Security and Compliance Certifications

SOC 2 Type 2

Achieving SOC 2 Type 2 confirms that our security measures have been extensively tested and validated by an independent auditor, providing an objective and transparent evaluation of our data protection practices in accordance with the highest industry standards.

About SOC 2 Type 2: Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 Type 2 is an external auditing framework that assesses service businesses internal controls related to security, availability, processing integrity, confidentiality, and privacy.

ISO/IEC 27001

Conforming with ISO/IEC 27001 demonstrates that Connecteam has established a system to manage risks related to the security of company-owned data and respects all best practices of this policy.

About ISO/IEC 27001: This international standard was originally published jointly by the International Organization for Standardization and the International Electrotechnical Commission in 2005, and outlines requirements for establishing, implementing, maintaining, and continually improving information security management systems (ISMS). ISO/IEC 27001 ensures businesses manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.

GDPR

GDPR compliance not only safeguards customer data against unauthorized access and breaches but also aligns with global best practices. Our commitment to GDPR ensures that we provide the highest standards of data protection and privacy to our customers.

Connecteam adheres to both of the primary roles defined by GDPR:

- **Data Controller** – an entity that determines the means and purposes of processing personal data. For more information regarding Connecteam's role as a data controller, and our related processing activities and privacy practices, please refer to our Privacy Policy.
- **Data Processor** – an entity that processes personal data on behalf of a Data Controller. For more information on how Connecteam collects and processes personal data on our customer's behalf, as their data processor, please refer to our Data Processing Addendum.

About GDPR: The General Data Protection Regulation (GDPR) sets guidelines for the collection, processing, and disclosure of personal information. While this data protection law was passed by the European Union (EU), it applies to all companies that target or collect data from or related to people in the EU.

HIPAA

Connecteam's commitment to HIPAA compliance confirms that our customers can maintain confidentiality, integrity, and security of health data while using our software.

*Please note that each account must first register and complete a business associate agreement (BAA) for HIPAA compliance to apply.

About HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is a federal US law that provides data privacy and security provisions for safeguarding medical information. It requires healthcare providers, organizations, and their business associates to implement appropriate physical, administrative, and technical safeguards to ensure the confidentiality, integrity, and security of protected health information (PHI).

CCPA

Adhering to the CCPA, we guarantee that the personal information of our California customers is managed with exceptional privacy and security, in strict accordance with rigorous legal requirements.

About CCPA: The California Consumer Privacy Act (CCPA) regulates how businesses all over the world are allowed to handle the personal information of California residents. To adhere to CCPA, businesses must implement measures that ensure the privacy and protection of the personal information of California residents, including transparent data collection practices, secure data handling, and responding to consumer requests regarding their data.

PCI DSS

PCI DSS compliance ensures that Connecteam adheres to the highest security protocols for credit card transactions. This compliance minimizes the risk of data breaches and financial fraud and ensures our customers that we handle transactions securely.

About PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) was established by major credit card companies and includes a set of security standards that ensure all companies that accept, process, store, or transmit credit card information do so in a secure manner. This standard protects cardholder data from theft and reduces fraud, requiring businesses to adhere to strict security measures when handling credit card transactions.