Risk Assessment and Threat Detection Document

1. **Potential Threats**
   1. **Load Shedding**

Frequent national power outages due to strain on the electricity grid.

**Results**:

* + Disruption of learning sessions.
  + Data loss due to unsaved work.
  + Forced reversion to paper-based methods.

**Business Risk**: Undermines investment in digital infrastructure; reduces teaching quality.

* 1. **Internet Connectivity**

Limited or unreliable internet access in rural areas.

**Results**:

* Failure to sync offline learning content.
* Inability to access real-time educational materials.
* Upload/download interruptions.

**Business Risk**: Reduces efficiency and real-time learning capacity.

* 1. **Natural Disasters**

Flash floods during the summer season damage learning infrastructure.

**Results**:

* Physical loss of devices and solar hardware.
* High recovery and replacement costs.

**Business Risk**: Prolonged service disruption, loss of data and learning materials.

* 1. **Theft and Vandalism of Infrastructure**

High risk of theft or damage to ICT and solar systems due to poverty and low security.

**Results**:

* + Financial loss.
    - Interruption in learning and energy provision.

**Business Risk**: Significant capital loss and operational setbacks.

* 1. **Malware**

Malware spreads through infected USBs used by teachers and staff in offline environments.

**Results**:

* System compromise or data corruption.
* Propagation of malicious software across devices.

**Business Risk**: Loss of instructional material, potential for larger-scale system issues.

**Risk Matrix**

**🟩 Low Risk | 🟨 Moderate Risk | 🟧 High Risk | 🟥 Severe/Critical Risk**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Impact ↓ / Likelihood →** | **Rare** | **Unlikely** | **Possible** | **Likely** | **Almost Certain** |
| **Severe** |  |  | Natural Disasters (Flooding) | Load Shedding | Theft & Vandalism |
| **High** |  |  | USB Malware | Internet Loss |  |
| **Moderate** |  |  |  |  |  |
| **Low** |  |  |  |  |  |

**Scenario 1: Power Outage During Critical Learning Activities**

**Risk Category**: Infrastructure (Energy Disruption)  
**Description**:  
A critical failure of the solar inverter coincides with a national load-shedding event during digital assessments, leading to a total loss of power across the school premises.

**Response Strategy**:

* **Immediate Action**: Deploy printed emergency assessment packs to continue scheduled exams.
* **Short-Term Measures**: Access alternative power sources through local partnerships or mobile UPS solutions to support critical operations.
* **Long-Term Interventions**: Upgrade energy systems with inverter monitoring and install a secondary generator to provide emergency power redundancy.

**Recovery Time Objective (RTO)**:

* **Initial Service Continuity**: 6–12 hours
* **Full System Recovery**: 3–5 business days

**Scenario 2: Malware Infection Introduced via USB Drive**

**Risk Category**: Cybersecurity  
**Description**:  
Malicious software is inadvertently introduced to multiple school devices through an infected USB drive, causing system shutdowns and data integrity concerns.

**Response Strategy**:

* **Immediate Action**: Disconnect and isolate infected devices to prevent further spread.
* **Short-Term Measures**: Perform scans using offline antivirus tools and restore affected systems from clean backups.
* **Long-Term Interventions**: Implement a strict USB policy and conduct regular cybersecurity training for all staff and learners.

**Recovery Time Objective (RTO)**:

* **Basic Functionality Restored**: 1–2 days
* **Full System Cleansing and Policy Reinforcement**: Up to 5 business days

**Scenario 3: Theft of Digital Learning Assets**

**Risk Category**: Socioeconomic (Theft and Vandalism)  
**Description**:  
ICT devices (tablets, routers) and solar storage components are stolen over a weekend due to insufficient security infrastructure, directly impacting digital learning operations.

**Response Strategy**:

* **Immediate Action**: Report the incident to law enforcement and inform education district authorities.
* **Short-Term Measures**: Utilize remaining devices in a shared format or switch to analog resources temporarily.
* **Long-Term Interventions**: Invest in secure storage, implement asset tracking solutions, and explore community-led security collaborations.

**Recovery Time Objective (RTO)**:

* **Interim Operational Continuity**: 2–3 business days
* **Complete Equipment Replacement**: 2–4 weeks, depending on funding and procurement turnaround

**Scenario 4: Environmental Damage to Solar Infrastructure**

**Risk Category**: Environmental (Flooding and Natural Disasters)  
**Description**:  
Flash flooding results in significant damage to solar panels and inverters, causing the loss of power and associated digital services.

**Response Strategy**:

* **Immediate Action**: Relocate learners and staff to undamaged facilities; resume lessons using printed material.
* **Short-Term Measures**: Coordinate temporary access to electricity via nearby schools or generators.
* **Long-Term Interventions**: Retrofit solar infrastructure with flood protection, and redesign layouts to elevate critical components above known flood lines.

**Recovery Time Objective (RTO)**:

* **Interim Learning Recovery**: 1–2 business days
* **Full Infrastructure Restoration**: 2–3 weeks

**Scenario 5: Internet Disruption During Scheduled Training**

**Risk Category**: Connectivity (ISP Outage)  
**Description**:  
A regional internet service disruption coincides with scheduled virtual training for educators, impeding access to critical professional development resources.

**Response Strategy**:

* **Immediate Action**: Notify stakeholders of the delay and reschedule the session.
* **Short-Term Measures**: Share training content via physical storage media (e.g., USB) and explore the use of mobile data as an interim solution.
* **Long-Term Interventions**: Establish service redundancy through multiple ISP contracts and ensure that all training resources are available offline where possible.

**Recovery Time Objective (RTO)**:

* **Immediate Workaround Activation**: Within the same day
* **Full Digital Training Functionality Restored**: 2–5 business days