Business Continuity and Disaster Recovery Policy

Organization: AegisCISO
Document ID: POL-BC-001
Version: 1.0
Effective Date: January 2026
Classification: Internal
Owner: Chief Information Security Officer (CISO)
Co-Owner: Chief Operations Officer (COO)

---

1. Purpose

This policy establishes the framework for business continuity and disaster recovery to ensure AegisCISO can maintain essential operations during disruptions and recover critical systems within acceptable timeframes.

2. Scope

This policy applies to:

- All critical business processes
- All information systems and infrastructure
- All personnel with BC/DR responsibilities
- All locations and facilities

3. Business Impact Analysis

3.1 BIA Requirements

POL-BC-001-01: Business Impact Analysis shall be conducted.

Requirements:

- BIA conducted annually
- All business processes evaluated
- Critical processes identified
- Dependencies documented
- Impact quantified (financial, operational, reputational)

3.2 Criticality Classification

POL-BC-001-02: Systems shall be classified by criticality.

Tier	Description	RTO	RPO
Tier 1 - Critical	Business cannot operate without	< 4 hours	< 1 hour
Tier 2 - Essential	Significant impact to operations	< 24 hours	< 4 hours
Tier 3 - Important	Moderate impact, workarounds e:	< 72 hours	< 24 hours
Tier 4 - Non-Critical	Minimal impact, can be deferred	< 7 days	< 72 hours

3.3 Recovery Objectives

POL-BC-001-03: Recovery objectives shall be defined.

Definitions:

- RTO (Recovery Time Objective): Maximum acceptable downtime
- RPO (Recovery Point Objective): Maximum acceptable data loss
- MTPD (Maximum Tolerable Period of Disruption): Beyond which viability threatened

4. Business Continuity Planning

4.1 BC Plan Requirements

POL-BC-001-04: Business Continuity Plans shall be maintained.

Plan Contents:

- Scope and objectives
- Activation criteria and procedures
- Roles and responsibilities
- Communication procedures
- Recovery procedures
- Resource requirements
- Dependencies and contacts

4.2 BC Plan Development

POL-BC-001-05: BC plan development process.

Requirements:

- Plans developed for each critical process
- Process owners involved in development
- Dependencies identified and documented
- Manual workarounds defined
- Resource requirements quantified

4.3 BC Plan Maintenance

POL-BC-001-06: BC plans shall be maintained.

Requirements:

- Annual review and update
- Update after significant changes
- Update after exercises/incidents
- Version control maintained
- Distribution list current

5. Disaster Recovery Planning

5.1 DR Plan Requirements

POL-BC-001-07: Disaster Recovery Plans shall be maintained.

Plan Contents:

- System inventory and classification
- Recovery priorities
- Technical recovery procedures
- Data recovery procedures
- Infrastructure requirements
- Testing procedures

5.2 Recovery Strategies

POL-BC-001-08: Recovery strategies by system tier.

Tier	Strategy	Description
Tier 1	Hot Site / Active-Active	Immediate failover capability
Tier 2	Warm Site / Active-Passive	Rapid recovery from standby
Tier 3	Cold Site / Backup Restore	Recovery from backups
Tier 4	Rebuild	Rebuild from installation media

5.3 Alternate Processing Site

POL-BC-001-09: Alternate site requirements.

Requirements:

- Geographic separation from primary (minimum 100km)
- Sufficient capacity for critical operations
- Network connectivity established
- Security controls equivalent to primary
- Regular readiness verification

6. Backup and Recovery

6.1 Backup Requirements

POL-BC-001-10: Data backup requirements.

Data Type	Frequency	Retention	Storage
Tier 1 Systems	Continuous/Hourly	90 days	On-site + Off-site
Tier 2 Systems	Daily	60 days	On-site + Off-site
Tier 3 Systems	Daily	30 days	On-site + Off-site
Tier 4 Systems	Weekly	30 days	Off-site

6.2 Backup Security

POL-BC-001-11: Backup security requirements.

Requirements:

- Encryption of backup data (AES-256)
- Secure transmission to off-site location
- Access controls for backup systems
- Backup integrity verification
- Immutable backup copies for ransomware protection

6.3 Recovery Testing

POL-BC-001-12: Backup recovery testing.

Requirements:

- Quarterly recovery testing for Tier 1 systems
- Semi-annual recovery testing for Tier 2 systems
- Annual recovery testing for all systems
- Results documented and remediated

7. Emergency Response

7.1 Emergency Procedures

POL-BC-001-13: Emergency response procedures.

Requirements:

- Emergency notification procedures
- Evacuation procedures
- Emergency contact lists
- Assembly points identified
- Emergency supplies maintained

7.2 Crisis Management

POL-BC-001-14: Crisis management structure.

Crisis Management Team:

- Crisis Manager (Executive Leadership)
- BC Coordinator
- IT/DR Lead
- Communications Lead
- Operations Lead
- Legal/Compliance Lead

7.3 Communication During Crisis

POL-BC-001-15: Crisis communication procedures.

Requirements:

- Internal communication channels (primary and backup)
- External communication protocols

- Customer notification procedures
- Regulatory notification requirements
- Media handling procedures

8. Plan Activation

8.1 Activation Criteria

POL-BC-001-16: BC/DR activation triggers.

Automatic Activation Triggers:

- Primary data center unavailable > 4 hours
- Critical system failure > RTO threshold
- Facility inaccessible
- Natural disaster affecting operations

Assessment-Based Activation:

- Partial system failures
- Localized incidents
- Vendor/supplier disruptions

8.2 Activation Authority

POL-BC-001-17: Plan activation authority.

Plan Type	Primary Authority	Backup Authority
BC Plan	COO	CEO
DR Plan	CIO	CISO
Crisis Management	CEO	COO
Emergency Response	Facility Manager	Security Manager

8.3 Declaration Process

POL-BC-001-18: Disaster declaration process.

Steps:

1. Incident assessment
2. Impact determination
3. Recovery options evaluation
4. Declaration decision
5. Plan activation notification
6. Team mobilization

9. Testing and Exercises

9.1 Exercise Program

POL-BC-001-19: BC/DR testing program.

Exercise Type	Frequency	Participants
Tabletop	Quarterly	BC Team + Management
Walk-through	Semi-annually	BC Team + IT
Simulation	Annually	Extended team
Full DR Test	Annually	IT + Operations

9.2 Exercise Objectives

POL-BC-001-20: Exercise objectives.

Objectives:

- Validate plan effectiveness
- Test communication procedures
- Verify recovery capabilities
- Identify gaps and improvements
- Train personnel

9.3 Exercise Documentation

POL-BC-001-21: Exercise documentation requirements.

Requirements:

- Exercise plan and scenario
- Participant list
- Observations and findings
- Lessons learned
- Corrective action plan
- Plan updates resulting

10. Vendor and Third-Party Continuity

10.1 Critical Vendor Management

POL-BC-001-22: Critical vendor BC requirements.

Requirements:

- BC capabilities assessed during selection
- BC plans reviewed annually
- Recovery testing evidence required
- Alternative vendors identified
- SLAs include recovery requirements

10.2 Supply Chain Resilience

POL-BC-001-23: Supply chain continuity.

Requirements:

- Critical supplies identified

- Alternative suppliers documented
- Emergency stock for critical items
- Supplier geographic diversity

11. Training and Awareness

11.1 BC/DR Training

POL-BC-001-24: Training requirements.

Role	Training	Frequency
BC Team	Comprehensive BC/DR	Annual + after changes
IT Staff	Technical DR procedures	Annual
All Staff	BC awareness	Annual
Management	Crisis management	Annual

12. Documentation and Records

12.1 Required Documentation

POL-BC-001-25: BC/DR documentation.

Required Documents:

- Business Impact Analysis
- Business Continuity Plans
- Disaster Recovery Plans
- Emergency Response Procedures
- Crisis Communication Plan
- Test/Exercise Reports
- Incident Reports

12.2 Document Control

POL-BC-001-26: Document management.

Requirements:

- Version control maintained
- Secure storage with backups
- Access control for sensitive plans
- Distribution managed
- Retention per records schedule

13. Compliance

13.1 Regulatory Requirements

This policy supports:

- NCA Essential Cybersecurity Controls (ECC-1: 2-11)
- ISO/IEC 22301 (Business Continuity)
- ISO/IEC 27001:2022 - A.17 Business Continuity

14. Roles and Responsibilities

Executive Management

- Approve BC strategy
- Provide resources
- Activate plans
- Crisis decision-making

BC Coordinator

- Maintain BC program
- Coordinate planning
- Manage exercises
- Track improvements

IT/DR Team

- Maintain DR plans
- Execute technical recovery
- Test backup/recovery
- Document procedures

Department Managers

- Develop department plans
- Identify critical processes
- Participate in exercises
- Train staff

All Employees

- Know emergency procedures
- Participate in exercises
- Report disruptions
- Follow BC procedures

15. Metrics

Key Metrics:

- Plan coverage (% critical processes)
- RTO/RPO achievement in tests
- Exercise completion rate
- Issue remediation time

- Training completion rate

16. Enforcement

Non-compliance may result in:

- Recovery failures
- Extended downtime
- Management escalation
- Disciplinary action

17. Review

This policy shall be reviewed annually and updated for:

- Business changes
- Technology changes
- Regulatory requirements
- Lessons learned

18. References

- NCA Essential Cybersecurity Controls
- ISO/IEC 22301 (Business Continuity Management)
- ISO/IEC 27031 (ICT Readiness for Business Continuity)
- NIST SP 800-34 (Contingency Planning)

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release