Pabau IT Disaster Recovery Plan

Overview

This document is governed in conjunction with Pabau's Terms of Use, available at https://pabau.com/terms. In any conflict, the Terms of Use shall prevail, including clauses on service availability, liability, and customer responsibilities during outages.

The goal of this plan is to outline the key recovery steps to be performed during and after a disruption of the Pabau CRM service or any of its subservices, to ensure that issues regardless of their severity will be resolved in the timeliest possible manner, as well as appropriate action steps will be taken to ensure that the likelihood of them reoccurring in the future is minimal.

Disaster is defined as an unplanned event or circumstance causing business disruptions resulting from catastrophic events. Such events may be human-made or natural, including everything from equipment failures and localized power outages to cyberattacks, civil emergencies, criminal or military attacks, and natural disasters, any of which causing an adverse effect on the client's business operations.

Pabau's infrastructure team is heavily focused on strategies and systems for preventing disasters from occurring in the first place, and also developing strategies for recovering from disasters as soon as possible, should such occur.

Pabau's infrastructure team has taken the preventive measures below, to ensure that should such situations occur, the likelihood of seriously affecting a client will be minimal, and the recovery time as quick as possible:

- Separating clients' Pabau accounts to dedicated and isolated servers (pods) which can be further vertically scaled (upgraded), should the need arise - this ensures that each account will have more resources at their disposal, and significantly reduces the likelihood of being affected by disasters;

- Strict revision of new code - every new line of code submitted for revision undergoes automated testing first, and then is peer-reviewed by two senior developers, and ultimately by a quality assurance team;

- Controlled process for releasing new features and improvements - new features and improvements are first released on a group of test servers, where they are thoroughly tested, and then they are sequentially released to groups of clients with a time window of one day;

- Regular server and code maintenance is carried out, which ensures that the best practices are always applied;

- Automated daily backups of the client's data, with additional team member validation that a backup was made;

- Multi-factor authentication options, to prevent unauthorized use, and to make sure that only the true owner of the Pabau account (staff member) can access the account;

- Constant monitoring on the health of the servers to detect and prevent anomalies before they affect the customer;

- Writing internal SOPs, and training of Pabau staff members on responding to disastrous situations.

Recovery Objectives

Pabau adheres to industry-standard Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for SaaS platforms. Our RTO is under 4 hours, ensuring that services are restored swiftly. Our RPO is under 24 hours, ensuring minimal data loss.

Service Level Objectives (SLOs)

Pabau targets 99.9% availability for core services on a monthly basis. This is a goal and not a guarantee, and is subject to the uptime SLA of DigitalOcean and critical third-party services.

Scope of the disaster recovery plan

Pabau as a CRM software offers features used by staff members, and patients, for booking appointments, sending communication, generating and paying invoices, and more. Some, or all of those features can become non-responsive, due to various factors. To prevent this from occurring, and minimize its impact, all the features are constantly being monitored.

List of the Pabau services covered in this plan are:

Service	Description
Pabau CRM web application	Used by staff members. Coverage includes logging in, client card, calendar, point of sale, schedule manager, access to setup pages and more.
Pabau Connect	Used by patients for booking appointments, viewing appointments, paying for appointments, viewing invoices, documents, and more.
Communications	Used automatically and manually to send email and SMS message to clients, for appointment confirmation, reminders, cancellation of appointments, recalls, sending email and SMS calls, and more.
Video conference	Used for online video calls to take place between patients and staff members.
iOS app	Used to communicate with the web version of Pabau to book appointments, view patient details, fill in medical forms, take patient photos, and more.

Disaster Response Processes

Client Communication During Incidents

The Incident Commander is responsible for updating affected clients at least once per hour

during major service disruptions. Updates will be published at https://pabau.instatus.com/, with additional communications via email if necessary. Milestone updates (diagnosed, resolved) will also be noted.

A high-level overview of the journey for responding to disaster-level events is described below:

1. An incident is reported:
   a) by a client to a customer support team member or account manager;
   b) by any Pabau team member who has access to monitoring tools, or spotted an issue while testing;
   c) by an automated alert set in place to warn when a threshold is reached.
2. Evidence is obtained and documented in a ticket sharing all the known information: (when the issue was detected, in which module, which action steps triggered the issue, screenshots, screencasts);
3. The assignee of the ticket does action steps to validate the root cause of the issue;
4. The issue is resolved and comments are left by the assignee as to what the cause was;
5. Quality assurance team member verifies the resolution;
6. The ticket is closed and it remains available for future reference;
7. The client is notified that the issue has been resolved (if reported by the client).

Monitoring and Incident Detection

Pabau uses New Relic for real-time performance monitoring and anomaly detection. All service status updates and incidents are transparently published at https://pabau.instatus.com/.

Pabau's server infrastructure is hosted on the DigitalOcean platform, which guarantees over 99% uptime SLA: https://docs.digitalocean.com/products/droplets/details/sla/#definitions

However, should issues occur, the actions steps that will take place to diagnose and fix the issue that led to a (potential) disaster:

1. Check if the site loads from a different ISP, or location or VPN to rule out ISP issues;
2. Check DigitalOcean's service status: https://status.digitalocean.com/;
3. Check if emails arrived for the service provider;
4. Check if recent code merge caused a conflict, and fix it;
5. Reboot the servers;
6. Check domain names and SSL certificates;
7. Refer to the our internal coda system to see if a similar incident occurred in the past and how it was resolved, then run the appropriate playbook
8. Notify the Lead DevOps Engineer and relevant developers;

In the event if the investigation showed that DigitalOcean itself is the culprit, by taking actions like restarting the servers, DigitalOcean's team will immediately be notified. They offer a support channel available 24/7.

Backup Policy

All Pabau client data, including flat files and databases, is backed up daily. Backups are securely stored and retained for a period of 6 months to support data integrity and recovery.

Personal Data Breach Response

If an incident is identified as a personal data breach under UK GDPR, Pabau will notify the client (Data Controller) without undue delay. The notice will detail the nature of the breach, affected data types, mitigation steps, and guidance for regulatory obligations. Pabau does not report breaches directly to the ICO on the client's behalf, but provides full transparency and technical context to support their reporting process.

In a very unlikely scenario of data corruption, and data loss, the last known good configuration shall be restored from the backup files.

While the issue is being resolved, as well as once the issue is resolved, progress updates will be shared with the client frequently, via email, slack, and via the https://status.pabau.com/ page.

In the event if post-disaster data restoration is needed, the following steps will take place:

1. Account manager to notify the client that data restoration will take place and that they shouldn't attempt to log-in and use the system;
2. Infrastructure team member to restore the client's server in the state it was prior to the disaster;
3. Infrastructure team member to restore the last backup file and verify that it's properly restored;
4. Quality assurance team member to perform tests and validate that the server and all its components are operational, as well as if the data is properly restored;

Leadership & Oversight

In disaster scenarios, the COO or CEO typically assumes the Incident Leader role, supported by the DevOps team. The COO also serves as the designated Data Protection Officer (DPO) for regulatory compliance, including ICO reporting.

Post-Incident Review

Following resolution of any major incident, a formal review is conducted and documented in Coda. The review includes a timeline of the event, root cause analysis, corrective actions taken, and recommendations for prevention. The findings are used to update internal playbooks and train relevant teams.

5. Account manager and staff members to validate the restored data, and sign off that the process was successfully completed;
6. Account manager to notify the staff members that their Pabau account is operational and that they can log in and resume with their activities.

Roles and Responsibilities

Disaster Severity Classification

To guide escalation and ensure timely response, all incidents are categorized using the matrix below:

Severity Level	Example Incident	Response Time	Escalation Path
Level 1 – Critical	Full platform outage or data loss	< 15 minutes	Incident Commander + CEO/COO + DevOps
Level 2 – High	Partial system degradation	< 1 hour	Support + DevOps
Level 3 – Low	Minor bug, no impact on usage	Next business day (issue will be logged and dealt with under normal triage)	Support Team

Document Ownership and Review

This Disaster Recovery Plan is reviewed on a quarterly basis to ensure accuracy and relevance. Responsibility for the document lies jointly with the CTO and COO.

Third-Party Service Dependencies

Pabau relies on key third-party providers for core functionality: AWS (file hosting), Stripe (payment processing), SendGrid (email delivery), Txtlocal (SMS within the UK), and Telynx (SMS outside the UK). These are monitored and included in our recovery considerations.

The personnel roles listed in the table below will be involved in resolving incidents of all levels:

Role	**Responsibility**
Customer Support or Account Manager	The first point of contact for the client. Responsible for obtaining information about and escalating the issue to the infrastructure team, and managing the communication between the client and the team working on resolving the incident.
Developer(s)	Responsible for identifying and fixing code-related issues, if such led to service interruption.
DevOps	Responsible for identifying and fixing server-related issues, and documentation
Quality Assurance	Responsible for validating that the issue has been resolved, effectively.
Incident Leader	Responsible for leading the response and coordination of resource

Revision of the recovery plan and training

Periodic disaster recovery plan reviews take place to ensure that the plan remains up to date and includes the latest trends and the business processes.

The periodic reviews shall also reflect any updated organizational priorities, changes or goals, ensuring that call lists and team lists remain up to date.

Regular training and surprise exercises are conducted with all the team members involved including deputies for each role, to ensure that the disaster recovery plan can be executed smoothly and effectively at any time, by all the team members involved.