

Business Continuity Plan

IronHub Inc

August 2026

Contents

1	Introduction	3
1.1	Purpose	3
1.2	Scope	3
1.3	Objectives	3
2	Risk Assessment and Business Impact Analysis	3
2.1	Risk Identification	3
2.2	Business Impact Analysis (BIA)	3
3	Roles and Responsibilities	4
3.1	Crisis Management Team	4
3.2	Key Contacts	4
4	Business Continuity Strategies	5
4.1	Preventative Measures	5
4.2	Response Strategies	5
4.3	Recovery Strategies	5
5	Communication Plan	5
6	Data Management and IT Resilience	5
7	Plan Testing and Maintenance	6
8	Appendices	6
8.1	Appendix A: Organization Chart	6
8.2	Appendix B: Employee Contact Information	6
8.3	Appendix C: Vendor and Critical Service Provider List	6

Table 1: Document history

Date	Comment
Jan 10 2025	Initial document
Apr 21 2026	Updated crisis management team, key contacts, vendor list, and plan testing requirements

1 Introduction

1.1 Purpose

The purpose of this Business Continuity Plan (BCP) is to outline the strategies and procedures for IronHub to respond to, recover from, and continue operations during disruptions.

1.2 Scope

This plan applies to all departments, employees, critical business functions, and technology infrastructure within IronHub. It focuses on network and server infrastructure, data storage, backup systems, and other IT devices such as end-user computers. Non-IT related disasters such as personnel, human resources, and real estate matters are beyond its scope.

1.3 Objectives

- Ensure the safety of employees and stakeholders.
- Minimize financial and operational losses.
- Maintain essential business functions.
- Ensure effective communication during crises.

2 Risk Assessment and Business Impact Analysis

2.1 Risk Identification

A disaster can be caused by man or nature and may include:

- Cyber-attacks, including ransomware, phishing, and data breaches.
- Server and internet outages impacting critical business operations.
- Fire, flooding, earthquake, blizzard, or other environmental events.
- War or terrorist attacks.
- Theft.
- Pandemics.
- Any event that puts the health or safety of personnel or the public at risk.

2.2 Business Impact Analysis (BIA)

- Vital systems must be functional for business continuity.
- Risks include IT infrastructure failures and inability to access office premises.

- Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined based on criticality and documented in the Disaster Recovery Policy.

System / Function	RTO	RPO	Criticality
Production platform (Heroku/AWS)	4 hours	24 hours	Critical
Customer database	4 hours	24 hours	Critical
Internal communications (Slack, Email)	8 hours	24 hours	High
Development environment	48 hours	48 hours	Medium
Office premises	48 hours	N/A	Medium

3 Roles and Responsibilities

3.1 Crisis Management Team

Name	Role	Responsibilities
Taylor Assaly	President & CEO	Officially declare disaster status, sign contractual agreements for recovery.
Ray Yip	CTO	Oversee IT infrastructure restoration and data recovery.
Mathieu Spehler	Operations Manager	Ensure employees have necessary tools, manage external communications.
[HR Manager]	HR Manager	Employee safety and communication.

3.2 Key Contacts

Contact	Role / Organization	Phone / Email
Taylor Assaly	President & CEO	(587) 783-8393 / taylor@theironhub.com
Ray Yip	CTO	ray@theironhub.com
Mathieu Spehler	Operations Manager	+1 403-912-5930 / mathieu@theironhub.com
Arie Prins	CFO	arie@theironhub.com
Mavis Andersen-Busch	Account Manager	403-807-9299 / mavis@theironhub.com
Heroku Support	Platform provider	https://help.heroku.com/
AWS Support	Cloud infrastructure	https://aws.amazon.com/support/
Cyber Insurer	Cyber incident response	See cyber insurance policy documents

4 Business Continuity Strategies

4.1 Preventative Measures

- Regular automated data backups (daily, retained for 30 days) via Heroku Postgres.
- IT security protocols including MFA, encryption, and vulnerability management.
- Disaster preparedness training conducted at least annually.
- Cyber insurance coverage for cyber events including ransomware and business interruption.

4.2 Response Strategies

- Activation of the BCP upon declaration by the CEO or designated delegate.
- Evacuation and emergency response procedures per local emergency protocols.
- Employee safety protocols communicated via Slack and personal email.
- Immediate notification of cyber insurer for cyber-related disruptions.

4.3 Recovery Strategies

- Restoring IT systems and infrastructure per the Disaster Recovery Policy.
- Remote work capability for all employees as primary continuity option.
- Customer communication plans coordinated by Operations Manager.

5 Communication Plan

- **Internal Communication:** IronHub email, Slack, mobile phone, personal email, video conference.
- **External Communication:** Customers informed via website updates, email notifications, and direct outreach from the Operations team.
- **Regulatory Notification:** The ISM is responsible for notifying applicable regulators within required timeframes in the event of a breach or significant outage.

6 Data Management and IT Resilience

- Daily automated backups of production database via Heroku Postgres, retained for 30 days.

- Backups tested for recoverability at least quarterly per the Availability Policy.
- Cybersecurity measures including WAF (Cloudflare), MFA, encryption, and access controls.
- All production data replicated across Heroku and AWS managed infrastructure with built-in redundancy.

7 Plan Testing and Maintenance

- The BCP is reviewed and updated at least annually, or following any significant incident or infrastructure change.
 - Tabletop exercises are conducted at least annually involving the Crisis Management Team to identify and resolve gaps.
 - Disaster recovery testing is conducted at least annually per the Disaster Recovery Policy.
 - Test results and action items are documented and incorporated into updates to this plan within 30 days of the exercise.
-

8 Appendices

8.1 Appendix A: Organization Chart

Maintained by Human Resources. Current version available upon request.

8.2 Appendix B: Employee Contact Information

Maintained by Human Resources. Current version available upon request.

8.3 Appendix C: Vendor and Critical Service Provider List

Service	Provider	Contact
Development Consultants	Ascendcor	support@ascendcor.com
Application & DB	Heroku	https://help.heroku.com/
Hosting	(Salesforce)	
Cloud Storage & IAM	AWS	https://aws.amazon.com/support/
DNS / WAF	Cloudflare	https://support.cloudflare.com/
Monitoring & Alerting	DataDog	https://www.datadoghq.com/support/
Error Tracking	Rollbar	https://rollbar.com/support/
Internet Service Provider	Shaw Cable	1-888-472-2222