Disaster Recovery Plan

**Eastern Cape Department of Education -- Digital Learning Environment**

1. **Purpose**

This Disaster Recovery Plan outlines the strategies and procedures for restoring critical digital education services in the Eastern Cape in the event of a disaster or major disruption. It aims to minimize downtime, protect data integrity, and ensure continuity of learning and administrative operations.

The primary purposes of this DRP are to:

* + Ensure minimal disruption to teaching and learning during disasters.
  + Restore critical systems and services within the defined Recovery Time Objective (RTO).
  + Protect student and institutional data from loss and breaches.
  + Provide clear roles and responsibilities for recovery actions.
  + Establish communication protocols for stakeholders during and after a disaster.

1. **Scope**

This plan covers digital education services and systems including:

* + Learning Management Systems (LMS)
  + Student Information Systems (SIS)
  + Communication & Collaboration Tools
  + Digital Content Repositories
  + Assessment & Examination Platforms
  + Technical Support & Helpdesk Operations
  + Administrative and Compliance Systems
  + Devices and Connectivity Services

|  |  |  |
| --- | --- | --- |
| **Function** | **Core Activities** | **Impact if Disrupted** |
| Learning Management  System (LMS) | Course content delivery,  assessments, tracking | Students & educators lose access to content,  grading, and feedback |
| Student Information System  (SIS) | Registration, records management,  grading | Learners can't enroll, marks can't be processed |
| Communication Tools | Live classes, admin coordination,  learner support | Classes missed, student isolation, admin  bottlenecks |
| Content Repositories | Access to textbooks, research, OERs | Delays in research, self-paced learning  interrupted |
| Assessment Systems | Tests, quizzes, exams, marking | Missed exams, data loss, academic disputes |
| Technical Support/Helpdesk | Troubleshooting, updates, user  assistance | System downtime increases, unresolved user  issues |
| Admin & Compliance | Budgeting, HR, procurement,  reporting | Delays in reporting to DBE/Umalusi, risk of  non-compliance with POPIA |
| Devices & Connectivity | Student and teacher hardware and  internet access | Learning completely disrupted for affected  individuals |

1. **Critical Business Functions**
2. **Potential Disasters & Mitigation Measures**

|  |  |  |
| --- | --- | --- |
| Disaster/Disruption | Impact | Mitigation Strategies |
| **Load Shedding / Power**  **Outage** | LMS, routers, charging affected | Solar power, offline LMS modules, asynchronous  materials |
| **Severe Weather Events** | Infrastructure damage, road delays | Resilient hardware, cloud storage, SMS alerts |
| **Connectivity Failures** | Platform inaccessibility, content  upload failures | Hybrid (offline + online) packages, satellite  internet |
| **Cybersecurity Threats** | Data breaches, ransomware, POPIA  issues | Regular backups, cyber training, 2FA for admins |
| **Political Unrest / Protests** | School visits, infrastructure, safety  disrupted | Decentralized cloud systems, remote working  toolkits |
| **Vandalism / Theft** | Loss of hardware, network  downtime | Community engagement, tamper-proof  equipment, device tracking |

1. **Backup & Redundancy Strategies**
   * **Cloud-Based Backup**: Use secure cloud storage (e.g., Google Drive, Azure, AWS) with encrypted, automated backups.
   * **Offline LMS Content**: Weekly syncing of modules to USBs/DVDs for schools with limited internet.
   * **Redundant Servers**: Host redundant LMS and SIS servers in other provinces or on decentralized infrastructure.
   * **Device Preload**: Preload student tablets/laptops with term content and auto-sync when online.
   * **Community Access Points**: Equip libraries or community halls with synced digital repositories

|  |  |
| --- | --- |
| Role | Responsibility |
| Provincial ICT Manager | Oversee system recovery, coordinate with DBE and vendors |
| School ICT Coordinators | First line of system troubleshooting, escalate issues, manage backups |
| Educators | Report issues, use offline materials during disruptions |
| Learners | Follow SMS/WhatsApp alerts, switch to offline work when notified |
| Helpdesk Teams | Log, triage, and resolve access and functionality issues |
| Vendors/ISPs | Maintain hardware, provide rapid on-site support for devices and connectivity |

1. **Roles & Responsibilities**
2. **Communication Plan**
   * **Crisis Alerts**: Via SMS, WhatsApp, and local radio stations within 1 hour of disaster detection.
   * **Instructional Updates**: LMS banners and emails for scheduled recovery status.
   * **Helpdesk Escalation**: Hotline and ticketing system open 24/7 during crisis periods.
3. **Testing & Review**
   * **Biannual DR Simulation**: Simulate system failure and test recovery steps.
   * **Monthly Backup Audits**: Verify RPO adherence and test restoration capabilities.
   * **Annual Review**: Update DRP based on new threats, systems, or feedback.