CYBER-INCIDENT RESPONSE PLAN

Purpose and Goals

This cyber incident response plan ("IRP") provides a structured and systematic incident response process for all information security incidents (as defined in Definitions) that affect any of Caylent's information technology ("IT") systems, network, or data, including Caylent's data held or IT services provided by third-party vendors or other service providers. This IRP:

- Defines and provides step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
- Assists Caylent and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.
- Mitigates or minimizes the effects of any information security incident on Caylent, its customers, employees, and/or its partners.
- Helps Caylent consistently document the actions it takes in response to information security incidents.
- Reduces overall risk exposure for Caylent.
- Engages stakeholders and drives appropriate participation in resolving information security incidents while fostering continuous improvement in Caylent's information security program and incident response process.

Caylent develops and maintains this IRP as may be required by applicable laws and regulations.

Scope

This IRP applies to all Caylent business groups, divisions, and subsidiaries; their employees, contractors, officers, and directors; and Caylent's IT systems, network, data, and any computer systems or networks connected to Caylent's network.

1. **Other Plans and Policies.** Caylent may, from time to time, approve and make available more detailed location or work group-specific plans, policies, procedures, standards, or processes to address specific information security issues or incident response procedures. Those additional plans, policies, procedures, standards, and processes are extensions to this IRP.

2. **Accountability**. Caylent has designated Danielle Green, IT Manager (danielle.green@caylent.com) to implement and maintain this IRP (the "information security coordinator").

3. **Information Security Coordinator Duties.** Among other information security duties, as defined in Caylent's written information security policy ("WISP") available on Notion, the information security coordinator shall be responsible for:
    - Implementing this IRP.
    - Identifying the incident response team ("IRT") and any appropriate sub-teams to address specific information security incidents, or categories of information security incidents (*see Incident Response Team section*).
    - Coordinating IRT activities, including developing, maintaining, and following appropriate procedures to respond to, appropriately escalate, make decisions regarding, and document identified information security incidents (*see Incident Response Procedures section*).
    - Conducting post-incident reviews to perform "lessons learned" analysis, gather feedback on information security incident response procedures, and address any identified gaps in security measures (*see Post-Incident Review section*).
    - Providing training and conducting periodic exercises to promote employee and stakeholder preparedness and awareness of this IRP (*see Plan Training and Testing section*).
    - Reviewing this IRP at least annually, or whenever there is a material change in Caylent's business practices that may reasonably affect its cyber incident response procedures (*see Plan Review section*).
4. **Enforcement**. Violations of or actions contrary to this IRP may result in disciplinary action, in accordance with Caylent's information security policies and procedures and human resources policies.

Definitions

The terms defined below apply throughout this IRP:

"Confidential information." Confidential information means "Confidential Information" as defined in the WISP, and that may cause harm to Caylent or its customers, employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available.

"Personal information." Personal information means individually identifiable information that Caylent owns, licenses, or maintains and that is from or about an individual including, but not limited to (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online information, such as a username and password; (d) telephone number; (e) government-issued identification or other number; (f) financial or payment card account number; (g) date of birth; (h) health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a healthcare professional/created or received by Caylent and (i) any information that is combined with any of (a) through (h) above.

"Information security incident" Information security incident means an actual or reasonably suspected (a) loss or theft of confidential or personal information; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of confidential or personal information that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information; or (c) unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of Caylent's IT systems or third party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information or Caylent's operating environment or services.

Incident Response Team

The incident response team ("IRT") is a predetermined group of Caylent employees and resources responsible for responding to information security incidents.

Role. The IRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to Caylent's IT systems, network, and data; (b) minimize economic, reputational, or other harms to Caylent and its [customers/clients], employees, and partners; and (c) manage litigation, enforcement, and other risks.

Authority. Through this IRP, Caylent authorizes the IRT to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in this IRP.

Responsibilities. The IRT is responsible for:

- Addressing information security incidents in a timely manner, according to this IRP.
- Managing internal and external communications regarding information security incidents.
- Reporting its findings to management and to applicable authorities, as appropriate.
- Reprioritizing other work responsibilities to permit a timely response to information security incidents on notification.

IRT Roster. The IRT consists of a core team, led by the information security coordinator, with representatives from key Caylent groups and stakeholders. The current IRT roster includes the following individuals:

Randall Hunt, VP of Cloud Strategy & Solutions
Randall.hunt@caylent.com Phone: 650-690-0657

Danielle Green, IT Manager
Danielle.green@caylent.com Phone: 941-447-3067

Paolo Ferrer, IT Manager
paolo.ferrer@caylent.com Phone: 650-892-3042

Sub-Teams and Additional Resources. The information security coordinator assigns and coordinates the IRT for any specific information security incident according to incident characteristics and Caylent needs. The information security coordinator may:

Identify and maintain IRT sub-teams to address specific information security incidents, or categories of information security incidents.

Legal:
Lisa Cohrs, VP/General Counsel
lisa.cohrs@caylent.com Phone: 949-290-4059

Call on external individuals, including vendor, service provider, or other resources, to participate on specific-event IRTs, as necessary.

Caylent Professional Liability Insurance Broker:
Marsh & McLennan Agency LLC
Chelsea Hilgert, CISR, Client Executive, Select Accounts
Chelsea.Hilgert@MarshMMA.com Phone: 763 746 8646

Incident Response Procedures

Caylent shall develop, maintain, and follow incident response procedures as defined in this section to respond to and document identified information security incidents.

Caylent recognizes that following initial escalation, the information security incident response process is often iterative, and the steps defined in Investigation and Analysis, Containment, Remediation, and Recovery; Evidence Preservation; and Communications and Notification sections may overlap or the IRT may revisit prior steps to respond appropriately to a specific information security incident.

1. **Detection and Discovery.** Caylent shall develop, implement, and maintain procedures to detect, discover, and assess potential information security incidents through automated means and individual reports.
    - Automated Detection. Caylent shall develop, implement, and maintain automated detection means and other technical safeguards in accordance with industry standards. More information is set forth in Caylent's WISP.
    - Reports from Employees or Other Internal Sources. Employees, or others authorized to access Caylent's IT systems, network, or data, shall immediately report any actual or suspected information security incident to it@caylent.com. Individuals should report any information security incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.
    - Reports from External Sources. External sources who claim to have information regarding an actual or alleged information security incident should be directed to it@caylent.com. Employees who receive emails or other communications from external sources regarding information security incidents that may affect Caylent or others, security vulnerabilities, or related issues shall immediately report those communications to it@caylent.com and shall not interact with the source unless authorized.
    - Assessing Potential Incidents. Caylent shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. Caylent shall document each identified information security incident.
    - Lost, Stolen, Broken Devices. In the event that a company-assigned device is lost or stolen, it is the responsibility of the employee to contact IT immediately. This is to ensure that the device is properly locked or wiped to prevent any data breaches or misuse of company or client information. In the event that a device is damaged or broken, the employee/resource is required to communicate this to IT without delay. This is to allow us to verify warranty and provide guidance on the next steps. IT should be contacted via email, it@caylent.com or in slack via #ask-it. Failure to adhere to these guidelines may result in disciplinary action.
2. **Escalation.** Following identification of an information security incident, the information security coordinator, or a designate, shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to Caylent and its customers, employees, or others.

Based on the initial assessment, the information security coordinator, or a designate, shall:

- IRT Activation. Notify and activate the IRT, or a sub-team, including any necessary external resources (*see IRT Roster section*).

  Any security breach, error, or extended period of unavailability in a system categorized as P1 or P2 activates our IRT and process.

- IRT Expectations. Set expectations for IRT member reply and engagement.

  IRT members determine the immediate scope of impact, potential immediate mitigations, and time to recovery (TTR) estimates. These criteria are communicated to relevant stakeholders (customers and/or employees).

  Scope of Impact: The IRT determines the initial scope of impact within 30 minutes of activation.

  Immediate Mitigations: If this issue can be resolved immediately, the IRT takes direct action to immediately resolve the issue. If the issue can be partially mitigated, the IRT is empowered to deploy those mitigation procedures.

  Time to Recovery: The IRT will provide an initial estimate of time to recovery within 1 hour of notification. This initial TTR is non-binding but is continuously updated (TTR) for reporting to relevant stakeholders.

- Initial Notifications. Notify (if necessary) organizational leadership and any applicable business partners or service providers, Caylent's cyber insurance carrier, and law enforcement or other authorities (*see Communications and Notifications section*).
- Determine Decision-Making Authority. Following initial notifications, work with organizational leadership (if necessary) to establish any decision-making authority levels according to the information security incident's specific facts and circumstances. Members of the IRT have full authority to implement partial mitigations that do not affect customer or employee information, security, or availability. If the **scope of impact** is determined to involve >50% of the Caylent workforce or >10% of the Caylent customer base, then the mitigations or resolutions must have approval from the executive team.

3. **Investigation and Analysis.** On activation, the IRT shall collaborate to investigate each identified information security incident, analyze its effects, and formulate an appropriate response plan to contain, remediate, and recover from the incident.

   - The IRT shall document its investigation and analysis for each identified information security incident.
   - The document shall contain relevant records of decisions made throughout the investigation process, including timestamps, as specified in this Plan.

4. **Containment, Remediation, and Recovery.** Next, the IRT shall direct execution of the response plan it formulates according to its incident investigation and analysis to contain, remediate, and recover from each identified information security incident, using appropriate internal and external resources (see *Investigation and Analysis section*).

5. **Evidence Preservation.** The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified information security incident during investigation, analysis, and response activities (see Investigation and Analysis and, Containment, Remediation, and Recovery). The IRT shall seek counsel's advice as needed to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

6. **Communications and Notifications.** For each identified information security incident, the IRT shall determine and direct appropriate internal and external communications and any required notifications. Only the IRT may authorize information security incident-related communications or notifications. The IRT shall seek counsel's advice as needed to review communications and notifications targets, content, and protocols.

   - Internal Communications. The IRT shall prepare and distribute any internal communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

Organizational Leadership. The IRT shall alert organizational leadership to the incident and explain its potential impact on Caylent, its customers, employees, and others as details become available.

General Awareness and Resources. As appropriate, the IRT shall explain the incident to Caylent's employees and other stakeholders and provide them with resources to appropriately direct questions from customers, media, or others.

- External Communications. Working with the Alliances & Marketing Team (marketing@caylent.com) IRT shall prepare and distribute any external communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

  Public Statements. If Caylent determines that external statements are necessary, the IRT shall provide consistent, reliable information to their public relations partners, the media, and public regarding the incident using Caylent's website, press releases, or other means.

  Law Enforcement. The IRT shall report criminal activity or threats to applicable authorities, as Caylent deems appropriate.

- Notifications. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require Caylent to notify various parties of some information security incidents. If applicable to a specific information security incident, as required, the IRT shall:

  Authorities. Notify applicable regulators, law enforcement, or other authorities.

  Affected Individuals. If an applicable breach of personal information occurs, prepare and distribute notifications to affected individuals.

  Cyber Insurance Carrier. Notify Caylent's cyber insurance carrier according to the terms and conditions of its current policy, including filing a claim, if appropriate.

  Others. Notify customers or business partners according to current agreements.

Incident Response Review

At a time reasonably following each identified information security incident, the information security coordinator, or a designate, shall reconvene the IRT, others who participated in response to the incident, and affected work group representatives, as appropriate, as a post-incident review team to assess the incident and Caylent's response.

- Review Considerations. The post-incident review team shall consider Caylent's effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The post-incident review team shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.
- Report. The post-incident review team shall document its findings using industry standard Root Cause Analysis and Post Mortem processes.
- Follow-Up Actions. The information security coordinator shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from Caylent leadership.

Plan Training and Testing

Training. The information security coordinator shall develop, maintain, and deliver training regarding this IRP that periodically:

- Informs all employees, and others who have access to Caylent's IT systems, network, or data, about the IRP and how to recognize and report potential information security incidents.
- Educates IRT members on their duties and expectations for responding to information security incidents.

Testing. The information security coordinator shall coordinate exercises to test this IRP periodically (but at least annually). The information security coordinator shall document test results, lessons learned, and feedback and address them in plan reviews (see Plan Review).

Plan Review

Caylent will review this IRP at least annually, or whenever there is a material change in Caylent's business practices that may reasonably affect its cyber incident response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The information security coordinator must approve any changes to this IRP and is responsible for communicating changes to affected parties.

Revision History

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