Classification: Public

BCC

Certifying Authority

Disaster Recovery Policy (DRP)

Version: 1.0.0

Bangladesh Computer Council

Information and Communication Technology Division

Summary of the Revision

Bangladesh Computer Council (BCC) Certifying Authority Disaster Recovery Plan version 1.0.0 (first version) has been prepared.

Sl.	Reference Section/Clause	Changes Summary
1.		
2.		

Revision History

Version	Date	Revision Number	Updates
1.0.0	31 July 2025	-	First time prepared

Document Control

Document Name	Bangladesh Computer Council CA Disaster Recovery Policy (DRP)
Classification	Public
Document Location	https://bcc-ca.gov.bd/content/downloads
Maintenance Owner	BCC CA Document Manager
Approval owner	BCC CA Director
Release Date	31 July 2025
Next Review Date	As when necessary

Contents

1. Introduction

1.1 Purpose

This Disaster Recovery Plan (DRP) outlines the procedures and strategies for recovering the critical IT systems, data, and operations of the Bangladesh Computer Council Certifying Authority (BCC-CA) in the event of a disaster. BCC-CA, as the government-licensed Certifying Authority under the Bangladesh Computer Council (BCC), provides digital certificates (Class-1, Class-2, and Class-3) for individuals and organizations in accordance with the Controller of Certifying Authorities (CCA) guidelines, the Information and Communication Technology (ICT) Act 2006 (amended), and the IT (Certifying Authorities) Rules 2010.

The plan ensures minimal disruption to certificate issuance, revocation, validation services, and Public Key Infrastructure (PKI) operations. It is designed to comply with third-party audit requirements, incorporating elements from international standards such as ISO 22301 (Business Continuity Management), ISO 27001 (Information Security Management), and CCA's Root CA Certificate Policy (CP) and Certification Practice Statement (CPS), which emphasize compromise recovery, backups, and business continuity.

1.2 Scope

This DRP covers:

- All BCC-CA systems, including Root CA servers, cryptographic modules, databases, backup systems, and network infrastructure located at BCC Bhaban, Agargaon, Dhaka.
- Recovery from natural disasters (e.g., floods, earthquakes), man-made incidents (e.g., cyberattacks, power failures), and key compromises.
- Integration with BCC-CA's Business Continuity Plan (BCP) for broader operational resilience.

Exclusions: This plan does not cover general BCC operations outside CA services or non-IT disasters (e.g., personnel safety, handled by separate emergency response plans).

1.3 Assumptions

- BCC-CA maintains off-site backups and redundant systems as per CCA CPS requirements.
- Key personnel are trained and available for recovery.
- Third-party vendors (e.g., for hardware or cloud services) have service level agreements (SLAs) supporting recovery.

1.4 Definitions

- **RTO (Recovery Time Objective)**: Maximum acceptable downtime (e.g., 4 hours for critical systems).
- **RPO (Recovery Point Objective)**: Maximum acceptable data loss (e.g., 1 hour of data).
- **CA Key Compromise**: Unauthorized access or loss of control over private keys used for certificate signing.
- **CRL (Certificate Revocation List)**: List of revoked certificates, must be maintained and distributed post-recovery.

2. Risk Assessment

BCC-CA faces risks specific to its role as a CA, including cyber threats targeting PKI integrity. The following table summarizes key risks, likelihood, impact, and mitigation strategies:

Risk Category	Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Mitigation
Natural Disaster	Floods, earthquakes damaging facilities in Dhaka.	Medium	High	Off-site backups in secure locations; redundant data centers.
Cyber Attack	Hacking attempts leading to key compromise or data breach.	High	High	Multi-factor authentication; regular penetration testing; incident response protocols.
Power Failure	Extended outages affecting servers.	Medium	Medium	Uninterruptible Power Supply (UPS) and generators; cloud-based failover.
Hardware Failure	Failure of cryptographic modules or servers.	Medium	High	Redundant hardware; scheduled maintenance.
Key Compromise	Loss or theft of CA private keys.	Low	Critical	Multi-person control for key access; encrypted backups.

Risks are assessed annually or after incidents, aligning with CCA CPS Section 5.7 on compromise and disaster recovery.

3. Business Impact Analysis (BIA)

Critical functions include:

- Certificate issuance and renewal.
- CRL publication and Online Certificate Status Protocol (OCSP) services.
- Subscriber validation and key management.

Impact of disruption:

- Financial: Loss of revenue from certificate services.
- Reputational: Erosion of trust in digital signatures under Digital Bangladesh initiative.
- Legal: Non-compliance with ICT Act, potentially leading to license revocation.

RTO/RPO Targets:

- Critical Systems (e.g., CA Signing Servers): RTO = 4 hours; RPO = 1 hour.
- Supporting Systems (e.g., Databases): RTO = 24 hours; RPO = 24 hours.

4. Recovery Strategies

4.1 Backup and Restoration

- **Frequency**: Full backups daily; incremental hourly. Off-site backups stored in a secure, fireproof location (e.g., secondary data center) and on tape/DVD as per CCA CPS (at least 2 copies: one in strong room, one off-site).
- **Data Included**: CA databases, audit logs, certificates, CRLs, and cryptographic keys (backed up in encrypted tokens with multi-person control).
- **Restoration Process**: Use system state backups or manual CA backups to restore ADCS (Active Directory Certificate Services) if applicable. Test restorations quarterly.

4.2 Redundancy and Failover

- Clustered issuing CAs for high availability.
- Off-site disaster recovery site with mirrored systems.
- Cloud-based backups (if compliant with CCA guidelines) for quick failover.

4.3 Key Compromise Recovery

As per CCA CPS Section 5.7:

- Detect compromise via monitoring and audits.
- Revoke compromised keys immediately.
- Generate new key pairs.
- Notify subscribers, licensed CAs, and publish public notices (web and at least 3 national newspapers).
- Terminate services using compromised keys and issue new certificates.

4.4 Incident Response Integration

Link to BCC-CA's Incident Response Plan for initial detection and containment.

5. Roles and Responsibilities

The following table outlines key roles:

Role	Responsibilities	Contact
DR Coordinator	Overall plan activation; coordination with CCA.	Muztaba Seraji, Phone: +88-02-55006450, Email: muztaba.seraji@bcc.gov.bd
IT Recovery Team Lead	System restoration; backup verification.	Hasan uj Jaman, Phone: +88-02-55006452 Email: hasan.jaman@bcc.gov.bd
Security Officer	Key compromise handling; compliance checks.	Samidhya Sarker, Phone: +8801715297522 Email: samidhya.sarker@bcc.gov.bd
Communications Lead	Notify stakeholders (subscribers, CCA, media).	Mohammad Masudur Rahaman, Phone: +88-01711486209 Email: masud@bcc.gov.bd
Executive Sponsor (Director, CA Operation & Security)	Approve plan activation; resource allocation.	Mohammad Mohidur Rahman Khan, Phone: +88-02-55006854 Email: mohidur.khan@bcc.gov.bd

All roles require annual training.

6. Recovery Procedures

6.1 Plan Activation

- Declare disaster via executive approval if RTO is threatened.
- Assemble recovery team at alternate site (e.g., secondary BCC facility).

6.2 Step-by-Step Recovery

1. **Assessment**: Evaluate damage (e.g., physical inspection, system logs).
2. **Notification**: Alert team, CCA, and subscribers within 1 hour.
3. **Restoration**:
    - Restore from backups: Load tapes/DVDs to redundant servers.
    - Re-establish PKI: Install new CA if keys compromised; re-issue certificates.
    - Test services: Validate CRL publication and certificate issuance.
4. **Failback**: Return to primary site once stable.
5. **Deactivation**: Document lessons learned; update plan.

For Root CA-specific disasters (if BCC-CA acts as subordinate): Request revocation from CCA and rebuild per agreement.

7. Testing and Exercises

- **Types**: Tabletop exercises (annual), full simulations (bi-annual), key compromise drills.
- **Criteria**: Measure against RTO/RPO; document results.
- **Post-Test**: Update plan based on findings.

8. Plan Maintenance

- **Review Cycle**: Annual or after major changes/incidents.
- **Audits**: Align with third-party audits; include evidence of backups and tests.
- **Document Control**: Versioned and stored securely; distributed to key personnel.

Appendices

A: Contact List (Detailed).
B: Backup Schedules and Locations.
C: System Inventory (Servers, Software Versions).
D: References (ICT Act Revised 2013, CCA CPS, ISO 22301).