FinalForms Disaster Recovery Plan (Updated)

1. Purpose

1. Introduction and Objectives

This Disaster Recovery Plan (DRP) is designed to restore critical systems, operations, and services for FinalForms in the event of a disaster or major incident. The goal is to minimize downtime, avoid data loss, and ensure that the critical functions of FinalForms, particularly those involving student enrollment and emergency medical information, are restored as quickly as possible.

The key objectives of this DRP are:

- Ensure the recovery of essential data and services.
- Minimize operational disruption and financial loss.
- Protect FinalForms' reputation and customer trust.
- Establish clear responsibilities and procedures for recovery efforts.

---

2. Critical Systems and Recovery Priorities

FinalForms' core business operations revolve around data collection, verification, and distribution services. The following are the **critical systems** that need to be restored immediately:

1. **FinalForms Online Registration System**:
    - **RTO (Recovery Time Objective)**: 2 hours
    - **RPO (Recovery Point Objective)**: 0 data loss
    - **Impacts of Disruption**: Schools and parents are unable to register students, access emergency medical information, or manage compliance tasks.
2. **Student and Guardian Data (including emergency medical information)**:
    - **RTO**: Immediate (within 1 hour)
    - **RPO**: 0 data loss (real-time backup)
3. **Internal Communication Systems** (email and document sharing for the FinalForms team):
    - **RTO**: 4 hours
    - **RPO**: Minimal data loss (1-hour backup)

Other non-critical systems will follow as resources allow, with a general RTO of 12–24 hours and acceptable RPO depending on system priority.

---

3. Risk Assessment and Threat Scenarios

The primary risks identified for FinalForms include:

- **Cyberattacks** (e.g., ransomware, phishing, DDoS)
- **Data Breaches**

- **Natural Disasters** (e.g., fire, flood, severe weather affecting infrastructure)
- **Hardware/Software Failure**
- **Human Error**

---

4. Disaster Recovery Team (DRT)

The Disaster Recovery Team (DRT) is responsible for coordinating and executing recovery efforts during a disaster. This team will include the following key roles:

- **Clay Burnett (CEO)** – Overall coordination, external communication, and public relations.
- **Macklin Chaffee (CTO)** – Lead on system recovery, technical restoration, and liaison with third-party services (e.g., AWS).
- **Griffith Chaffee (CSO)** – Data security, threat assessment, and compliance reporting.
- **[Additional IT Staff]** – System monitoring and technical support during recovery efforts.

Each team member should have alternate contact details available in case primary communication methods are down.

---

5. Disaster Response and Recovery Procedures

5.1. Immediate Actions (First 30 minutes)

1. **Incident Detection and Notification**:
    - Any team member detecting a disaster or major incident must immediately notify the CTO and CEO.
    - The CTO will assess the scope of the incident, its impact on critical systems, and decide whether to initiate full disaster recovery mode.
2. **DRT Activation**:
    - Once the incident is confirmed as a disaster, the DRT is activated. Each member will follow the pre-assigned roles and recovery responsibilities.
3. **Preliminary Damage Assessment**:
    - The CTO and IT staff will perform a quick assessment of the affected systems (e.g., is the entire network down, isolated service outages, or data corruption?).

5.2. System and Data Recovery

1. **Critical Systems Restoration (Priority 1)**:
    - **FinalForms Online Registration System**: Utilize the most recent backups from AWS to restore operations. Redundant AWS systems should automatically failover, but manual intervention may be required.
    - **Student Data and Emergency Medical Information**: Ensure immediate restoration of real-time data backups from AWS. This data is critical for school emergency responses.
2. **Verification of Data Integrity**:

    - Once data and services are restored, the DRT will verify the integrity of all restored systems and ensure no data loss or corruption occurred.
3. **Communication to Customers**:
    - The CEO will issue updates to affected schools, partners, and clients, informing them of the incident status and estimated restoration timelines.
    - An additional follow-up notification will be sent once systems are fully restored.

5.3. Non-Critical Systems Restoration (Priority 2)

Following the restoration of critical systems, the remaining services (such as internal communication tools, customer support channels, and financial processing systems) will be restored within 12-24 hours.

---

6. Backup and Data Retention Strategy

FinalForms uses **real-time backups stored securely off-site with AWS**, ensuring that:

- **Data is encrypted** both in transit and at rest.
- Backups are retained for a rolling period of **90 days** to enable the recovery of historical data if necessary.
- Redundant systems across multiple AWS regions provide geographic failover in case of localized outages.

---

7. Communication Plan

In the event of a disaster, the following communication steps will be implemented:

1. **Internal Communication**:
    - The DRT will use email as the primary communication method, but alternate channels such as phone and text messaging will be used if email is unavailable.
2. **External Communication**:
    - Customers will be notified via email and, if applicable, public channels (such as the FinalForms website or social media).
    - All communications will include the nature of the incident, expected recovery time, and any necessary actions customers should take.

---

8. Post-Recovery Review and Lessons Learned

After systems have been fully restored and normal operations have resumed, the DRT will:

1. Conduct a **post-mortem review** of the incident to identify areas for improvement in both the DRP and the response process.

2. Implement any corrective actions needed to enhance system resilience and response time for future incidents.
3. Prepare a formal incident report and share key findings with relevant stakeholders (e.g., schools, partners).

---

9. Plan Maintenance and Testing

The DRP will be reviewed annually as part of FinalForms' business continuity planning process. Additionally, **regular disaster recovery drills** will be conducted twice a year to ensure the readiness of the DRT and the effectiveness of recovery procedures.

---

10. Conclusion

This Disaster Recovery Plan provides the FinalForms team with a clear framework to respond to and recover from disasters while maintaining the availability and integrity of critical services and data. By regularly updating and testing this plan, FinalForms can reduce the impact of disasters and continue to serve schools, students, and families effectively.