

Appendix #5_Disaster Recovery Policy

Disaster Recovery Policy, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document Owner: Finance and Operations Team

Last Review Date: September 2024

Disaster Recovery Policy

Purpose

The purpose of The Mind Trust's Business Continuity and Disaster Recovery Policy is to provide direction and general rules for the creation, implementation, and management of The Mind Trust's Disaster Recovery Plan (DRP).

Audience

The Mind Trust's Disaster Recovery Policy applies to individuals accountable for ensuring a disaster recovery plan is developed, tested, and maintained.

Policy

- The Mind Trust must create and implement a Business Continuity and Disaster Recovery Plan (“BDRP”).
- The DRP must be periodically tested and the results should be used as part of the ongoing improvement of the DRP.
- The DRP, at a minimum, will identify and protect against risks to critical systems and sensitive information in the event of a disaster.
- The DRP shall provide for contingencies to restore information and systems if a disaster occurs. The concept of a disaster recovery includes business resumption.
- The Mind Trust’s disaster recovery planning must ensure that:
 - o an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
 - o personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated;
 - o documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.
- The Mind Trust’s DRP must include at a minimum, the following elements:
 - o Business impact analysis and potential disruption to staff
 - o A classification system to identify critical systems and essential records
 - o Mitigation strategies and safeguards to avoid disasters.
 - o Backups
 - o Information Resource role in business resumption
 - o Contingency plans for different types of disruptions to Information Resource and systems availability
 - o Organizational responsibilities for implementing the disaster recovery plan
 - o Procedures for reporting incidents, implementing the disaster recovery plan, and escalating (District/Organization)’s response to a disaster
 - o Annual review and revision

Version History

| Version | Modified Date | Reason/Comments |
|---------|----------------|----------------------|
| 1.0.0 | October 2022 | Document Origination |
| 1.0.1 | September 2024 | Annual review |
| | | |
| | | |