Critical Systems Disaster Recovery Standard Operating Procedure

Gotham City IT Department

Infrastructure and Operations Team

Document Number: SOP-IT-DR001

Revision: 1.0

Effective Date: 11/17/2024

Contents

Document Revision History

Version	Author	Description of Changes
1.0	Blake Gordon	Initial Release

Document Review and Approval

Role	Name	Date
Author	Blake Gordon	11/16/2024
Reviewer	Dick Grayson	11/16/2024
Technical Reviewer	Lucius Fox	11/16/2024
Quality Control	Timothy Drake	11/16/2024
Manager	James Gordon	11/16/2024

1 Purpose

To establish standardized procedures for the recovery of Gotham City's critical IT infrastructure and systems in the event of a disaster or major service disruption. This SOP ensures consistent, timely, and secure recovery operations while maintaining compliance with security protocols.

2 Scope

This procedure encompasses the disaster recovery processes for all critical IT systems including:

- GCPD Criminal Database Cluster (Windows/SQL)
- Emergency Response System (Linux/Oracle)
- City Infrastructure Management (AIX)
- Arkham Security Systems (Linux/VMware)
- Access Control Infrastructure (Windows)
- Core Network Systems (Cisco UCS)
- CyberArk Privileged Access Management
- Azure DR Site Resources
- Zerto Replication Infrastructure

3 Responsibilities

- **DR Manager (Barbara Gordon)**
  - Overall DR operation coordination
  - Communication with stakeholders
  - Decision-making authority during DR events
- **Network Team (Luke Fox)**
  - Cisco UCS recovery operations
  - DR site connectivity
  - Firewall and security appliance recovery
- **Systems Team (Tim Drake)**

  - VMware environment recovery
  - Windows/Linux/AIX systems recovery
  - Application service restoration
- **Security Team (Lucius Fox)**
  - CyberArk vault recovery
  - Access management restoration
  - Security validation

4 Definitions

- **DR Site**: Azure East US 2 Region
- **RPO**: Recovery Point Objective
- **RTO**: Recovery Time Objective
- **VPG**: Virtual Protection Group (Zerto)
- **PAM**: Privileged Access Management
- **UCS**: Cisco Unified Computing System
- **LPAR**: Logical Partition (AIX)

5 Procedure

5.1 Disaster Declaration

1. DR Manager evaluates situation and declares disaster
2. Initiates automated alert through ServiceNow
3. Establishes DR command bridge (Teams/Phone)
4. Notifies key stakeholders

5.2 Initial Assessment

1. Network Team validates Azure ExpressRoute status
2. Verify Zerto replication health
3. Check CyberArk vault availability
4. Assess VMware site recovery readiness
5. Confirm UCS DR profiles status

5.3 Network Recovery

1. Activate DR UCS service profiles
2. Configure DR site firewalls
3. Establish VPN tunnels
4. Enable load balancers
5. Verify network connectivity

5.4 Security Infrastructure

1. Activate DR CyberArk vault
2. Enable emergency access procedures
3. Deploy DR security policies
4. Start MFA services
5. Verify security controls

5.5 System Recovery (Prioritized)

1. Execute Zerto VPG failovers:
    - Priority 1: Active Directory/DNS
    - Priority 2: CyberArk Services
    - Priority 3: GCPD Database
    - Priority 4: Emergency Response
    - Priority 5: Arkham Security
    - Priority 6: Infrastructure Management
2. Start AIX LPARs in sequence
3. Verify VMware cluster health
4. Enable application services
5. Test system connectivity

6 References

Document ID	Description
DR-ZERTO-001	Zerto Recovery Runbook
DR-AZURE-001	Azure DR Site Configuration
DR-VMW-001	VMware Site Recovery Plan
DR-CYB-001	CyberArk DR Procedures
DR-NET-001	Network Recovery Guide

7 Acronyms

Acronym	Definition
DR	Disaster Recovery
RPO	Recovery Point Objective
RTO	Recovery Time Objective
VPG	Virtual Protection Group
PAM	Privileged Access Management
UCS	Unified Computing System
LPAR	Logical Partition
MFA	Multi-Factor Authentication

A Appendix A: Recovery Time Objectives

System	RPO	RTO
Active Directory	5 min	15 min
CyberArk Services	5 min	15 min
GCPD Database	15 min	30 min
Emergency Response	5 min	15 min
Arkham Security	10 min	20 min
Infrastructure Management	30 min	60 min

B Appendix B: Emergency Contacts

Role	Primary	Secondary
DR Manager	Barbara Gordon	Dick Grayson
Network Lead	Luke Fox	Kate Kane
Systems Lead	Tim Drake	Stephanie Brown
Security Lead	Lucius Fox	Helena Bertinelli
Database Lead	Oracle Team	Jason Todd