Disaster Recovery Plan

Castle

Table of Contents

Disaster Recovery Plan

Purpose

Having a viable Disaster Recovery Plan (DRP) is a fundamental responsibility of every organization. This plan has been written for use in the event of a disaster affecting the data centers or other computing facilities of Castle.

In the event that Castle leadership initiates disaster recovery procedures, then all members of the Disaster Recovery Team will follow the procedures contained in this plan until recovery and resumption of service is complete. Operational day-to-day incidents are not addressed by this plan, but rather by the Castle procedures and Security Incident Response Policy.

Once completed, tested, and approved, this plan will contain all the information necessary to guide the restoration of operational services in the event of a serious disruption of computer or communication services at Castle.

Business Continuity

This DRP covers all the necessary recovery elements that would assist Castle in case of a disaster. While a formal Business Continuity Plan (BCP) does not exist separately, it is considered incorporated by reference into this DRP.

Castle is a fully-virtualized organization, with no physical (local or otherwise) centralized IT resources (servers, networks, etc.) under direct management. All of Castle‘s operations are managed in cloud environments; its service delivery environment is in AWS, and it’s back-office operations are outsourced to a variety of cloud-based SaaS providers.

Because of the nature of the Castle as fully virtualized, there is no difficulty in ensuring business continuity even in the event that a disaster strikes the area of its headquarters. Operations will generally continue uninterrupted, with surviving employees managing them remotely as they normally do. Even if a major disaster results in a complete loss of all Castle leadership and/or technical staff, the venture capital shareholders will simply be able to restaff the organization to continue operations as necessary.

For this reason, Castle does not maintain an independent Business Continuity Plan (BCP). This decision will regularly review by the Security Leadership Committee (SLC), and may change at any time to address emerging business needs.

Scope

Within the context of this document, a disaster is defined as an incident that results in the loss of computer processing or telecommunications at a Castle location to the extent that relocation to an alternate facility (physical or virtual) must be considered. A disaster can result from several accidental, malicious, or environmental events such as fire, flood, earthquake, terrorist attack, human error, or software/hardware failures.

The primary objective of this DRP is to ensure the continued operation of identified critical operations in the event of a disaster. This plan is not meant to respond to daily operational outages such as a single system outage, but rather an incident that requires a significant portion of the infrastructure in a location to be rebuilt, a majority of the systems to be restored, or a move out of a primary location or region for more than a day.

Specific goals of this plan are:

- To reinstate Castle's computer operations and network communications in a rapid and timely manner.
- To reinstate Castle's critical management tools at the recovery site or region in a rapid and timely manner.
- To minimize the disruption to Castle's critical business processes.

Exceptions

This plan specifically does not address the disaster recovery needs of customers with services located at an affected location. While Castle will make every effort to assist customers impacted by a disaster-level event, responding to customer requests to relocate, repair, or replace equipment, restore network services, or otherwise integrate into customer disaster recovery plans is outside the scope of this document.

Policy

Team Structure

The Disaster Recovery Team (DRT) is comprised of members of Engineering, Facility, Information Technology, and Operations teams deemed critical to the success of likely disaster response and recovery efforts. These personnel form the core of the DRT, but this list is not exhaustive; at the discretion of DRT leadership, other Castle personnel or other outside resources may be leveraged as an extended member of the DRT.

DRT Leadership

The leaders of the Disaster Recovery are as follows:

Executive Sponsor	Johan Brissmyr	CEO
Disaster Recovery Team Lead	Sebastian Wallin	CTO

DRT Team Members

Name	Role
Filip Tepper	Software Engineer
Valerie Kirk	Business Operations Manager

Disaster Recovery Plan

Tomasz Pajor	Senior Developer

Disaster Recovery Roles & Responsibilities

DRT members are expected to work cooperatively during the course of a disaster-level event to mitigate or correct effects resulting from the event. In addition to the general duties of a DRT member, the following specific roles are identified within the structure of this plan:

Disaster Recovery Manager (DRM)

For each activation of the plan, there will be an identified DR Manager (DRM), who will be responsible for coordinating recovery efforts, recording steps and actions taken, and ensuring effective communicating with senior leadership, external vendors, and customers. This will normally be the DRT Lead, unless he or she is unavailable.

The DRM is responsible for holding a Root Cause Analysis (RCA) review following any activation of this plan within 1 week of plan deactivation.

Response Action Plan

Because of the unpredictable nature of disaster-level events, and expectation that they will vary in nature and the detailed response required, this plan is intended to provide a general framework to guide response and recovery efforts without dictating a specific structure. However, this plan has established the following general steps following declaration of a disaster and plan activation:

Damage Assessment

Expected Duration: T + 15 mins to 2 hours

Immediately following activation, members of the DRT will gather any available information necessary to characterize and ascertain the specific nature of the event, including:

- Affected system(s)
- Nature of damage
- Root cause(s)
- Any functional assets
- Impact(s) to Castle and its customers

This information will be provided to the DRM and the other members of the DRT to aid in their information gathering and further recovery efforts.

Containment & Initial Mitigation

Expected Duration: T + 4 to 24 hours

Following initial assessment information gathering, and once the team and the DRM are confident they have a thorough understanding of the event, containment and initial mitigation efforts will commence.

Containment

Where possible, the DRT will attempt to prevent the spread or expansion of the event. In cases where a location is partially available, this may mean disabling or powering down affected assets, deactivating environmental or network countermeasures, or other tasks designed to maintain the operational status of functional assets. In more extreme cases where entire locations are offline, network links may be disabled to prevent corrupted data (such as invalid routing table entries) from propagating.

Initial Mitigation

DRT members will begin to mitigate the effects of the disaster, using whatever assets, tools, and temporary workarounds available to stabilize and restore services (if possible). Mitigation efforts during this phase are focused on immediate results rather than long-term planning.

Recovery Planning

Expected Duration: 8 to 48 hours

Once containment and initial mitigation efforts are well underway or complete, DRT leadership will begin defining the longer-term recovery plan. The recovery plan is intended to guide the business in establishing short (3 days or less), medium (1-3 weeks), and long (1 month or longer) term recovery milestones and operating plans to compensate for the disruption caused by the event.

The recovery plan is expected to be an evolving document, and in many cases only the short-term milestones will be established prior to entering the Recovery phase.

Recovery

Expected Duration: 3 days to 1 month

Upon agreement on a Recovery Plan, the DRT will begin to implement changes, engage outside vendors, move resources (including people and system) to alternate locations, and operationalizing any workarounds deployed during the initial mitigation phase.

During the Recovery phase, the DRT will focus on re-establishing normal operations (to the extent possible) while maintaining availability of all operational assets. Efforts during this phase should, wherever possible, balance long-term operating goals against immediate needs.

Operational Transition

Once the Castle's operations have stabilized to the extent possible within the confines of disaster response and the DRT, and recovery efforts are underway, this plan may be deactivated at the discretion of the DRM, DRT Lead, and executive sponsor. As part of plan deactivation, all assets, documentation, and records will be provided to operational teams as part of the handoff. All emergency changes made as part of the plan are to be recorded in change management systems.

Updates to this Plan

This plan must be kept up-to-date to successfully guide recovery efforts.

It is the responsibility of the DRT Lead to ensure that procedures are in place to keep this plan up to date. It is also the role of the Disaster Recovery Team members to notify the DRT Lead as significant changes and upgrades are made in the production environment, and assist in updating the plan. The DRT Lead is required to update this plan no less than once per calendar year.

Following any real or simulated activation of the DR plan, the DRT Lead is expected to work with DRT members and senior leadership to update the plan with any lessons learned or other plan deficiencies identified in the plan.

Plan Distribution

Any time this plan is revised, copies are to be provided to all DRT members, the executive sponsor, and Engineering team. Additionally, a physical copy of this plan is to be stored in each data center location or other Castle facility.

Testing the Plan

In order to ensure that this plan is as current, accurate, and relevant as possible, as well as proactively identify issues with this plan, the DRT Lead is responsible for ensuring that this plan is tested regularly, and improvements are made following plan tests. The DRT Lead must work with team members to perform a structured walkthrough of this plan at least once per calendar year.

Process

Plan Activation

The decision to initiate DR procedures will be made by the Chief Technical Officer (CTO) or their backup (CEO) after assessing the situation following a disaster or crisis. In the event that neither party is available, a consensus decision can be made by a majority of the available DRT members. At this time, the person(s) activating the plan will identify the DR Manager (DRM) (see *Roles & Responsibilities* above.)

Once the plan has been activated, attempts will be made to contact all DRT members required to respond to the nature of the event, and request that they join the incident conference bridge. The DRM will establish a conference bridge using Castle VOIP conference account.

Response Management

The DRM is responsible all oversight during the initial and follow-up phases of this plan. During all phases of the plan, the DRM will establish regular communication intervals when he or she

expects to receive updates from DRT members. If, during the course of the event, the team cannot reach consensus on the correct approach, the DRM will arbitrate a conclusion.

In the event that the DRM cannot reach members of senior leadership during the *Damage Assessment* or *Containment & Initial Mitigation* phases of the response, they are empowered to follow the recommendations of the DRT and act in the Castle's best interest, with the overriding goal of stabilizing Castle operations.

Communication

The DRM will communicate regularly with employees, senior leadership, and customers during any plan activation. The DRM is expected to provide updates at the following milestones:

- **During initial damage assessment**
  - The DRM will notify all available senior leadership of activation plan and any initial information regarding the event once the DRT has begun initial damage assessment, and provide an expected timeline for further information.
  - Depending on how long the assessment phase is expected to take, the DRM may elect to send an initial message to customers notifying them of the event and when to expect further information.
- **When damage assessment is complete**
  - The DRM will update leadership once the event is fully qualified and understood, providing them information about the details of the event, expected impacts, and any initial planned containment and mitigation steps.
  - At this time, the DRM and senior leadership will decide what external and broader internal communication is required.
- **During containment and initial mitigation**
  - The DRM will provide updates as necessary during the initial containment and mitigation phases, updating leadership on progress and the results of mitigation efforts.
  - At the end of mitigation efforts, the DRM will send a summary to leadership and present an estimated timeline for recovery planning.
- **Upon completion of the recovery plan**
  - Once the recovery plan has been formulated, the DRM will present it to leadership for evaluation, comment, and feedback.
  - Once the recovery plan has been agreed upon and approved, customer communication will be crafted and sent.
- **During recovery**
  - During implementation of the recovery plan, the DRM will provide updates to senior leadership, employees, and customers at a frequency established by senior leadership.

Appendix A: Contact Information

DRT Emergency Contact Information

Below is a list of the emergency contact information for all current members of the Disaster Recovery Team (DRT):

Name	Role	E-Mail	Cell Phone
Johan Brissmyr	CEO	johan@castle.io	+14152549224
Sebastian Wallin	CTO	sebastian@castle.io	+46701739939
Filip Tepper	Software Engineer	filip@castle.io	+48789282345
Valerie Kirk	Business Operations Manager	valerie.kirk@castle.io	+16127355695
Tomasz Pajor	Senior Developer	tomek@castle.io	+48518612810

Critical Vendor Contact Information

Below is a list of vendors or suppliers that, depending on the nature of the event, may be critical in aiding in recovery:

Vendor	Service	Contact Name	Contact Method	Phone(s)
Multi-Site / Shared Services				
AWS	Cloud Services	AWS Support	AWS Support Console	NA