CAYLENT

Information Security Policies

Last Updated: January 2025

Overview

The Policies below address each Caylent-employee or contractor's use of the following:

- ➔ Caylent issued laptops or devices
- ➔ Personal devices used for work purposes
- ➔ Company email systems and accounts
- ➔ Internet and intranet access
- ➔ Cloud environments
- ➔ Training platforms
- ➔ Third-party tools (such as Slack, Rippling, Deel, Salesforce, etc.)
- ➔ Telephone and voicemail systems, including mobile phones/smartphones
- ➔ All other associated computer, network, and communications systems, hardware, peripherals, and software, including network key fobs and other devices

Unless otherwise required by a Caylent customer, the practices described in these Policies should also be followed whenever using or accessing the systems made available to you by Caylent's customers (for example, as you are doing work for a Caylent customer within the customer's systems, AWS environments, or using the customer's tools).

IT Security Policy

Devices

All devices used for Caylent's business or on behalf of Caylent must be registered with and/or authorized by Caylent's IT Department.

To protect Caylent data, Caylent employees and contractors ("Resource(s)") must immediately report any device used for Caylent's business that is lost, stolen, accessed by unauthorized persons, or otherwise compromised. Prompt reporting allows Caylent IT to assess risk, containment, and, if necessary, remotely wipe all Caylent content or the entire contents of the device (including personal content) at Caylent's sole discretion. You must also promptly provide Caylent with access to the device when requested for Caylent's legitimate business purposes, including in the event of any security incident or investigation.

In addition, Caylent employees and contractors must:

- ➔ Install and maintain MDM (Mobile Device Management) and all of its deployed packages, including but not limited to, EDR (Endpoint Detection & Response) software on corporate-issued devices used to access Caylent systems, as directed by Caylent's IT Department.

- ➔ Comply with Caylent's device configuration requirements.
- ➔ Password/PIN-protect devices accessing Caylent resources through the use of strong passwords consistent with Caylent's password requirements (see Password section).
- ➔ Maintain the corporate-issued device's original operating system (unless authorized by Caylent IT) and keep it current with security patches and updates, as instructed by Caylent IT.
- ➔ Preserve the device's security settings and configs, as deployed and enforced by MDM, unless permitted with explicit written permission from Caylent IT.
- ➔ Not download, transfer back-up, or otherwise store Caylent content, including Confidential Information and/or Strictly Confidential Information, locally or to unapproved cloud-based storage or services without Caylent's consent. Any such backups or other stored copies of Caylent content inadvertently created must be deleted immediately. To the extent you create backups or otherwise store Caylent content with Caylent's consent, you must provide Caylent with access to your local or cloud-based storage to access and review any such backups or other stored copies of Caylent content when requested or required for Caylent's legitimate business purposes, including in the event of any security incident or investigation.
- ➔ Not access or transmit any Confidential or Strictly Confidential information over unsecured networks, unless using secure and encrypted channels such as a VPN or TLS.
- ➔ All devices must use full disk encryption.
- ➔ At all times, Cayliens must use their best efforts to physically secure the device against loss, theft, damage, or use by persons who have not been authorized to access the device by Caylent.

Passwords

Passwords are an important aspect of cybersecurity. A poorly chosen password may result in unauthorized access and/or exploitation of Caylent's resources. All users, including employees, contractors and vendors with access to Caylent's systems (which include customer systems), are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- ➔ All user-level passwords (e.g., email, web, desktop computer, etc.) and system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least on an annual basis.
- ➔ All production system-level passwords must be part of the IT Department-administered password manager.
- ➔ User accounts must have a unique password from all other accounts held by that user.
- ➔ All user-level and system-level passwords are enforced through Rippling as follows:

1. All new passwords should not be identical to the previous 10 passwords.

2. Passwords will be locked after 10 unsuccessful attempts.

3. Passwords will expire after 90 days, and the user will be prompted to change it 5 days before the expiration date.

- ➔ Customer-specific passwords must be stored in a Caylent-approved password manager (e.g. 1Password) and be shared with at least 1 other person on the engagement (ideally a manager) for redundancy.

Password Protection Standards

Employees and contractors should adhere to the requirements below with regard to passwords to access Caylent's systems:

- ➔ Excepting designated shared accounts, do not share personal login credentials with anyone, including supervisors or other employees or contractors. All passwords are to be treated as Strictly Confidential Information (see Data Classification Policy below).
- ➔ Passwords should never be written down or stored electronically without encryption.
- ➔ Do not reveal a password in email, chat, or other plaintext electronic communication (e.g. questionnaires or security forms).
- ➔ Do not speak about a password in front of others.
- ➔ Do not hint at the format of a password (e.g., "my family name").
- ➔ If someone demands a password, refer them to this document and direct them to the IT Department (it@caylent.com).
- ➔ Always decline use of the "Remember Password" feature in applications (e.g. iCloud Keychain) or browsers (e.g.: Chrome, Edge, Safari), except for the Caylent-approved password manager.

Use of Passwords and Passkeys for Remote Access Users

Access to Caylent systems via remote access is to be controlled using either a one-time password authentication, a public/private key system with a strong passphrase, or a standard password with a multi-factor authentication device.

Passkeys

- Passkeys are a cryptographic authentication method that employs public and private keys. Whenever possible, IT encourages use of this authentication method as it offers the highest level of account security.
- Passkeys are not the same as passwords. A passkey is a longer version of a password and is, therefore, more secure. A passkey is typically composed of multiple characters. Because of this, passkeys are more secure against "dictionary attacks."

System Administration Standards

All Caylent systems will be configured to enforce the following:

- ➔ Protection with regards to the retrieval of passwords and security details, identity verification is performed via Zoom or Slack Huddle before any passwords or security details are disclosed or administered
- ➔ System access monitoring and logging via Rippling MDM at a user level.
- ➔ Role management via Rippling permissions and groups so that administrative functions can be performed without sharing passwords.

- ➔ Password administrative processes must be properly logged, controlled, secured, and auditable.

Access Control Standards

Each Resource will be allocated access rights and permissions to systems and data that are necessary for the tasks that they are expected to perform as part of their essential job functions (Role-based Access Control - RBAC).

Human Resources (hr@caylent.com) must initiate the access control approval process for all new employees and contractors. These steps are required for network access:

- ➔ Human Resources determines that a new Resource has been hired by a department and notifies the IT Department
- ➔ The new Resource is given a Caylent email account.
- ➔ Human Resources assigns the standard basic information security awareness training based upon position/role. Additional training may be assigned by a supervisor based on specific role or information sensitivity.
- ➔ Upon completion of awareness training by the new Resource, Human Resources and the IT Department grants the proper access, which remains in effect until an audit determines that the role no longer requires access or the employee/contractor leaves Caylent.

Resource access rights are reviewed at regular intervals to ensure that the appropriate access rights are still allocated at the correct levels (or whether they need to be increased, decreased or removed). System administration accounts are only provided to Resources that are required to perform system administration tasks.

Multi-Factor Authentication

Multi-factor authentication "MFA" is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism - typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). MFA services can be accessed via APIs, SDKs or both, therefore MFA controls should be put in place to balance strong security with user experience. Not using MFA increases the likelihood of unauthorized access and/or exploitation of Caylent's resources.

All users, including employees, contractors, and vendors with access to Caylent systems, are responsible for taking the appropriate steps, as outlined below, to use the MFA provided by Caylent.

- ➔ MFA systems can include the use of mobile devices, push notifications, SMS, biometrics, hardware authentication keys, and soft or hard tokens.
- ➔ All users must use MFA to authenticate into the systems whenever possible.
- ➔ All systems having the MFA feature must have it enforced.

General Configurations for MFA Usage

- ➔ Resources will have to register a device or alternative contact to provide a secure method for Caylent and its services to authenticate access during the login process. Examples include a cellphone that can receive texts, a personal SMS-enabled VoIP service, or a non-Caylent email address. If you do not register a MFA method, you will not be able to use systems or services for which MFA is enforced.
- ➔ When you attempt to log into a Caylent system protected by MFA, the system will "challenge" you by requesting a secret security code. This code will be provided through the secure method you selected during registration or as a confirmation request in the MFA application. If you enter the correct code, you will be allowed into the system. Failed attempts will be handled according to current Caylent account policies and procedures referenced in the Policy's Repository.
- ➔ Applications can also require MFA for login. All Resources should be assigned permissions through profiles and/or roles. Due to the evolving nature of technology, cyber threats and the changing roles of users at Caylent, all exemptions will be reviewed periodically and at the discretion of the IT Department. This review will verify that the need stated in the request is still valid and/or that the Resource still requires the approved MFA exempted access.

Device & Virtual Machine Encryption

All users of desktops, laptops, tablets, mobile devices and virtual machines (whether provided by Caylent or not) must take care to protect information that users are given access to. As a result, all devices used for work purposes (including personal devices) must be encrypted using an encryption solution that has been approved by the Caylent IT Department.

In situations where a Resource needs to access Confidential Information and/or Strictly Confidential Information (see Data Classification Policy below) from any device, secure channels must be used. Examples of known secure channels are: supported remote access connections, known private Wi-Fi networks secured with a password (not public café or hotel networks, unless otherwise secured by VPN), or webmail.

Removable Storage Devices

Confidential Information and/or Strictly Confidential information, if storage on removable storage devices has been explicitly authorized by IT, must be encrypted. Examples of removable storage devices include, but are not limited to, flash drives, external hard drives, memory cards, and optical discs. Strong hardware- or software-based encryption algorithms such as the Advanced Encryption Standard (AES) with at least 256-bit keys should be used. Examples of compliant encryption software for removable storage devices include Apple FileVault, Microsoft BitLocker, LUKS (for Linux systems), and VeraCrypt (open source). When encrypted removable storage devices are used to share Confidential Information and/or Strictly Confidential Information, the encryption password must be shared separately and in a secure manner, such as a Caylent-approved password manager.

Lost or Stolen Devices

If a Resource's device or data is suspected to be stolen, lost, or compromised, the resource must contact the IT Department immediately (within 24-hours) at it@caylent.com.

Response to IT Department Requests or Inquiries

Resources agrees to timely review of all communications from Caylent's IT Department. Should a response be required, Resources agree to respond to any IT Department inquiries or communications within 72 hours.

Privacy

All users should have no expectation of privacy whatsoever in any message, file, data, document, telephone conversation, social media post, conversation, or any other kind of information or communication transmitted to, received, or stored or recorded on Caylent's electronic information and communications systems.

You are expressly advised that to prevent against misuse, Caylent reserves the right to monitor, intercept, and review, without further notice, every Resource's activities using the company's IT resources and communications systems, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, chat messages, internet and social media postings and activities, and you consent to such monitoring by your acknowledgement of this Policy and your use of such resources and systems. Do not use Caylent's IT resources and communications systems for any matter that you desire to be kept private or confidential from Caylent.

Personal Use of the Internet

Company endpoints are deployed as COPE (Company Owned, Personally Enabled). We recognize that Resources may desire to access the internet (including social media) for personal activities using the company's computers, networks, and other IT resources and communications systems. We authorize such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your responsibilities or productivity.

Using the internet (including social media) to access pornographic, sexually explicit, or "hate" sites, or any other website that might violate law or Caylent's policies against harassment and discrimination, is never permitted.

Inappropriate Use of Company IT Resources and Communications Systems

You are never permitted to use Caylent's IT resources and communications systems, including email, text messaging, internet access, social media, telephones, and voicemail, for any inappropriate or unlawful purpose. This includes but is not limited to:

- ➔ Misrepresenting yourself as another individual or company.
- ➔ Sending, posting, recording, or encouraging receipt of messages or information that may be offensive because of their sexual, racist, or religious content.
- ➔ Revealing Caylent's proprietary or Confidential Information, or intellectual property without authorization.
- ➔ Conducting or soliciting illegal activities.
- ➔ Representing your personal opinion as that of Caylent.

- ➔ Interfering with the performance of your job or the jobs of other Caylent employees/contractors.
- ➔ For any other purpose that violates Caylent's policies or practices.

Telecommuting / Work From Home Policy

Caylent is a fully-remote workforce, where work is expected to be done via telecommuting. (work remotely or work from home). This Policy outlines telecommuting requirements and best practices.

Work Location

Cayliens permitted to telecommute (work remotely) must input their work location into Rippling (street address, city, state, zip code) at the time of hire (“worksite”). In the event that your worksite permanently moves or changes long term (6+ months) at any time during the course of your employment, you must notify your supervisor and Human Resources at hr@caylent.com, and obtain prior written consent.

Short-term changes to work location do not need to be updated in Rippling but do require written approval by email as follows:

- ➔ For location changes up to two (2) weeks or ten (10) consecutive working days, approval by your supervisor is required
- ➔ For location changes longer than two (2) weeks or ten (10) consecutive working days requires approval by your supervisor and HR

Any changes to standard work hours/time zones when working in a different location must be pre-approved by your supervisor.

Wi-Fi / Stable Connectivity Requirements

Cayliens permitted to work remotely must maintain consistent and stable internet connectivity (sufficient to be able to attend video conference calls, screen-share, and file share without significant delay or interruption. At a minimum you will also need to consistently meet the internet speed requirement of 100 Mbps download and 50 Mbps upload speed. If you don't know what your download and upload speeds are, you can take a speed test online at speedtest.net or Google "test internet speed".

Caylent's Policies Remain in Effect

Resources permitted to telecommute must continue to abide by the policies set forth in this Manual, as well as other policies that are subsequently issued. Failure to follow Caylent policies may result in disciplinary action, and in certain instances termination of employment.

Equipment and Technology Support

Caylent will provide each Resource with a laptop computer (subject to acceptance of an Equipment Agreement in connection with receipt of the laptop). Each Resource will be responsible for providing all furniture and equipment that he/she will need to telecommute. Caylent will not be responsible for any damage to your furniture or equipment resulting from your work with Caylent or use of Caylent-provided equipment. Each Resource must return all Caylent equipment when employment with Caylent ends.

Offsite Security Best Practices

Resources must follow Caylent's IT Security Policy when working remotely. This includes but is not limited to the following requirements:

- ➔ Resources must use secure remote access procedures. All access to third party tooling needs to be encrypted. If you are using an unencrypted wi-fi network network, you are not authorized to access any Confidential Information or Strictly Confidential Information. Resources must ensure tools use a secure protocol for remote access (e.g. TLS/SSH/RDP).
- ➔ Resources must maintain confidentiality by using passwords and maintaining regular anti-virus protection and computer backups.
- ➔ Resources must not download company Confidential Information or Strictly Confidential Information, or trade secrets onto a non-secure device.
- ➔ Resources must not share their password with anyone outside of Caylent. If any unauthorized access or disclosure occurs, you must inform Caylent IT immediately.
- ➔ Resources must use locked file cabinets and/or locked offices to secure the area where any device is stored.

Confidential Information Policy

We understand that Resources may want to talk about Caylent with other life-forms. That said, Caylent keeps certain types of information confidential for important business reasons. Because of the importance of maintaining the confidentiality of certain information, and because effective confidentiality protocols require the involvement and cooperation of Resources, Caylent has implemented this Confidential Information Policy.

Definition of Confidential Information

In the course of your employment with Caylent, you may be exposed to and/or provided with Trade Secrets and/or Confidential Information of Caylent relating to the operation of Caylent’s business and its customers (collectively referred to as “Trade Secrets/Confidential Information”).

“Trade Secrets" mean information, including a formula, pattern, compilation, program, device, method, technique or process, that: (1) derives independent economic value, actual or potential, from not being generally known to the public or

to other persons or entities who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Caylent's Trade Secrets are: (1) not generally known to the public or to Caylent's competitors; (2) were developed or compiled at significant expense by Caylent over an extended period of time; and (3) are the subject of Caylent's reasonable efforts to maintain their secrecy.

"Confidential Information" means information belonging to Caylent, or Caylent's customers or partners, whether reduced to writing or in a form from which such information can be obtained, translated, or derived into reasonably usable form. Confidential Information may be provided to Resources during their employment with Caylent and/or Resources may gain access to or develop such information while employed by Caylent.

Protocols for Maintaining Confidentiality

Caylent limits disclosure of its Trade Secrets/Confidential Information to Resources that have a "need to know" in order to perform their role-based work responsibilities. Resources must treat all Trade Secrets/Confidential Information as strictly confidential both during and after employment with Caylent ends. To maintain the confidentiality of Caylent's Trade Secrets/Confidential Information, all Resources must follow these protocols:

- ➔ Resources should not access or use any Trade Secrets/Confidential Information to which Caylent has not provided him/her access or authorization to use.
- ➔ Resources should not directly or indirectly disclose, publish, communicate, or make available Trade Secrets/Confidential Information to any entity or person that does not have a need, nor the authority to know and use the Trade Secrets/Confidential Information, except as required for the Resource to perform authorized job duties or otherwise permitted by this Policy.
- ➔ If a Resource's authorized job duties require sharing Trade Secrets/Confidential Information with a third party, the Resource must not do so until Caylent and the third party enter into a confidentiality agreement and the Resource receives advance consent in writing from his/her supervisor.
- ➔ Caylent's trade secrets and Trade Secrets/Confidential Information must be kept and stored in a secure location with limited access, and with physical and/or electronic access controls.
- ➔ Resources should not discuss Trade Secrets/Confidential Information in public where it may be overheard, including elevators, restaurants, rideshare services (e.g. Ubers/Lyfts), and public transportation.
- ➔ In the event of an inadvertent disclosure of Trade Secrets/Confidential Information, Resources must immediately inform their supervisor and Legal (legal@caylent.com) so that measures can be taken to minimize damage to Caylent.
- ➔ Departing Resources must return any Trade Secrets/Confidential Information in his/her possession to Caylent on termination of employment and will be required to sign an acknowledgment of the same.
- ➔ Resources should not forward from their Caylent email account to their personal email account(s) any emails or documents containing any Trade Secrets/Confidential Information.
- ➔ Resources should not copy, transfer, or upload to their personal cloud-based or online storage accounts (such as a personal Dropbox or Google Drive account) any documents containing any Trade Secrets/Confidential Information.

Any Resource who is unsure whether information should be kept confidential should always check with his/her supervisor or Legal (legal@caylent.com) before disclosing the information or taking any other action.

Data Classification Policy

Caylent considers its information a key resource for ensuring the achievement of its strategic objectives and as a result requires that it be properly safeguarded from potential security risks. Data Classification is the process of categorizing information based on its value to Caylent. This Policy provides guidelines for Data Classification within Caylent.

Roles

Data Owner: All information possessed by or used by a particular organizational unit must have a designated Data Owner who is responsible for: (a) determining appropriate sensitivity classifications; (b) making decisions about who can access the information, and (c) ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

Information Custodian: Each significant type of information must have a designated Custodian who will properly protect the information by keeping with the designated Data Owner's access control and data sensitivity instructions.

Classification

All data handled within Caylent must be classified in such a way as to ensure the effective case-by-case application of appropriate security measures. Caylent requires that data be classified according to the following table:

Classification	Definition	Example(s)
Information without a label/designation is by default classified as Confidential. Any data that contains personally identifiable information concerning any individual or that is covered by local, state, or Federal regulations, or by any voluntary industry standards concerning protection of personally identifiable information that Caylent chooses to follow, is automatically classified as C4/Strictly Confidential.		
Public	An unauthorized disclosure of Public data has a minimal impact on Caylent's business, on employees/contractors, on Caylent's image, or on any of its customers or business partners. Information classified as "Public" is by nature in the public domain, and for this reason does not need to be protected in a specific way.	➔ Press Releases (published) ➔ Materials used at public events ➔ Material available on caylent.com
Internal	An unauthorized disclosure of Internal data has limited impacts on Caylent's business, on employees/contractors, on Caylent's image, or on any of its customers or business partners.	➔ Caylent Policies
Confidential	An unauthorized disclosure of Confidential data may have serious impacts on Caylent's business, on employees/contractors, on Caylent's image, or on any of its customers or business partners.	➔ Information available on Caylent's wiki (Notion), Google Drive, or Slack ➔ Org charts

		➔ Data from Salesforce: customer contracts, customer information (names, project information), and customer data (information made available to Caylent by a potential/actual customer). ➔ Sales data, accounting and budget data, financial records, compensation data, etc.
Strictly Confidential	An unauthorized disclosure of Strictly Confidential data may have severe impacts on Caylent's business, on employees/contractors, on Caylent's image, or on any of its customers or business partners.	➔ Any data that contains personally identifiable information (PII) concerning any individual and is regulated by local, state, or Federal privacy regulations, or by any voluntary industry standards or best practices concerning protection of personally identifiable information that Caylent chooses to follow. ➔ Customer Intellectual Property ➔ Passwords ➔ Trade secrets ➔ "Inside information" (corporate restructuring, strategic planning information, board presentations, organizational documents)

Declassification And Downgrading

The designated Data Owner may declassify or downgrade the classification of information entrusted to his or her care. To achieve this, the Data Owner must change the classification label appearing on the original document, notify the Data Custodian, and inform all known recipients. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical.

Information Handling

Resources shall protect information effectively, based on the classification level, throughout its lifecycle to minimize the risk of loss of information confidentiality. Any action performed on information shall comply with the following information handling rules.

1. Information sharing with others shall comply with the 'need-to-know' principle, irrespective of the means chosen for sharing (e.g., electronic means, voice, or hardcopies). Resources shall ensure that the recipient knows and applies the protection rules defined for the classification level of the shared information.
2. Information disposal is necessary when information is no longer required for business use. Resources shall ensure to destroy information in compliance with rules defined for its classification level.

3. “Internal Information”
   Shall be processed only with means and tools authorized by Caylent; it shall not be processed with personal (e.g.: personal email) or unauthorized public applications (e.g., cloud storage applications).

4. “Confidential Information”

    a. Shall not be discussed in public places.

    b. Shall be processed paying particular attention to prevent unnecessary communication or disclosure.

    c. Shall not be processed via any applications, tools and systems not provided by the company nor expressly secured and authorized (e.g., public exchange folders).

5. “Strictly Confidential Information”

    a. Shall be protected with the minimum protections of “Confidential information”.

    b. Shall be accessed and shared with implicit control and approval by the Data Owner.

    c. Shall be processed during each phase of its lifecycle by specific company applications, tools, and systems, that ensure a higher security level (e.g. encryption, strong authentication).

Social Media Policy

Caylent respects the right of all Resources to use social media. However, to protect the company's interests and ensure that Resources focus on their job duties, Resources must adhere to the general internet use guidelines and rules in this Policy.

- ➔ Like other uses of the internet, occasional personal use of computers and other IT resources for social media activities is authorized, so long as it does not involve unprofessional or inappropriate content, does not otherwise violate any policy, and does not interfere with your responsibilities or productivity.

- ➔ Remember that anything you post or send using social media, even outside the workplace, could reflect on Caylent, in addition to yourself, and might create legal liabilities for Caylent or damage its business or reputation.

- ➔ If your job duties require you to speak on behalf of Caylent in a social media environment, you must be authorized by or otherwise seek approval for such communication from, the Alliances & Marketing Department (marketing@caylent.com) and/or PeopleOps (peopleops@caylent.com) to act as Caylent's representative. Likewise, if you are not a member of the Alliances & Marketing Department and you are contacted for Caylent's comment for any publication, including any social media outlet, direct the inquiry to Alliances & Marketing (marketing@caylent.com) and do not respond without written approval. Note that Caylent owns all social media accounts used for business purposes on behalf of Caylent, including any and all content associated with each account, such as followers and contacts.

- ➔ If you are unsure about the appropriateness of any posting or communication, discuss it with your supervisor or Alliances & Marketing (marketing@caylent.com), or PeopleOps (peopleops@caylent.com) and refrain from making the posting or communication until you have had it approved. Any conduct that under the law is impermissible if expressed through any other public forum is also impermissible if expressed through social

media. If you see content in a social media environment that reflects poorly on Caylent, please notify your manager and Human Resources immediately.

Other Communications Policy

Email

Abuse of email, as well as the receipt and transmission of unsolicited commercial email places an incredible drain on Caylent's resources and reputation, and imposes significant monetary costs to filter and remove unsolicited emails from our systems. To eliminate the receipt and transmission of unsolicited commercial email, Caylent complies with the federal "CAN-SPAM" law. You are responsible for complying with the federal Anti-Spam regulations and therefore you may not use Caylent's IT to transmit unsolicited commercial email:

- ➔ Promoting Caylent's business, goods, products, and services without prior authorization.
- ➔ Promoting your own personal business, goods, products, and services.
- ➔ To Caylent's customers who have elected to "opt-out" of receiving Caylent's electronic advertisements.
- ➔ That contains or is accompanied by maliciously false information.

In addition to helping Caylent eliminate the receipt of unsolicited commercial email from outside parties advertising various websites, products, or services and to further prevent the receipt of offensive or undesired outside email, you should delete unfamiliar or suspicious email from outside Caylent without opening it.

Use of Mobile Devices

Resources are prohibited from taking photographs or making audio or video recordings of our customers without prior written permission from both the customer and Legal (legal@caylent.com). Resources are also prohibited from taking photographs or copying for their own use confidential business documents not related to Resource wages or working conditions at any time. Resources who violate this Policy are subject to disciplinary action, up to and including immediate termination of employment.

Revision History

Original publication: March 28, 2022

Reviewed & Revised: January 2025