DISASTER RECOVERY & BUSINESS CONTINUITY PLAN

Purpose

This Disaster Recovery and Business Continuity Plan ("DR/BCP" or "Plan") covers protocols in the event of extended service outages caused by unforeseen and/or unavoidable disasters and to restore services to the widest extent possible in a reasonable time frame. The disaster could be natural, environmental, or man-made. Man-made disasters could be intentional (for example, an act of terrorism) or unintentional (that is, accidental, such as a system misconfiguration). This Plan covers mission-critical business functions and associated systems.

- Disaster Recovery is a documented set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a disaster.
- Business continuity ensures all essential aspects of Caylent's business functions are able to operate despite significant disruptive events.

Assumptions

This Plan is developed based on the following assumptions

1. Key people (team leaders or alternates) will be available following a disaster.
2. This document and all vital records, which are stored in a secure off-site location, not only survive the disaster but also are accessible immediately following the disaster. The electronic document lives within Caylent's internal policy documentation site.
3. Each critical business segment has its own plan consisting of unique recovery procedures, critical resource information.
4. Alternate sites are available for working.
5. Critical systems are hosted by third party providers.

Objectives

During a disaster, this Plan will seek to achieve the following objectives:

- Secure employee safety and well-being. This includes the safety and well-being of employee's families. In certain disaster circumstances, this may be the only objective;
- Protect Caylent clients' ability to continue to do their business;
- Protect Caylent's reputation with customers, suppliers, and investors; and
- Protect Caylent's revenue streams.

Scope

Mission Critical Activities

The scope of this Plan includes mission-critical business activities and the associated systems to achieve the objectives outlined above. The scope also includes how Caylent will address the unavailability of a key supplier or partner, including temporary workarounds or partial mitigations to provide business continuity. The primary activity in a disaster and business continuity scenario is support for existing customers, including Hotfixes, which is an urgent measure taken to address a critical issue outside the normal workflow, as needed.

Geographic Locations

The scope covers business continuity and emergency response for all of our employees and contractors ("Resources") globally, including those working remotely.

Threats

The DR/BCP is invoked following an incident or series of incidents that impacts the ability of the organization to provide an acceptable level of service, or otherwise affects other key operations for an unacceptable period of time. The type of disasters / incidents that may impact the business operations are listed below:

- **Human (Internal)** - Intentional or unintentional human intervention has affected systems or the business. This can include an internal hacker, an intruder on-site, employee manual error, etc.
- **Human (External)** - Intentional or unintentional actions by a person or group that has affected systems or the business. These may include an external hacker, terrorist threats, explosions, etc.
- **Natural** - Natural disasters such as flooding, fires, earthquakes, etc.
- **Vendor/Service Provider** - A key vendor has an unacceptable level of downtime such that Caylent operations are impacted, or supply chain issues arise where a key vendor on which Caylent relies is no longer available.

Any one of these events can have varying degrees of impact. The scope of this Plan includes the roles, responsibilities, and processes that will be followed to allow effective response. This Plan focuses on the following scenarios as a basis from which to build on other scenarios:

- Employees or contractors cannot leave their homes (lockdown, transportation systems are down, etc.);
- Critical systems, equipment, or other tools are down or inaccessible; and
- An internal situation is preventing employee or contractor ("Resource") productivity.

Emergency Response Team

Composition

The ERT manages Caylent's response to major threats, emergencies or disasters. It is made up of members from each of the following departments with a mission critical business activity. These include:

- Finance
- Customer Success and Delivery
- Support
- Engineering
- Compliance
- Human Resources
- Sales
- Executives

The ERT Chair is currently the CEO of Caylent. The Chief Financial Officer and General Counsel serve as delegates in case the CEO is unavailable. The chair may rotate depending upon the nature of the disaster at the discretion of the CEO. If a security incident which threatens the continuity of business operations is identified, the Security Incident Response Team will lead the response. Please see the security incident response Plan for additional information. If not already included in the above, representation from both offices will be included in the ERT.

Responsibilities

The major responsibilities of the ERT are:

- **Evaluation:** Evaluate incidents to determine if this Plan should be invoked.
- **Decision-making**: Make decisions on how and when to respond to disasters and ensure continuity of the business.
- **Communications**: Coordination of communications to employees, partners, customers, vendors, investors and media as needed.
- **Monitor and escalate**: Monitor recovery efforts and on-going business impact. Escalate to Board if recovery efforts are off-track. Provide status of recovery efforts to key stakeholders.
- **Coordination**: Provide a single point of coordination for recovery needs as necessary. This includes ensuring that financial, legal and logistical support is available.
- **Resources**: Ensure that appropriate resources are allocated to facilitate recovery from the disaster.

Activation of ERT

The ERT Chair is notified of a potential disaster through the following:

- Incident response process
- Building management
- Government disaster communications
- Other employees
- Peer companies/vendors

The ERT Chair will either unilaterally make a decision or confer with ERT team members to evaluate the disaster and determine if the DR/BCP will be activated. Any member of the ERT team may 'activate the ERT' in the event the Chair is detained. Upon ERT activation, ERT team members who are not already in conference are notified to report to the ERT Chair.

- ERT team members report to the ERT Chair (or report their status as required)
- ERT team members will coordinate a call in which the ERT will:
    - **Assess the impact** - Determine who, what, when, where, how & why ("what's going on & how bad is it?")
    - **Decide** - Determine what's broken; ignore what's working & prioritize the issues & choose course of action
    - **Act** - Take timely and decisive action based on urgency and importance of resolution

Throughout the recovery process, the ERT team will meet regularly to monitor progress of recovery. Frequency will be defined by the ERT Chair, depending upon the nature of the disaster and may change throughout the recovery process. This process will end once operations are restored to original working conditions.

Disaster Response and Recovery Coordinator

The Disaster Response and Recovery Coordinators ("DR Coordinators") are charged with the responsibility for responding to disasters for Caylent, and for implementing the decisions made by the ERT during a disaster. The function of the DR Coordinators is vitally important to maintaining the Plan in a consistent state of readiness. The DR Coordinator's role is multifaceted. Not only do they assume a lead position in the ongoing life of the Plan, but they also have the following responsibilities:

- Distribution of the Disaster Recovery Plan
- Review, change and update the Disaster Recovery Plan
- Facilitate communication between technical and non-technical staff
- Report progress of response and recovery to the ERT
- Act as a Project Manager to coordinate the efforts of:
    - Technical staff
    - Management team
    - Vendors
    - Other personnel as needed

Facility and Alternate Business Site Strategy

Caylent Resources are fully remote and Caylent does not maintain corporate offices. Further, Caylent does NOT maintain any sensitive customer data on any on-premise servers or on Caylent computers/devices. Caylent Resources can access any critical cloud-based systems from any secure location with an internet connection (subject to compliance with Caylent's IT Security Policies).

Key Systems

The key objective of Caylent's DR/BCP is the quick continuation of services to our clients. Beyond our people, our key technical assets include third-party applications on which our business depends. It is access to, and availability of these tools that Caylent staff utilizes to conduct day-to-day operations.

None of these systems have direct or indirect connections to our clients' operational systems or sensitive customer data as Caylent does not maintain or store any Client data.

- **P1** systems are those that must be restored within 24 hours in order for Caylent to maintain normal day-to-day operations.

- **P2** systems are those where workarounds exist, however, system restoration must occur within 2 business days or longer term damage may occur.
- **P3** systems are those that the organization can do without for longer than 3 business days without material impact to day-to-day operations.

Function	Priority	Hosting Platform	Description
Email	P1	Google Apps for Business - Gmail	Internal and customer communication.
Documents	P1	Google Drive	Storage and sharing of documents for each functional area of the Caylent.
HRIS	P1	Rippling	Human Resource Information Systems
DNS	P1	Amazon Web Services - Route53	Domain name resolution for external facing and internal facing Caylent systems.
Timekeeping	P2	Harvest	Tracking hours billed on each customer project
Cloud Platforms	P2	Amazon Web Services	Limited Single Sign-On capabilities and customer communication
Finance Tooling	P2	Intuit QuickBooks Deel	Contractor Platform (for processing of contracts and payment administration)
Communication	P2	Slack	Internal and customer communication
Development	P2	Github	Caylent's source code is stored in a Github repository.
Issue Tracking	P2	Jira (Atlassian)	Caylent uses Jira to track project backlog items, and customer requests.
CRM	P2	Salesforce.com	Our primary customer CRM.
Other	P3	All other Caylent Systems	N/A

Recovery Plans for Core Data Systems

Since all of the core systems are hosted by a third party, Caylent relies on the back-up, availability, and disaster recovery capabilities of its service providers. All providers were chosen, in part, due to their proven track record of high availability. Requirements for proof of high availability include:

- Facilities with reliable power, cooling, and network infrastructure
- High-availability infrastructure: networking, server infrastructure, and software
- N+1 redundancy
- Detailed historical availability data on the entire service, not just on individual server
- Uptime guarantees of at least 99.99%
- SLAs for support and maintenance obligations.
- Disaster Recovery and Business Continuity Plans that include:
  - Data backup procedures that create multiple backup copies of data, in near real time, at the disk level
  - Archival backup strategies with routinely tested restoration patterns

Maintenance and Testing Guidelines

On an annual basis, Caylent will review and update this Plan, and associated appendices. Testing and/or exercises will be conducted for high priority activities and associated systems on a periodic basis. This testing will include:

- Test and/or exercise the Plan at least annually to determine the Plan's effectiveness and the organization's readiness to execute the Plan; and
- Review the BCP/DR Plan test/exercise results and initiate corrective/fine-tuning actions (if any).

Caylent shall ensure that testing and/or exercises also include an assessment of the effects on operations, assets and individuals arising due to contingency operations in accordance with the Plan.

Revision History

Original publication: March 28, 2022
Reviewed & Revised: February 2024