

Disaster Recovery Policy

IronHub Inc

August 2026

Contents

1 Purpose and Scope	2
2 Background	2
3 Policy	3
4 Appendix A: Relevant Points of Contact	5
5 Appendix B: Recovery Steps for Information Systems Infrastructure & Services	6

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	A1.2, A1.3

Table 2: Document history

Date	Comment
Jun 1 2022	Initial document
Jan 1 2023	Updated contact info
Jan 10 2025	Updated contact info

1 Purpose and Scope

- a. The purpose of this policy is to define IronHub's procedures to recover Information Technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident. The objective of this plan is to complete the recovery of IT infrastructure and IT services within a set Recovery Time Objective (RTO).
- b. This policy includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management.
- c. This policy applies to all management, employees and suppliers that are involved in the recovery of IT infrastructure and services within IronHub. This policy must be made readily available to all whom it applies to.

2 Background

- a. This policy defines the overall disaster recovery strategy for IronHub. The strategy describes IronHub's Recovery Time Objective (RTO), which is defined as the duration of time and service level for critical business processes to be restored after a disaster or other disruptive event, as well as the procedures, responsibility and technical guidance required to meet the RTO. This policy also lists the contact information for personnel and service providers that may be needed during a disaster recovery event.
- b. The following conditions must be met for this plan to be viable:
 - i. All equipment, software and data (or their backups/failovers) are available in some manner.
 - ii. If an incident takes place at IronHub's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.
 - iii. The Information Security Officer is responsible for coordinating and conducting a bi-annual (at least) rehearsal of this continuity plan.
- c. This plan does not cover the following types of incidents:
 - i. Incidents that affect customers or partners but have no effect on IronHub's systems; in this case, the customer must employ their own continuity processes to make sure that they can continue to interact with IronHub and its systems.
 - ii. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Heroku, and Amazon Web Services. IronHub depends on such suppliers to employ their own continuity processes.

3 Policy

a. *Relocation*

- i. If IronHub's primary work site is unavailable, an alternate work site shall be used by designated personnel. IronHub's alternate work site is located at Platform Calgary, 407 9 Ave SE, Calgary, AB T2G 2K7.
- ii. The personnel required to report to the alternate work site during a disaster includes CEO, CTO, and Operations Manager.

b. *Critical Services, Key Tasks and, Service Level Agreements (SLAs)*

- i. The following services and technologies are considered to be critical for business operations, and must immediately be restored (in priority order):
 1. Client support phone line
 2. Client support email service
 3. Network connectivity
 4. IronHub production application servers
 5. IronHub production database
- ii. The following key tasks and SLAs must be considered during a disaster recovery event, in accordance with IronHub's objectives, agreements, and legal, contractual or regulatory obligations:
 1. Determine the level of severity and escalate to senior executives when the situation has high level impact or severity
 2. Notify all clients immediately regarding the situation, actions taken, and recovery ETA when it's available
 3. Provide regular updates to all clients at least hourly regarding current status, actions taken, and recovery ETA when it's available
 4. Restore all production servers and databases within RTO

c. IronHub's Recovery Time Objective (RTO) is 4 hours during weekdays and 12 hours during weekends. Relocation and restoration of critical services and technologies must be completed within this time period.

d. *Notification of Plan Initiation*

- i. The following personnel must be notified when this plan is initiated:
 1. Taylor Assaly, President & CEO
 2. Ray Yip, CTO
- ii. VP Operations is responsible for notifying the personnel listed above.

e. *Plan Deactivation*

- i. This plan must only be deactivated by Taylor Assaly, President & CEO or Ray Yip, CTO.
- ii. In order for this plan to be deactivated, all relocation activities and critical service / technology tasks as detailed above must be fully completed and/or restored. If IronHub is still operating in an impaired scenario, the plan may still be kept active at the discretion of Taylor Assaly, President & CEO or Ray Yip, CTO.
- iii. The following personnel must be notified when this plan is deactivated:
 1. CEO
 2. CTO
 3. Operations Manager
- f. IronHub must endeavor to restore its normal level of business operations as soon as possible.
- g. A list of relevant points of contact both internal and external to IronHub is enclosed in Appendix A.
- h. During a crisis, it is vital for certain recovery tasks to be performed right away. The following actions are pre-authorized in the event of a disaster recovery event:
 - i. CTO must take all steps specified in this disaster recovery plan in order to recover IronHub's information technology infrastructure and services.
 - ii. CTO is authorized to make urgent purchases of equipment and services up to \$10,000.
 - iii. Operations Manager is authorized to communicate with clients.
 - iv. Operations Manager is authorized to communicate with the public.
 - v. Operations Manager is authorized to communicate with public authorities such as state and local governments and law enforcement.
 - vi. CTO is authorized to cooperate with Google, Heroku, and Amazon Web Services.
- i. Specific recovery steps for information systems infrastructure and services are provided in Appendix B.

4 Appendix A: Relevant Points of Contact

Internal Contacts

Name	Job Title	Phone Number	Email Address
Taylor Assaly	President & CEO	(587) 783-8393	taylor@theironhub.com
Ray Yip	CTO	403-605-7012	ryip@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

External Contacts

Name	Job Title	Phone Number	Email Address
Ashley Lloyd	Director Of Operations	204-291-4428	ashley@chatterson.co

5 Appendix B: Recovery Steps for Information Systems Infrastructure & Services

Specific recovery procedures are described in detail below:

Recovery Procedure	Person Responsible	Person(s) Notified When Complete
Restore production servers :	CTO	CEO
1. Restore AWS connectivity	Lead Developer	CTO
2. Restore Heroku Pipeline	Lead Developer	CTO
3. Restore production database	Lead Developer	CTO
4. Restore production API	Lead Developer	CTO
5. Restore production client app	Lead Developer	CTO
6. Restore production admin app	Lead Developer	CTO
Restore staging/demo servers :	CTO	CEO
1. Restore staging database	Lead Developer	CTO
2. Restore staging API	Lead Developer	CTO
3. Restore staging client app	Lead Developer	CTO
4. Restore staging admin app	Lead Developer	CTO