Business Continuity and Disaster Recovery Plan

Business Continuity and Disaster Recovery (BC/DR) Plan

Policy Owner: Valentín Torassa Colombero

Effective Date: Jun 30, 2025

Purpose

The purpose of this business continuity plan is to prepare Teramot in the event of service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Scope

All Teramot IT systems that are business critical. This policy applies to all employees of Teramot and to all relevant external parties, including but not limited to Teramot consultants and contractors.

In the event of a loss of availability of a hosting service provider, the Chief Technology Officer (CTO) / Chief Information Security Officer (CISO) will confer with the Platform Engineer to determine an appropriate response strategy.

General requirements

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the Teramot office, senior managers and executive staff shall determine mitigation actions.

A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.

Alternate work facilities

If the Teramot office becomes unavailable due to a disaster, all staff shall work remotely from their homes or any safe location.

Communications and escalation

Executive staff and senior managers should be notified of any disaster affecting Teramot facilities or operations.

Communications shall take place over approved channels such as Slack and email.

Teramot maintains key contact information via our corporate Slack workspace and email system. All team members can be reached through their @teramot.com email addresses or Slack handles. In the event of an incident, escalation paths follow the company's organizational chart and are handled directly via Slack channels and email.

Roles and responsibilities

Role	Responsibility
Chief Technology Officer (CTO)	Leads Business Continuity and Disaster Recovery (BC/DR) efforts to mitigate service disruption and recover Teramot's infrastructure, systems, and network environments. Coordinates with security and platform teams to ensure secure recovery.
Department Heads	Responsible for communicating with their respective departments and ensuring continuity of business operations. They coordinate closely with executive leadership to align response actions.
Team Leads / Functional Managers	Ensure communication and support for their direct reports during incidents. Facilitate continued productivity from alternate locations or under degraded conditions.
Chief Executive Officer (CEO)	Responsible for high-level decision-making and for leading external communications to customers, partners, and other stakeholders regarding the organization's continuity status.
Product Owner	Coordinates with engineering and operations to prioritize service recovery efforts from a product and customer experience perspective.
Cybersecurity & Compliance Analyst	Ensures all BC/DR activities comply with security, privacy, and regulatory requirements. Provides guidance on secure recovery and incident response alignment.
Office Manager / Operations Lead	Oversees employee safety and physical office matters during continuity events. Coordinates logistics, access, or relocation efforts as needed.

Continuity of critical services

Procedures for maintaining continuity of critical services in a disaster can be found in Appendix A.

Recovery Time Objectives (RTO) and Recovery Point Objects (RPO) can be found in Appendix B.

Strategy for maintaining continuity of services can be seen in the following table:

Key business process	Continuity strategy
Customer (Production) Service Delivery	Teramot services are deployed on AWS. We rely on AWS's high-availability architecture and SLAs. Services are containerized and can be redeployed across regions if needed.
IT Operations	All infrastructure is cloud-based and managed via Infrastructure as Code (Terraform).
Email	Email is handled via Google Workspace (Gmail), leveraging Google's geo-redundant infrastructure and SLA.
Finance, Legal, and HR	These functions are handled through third-party SaaS providers with their own continuity strategies. No on-premise systems are required.
Sales and Marketing	All sales and marketing tools (CRM, automation platforms, etc.) are cloud-based SaaS applications, with multi-factor authentication enabled and vendor SLAs in place.
Internal Communications	Slack is used for internal communications. In the event of disruption, fallback communication occurs via email and predesignated channels.
Code Repositories and Development Tools	Hosted on GitHub and cloud services. Engineers can work remotely, with all assets accessible via VPN or secure cloud credentials.
Incident Response and Security Monitoring	Managed internally and monitored via cloud-native tools. Critical event workflows are documented and accessible via secure channels.

Plan activation

This BC/DR shall be automatically activated in the event of the loss or unavailability of the Teramot office, or a natural disaster (i.e., severe weather, regional power outage, earthquake) affecting the larger Lewes, Delaware region.

Version history

Version	Date	Description	Author	Approver
1.0	Jun 30, 2025	Version 1.0	Valentín Torassa Colombero	Bruno Ruyu

Appendix A - Business continuity procedures by scenario

Business Continuity Scenarios

HQ Offline (Power and/or Network)

- Slack, GitHub, Google Workspace (Email, Calendar, Drive), AWS **unaffected**
- Support operations continue via remote staff
- Engineering and Deployment activities continue remotely

Procedure**:**

- HQ staff relocate to home offices (30-60 minutes)
- Verify VPN, AWS, GitHub, Slack and Google Workspace access (10 minutes)
- Remotely resume normal operations

Colo / Cloud Region Offline (Power and/or Network)

- Slack, Google Workspace, AWS and internal communications **unaffected**
- Some production workloads may be temporarily affected depending on failover configuration
- Engineering and Ops teams continue working remotely

Procedure:

- Notify impacted customers (via status page or support email)
- Failover to alternate AWS region if necessary
- Resume normal operations once infrastructure is restored

Disaster Event at HQ

- Corporate SaaS tools (Slack, Gmail, Google Meet, AWS) **unaffected**
- Office unavailable or partially accessible
- Support and Engineering continue via remote work

Procedure:

- All HQ staff switch to remote work
- Notify internal teams of potential delays
- Reassign critical tasks to remote engineers and team leads
- Ensure security controls remain active (VPN, IAM)

SaaS Tool Outage

Slack, Gmail, Google Meet, GitHub or other core SaaS tools are affected.

Impact:

- Support operations partially impacted (manual triage required)
- Development teams may be affected depending on tool

Sub-scenarios:

Slack Down

- Use fallback: internal group email threads or direct phone calls
- Critical incidents escalated via SMS or alternate channels

Gmail Down

- Use alternate backup addresses (pre-approved fallback addresses)
- Notify affected stakeholders via alternate channels
- Critical customer emails rerouted via Support Portal

GitHub Down

- Code changes paused; developers may continue work locally
- Resume pushing and deployment when service returns
- Security commits and patches prioritized on return

Google Meet / Zoom Down

- Use alternate conferencing tools (Jitsi, Whereby, etc.)
- Notify meeting participants of switch

Appendix B - RTOs/RPOs

Rank	Asset	Affected Assets	Business Impact	Users	Owners	RTO	RPO	Comments / Gaps
1	Google Datacenters	Site	Core collaboration tools (Gmail, Docs, Meet, Drive) offline	All	Engineering	2 hours	15 min	Rely on Google SLA and redundancy
2	Corporate Office	Site	Temporary office unavailability; no production impact	All	IT Ops	24 hours	N/A	All systems accessible remotely; fallback to home offices
3	Corporate Network	Network	On-premises resources (printing, internal WAP) unavailable	All	IT Ops	8 hours	N/A	Minimal impact due to cloud-first strategy
4	AWS Cloud (Primary)	Network / Compute / Storage	Full production service disruption (Auto-ETL, One, Web App)	All Customers	Engineering	1 hour	15 min	Critical. Multi-AZ failover, backups in S3. Rely on AWS high availability
5	Home Office ISP Networks	Network	Potential developer/staff unavailability	Dev / IT Ops	IT Ops	N/A	N/A	Mitigated by flexible scheduling, mobile hotspots
6	Personal Workers Laptops	Hardware	Developer or support agent cannot work	All	IT Ops	4 hours	30 min	Devices are monitored, encrypted, and replaceable; spares available
7	Personal Mobile Devices	Hardware	Potential productivity impact if staff uses mobile-only access	All	IT Ops	N/A	N/A	Not relied upon for critical access; fallback exists
8	Wireless Access Points (WAP)	Hardware	Loss of wireless network in office	All	IT Ops	8 hours	N/A	Wired fallback and LTE modems available