Business Continuity Policy

Business Continuity Policy • Version 1 • 8 October 2026

Department:	Information Security
Document Owner:	Security Officer
Owner Title:	Security Officer
Classification:	Confidential
Effective Date:	8 October 2026
Review Cycle:	Annually

1. Purpose and scope

This policy ensures that 786 Cyber can maintain or rapidly restore critical business service information systems during significant disruptions. We are committed to protecting our ope staff, clients and stakeholders from the impact of incidents that could prevent normal busin activities.

The aim of this policy is to establish clear requirements for business continuity manageme the organisation. This includes identifying critical services, understanding dependencies, p response and recovery procedures, and ensuring appropriate resources are in place to re operations within agreed timeframes when disruption occurs.

Scope

This policy applies to:

- All critical business services provided by 786 Cyber, including managed security service operations centre monitoring, incident response, vulnerability management and client advi services
- All information systems, applications and infrastructure that support these critical service
- All UK office locations and any remote working arrangements that deliver critical service
- All employees, contractors and third parties who support or have access to critical servic
- Third-party suppliers and service providers whose services are essential to maintaining c operations, including cloud hosting providers, telecommunications suppliers, IT hardware and specialist security tool providers

The business continuity management process covers the identification of critical services, impact analysis, risk assessment, development of continuity and recovery plans, and regu and maintenance of these arrangements.

This policy does not replace our incident response or disaster recovery procedures, but w alongside them to provide a comprehensive approach to operational resilience.

2. Business impact analysis and recovery objectives

786 Cyber conducts regular business impact analyses to identify and document our critica

systems, and processes that are essential to maintaining operations. This analysis evaluat
potential consequences of disruptions to each service, including financial, operational, and
reputational impacts.

The business impact analysis process examines dependencies between services, includin

- Technology infrastructure and applications required to deliver each service
- Third-party suppliers and service providers
- Key personnel and their specialist knowledge
- Data sources and information flows
- Physical facilities and equipment

Based on the business impact analysis findings, we establish recovery objectives for each
service. These objectives guide our continuity planning and resource allocation decisions.

For services classified as critical to our operations, we have established the following reco
objectives:

- **Recovery Time Objective (RTO):** Critical services must be restored within 24 hours of
disruption. This timeframe represents the maximum acceptable period that a critical servic
remain unavailable before causing unacceptable impact to our business operations.

- **Recovery Point Objective (RPO):** The maximum acceptable data loss for critical servi
hours. Our backup and data protection arrangements must ensure that we can recover dat
no more than 24 hours prior to any disruption.

These recovery objectives inform our backup schedules, system redundancy requirements
recovery procedures. We review and update our business impact analysis at least annually
significant changes occur to our services, systems, or business environment. The analysis
and recovery objectives are documented and made available to relevant personnel involve
business continuity planning and response activities.

3. Backup

We back up critical business data, systems and configurations on a daily basis. This includ
customer information, financial records, operational databases, and essential system conf
required to maintain business operations. The backup schedule ensures minimal data loss
event of system failure, cyber attack or data corruption.

At least one copy of all backups is maintained offline or in an immutable state, stored sepa
our live production systems. This backup copy is protected against ransomware and other
malicious encryption or deletion, ensuring we can recover our data even in the event of a s
security incident affecting our primary infrastructure.

All backup data is encrypted both in transit and at rest. Access to backup systems and dat
restricted to authorised personnel only, with access controls reviewed regularly. Authentica
mechanisms protect backup infrastructure from unauthorised access, and we maintain det
of all backup and restore activities.

We test our ability to restore from backups every 6 months. These tests verify the integrity
data, confirm that restoration procedures work as expected, and ensure our recovery time
can be met. Each test includes:

- Restoration of a representative sample of critical data

- Verification of data integrity and completeness
- Documentation of any issues encountered
- Measurement of time taken to complete restoration

All test results are formally recorded, including the date of the test, systems tested, outcor remedial actions required. These records are reviewed by management to ensure our bac recovery capabilities remain effective.

4. Disaster recovery

We maintain documented recovery plans for all critical systems identified through our busi impact analysis. These plans address multiple failure scenarios including loss of physical p unavailability of key suppliers, and cloud region outages.

Our premises recovery plan identifies alternative working locations and specifies the proce relocating operations. Staff can work remotely using secure access to cloud-based system maintain agreements with flexible workspace providers for scenarios requiring physical off

For key supplier failures, we document alternative providers and maintain contact details fo engagement. Critical supplier relationships include provisions for business continuity inform sharing, and we regularly review supplier resilience as part of our vendor management pro

Cloud region failure scenarios are addressed through our architecture decisions and recov procedures. We document the steps required to failover to alternative regions or restore se from backups, with specific timescales aligned to our recovery objectives.

Where recovery time objectives cannot be met through restore procedures alone, we impl technical redundancy measures. Critical systems requiring high availability operate with:

- Redundant infrastructure components to eliminate single points of failure
- Automated failover mechanisms between availability zones or regions
- Real-time or near-real-time data replication to secondary locations
- Load balancing across multiple instances

The technical lead for each critical system maintains responsibility for ensuring redundanc measures remain operational and tested. We review redundancy requirements annually ar whenever business requirements change, updating technical controls to maintain alignme recovery objectives.

5. Roles, invocation and communication

The Managing Director or Operations Director may invoke this plan when a disruption occu threatens normal business operations. In their absence, the IT Manager or Senior Project holds authority to activate business continuity procedures.

Upon invocation, the Business Continuity Response Team assembles immediately. This te comprises:

- Managing Director (overall command and strategic decisions)
- Operations Director (coordination of recovery activities)
- IT Manager (technical infrastructure and systems recovery)
- Senior Project Manager (client service continuity)
- Finance Manager (financial assessment and supplier liaison)
- Office Manager (facilities and staff welfare)

We maintain an up-to-date emergency contact list for all response team members, includi
contact methods for each individual.

Communication during disruption

We communicate promptly and transparently with all stakeholders during any business co
incident.

Staff receive immediate notification of disruptions through multiple channels including
and direct telephone contact. Updates continue at regular intervals, detailing the situation
expected duration and working arrangements.

Customers are contacted directly by their designated project manager or account lead
provide honest timescales for service restoration and implement alternative delivery meth
possible. Status updates occur daily or more frequently as circumstances require.

Suppliers essential to recovery efforts receive direct contact from the Finance Manage
Operations Director, explaining our requirements and expected timescales.

Regulators are notified where legally required, particularly regarding data breaches or
service unavailability. The Managing Director handles all regulatory communications with s
from our legal advisers.

All communications follow our data protection obligations and maintain professional standa
ensuring stakeholders receive necessary information.

6. Testing and maintenance

We exercise our business continuity plan every 12 months to validate its effectiveness and
areas for improvement. These exercises test our ability to respond to disruptions and main
operations under adverse conditions.

Each exercise is designed to simulate realistic scenarios that could impact our operations.
document the scope, objectives, and scenario details before each exercise begins. All rele
personnel participate according to their assigned roles in the plan.

During exercises, we evaluate:

- The effectiveness of response procedures and recovery strategies
- Communication channels and escalation processes
- Availability and adequacy of resources
- Staff competence and familiarity with their continuity roles
- Recovery time objectives and their achievability

We record the results of each exercise, including:

- Observations and findings identified during the test
- Issues or gaps that could prevent effective response
- Strengths demonstrated during the exercise
- Timing and sequencing of activities
- Participant feedback and lessons learned

Following each exercise, we conduct a formal debrief with participants. The debrief captur
immediate observations whilst they remain fresh. We then produce a comprehensive exerc
within four weeks of completion.

All findings from exercises are reviewed by management. We prioritise identified improvem assign responsibility for implementing corrective actions. The business continuity plan is u reflect lessons learned and address any deficiencies discovered.

We maintain records of all exercises, findings, and subsequent plan updates. These recor demonstrate our ongoing commitment to maintaining an effective and current business co capability. Ad-hoc tests of specific plan elements may occur between scheduled full exerci significant changes to our operations warrant validation.

7. Ownership, review and exceptions

The Information Security Lead owns this policy and is responsible for maintaining its accu effectiveness. The policy must be approved by senior management before publication and any substantial revisions.

We review this policy every 12 months to ensure it remains appropriate and effective. Revi also conducted following significant changes to the business, our operating environment, activation of business continuity arrangements or major incidents that test our resilience.

Exceptions

Exceptions to this policy may be necessary in specific circumstances. Any request for an e must:

- Be submitted in writing to the Information Security Lead with a clear business justificatio
- Include details of the specific requirement being excepted and the proposed alternative c mitigation
- Be approved by the Information Security Lead and a relevant senior manager
- Be formally recorded in the organisation's risk register with an assigned risk owner
- Include a defined expiry date, after which the exception will be reviewed or the standard requirement must be met

All exceptions are tracked and reviewed quarterly to ensure they remain valid and necessa

Policy breaches

Failure to comply with this policy may compromise our ability to respond effectively to disru incidents and protect critical business operations. Any breach of this policy will be investig may result in disciplinary action in accordance with our normal disciplinary process. The s the consequences will depend on the nature and impact of the breach, ranging from additi training and guidance to formal disciplinary measures up to and including dismissal for se repeated violations.