Data Security Continuity Planning Policy

Policy Created: March 2021

Last Reviewed: August 2026

Next Review: August 2027 (or sooner if significant changes in legislation, guidance, or organisational activities occur)

Reviewed by: Laurence Clark

Responsible Officer: Liam Vernon (Data Security and Protection Lead)

Approved by: CEO

Main Contact for Queries: info@pathwaysassociates.co.uk

1. Introduction

Pathways Associates CIC recognises that data security incidents can disrupt essential services, compromise sensitive information and affect our ability to support the people who rely on us. Continuity planning is therefore a core part of our data protection and cyber-security responsibilities. This policy sets out how Pathways prepares for, responds to and recovers from incidents that threaten the security, availability or integrity of our data. It also explains how we test our plans, how staff understand their roles and how we ensure senior management oversight. The National Data Guardian's data security standards require every organisation to have a continuity plan that specifically addresses data security incidents and to test that plan at least once a year. Pathways meets this requirement through a clear, practical and proportionate approach that reflects the size and nature of our organisation.

2. Business Continuity and Disaster Recovery

Continuity planning at Pathways focuses on how we maintain essential operations when unexpected events occur. As a small organisation, our continuity arrangements are straightforward but robust. We have incorporated data security into our existing business continuity plan so that we can respond effectively to incidents such as cyber-attacks, system failures, loss of internet access, power outages or physical events such as fire or flood. Disaster recovery forms part of this planning. It describes how we restore systems, recover data and return to normal operations after an incident. Our approach ensures that we can continue delivering critical functions, protect personal information and minimise disruption to staff, customers and partners.

3. Continuity Planning for Data Security Incidents

Pathways has considered a range of scenarios that could affect our ability to access or protect data. These include loss of broadband or telephone services, physical damage to premises, cyber-attacks such as ransomware and failures in third-party systems we rely on. The 2017 WannaCry incident demonstrated how vulnerable health and care organisations can be, and we have used lessons from national guidance to strengthen our own planning. Our continuity plan explains how staff

should respond to incidents, who they should contact, how essential information can be accessed and how services can continue safely. Staff are trained to understand the plan and know how to put it into action. The plan has been formally approved by our Senior Information Risk Owner (SIRO), who provides senior oversight and ensures that continuity planning remains aligned with our wider governance and risk management processes.

4. Testing the Continuity Plan

Pathways tests its continuity plan at least once a year. Testing helps us identify gaps, strengthen our response and ensure that staff understand what to do during an incident. Because we are a small organisation, live testing is not always practical or proportionate. Instead, we use desktop-based testing, which allows us to explore realistic scenarios in a structured and reflective way. Desktop testing involves presenting a scenario to staff and working through how we would respond. The purpose is not to simulate a full operational shutdown but to examine our decision-making, communication, processes and technology. These tests are honest, practical and designed to highlight areas for improvement. Senior management participates in the testing to ensure accountability and oversight. During each test, we record the scenario, the responses, any issues identified and the actions required. We then update the continuity plan accordingly. This ensures that learning is embedded and that our plan evolves as new risks emerge.

5. Roles and Responsibilities

Clear roles and responsibilities are essential during a data security incident. Staff must know who to contact and how to escalate concerns. Pathways maintains an up-to-date emergency contact list, stored securely in hard copy within the HR manager’s locked filing system and backed up electronically on the team’s private drive. The HR manager reviews and updates this list at least quarterly, recording the date of each review and ensuring a new printed copy is stored. During an incident, staff follow the continuity plan and contact the appropriate individuals. The SIRO provides senior oversight, while the Data Security and Protection Lead coordinates the operational response, records actions and ensures compliance with reporting requirements.

6. Lessons Learned and Continuous Improvement

Every test and every real incident contributes to our learning. We follow a Plan, Do, Check, Act cycle to ensure that improvements are identified and implemented. If new risks emerge or if weaknesses are found in our processes, we update our continuity plan and communicate changes to staff. This approach ensures that our planning remains relevant, responsive and aligned with DSPT Standard 5, which requires regular process reviews.

7. Supporting Information and Appendices

Pathways maintains supporting materials that help staff understand continuity planning. These include examples of data security scenarios, templates for recording test results and references to national guidance. These materials are used during desktop testing and staff training to ensure that our approach remains practical and grounded in real-world risks.

8. Conclusion

Pathways Associates CIC is committed to maintaining strong continuity planning for data security incidents. Our approach is proportionate to the size of our organisation but fully aligned with national standards. We ensure that staff understand their responsibilities, that senior management provides oversight and that our plan is tested and improved regularly. By doing so, we protect the people we support, safeguard sensitive information and maintain trust in our organisation.