5-2, 1U Database Server, EXADATA X5 | 1514NMI06B |
| 8 | X5-2L, 2U, Extreme Flash Server, EXADATA X5 | 1513NM70BP |
| 9 | X5-2L, 2U, Extreme Flash Server, EXADATA X5 | 1513NM704V |

# Conclusion

Proper decommissioning of a data center is a complex but essential task that requires careful planning, execution, and post-decommissioning review.
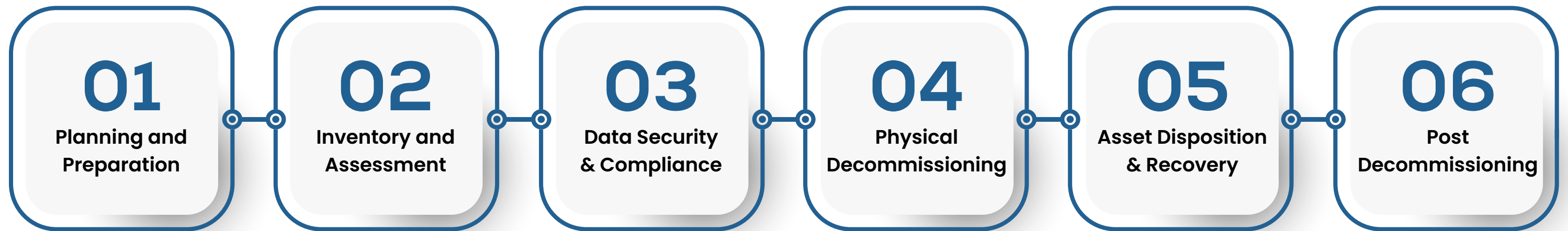
By following this guide, data center managers can ensure the secure, compliant, and environmentally responsible decommissioning of their facilities, while also learning from past projects to continuously improve their processes.

**We invite you to take the next step with OceanTech. Our comprehensive strategies and real-world experience make us the ideal partner for your data center decommission needs.**

OceanTech is committed to providing robust, secure, and environmentally conscious strategies for data center decommissioning.

We are equipped to handle the complexities of shutdowns while delivering value and peace of mind to our clients. If your organization is facing the need to decommission a data center, contact us to leverage our expertise and ensure a future-proof decommission.

Reach out today, and let's ensure a secure, efficient, and environmentally responsible transition for your business.

| 01 | 02 | 03 | 04 | 05 | 06 |
|----|----|----|----|----|----|
| Planning and Preparation | Inventory and Assessment | Data Security & Compliance | Physical Decommissioning | Asset Disposition & Recovery | Post Decommissioning |

# Appendices

A comprehensive checklist to guide the decommissioning process includes all essential tasks and considerations. This checklist serves as a practical tool for project managers and teams, ensuring that no important steps are overlooked.

## Stage 1: Planning and Discovery

☐ **Establish a Plan**

- Outline objectives, scope, and timeline.
- Identify and engage all relevant stakeholders.
- Assign a project manager.
- Develop a budget.
- Create a detailed scope of work, including safety procedures and stages of removal/ demolition.
- Schedule the decommissioning for off hours for live decommissions with a buffer for unexpected circumstances.

☐ **Network and Physical Discovery**

- Choose an optimal network discovery tool suitable for your environment (e.g., agentless tools for flat networks, NetFlow enabled tools for virtualized environments).
- Conduct a physical audit, double-verifying all inputs.
- Compile a hardware map from the physical review and relate it to your applications and data.

☐ **Expert Review and Updated Asset Map**

- Review existing CMDBs, discovery tool outputs, and physical audits with qualified experts (developers, operators, users, management).
- Finalize an updated environment map, including software, servers, storage systems, VMs, network equipment, air and cooling equipment, power equipment, and cabling dependencies.

☐ **Final Planning**

- Create an implementation plan listing all actions and responsibilities for project members.
- Establish go/no-go criteria and hold a formal meeting to approve the decommissioning initiation.
- Create a contact list for team members and vendor contacts.
- Inform end-users about potential downtime for live decommissions.
- Commission necessary tools or equipment (e.g., forklifts, drive shredders/degaussers, pallets, hoists, trucks, tip guards).
- Conduct background checks on temporary personnel.
- Use asset tags to denote future location, personnel responsibilities, and planned processes.

## Stage 2: Decommissioning Stage

☐ **Log and Determine Final Designation for Hardware**

- Log all servers to be decommissioned.
- Determine the final designation for all hardware assets (re-purpose, resale, recycling).
- Retain all associated software licenses.
- Schedule the cancellation of vendor maintenance contracts for systems not being migrated.

☐ **Data Backup and Erasure**

- Run tests/simulations on all backups or disaster recovery to ensure functionality.
- Create a comprehensive backup just before decommissioning and verify it.
- Complete data erasure using industry-approved methods and obtain a certificate of erasure.

☐ **Equipment Disconnection and Removal**

- Disconnect equipment from the network and remove it from ACLs, subnets, and firewalls.
- Cut power to all equipment being decommissioned.
- Pull all rack hardware and consider tip guards if moving racks.
- Shred or degauss remaining storage media if drives have not been erased.

☐ **Rack Teardown**

- Complete rack teardown
- Verify that all security policy requirements are met and leave a comprehensive audit trail.

## Stage 3: Disposition

☐ **Packing and Transportation**

- Complete hardware palletization and packing with appropriate materials (cut-to-fit polyethylene foam for servers, standard freight for other hardware).
- Coordinate with financial and accounting departments to take servers/fixed assets off the books and recover software licenses.

☐ **Recycling and Re-purposing**

- Identify a certified electronics recycler or downstream site for recyclable materials.
- Coordinate with other departments to transition hardware slated for re-purposed use.
- Move equipment to an assured facility in locked and sealed trucks for preparation for resale or recycling.

☐ **Documentation**

- Maintain detailed documentation throughout the process, including records of asset disposal, data sanitization certificates, recycling receipts, and compliance with regulations.

## Additional Security Measures

- **Encryption:** Encrypt data in transit and at rest.
- **Access Controls:** Limit access to authorized personnel only, using multi-factor authentication.
- **Physical Security:** Implement stringent physical security measures to prevent unauthorized entry to decommissioning areas.

## Key Considerations

- **Environmental Impact:** Work with reputable electronics recyclers to minimize the ecological footprint.
- **Data Security and Privacy:** Implement strict data sanitization protocols and conduct thorough audits to ensure no data vulnerabilities remain.
- **Logistical Coordination:** Develop a detailed logistical plan for removal, transportation, and delivery to recycling facilities, minimizing downtime and streamlining the process.

## Final Checklist

- **Hardware Inventory:** List all equipment with conditions and locations.
- **Data Backup:** Ensure all critical data is backed up securely.
- **Data Sanitization:** Document data erasure and destruction methods.
- **Physical Equipment Disposition:** Outline how hardware will be decommissioned, recycled, or resold.
- **Security Measures:** Detail access controls and security protocols.



# Notes

# Data Center Decommissioning Plan Template

This template provides a structured approach to planning and executing a data center decommissioning project, ensuring all critical aspects are covered and managed effectively.

☐ **Executive Summary**

- **Objective:** Briefly describe the purpose and goals of the decommissioning project.
- **Scope:** Outline the extent and boundaries of the project.
- **Key Stakeholders:** List the primary stakeholders and their roles.

☐ **Project Scope**

**Assets To be Decommissioned:**
- List of hardware (servers, storage devices, networking equipment, etc.)
- Software and applications
- Ancillary equipment (cables, racks, UPS, etc.)

**Geographical Scope:** Locations and sites involved.

**Deliverables**
- Final status reports
- Certificates of data destruction
- Inventory reconciliation

☐ **Timeline**

**Project Milestones:**
- Project kickoff
- Inventory and asset discovery
- Data backup completion
- Data sanitization
- Physical removal of equipment
- Final audit and reconciliation
- Disposal or re-purposing of equipment
- Project closure

**Schedule:** Detailed Gantt chart or timeline with start and end dates for each milestone.

☐ **Roles and Responsibilities**

**Project Manager:** _____

Responsibilities: Overall project oversight, timeline management, stakeholder communication.

**IT Asset Manager:** _____

Responsibilities: Asset inventory, reconciliation, and documentation.

**Data Security Officer:** _____

Responsibilities: Data backup, sanitization, and destruction verification.

**Physical Logistics Coordinator:** _____

Responsibilities: Equipment disconnection, packing, transportation, and disposal coordination.

**Compliance Officer:** _____

Responsibilities: Ensuring compliance with regulations and internal policies.

☐ **Risk Assessment**

**Potential Risks**
- Data breaches
- Equipment damage during removal
- Environmental hazards
- Downtime and business interruption

**Mitigation Strategies**
- Implement strict data sanitization protocols
- Use professional moving and packing services
- Partner with certified electronics recyclers
- Schedule decommissioning during off-peak hours

**Contingency Plans**
- Backup solutions
- Alternate disposal methods
- Additional security measures

## ☐ Inventory and Asset Discovery

### Tools and Methods
- Network discovery tools (e.g., agentless tools, NetFlow enabled tools)
- Physical audits
- Existing CMDB reviews

### Documentation
- Updated asset map with dependencies
- Detailed inventory list with conditions and locations

## ☐ Data Backup and Sanitization

### Backup Procedures
- Secure backup methods and storage locations
- Final verification of backup integrity

### Sanitization Methods
- Certified data erasure software
- Physical destruction (shredding, degaussing)

### Compliance and Reporting
- Certificates of data destruction
- Audit trails and documentation

## ☐ Equipment Disconnection and Removal

### Disconnection Procedures
- Network and power disconnection
- Removal from ACLs, subnets, and firewalls

### Physical Removal
- Rack hardware disassembly
- Packing and transportation logistics

### Safety Measures
- Tip guards for moving racks
- Background checks on personnel

## ☐ Disposal and Re-purposing

### Final Designation
- Re-purpose
- Resale
- Recycling

### Vendors and Partners
- Certified electronics recyclers
- Downstream sites for recycling

### Documentation
- Recycling receipts
- Asset disposition reports

## ☐ Communication Plan

### Stakeholder Communication
- Regular updates to stakeholders
- Go/no-go decision meetings

### End-User Notification
- Inform users about potential downtime
- Provide alternative solutions during decommissioning

## ☐ Final Audit and Project Closure

### Audit Procedures
- Comprehensive audit of decommissioning tasks
- Reconciliation of inventory count

### Project Closure
- Final report and presentation to stakeholders
- Handover of documentation and certificates
- Lessons learned and post-project review

---

**Project Manager:** _____  **Date:** _____

**IT Asset Manager:** _____  **Date:** _____

**Data Security Officer:** _____  **Date:** _____

**Physical Logistics Coordinator:** _____  **Date:** _____

**Compliance Officer:** _____  **Date:** _____