COLORADO
Office of the State Architect
Department of Personnel & Administration

ALERT 002 IHE

TO: SBP Delegates of Institutions of Higher Education

FROM: Cheri Gerou, State Architect

DATE: October 1, 2021

SUBJECT: LCPTracker Task Order Process
Prevailing Wage and Apprenticeship Expectations and Timing
New OSA Personnel

Good Afternoon -

We at OSA hope this email finds you and your family well.

In an effort to address some questions and concerns on the upcoming implementation of LCPtracker for the state's prevailing wage and apprenticeship utilization requirements which will be "live" on January 1, 2022, we offer the following:

It is our intent to:

- provide updated information on the implementation of the LCPtracker software including purchasing, timing, training, clarification of exempted IHE projects and lastly a request for a volunteer project to beta test the software

LCPTRACKER TASK ORDER PROCESS

1) Agency/Institution is to reach out to LCPTracker to request a proposal based on the agency's predicted *Public Project* construction volume (all non-exempt projects over $500,000). (Please note that the apprenticeship requirements of this statutory change does not impact apprenticeship utilization until the project cost is $1M or more.)
2) LCPTracker is to provide a proposal to Institution
3) Agency/Institution to complete Task Order template, attaching the proposal to the pdf, and load to DocuSign for execution.
   a. Please see FAQ sheet attached regarding task order template.
4) Executed Task Order is returned to agency with a copy to OSA:
   c/o Ishmael Darjean (303.866.5877) (ishmael.darjean1@state.co.us).
5) While we understand that our 13 Universities are outside the Procurement/Fiscal and OIT requirements, these institutions are bound by OSA process and our statutory authority requires your participation per the requirements of the Prevailing Wage statute. Please see attached information on the IT component of LCPtracker.
6) There are 3 types of training:

   a. Training will be done in two phases: (This training is offered upon execution of the Task Order)

      i. General overview and familiarization for all agencies anticipated in November or December.

ii. Agency-specific implementation meetings and trainings will be scheduled based on each Agency's anticipated construction dates to align training with utilization. This will include training of end users (Contractors) as well as Agency users.

iii. LCPTracker University for Certification – This program is available at an additional charge but is NOT required for implementation

Important: Please remember that prevailing wage and apprenticeship **does** apply to tenant finish work (in leasing transactions) provided by building owner if over $500k - whether the building is state-owned or private.

OSA Expectations and Timing For Delegates:

- Executed Task Orders for all 43 agencies/institutions by **October 31, 2021** (as was communicated on September 13, 2021)
- All agencies/institutions in the State **must** be contracted with LCPtracker prior to training
- Training to begin in late November 2021
- Any IHE exempted projects (as voted on before July 1, 2021 by your governing boards) **must** be reported to OSA by October 15, 2021
- OSA is seeking a volunteer project to beta test the LCPtracker (this testing would begin in late November 2021)

New OSA Personnel:

Introduction of OSA personnel to assist with prevailing wage and apprenticeship utilization:

Kathy Miller, Payroll Specialist (303.866.2562) Kathleen.miller@state.co.us
Ishmael Darjean, Trainer/Prevailing Wage Analyst (303.866.5677) Ishmael.darjean1@state.co.us

We will be hosting a virtual meeting with everyone as we approach our training and you will have an opportunity to meet Kathy and Ishmael.

INSTITUTIONS OF HIGHER EDUCATION
FAQ – TASK ORDER TEMPLATE
1 OCTOBER, 2021

In using the Task Order Template – please see the following common questions and answers:

- The LCP proposal is based on a calendar year of 2022. The Task Order template has Fiscal years dates at the top. Which are we to use?

  It depends where the date is going. The assumption is the Task Order is valid for 1 full calendar year from execution date. Operational Funding is by fiscal year, thus the Task Order Maximum amount for Fiscal year 2021-22 will only be from October to June 30 2022

- There is a block for Task Order #. Not sure what to place in this box.

  If your institution of higher ed has a standard for numbering encumbrance documents that should be put here.

- Same question on the Contract # box.

  This is the CMS number, please insert 170052 in this box

- Do we put the Beginning Date as the Effective date(of the signature), November 1st based on having it implemented by Oct 31st, or January 1st, 2022?

  OSA recommends using the date of the LCPTracker proposal, as it should be the date it is executed, but will we really know the date that it will be fully executed? It may be best to put the estimated date that your proposal will be executed.

- What do we put in the TO max amount box? We assume we insert the proposal amount, but why are there several years?

  You only need to complete the First Fiscal Year per the proposal amount. Next year, will be the second line, third year of the contract will have the 3rd line etc.

- The signature blocks have state personnel names already inserted. Do we leave these alone or do we infill with our local folks?

  Yes, please edit the Chief Information Office and State Controller as needed

LCPtrackerA ProfessionalA

[INFO]

The Preferred Construction Site Compliance Solution

- Saves time for the agency, prime and subcontractor
- Saves money by reducing the administrative work
- Cloud-based, highly automated system streamlines processes
- Dramatically reduces the risk of fines and negative audits
- World-class. hands-on support and training from the LCPtracker support team

Core Functionality

- Prevailing Wage/Davis Bacon Compliance and Reporting
- Workforce Demographics Tracking and Reporting
- Living/Minimum Wage Compliance
- Document Management
- Contractor/Administrator Communications
- Paper Free
- Online Access

LCPtracker Professional is a powerful cloud-based, prevailing wage and workforce compliance and management solution. It is ideal for Agencies and Prime Contractors working on construction projects who need to generate certified payroll reports and may need to track and enforce detailed worker information for compliance and workforce reporting. The software is comprehensive, easy to deploy, configurable, user-friendly, highly scalable, and time-tested in thousands of construction projects throughout the nation.

The core LCPtracker validation system checks payrolls for local, state, and federal Davis-Bacon wage and labor compliance by flagging any error or omission discrepancies the contractor may have on a report. Our software streamlines the process of inputting payrolls for contractors by interfacing with top payroll companies by a simple three step manual reporting process. Administrators can easily view, approve or reject payrolls and provide immediate feedback to contractors.

Info: lcptracker.com/solutions/lcptracker

Phone:A14.669. 2 **Email:A**nfo@lcptracker.com **Web:A**cptracker.com

LCPtracker

FOR PREVAILING WAGE AND WORKFORCE MANAGEMENT

Benefits for Administrators and Prime Contractors

- Fast easy startup in as little as a week
- Up to 80% savings of prevailing wage administrative costs as reported by our clients
- Automatic checking of certified payroll reports for compliance with wage and hour laws and prevailing wage laws
- Automatic logging and filing of certified payroll reports and related documents
- Provides the ability to identify problems when they first occur so prompt action can be taken
- All certified payroll reports are in the same format and refer to the exact prevailing wage craft names
- Automatic notification of compliance violations
- Communication with contractors with automatic audit trails
- Ability to specify associated documents required such as contractor license, insurance certificate, and apprentice certification
- Checks Federal (Davis Bacon), state, and local hire requirement simultaneously
- Site interview tool.
- Ability to create files for importing into government compliance monitoring systems: California DIR XML, Maryland CPR Upload, BRJP (City of Boston), ENG3180 (Army Corps of Engineers)
- Extensive reports on:
  Contractors, Employees, Documents Submitted/Due, Certified Payroll Report logs, Workforce (Gender, Local, Ethnicity, Disadvantaged, etc.), Apprentice Status / Apprentice Utilization)
- Drastically reduces risk of fines and negative audits
- Makes audits easy and clean; gives your organization credibility that you are taking compliance seriously
- Ability to track all subcontractor's compliance status
- Top of the line support – 95% of calls are answered immediately

Benefits for Subcontractors

- Electronic signature submittal of certified payroll reports
- Manual entry of payroll information by contractor
- Ability to import payroll/employee data from numerous payroll systems
- Easy to learn to use – less than an hour is typical
- Immediate check of compliance with Wage and Hour regulations and Prevailing Wage laws
- Tracks other employment requirements such as local hire goals and apprentice use
- Ability to check subcontractor compliance status
- Ability to submit required documents by upload
- Audit trail of submittal and compliance
- Extensive reporting

Phone: 714.669.0052 **Email:** info@lcptracker.com **Web:** lcptracker.com **Address:** 117 E. Chapman Ave, Orange, CA 92866

LCPtracker, Inc. is a service provider specializing in labor compliance and other workforce related software. We provide a powerful web-based software for collecting, verifying and managing certified payrolls and other labor compliance related documents. Numerous government agencies and prime contractors have already chosen LCPtracker for their certified payroll reporting and our software manages $180 Billion worth of construction projects across the nation.

LCPtracker

Supported Internet Browsers

- Microsoft Edge
  
- Google Chrome
  
- Fire Fox
  
- Opera
  

User Login address- https://prod-cdn.lcptracker.net

To ensure that you get all emails from LCPtracker, please set your system spam blocker so that:
1) all emails from the domain “lcptracker.com” are permitted and
2) all emails that originated from “lcptracker.com” but have your return email address and are returned to you because of bad email addresses are allowed also.
You will not receive important messages from LCPtracker without making these settings.

Hosted Server Infrastructure, Security, Backup and Disaster Recovery

Microsoft Partnership

LCPtracker has contracted with Microsoft to host our application infrastructure. LCPtracker's applications are hosted on Microsoft's Azure cloud platform, which provides a robust, highly scalable and highly available virtual infrastructure. Scalability, high-availability, backup and recovery, multi-region data replication, and disaster recovery are built-in. Microsoft's Azure cloud platform is a FedRAMP, SOC1, SOC2, as well as ISO 27001 certified service, and LCPtracker is AZRamp Authorized for confidential State data.

Availability

LCPtracker guarantees at least 99.5% availability for our SaaS software solutions over a one-year period. Downtime calculations do not include failures of LCPtracker's or the customer's Internet Service Provider, Microsoft Azure, or any planned LCPtracker maintenance time. Our trend over the last several months has been >99.9% availability. Production workloads are run from the WEST US region Azure datacenter (California). All data is replicated to the EAST US region Azure datacenter (Virginia).

Backup

Azure SQL runs back-ups periodically and runs consistency checks to recover from a hardware failure. This is a built-in internal operation that supports the overall health of the service and provides for automatic recovery. Additionally, LCPtracker backs-up all data on a nightly basis to a separate data store in the EAST US region Azure datacenter. Daily backups are retained for one month. Monthly backups are retained for one year. Backup integrity is tested at least annually.

Firewall

Access to LCPtracker's SaaS software solutions is controlled by Web Application Firewalls provided by Imperva. Access to the databases backing LCPtracker's applications is further controlled by firewalls within the Azure platform. These firewalls are configured to allow controlled access to the databases for users via the LCPtracker program only, and from specific trusted IP addresses including LCPtracker development in California.

Data Transmission Security

The lock icon in the browser when connected to our web applications indicates that all data is fully encrypted while in transit. LCPtracker uses TLS 1.3 and the AES encryption algorithm with 256-bit key length to encrypt all data in transit.

Physical Security

Online Services Security and Compliance (OSSC) manages the physical security of Microsoft's data centers. Industry-leading procedures in security design and operations are utilized for each facility. Microsoft ensures the establishment of outer and inner perimeters with increasing controls through each perimeter layer.

The security system applies the combined use of technology solutions including cameras, biometrics, card readers, and alarms with traditional security measures such as locks and keys. Operational controls are incorporated to facilitate automated monitoring and early notification if a breach or problem occurs, and enables accountability through the provision of auditable documentation of the data center's physical security program. The following list provides additional examples of how Microsoft applies controls to physical security:

- Restricting access to data center personnel – Microsoft provides security requirements upon which data center employees and contractors are reviewed. In addition to contractual stipulations about site staff, a further layer of security within the data center is applied to personnel that operate the facility. Access is restricted by applying a least privilege policy, so that only essential personnel are authorized to manage customers' applications and services.

- Addressing high business impact data requirements – Microsoft has developed more stringent minimum requirements for assets categorized as being highly sensitive than for those of low or moderate sensitivity within the data centers used to provide online services. Standard security protocols regarding identification, access tokens, and logging and surveillance of site entry clearly state what type of authentication is needed. In the case of access to highly sensitive assets, multifactor authentication is required.

- Centralizing physical asset access management – As Microsoft continues to expand the number of data centers used to provide online services, a tool was developed to manage access control to physical assets, which also provides auditable records through the centralization of workflow for the process of requesting, approving, and provisioning access to data centers. This tool operates using the principle of providing the least access needed and incorporates workflow for gaining approvals from multiple authorization parties. It is configurable to site conditions and enables more efficient access to history details for reporting and compliance with audits.

Data Security

The data security of LCPtracker is established in several layers. These layers include:

- Encryption in transit using TLS 1.3 and the AES encryption algorithm with 256-bit key length
- Multiple Stateful and Web Application Firewalls
- Critical data is encrypted at rest using Azure's standard AES encryption with 256-bit key length
- Multi-Factor Authentication required for access to sensitive data
- Limits on login attempts
- A minimum password complexity requirement
- Separation of concerns among Technology and Product Development staff

Each client has isolated, secure data storage locations. Social Security numbers are optional in our databases. In cases where Social Security numbers are collected and entered by customers, we encrypt the Social Security number at the field level. All public reports referencing Social Security numbers have redacting capabilities. Only one report lists Social Security numbers: the CPR report (PDF only) and it is optional on that report. Only two forms display Social Security numbers: the contractor employee setup form and the administrator employee review form. This approach provides access to Social Security numbers as required by various enforcement agencies while preventing misuse.

Additionally, LCPtracker imposes the following internal security steps:

- Access to database is limited to a small set of highly vetted, senior employees
- Background checks are performed at time of hiring on all employees
- Tools built into LCPtracker limit the amount of data that can be accessed at one time except for those with direct database access.

Server Redundancy

Azure is a multiply redundant server environment.

The primary level of recovery is not having a failure in the first place. The system is fully redundant so that failure of any one component will not cause entire system failure. LCPtracker has automatic notification of failures so corrective action can begin immediately.

Disaster Recovery Plan

The LCPtracker Disaster Recovery plan assumes that an Azure datacenter can go down at some time. The goal is to recover from a disaster in an acceptable time while minimizing the loss of data.

Datacenter-Down Mitigation Plan

1. Web application

To mitigate lcptracker.net (web app) downtime during a datacenter outage an Active/Passive deployment topology has been implemented.

Traffic Manager

Traffic Manager is a service from Microsoft that allows LCPtracker to keep multiple web app instances in different datacenters. In the event that a datacenter goes down, users will be redirected to a healthy LCPtracker instance in a different datacenter. LCPtracker production/active applications and data are hosted in Azure's WEST US region datacenters.

Redundant Web App Instances

Redundant instances of the web app and all its supporting services are maintained at a secondary Azure datacenter within the US. The failover web app instances are always live and up to date. LCPtracker DR/passive applications and data are hosted in Azure's EAST US region datacenters.

2. Data

To mitigate data loss:

Databases Geo Replication

All LCPtracker databases are geo-replicated. In the event that the datacenter hosting the live/primary database servers goes down, the replicated database will be live in a separate datacenter with only a few seconds of data loss.

Disaster Recovery

In the event of an outage in the WEST US datacenter the following steps will be followed to bring the service back up.

1. Traffic Manager starts redirecting traffic to secondary (failover) instance of web app. This is done automatically once Microsoft Azure declares a datacenter down.
2. In the event that Traffic Manager does not fail over automatically, DNS settings are swapped to disaster recovery IP addresses.
3. Geo-replicated databases become primary
4. Geo-replicated storage becomes primary
5. Disaster recovery web app instances in secondary data center become primary
6. LCPtracker is available online within minutes with only a few seconds of data loss.

RTO

The recovery time objective (RTO) is the maximum amount of time allocated for restoring application functionality. LCPtracker RTO is up-to 30 minutes.

RPO

The recovery point objective (RPO) is the acceptable time window of lost data due to the recovery process. LCPtracker's RPO for account databases is 1 minute or less.

Disaster Recovery Testing

Testing of the Disaster Recovery plan is carried out on at least an annual basis. Tests are conducted and reviewed to verify the effectiveness of the recovery plan. Over and above the annual test frequency, additional tests are performed when material changes are made to the hosted infrastructure.

Highly Reliable Service

Microsoft Azure is considered the top web-hosted service in the industry. This service provides inherent advantages: there is multiple redundant backup and disaster recovery built into the base service. LCPtracker may choose to move its primary choice of data center as other locations become available in search of optimal performance. Every client database is configured separately for scalability and security and each is hosted in a separate machine in Microsoft's data center. Data is replicated to 2 other locations, one of which is guaranteed to be at least 100 miles away to provide failover and disaster recovery. Databases are backed up at 11pm PST Monday through Friday to storage accounts within a separate subscription in the data center that are themselves replicated to 2 other locations. Note that this means primary LCPtracker service is in three locations and backup of LCPtracker is in three different locations. Any of these six locations is capable of supporting the LCPtracker service.

System Monitoring

24 hours a day, 7 days a week all systems are monitored from several locations across the country. If performance, latency, or availability is degraded in any way, the DevOps group is automatically notified for immediate resolution.

McAfee SECURE Site Designation

Our LCPtracker site has been tested for external vulnerabilities and is certified as a McAfee SECURE site.

"Sites which are McAfee SECURE are tested daily to pass all external vulnerability audit recommendations of the Department of Homeland Security's National Infrastructure Protection Center (NIPC), the SANS/FBI Top 20 Internet Security Vulnerabilities list as well as the vulnerability audit

requirements of Visa's CISP and AIS, MasterCard's SDP, American Express' DSS and Discover Card's DISC security standards.

McAfee SECURE sites are also certified to be in compliance with the network perimeter security criteria mandated in such regulations as: the Health Insurance Portability & Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOA) and the Government Information Security Reform Act (GISRA), as well as Canada's Personal Information Protection and Electronic Documents Act.

LCPtracker, Inc. Accessibility Conformance Report
Revised Section 508 Edition
(Based on VPAT® Version 2.4)

Name of Product/Version:
LCPtracker Professional (referenced in the document as LCPtracker) – September 2021

Report Date: September 2021

Product Description: LCPtracker Professional is a cloud-based SaaS solution and is the leading solution for certified payroll reporting software, construction site compliance management, and workforce reporting.

Contact Information: Patrick Conlin, CTO/CISO / pconlin@lcptracker.com

Notes: This report reflects the accessibility of LCPtracker's latest cloud deployment as of September 2021 based on VPAT version 2.4. This report supersedes the VPAT from July 2019 (VPAT version 1.6).

LCPtracker, Inc. is currently in the process of significant system improvements that will be rolled out in a phased approach during 2022 and 2023. Included in these changes are enhancements in accessibility throughout the product.

Evaluation Methods Used:
Manual testing, Lighthouse Extension, WAVE tool by WebAim

Applicable Standards/Guidelines

This report covers the degree of conformance for the following accessibility standard/guidelines:

Standard/Guideline	Included In Report
Web Content Accessibility Guidelines 2.0	Level A (Yes) Level AA (Yes) Level AAA (No)

Standard/Guideline	Included In Report
Revised Section 508 standards published January 18, 2017 and corrected January 22, 2018	(Yes)

Terms

The terms used in the Conformance Level information are defined as follows:

- **Supports**: The functionality of the product has at least one method that meets the criterion without known defects or meets with equivalent facilitation.
- **Partially Supports**: Some functionality of the product does not meet the criterion.
- **Does Not Support**: The majority of product functionality does not meet the criterion.
- **Not Applicable**: The criterion is not relevant to the product.
- **Not Evaluated**: The product has not been evaluated against the criterion. This can be used only in WCAG 2.0 Level AAA.

WCAG 2.0 Report

Tables 1 and 2 also document conformance with Revised Section 508:

- Chapter 5 – 501.1 Scope, 504.2 Content Creation or Editing
- Chapter 6 – 602.3 Electronic Support Documentation

Note: When reporting on conformance with the WCAG 2.0 Success Criteria, they are scoped for full pages, complete processes, and accessibility-supported ways of using technology as documented in the WCAG 2.0 Conformance Requirements.

Table 1: Success Criteria, Level A

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.1.1 Non-text Content (Level A)	Partially Supports	LCPtracker provides most of our images, form elements, and navigations with appropriate alternative texts and aria descriptions. Through the testing platforms of Lighthouse and WAVE there are still some remaining pages that certain select dropdowns do not have associated labels.
1.2.1 Audio-only and Video-only (Prerecorded) (Level A)	Not Applicable	LCPtracker does not provide audio-only or video-only recordings in the application.
1.2.2 Captions (Prerecorded) (Level A)	Does Not Support	LCPtracker does not currently provide captions on audio/videos available in the system, but users are able to download the video as an mp4 file which can then be viewed on an alternate program.
1.2.3 Audio Description or Media Alternative (Prerecorded) (Level A)	Does Not Support	LCPtracker does not currently support this item.
1.3.1 Info and Relationships (Level A)	Supports	LCPtracker uses ARIA landmarks to properly structure the webpage and provide meaningful relationships and labels to each of the regions and their respective elements.
1.3.2 Meaningful Sequence (Level A)	Supports	The User Interface complies with meaningful descriptions. The

Criteria	Conformance Level	Remarks and Explanations
		navigation order is also logical and intuitive.
1.3.3 Sensory Characteristics (Level A)	Supports	LCPtracker relies on form controls with normal buttons and links. The system does not require users to perform certain actions or listen to sound to continue.
1.4.1 Use of Color (Level A)	Partially Supports	LCPtracker largely provides most form elements within the given contrast ratio that exceeds 4.5:1. Certain navigational elements do not meet the contrast ratio as the ratio drops to 2.9:1
1.4.2 Audio Control (Level A)	Support	LCPtracker fully supports Audio/Video controls with play, pause, mute, and other controls on the player.
2.1.1 Keyboard (Level A)	Supports	LCPtracker application largely supports utilizing keyboard interaction within the navigation and form elements. There are a few pages where there are tables that does not fully support the keyboard functionality.
2.1.2 No Keyboard Trap (Level A)	Supports	LCPtracker supports this item.
2.2.1 Timing Adjustable (Level A)	Partially Support	LCPtracker has a timed user experience session that has a pre-set duration and eventually expires.

Criteria	Conformance Level	Remarks and Explanations
		LCPtracker does offer an "Extend", where the user is warned before they are logged off due to inactivity and can continue to remain in the system. We do not currently offer a "Turn off" or "Adjust" options due to security requirements.
2.2.2 Pause, Stop, Hide (Level A)	Supports	LCPtracker does not provide any carousels, marquees, or animation and does not have any functionality that needs to be stopped or hidden.
2.3.1 Three Flashes or Below Threshold (Level A)	Supports	LCPtracker does not provide any of our pages with interactions that involve flashes. Changes stay static on forms for needed corrections.
2.4.1 Bypass Blocks (Level A)	Does Not Support	LCPtracker does currently not provide a "skip" navigation or directs them to the main content area on the given pages.
2.4.2 Page Titled (Level A)	Supports	LCPtracker provides a <title> tag in the html to display our Application for Browsers to use in their own device and browser tabs.
2.4.3 Focus Order (Level A)	Supports	The page navigation and form elements follow intuitive and logical order.
2.4.4 Link Purpose (In Context) (Level A)	Supports	Links are readily distinguishable, and every link can be determined from either the link context, list item, and table headers.

Criteria	Conformance Level	Remarks and Explanations
3.1.1 Language of Page (Level A)	Partially Supports	LCPtracker does not run in a Single Page Application (SPA) and a small number of pages do not have the required <html lang=**"en">**.
3.2.1 On Focus (Level A)	Supports	Focusing on page elements does not have any substantial change, pop-up windows, or additional change of keyboard focus. Only our Navigational elements can be adjusted but maintains focus on the selected element.
3.2.2 On Input (Level A)	Partially Supports	Most input and controls do not result in substantial changes, but some forms are accessible only through pop-up modals to add or update the given page list.
3.3.1 Error Identification (Level A)	Supports	LCPtracker provides support in identifying input values that are out of range, required, and in date ranges that reside in the Labels. We help identify these issues so the data will be in the accepted format before it is saved.
3.3.2 Labels or Instructions (Level A)	Supports	All Labels and Interactive Elements are properly positioned in the form which prevent users from making incomplete or incorrect form submissions.
4.1.1 Parsing (Level A)	Partially Supports	Elements have complete start and end tags and are nested according to specifications. Some pages have duplicate naming attributes

Criteria	Conformance Level	Remarks and Explanations
		preventing them from being totally unique.
4.1.2 Name, Role, Value (Level A)	Partially Supports	The large majority of pages and navigation use the name and role attributes where assisted technologies can provide aid to users. There are a few pages with no name/roles that do not lead to interactions for those assisted technologies.

Table 2: Success Criteria, Level AA

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.2.4 Captions (Live) (Level AA)	Not Applicable	LCPtracker only provides pre-recorded audio/videos so live captions are not applicable.
1.2.5 Audio Description (Prerecorded) (Level AA)	Does Not Support	LCPtracker does not currently support this functionality.
1.4.3 Contrast (Minimum) (Level AA)	Partially Supports	LCPtracker provides most form elements within the given contrast ratio that exceeds 4.59:1. There are certain elements on navigation, table headers, and section headers that does not meet the contrast ratio as it drops to a minimum of 2.9:1.

Criteria	Conformance Level	Remarks and Explanations
1.4.4 Resize text (Level AA)	Does Not Support	LCPtracker contains the text within a certain screen size and is not currently responsive by nature. A 200% increase in text size pushes elements beyond the given window.
1.4.5 Images of Text (Level AA)	Supports	LCPtracker does not rely on images to represent text alone. We support with Form attributes, ARIA Landmarks, and alternate text when images are present.
2.4.5 Multiple Ways (Level AA)	Does Not Support	Aside from the header navigation and sub-tiered pages, LCPtracker does not currently provide site maps, site searches, or list of all available web pages.
2.4.6 Headings and Labels (Level AA)	Supports	Headings and labels for forms and controls are distinguishable and do not duplicate. LCPtracker use repeatable buttons on tables and lists where actions are available where that item is informative and descriptive.
2.4.7 Focus Visible (Level AA)	Supports	LCPtracker allows only modern browsers and does not sacrifice the outline property in CSS so every focusable item is visible.
3.1.2 Language of Parts (Level AA)	Does Not Support	LCPtracker currently only provides language at the HTML tag level as a whole application and do not separate them into blocks.

Criteria	Conformance Level	Remarks and Explanations
3.2.3 Consistent Navigation (Level AA)	Supports	The main navigation does not change when users are moving throughout the site. This allows users the flexibility of easily moving throughout pages in the system.
3.2.4 Consistent Identification (Level AA)	Supports	All elements that have the same functionality are set in the header and footer of our application. They do not change within different pages.
3.3.3 Error Suggestion (Level AA)	Supports	LCPtracker looks to identify and validate form submissions for data integrity and when errors occur, the system tells users what to fix to properly meet requirements.
3.3.4 Error Prevention (Legal, Financial, Data) (Level AA)	Supports	LCPtracker keeps data secure and allows the user submissions to be verified and confirmed.

Revised Section 508 Report

Notes:

Chapter 3: Functional Performance Criteria (FPC)

Notes:

Criteria	Conformance Level	Remarks and Explanations
302.1 Without Vision	Does Not Support	LCPtracker currently does provide a screen reader necessary to support users without vision. Operating Systems

Criteria	Conformance Level	Remarks and Explanations
		or Browser Plugins may be used to assist these users.
302.2 With Limited Vision	Does Not Support	LCPtracker currently does provide a screen reader necessary to support users with limited vision. Operating System or Browser Plugins can aid with users that require hearing assistance.
302.3 Without Perception of Color	Supports	Color perception is not required to use LCPtracker.
302.4 Without Hearing	Partially Supports	Overall, use of LCPtracker does not require users to be able to hear. The one exception is the ability to listen to training videos. Alternately, written training material can be viewed.
302.5 With Limited Hearing	Partially Supports	Overall, use of LCPtracker does not require users to be able to hear. The one exception is the ability to listen to training videos. Alternately, written training material can be viewed.
302.6 Without Speech	Supports	LCPtracker does not require users to use speech in any way.
302.7 With Limited Manipulation	Does Not Support	LCPtracker does not currently support this functionality.
302.8 With Limited Reach and Strength	Supports	LCPtracker does not require users to have a certain reach or strength to utilize the software.

Criteria	Conformance Level	Remarks and Explanations
302.9 With Limited Language, Cognitive, and Learning Abilities	Does Not Support	LCPtracker does not currently support this functionality.

Chapter 4: Hardware

Notes: Chapter 4 is not covered in this report, as there is no hardware that needs to be evaluated.

Chapter 5: Software

Notes:

Criteria	Conformance Level	Remarks and Explanations
501.1 Scope – Incorporation of WCAG 2.0 AA	See WCAG 2.0 section	
502 Interoperability with Assistive Technology	Heading cell – no response required	Heading cell – no response required
502.2.1 User Control of Accessibility Features	Does Not Support	LCPtracker does not provide user customization for keyboards, audio, speech, or captions.
502.2.2 No Disruption of Accessibility Features	Does Not Support	LCPtracker does not provide user customization/settings for keyboards, audio, speech, or captions.
502.3 Accessibility Services	Heading cell – no response required	Heading cell – no response required
502.3.1 Object Information	Does Not Support	LCPtracker does not provide object information for screen reader, screen

Criteria	Conformance Level	Remarks and Explanations
		magnifier, speech recognition or Braille display.
502.3.2 Modification of Object Information	Does Not Support	LCPtracker does not provide modification programmatically through assistive technology.
502.3.3 Row, Column, and Headers	Partially Supports	For most tables rows and columns are well defined, but some pages do not provide table heading <th> tags in all tables.
502.3.4 Values	Partially Supports	Objects and graphics support names and roles in the application.
502.3.5 Modification of Values	Supports	Screen readers or speech recognition is not provided for modification of values or ranges.
502.3.6 Label Relationships	Supports	LCPtracker ensures accessible names of form fields match on-screen label.
502.3.7 Hierarchical Relationships	Supports	Heading and list items are supported in hierarchical order.
502.3.8 Text	Supports	LCPtracker utilizes standard system functions for writing content to the screen.
502.3.9 Modification of Text	Supports	LCPtracker does not modify text programmatically and allows assistive technology fully interact with text.

Criteria	Conformance Level	Remarks and Explanations
502.3.10 List of Actions	Supports	LCPtracker provides assistive technologies a way to list actions on a single object.
502.3.11 Actions on Objects	Supports	LCPtracker also provides assistive technologies a way to take actions on a single object
502.3.12 Focus Cursor	Supports	Exposes information to track focus, text insertion point, and selection attributes of user elements.
502.3.13 Modification of Focus Cursor	Supports	User can set focus, text insertion point, and selection attributes of the given elements.
502.3.14 Event Notification	Supports	LCPtracker notifies changes in the component's state and made available to assistive technology
502.4 Platform Accessibility Features	Does Not Support	LCPtracker does not provide customization or settings of keystrokes, audio, speech, or captions.
503 Applications	Heading cell – no response required	Heading cell – no response required
503.2 User Preferences	Does Not Support	LCPtracker provides contrast ratio within form elements of 4.5:1. User preferences for High Contrast, Color Settings, and System Settings are not supported.

Criteria	Conformance Level	Remarks and Explanations
503.3 Alternative User Interfaces	Does Not Support	LCPtracker provides no alternative user interfaces that function as assistive technology
503.4 User Controls for Captions and Audio Description	Heading cell – no response required	Heading cell – no response required
503.4.1 Caption Controls	Does Not Support	LCPtracker does not provide caption for audio or video
503.4.2 Audio Description Controls	Does Not Support	LCPtracker does not provide audio description for audio or video
504 Authoring Tools	Heading cell – no response required	Heading cell – no response required
504.2 Content Creation or Editing (if not **authoring tool, enter "not applicable")**	See WCAG 2.0 section	See information in WCAG 2.0 section
504.2.1 Preservation of Information Provided for Accessibility in Format Conversion	Not Applicable	
504.2.2 PDF Export	Partially Supports	PDF exported from LCPtracker are in PDF version 1.7. However, the files currently do not conform to ANSI/AIIM/ISO 14289-1:2016 (PDF/UA-1)
504.3 Prompts	Not Applicable	
504.4 Templates	Not Applicable	

Chapter 6: Support Documentation and Services

Notes:

Criteria	Conformance Level	Remarks and Explanations
601.1 Scope	Heading cell – no response required	Heading cell – no response required
602 Support Documentation	Heading cell – no response required	Heading cell – no response required
602.2 Accessibility and Compatibility Features	Does Not Support	LCPtracker does not provide accessibility documentation for the features that are built-in and compatible with assistive technologies.
602.3 Electronic Support Documentation	See WCAG 2.0 section	See information in WCAG 2.0 section
602.4 Alternate Formats for Non-Electronic Support Documentation	Not Applicable	LCPtracker only offers support documentation in electronic formats.
603 Support Services	Heading cell – no response required	Heading cell – no response required
603.2 Information on Accessibility and Compatibility Features	Does Not Support	LCPtracker does not provide accessibility documentation for the features that are built-in and compatible with assistive technologies.
603.3 Accommodation of Communication Needs	Partially Supports	LCPtracker's Support Team offers assistance through phone, email or chat, allowing for either verbal or written communication.

Legal Disclaimer (Company)

© 2021 LCPtracker, Inc. As of the date of its publication indicated in the information table at the beginning of this Conformance Report, this Conformance Report represents the current view to the best of its knowledge of LCPtracker, Inc. regarding information about the subject LCPtracker Professional in the ITI's "VPAT® 2.4 Revised Section 508 Edition." This Conformance Report is not intended to be a certification of compliance and does not in any way constitute legal advice. LCPtracker, Inc. cannot guarantee that any information in this Conformance Report will remain accurate after the aforementioned date of publication due to changes to the LCPtracker Professional SaaS product which may render some or all of this Conformance Report to become inaccurate. This Conformance Report is provided "as is" and for informational purposes only. LCPtracker, Inc. specifically disclaims any liability with respect to this Conformance Report and no contractual obligations are formed either directly or indirectly by this Conformance Report.

SOC 2 Gap Assessment from Vanta

FOR LCPTRACKER, INC.

The American Institute of Certified Public Accountants (AICPA) defined the SOC (System and Organization Controls) reporting framework to help businesses manage risks. Their SOC 2 standard defines criteria for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy.

Vanta performed a gap analysis of LCPtracker, Inc.'s security and IT infrastructure in preparation for a SOC 2 audit. Vanta's SOC 2 analysis identified gaps in LCPtracker, Inc.'s infrastructure and provided steps to correct them.

In this report, Vanta:

- Tests a complete set of security and infrastructure controls that may appear in a SOC 2 audit
- Identifies gaps and vulnerabilities in infrastructure and processes

Intended use

This gap assessment can be used by:

- LCPtracker, Inc. to identify issues critical for remediation
- LCPtracker, Inc.'s customers to understand the company's progress toward SOC 2 compliance

Continuous gap assessment approach: continuous monitoring

Vanta continuously monitors the company's policies, procedures, and IT infrastructure to ensure the company adheres to AICPA's Trust Service Principles of security, availability, and confidentiality.

To do this, Vanta connects directly to the company's infrastructure accounts, version control tools, task trackers, endpoints, hosts, HR tools, and internal policies. Vanta then continuously monitors these resources to determine if LCPtracker, Inc. meets the SOC 2 standard.

In compiling this gap assessment, Vanta took into account LCPtracker, Inc.'s unique requirements and technical environment, including business model, products and services, and interactions with customer data.

CC 1.0

Control Environment

CC 1.1

COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

6 CONTROLS

Code of Conduct acknowledged by contractors

✓ COMPLETE

The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.

2 TESTS

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to the Code of Conduct. ✓

Code of Conduct acknowledged by employees and enforced

✓ COMPLETE

The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.

4 TESTS

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to the Code of Conduct. ✓

Employees agree to Human Resource Security Policy: Verifies that all relevant employees have agreed to the Human Resource Security Policy. ✓

Confidentiality Agreement acknowledged by contractors

✓ COMPLETE

The company requires contractors to sign a confidentiality agreement at the time of engagement.

1 TEST

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Confidentiality Agreement acknowledged by employees

✓ COMPLETE

The company requires employees to sign a confidentiality agreement during onboarding.

1 TEST

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Employee background checks performed

✓ COMPLETE

The company performs background checks on new employees.

2 TESTS

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Background checks on new hires: Verifies that all employees for whom a background check is required have a background check on file. ✓

Performance evaluations conducted

✓ COMPLETE

The company managers are required to complete performance evaluations for direct reports at least annually.

1 DOCUMENT

Completed performance evaluations ✓

CC 1.2

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

2 CONTROLS

Board meetings conducted

✓ COMPLETE

The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

1 DOCUMENT

Board of directors meeting minutes and agenda ✓

Board oversight briefings conducted

✓ COMPLETE

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.

1 DOCUMENT

Board of directors meeting minutes and agenda ✓

CC 1.3

COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

3 CONTROLS

Management roles and responsibilities defined

✓ COMPLETE

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

4 TESTS

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Information Security Policy (AUP): Verifies that all relevant employees have agreed to the Information Security Policy (AUP). ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Organization structure documented

✓ COMPLETE

The company maintains an organizational chart that describes the organizational structure and reporting lines.

1 DOCUMENT

Company organization chart ✓

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 TEST

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

1 DOCUMENT

Job descriptions for key security roles ✓

CC 1.4

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

4 CONTROLS

Employee background checks performed

✓ COMPLETE

The company performs background checks on new employees.

2 TESTS

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Background checks on new hires: Verifies that all employees for whom a background check is required have a background check on file. ✓

Performance evaluations conducted

✓ COMPLETE

The company managers are required to complete performance evaluations for direct reports at least annually.

1 DOCUMENT

Completed performance evaluations ✓

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 TEST

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

1 DOCUMENT

Job descriptions for key security roles ✓

Security awareness training implemented

✓ COMPLETE

The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.

1 TEST

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

CC 1.5

COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

3 CONTROLS

Code of Conduct acknowledged by employees and enforced

✓ COMPLETE

The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.

4 TESTS

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to the Code of Conduct. ✓

Employees agree to Human Resource Security Policy: Verifies that all relevant employees have agreed to the Human Resource Security Policy. ✓

Performance evaluations conducted

✓ COMPLETE

The company managers are required to complete performance evaluations for direct reports at least annually.

1 DOCUMENT

Completed performance evaluations ✓

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 TEST

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

1 DOCUMENT

Job descriptions for key security roles ✓

CC 2.0

Communication and Information

CC 2.1

COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

3 CONTROLS

Control self-assessments conducted

✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

Log management utilized

✓ COMPLETE

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

5 TESTS

Blob containers used to hold Activity Logs have access logs enabled (Azure): Verifies that the insights-activity-logs Azure blob container has access logging enabled. ✓

Heroku logs archived for 365 days: Verifies that all Heroku apps are using a plugin that stores logs for 365 days, or are using a custom log drain. ✓

Subscription Activity Logs are being archived to a storage account (Azure): Verifies that all linked Azure subscriptions have activity logging enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

CC 2.2

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

8 CONTROLS

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Management roles and responsibilities defined

✓ COMPLETE

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

4 TESTS

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Information Security Policy (AUP): Verifies that all relevant employees have agreed to the Information Security Policy (AUP). ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 TEST

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

1 DOCUMENT

Job descriptions for key security roles ✓

Security awareness training implemented

✓ COMPLETE

The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.

1 TEST

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

30 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Asset Management Policy: Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to ✓

the Code of Conduct.

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Employees agree to Human Resource Security Policy: Verifies that all relevant employees have agreed to the Human Resource Security Policy. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Information Security Policy (AUP): Verifies that all relevant employees have agreed to the Information Security Policy (AUP). ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

Employees agree to Secure Development Policy: Verifies that all relevant employees have agreed to the Secure Development Policy. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Service description communicated

✓ COMPLETE

The company provides a description of its products and services to internal and external users.

2 DOCUMENTS

Network diagram ✓

Product documentation site ✓

System changes communicated

✓ COMPLETE

The company communicates system changes to authorized internal users.

1 DOCUMENT

Internal communication for system updates ✓

Whistleblower policy established

✓ COMPLETE

The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.

1 TEST

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

CC 2.3

COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

6 CONTROLS

Company commitments externally communicated

✓ COMPLETE

The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).

3 DOCUMENTS

MSA template ✓

Security information page ✓

Publicly available terms of service ✓

External support resources available

✓ COMPLETE

The company provides guidelines and technical support resources relating to system operations to customers.

2 DOCUMENTS

Customer support site or email alias ✓

Public change log or release notes ✓

Service description communicated

✓ COMPLETE

The company provides a description of its products and services to internal and external users.

2 DOCUMENTS

Network diagram ✓

Product documentation site ✓

Support system available

✓ COMPLETE

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.

3 DOCUMENTS

Customer support site or email alias ✓

Product documentation site ✓

Public change log or release notes ✓

System changes externally communicated

✓ COMPLETE

The company notifies customers of critical system changes that may affect their processing.

4 DOCUMENTS

Customer support site or email alias ✓

Product documentation site ✓

Public change log or release notes ✓

Application status page ✓

Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

1 TEST

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

2 DOCUMENTS

Publicly available privacy policy ✓

Publicly available terms of service ✓

CC 3.0

Risk Assessment

CC 3.1

COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

2 CONTROLS

Risk assessment objectives specified

✓ COMPLETE

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

1 TEST

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Risk management program established

✓ COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

CC 3.2

COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

3 CONTROLS

Continuity and disaster recovery plans tested

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

2 TESTS

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Risk management program established

✓ COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

4 TESTS

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Compliance reports for critical vendors: Verifies that all vendors marked as "High Severity" within Vanta have associated security assessment documents. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

1 CONTROL

Risk management program established

✓ COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

CC 3.4

COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

3 CONTROLS

Configuration management system established

✓ COMPLETE

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

3 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Standard production images: This feature is built into Heroku. ✓

Standard production image updated: This feature is built into Heroku. ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Records of penetration testing: Verifies that a penetration test has been conducted within the last 12 months and that evidence of that test has been uploaded to Vanta. ✓

Risk management program established

✓ COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

CC 4.0

Monitoring Activities

CC 4.1

COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

4 CONTROLS

Control self-assessments conducted

✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Records of penetration testing: Verifies that a penetration test has been conducted within the last 12 months and that evidence of that test has been uploaded to Vanta. ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

4 TESTS

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Compliance reports for critical vendors: Verifies that all vendors marked as "High Severity" within Vanta have associated security assessment documents. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

CC 4.2

COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

2 CONTROLS

Control self-assessments conducted

✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

4 TESTS

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Compliance reports for critical vendors: Verifies that all vendors marked as "High Severity" within Vanta have associated security assessment documents. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

CC 5.0

Control Activities

CC 5.1

COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

2 CONTROLS

Risk management program established

✓ COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

30 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Asset Management Policy: Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to ✓

the Code of Conduct.

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Employees agree to Human Resource Security Policy: Verifies that all relevant employees have agreed to the Human Resource Security Policy. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Information Security Policy (AUP): Verifies that all relevant employees have agreed to the Information Security Policy (AUP). ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

Employees agree to Secure Development Policy: Verifies that all relevant employees have agreed to the Secure Development Policy. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

CC 5.2

COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

3 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Development lifecycle established

✓ COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

30 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Asset Management Policy: Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to ✓

the Code of Conduct.

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy.

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy.

Employees agree to Human Resource Security Policy: Verifies that all relevant employees have agreed to the Human Resource Security Policy.

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan.

Employees agree to Information Security Policy (AUP): Verifies that all relevant employees have agreed to the Information Security Policy (AUP).

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities.

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy.

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy.

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy.

Employees agree to Secure Development Policy: Verifies that all relevant employees have agreed to the Secure Development Policy.

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy.

CC 5.3

COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

10 CONTROLS

Backup processes established

✓ COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

3 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Change management procedures enforced

✓ COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

1 TEST

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Data retention procedures established

✓ COMPLETE

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Development lifecycle established

COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta.

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy.

Incident response policies established

COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta.

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan.

Risk assessment objectives specified

COMPLETE

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

1 TEST

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta.

Risk management program established

COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta.

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy.

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 TEST

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

1 DOCUMENT

Job descriptions for key security roles ✓

Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

30 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Asset Management Policy: Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Company has an approved Code of Conduct: Verifies that a Code of Conduct has been created and approved within Vanta. ✓

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Company has an approved Human Resource Security Policy: Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Information Security Policy (AUP): Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to ✓

the Code of Conduct.

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Employees agree to Human Resource Security Policy: Verifies that all relevant employees have agreed to the Human Resource Security Policy. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Information Security Policy (AUP): Verifies that all relevant employees have agreed to the Information Security Policy (AUP). ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

Employees agree to Secure Development Policy: Verifies that all relevant employees have agreed to the Secure Development Policy. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

4 TESTS

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Compliance reports for critical vendors: Verifies that all vendors marked as "High Severity" within Vanta have associated security assessment documents. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

CC 6.0

Logical and Physical Access Controls

CC 6.1

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

17 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Data classification policy established

✓ COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Data encryption utilized

✓ COMPLETE

The company's datastores housing sensitive customer data are encrypted at rest.

2 TESTS

SQL databases encrypted (Azure): Verifies that all Azure SQL databases are encrypted at rest. ✓

User data is encrypted at rest (Heroku): Verifies that Heroku databases are encrypted at rest. This feature is automatically provided by Heroku Postgres plans on the Standard tier or higher. ✓

Encryption key access restricted

✓ COMPLETE

The company restricts privileged access to encryption keys to authorized users with a business need.

2 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

Infrastructure provider's key management used: This feature is built into Heroku. ✓

Firewall access restricted

✓ COMPLETE

The company restricts privileged access to the firewall to authorized users with a business need.

8 TESTS

Company has an approved Asset Management Policy: Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

EC2 instance public ports restricted (AWS): Verifies that each EC2 instance's attached Security Groups expose at most ports 80 and 443 to the public internet. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

SSH required for server access: This feature is built into Heroku. ✓

Public SSH denied (Azure): Verifies that no Azure security groups allow unrestricted access to TCP port 22. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. ✓

Password policy enforced

✓ COMPLETE

The company requires passwords for in-scope system components to be configured according to the company's policy.

1 TEST

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

Production application access restricted

✓ COMPLETE

The company restricts privileged access to the application to authorized users with a business need.

5 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Employees have unique email accounts: Verifies that every linked identity provider has more than one user. ✓

Employees have unique infrastructure accounts: Verifies that every linked AWS and Heroku account have at least one user. ✓

Service accounts used (Heroku): This feature is built into Heroku. ✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku. ✓

Production database access restricted

✓ COMPLETE

The company restricts privileged access to databases to authorized users with a business need.

1 TEST

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

Production deployment access restricted

✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

3 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days. ✓

Production inventory maintained

✓ COMPLETE

The company maintains a formal inventory of production system assets.

1 TEST

Inventory list tracks user data: Verifies that at least one item on Vanta's inventory list has been marked as containing user data. ✓

Production network access restricted

✓ COMPLETE

The company restricts privileged access to the production network to authorized users with a business need.

1 TEST

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

Production OS access restricted

✓ COMPLETE

The company restricts privileged access to the operating system to authorized users with a business need.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Remote access encrypted enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

1 TEST

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Unique account authentication enforced

✓ COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

6 TESTS

Employees have unique email accounts: Verifies that every linked identity provider has more than one user. ✓

Employees have unique infrastructure accounts: Verifies that every linked AWS and Heroku account have at least one user. ✓

Service accounts used (Heroku): This feature is built into Heroku. ✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku. ✓

SSH required for server access: This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. ✓

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

2 TESTS

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

SSH required for server access: This feature is built into Heroku. ✓

Unique production database authentication enforced

✓ COMPLETE

The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.

1 TEST

SSH required for server access: This feature is built into Heroku. ✓

CC 6.2

Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

5 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Access reviews conducted

✓ COMPLETE

The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

5 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that G Suite, Office 365, or Okta has been linked to Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

2 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed within the specified SLA. ✓

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

2 TESTS

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

SSH required for server access: This feature is built into Heroku. ✓

CC 6.3

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

5 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Access reviews conducted

✓ COMPLETE

The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

5 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that G Suite, Office 365, or Okta has been linked to Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

2 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed within the specified SLA. ✓

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

2 TESTS

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

SSH required for server access: This feature is built into Heroku. ✓

CC 6.4

The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

4 CONTROLS

Access reviews conducted

✓ COMPLETE

The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

5 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that G Suite, Office 365, or Okta has been linked to Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Data center access reviewed

✓ COMPLETE

The company reviews access to the data centers at least annually.

2 TESTS

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Physical access processes established

✓ COMPLETE

The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.

2 TESTS

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Visitor procedures enforced

✓ COMPLETE

The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.

2 TESTS

Company has an approved Physical Security Policy: Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

CC 6.5

The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

4 CONTROLS

Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

2 TESTS

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed within the specified SLA. ✓

Asset disposal procedures utilized

✓ COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

2 TESTS

Company has an approved Asset Management Policy: Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Customer data deleted upon leave

✓ COMPLETE

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

1 TEST

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Data retention procedures established

✓ COMPLETE

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

CC 6.6

The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

8 CONTROLS

Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

6 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Strong SSL/TLS ciphers used: Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

SSL configuration has no known issues: Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

4 TESTS

Blob containers used to hold Activity Logs have access logs enabled (Azure): Verifies that the insights-activity-logs Azure blob container has access logging enabled. ✓

Subscription Activity Logs are being archived to a storage account (Azure): Verifies that all linked Azure subscriptions have activity logging enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

Network and system hardening standards maintained

✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

7 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Azure): Verifies that no Azure security groups allow unrestricted access to TCP port 22. ✓

Network firewalls reviewed

✓ COMPLETE

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

4 TESTS

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Azure): Verifies that no Azure security groups allow unrestricted access to TCP port 22. ✓

Network firewalls utilized

✓ COMPLETE

The company uses firewalls and configures them to prevent unauthorized access.

4 TESTS

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Azure): Verifies that no Azure security groups allow unrestricted access to TCP port 22. ✓

Remote access encrypted enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

1 TEST

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

5 TESTS

Server configuration tool used: This feature is built into Heroku. ✓

Servers patched within 30 days: This feature is built into Heroku. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

2 TESTS

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

SSH required for server access: This feature is built into Heroku. ✓

CC 6.7

The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

3 CONTROLS

Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

6 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Strong SSL/TLS ciphers used: Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

SSL configuration has no known issues: Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

MDM system utilized

✓ COMPLETE

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

1 TEST

Malware detection on computers: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed. ✓

Portable media encrypted

✓ COMPLETE

The company encrypts portable and removable media devices when used.

1 TEST

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

CC 6.8

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

3 CONTROLS

Anti-malware technology utilized

✓ COMPLETE

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

2 TESTS

Malware detection on computers: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

Development lifecycle established

✓ COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

5 TESTS

Server configuration tool used: This feature is built into Heroku. ✓

Servers patched within 30 days: This feature is built into Heroku. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

CC 7.0

System Operations

CC 7.1

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

4 CONTROLS

Change management procedures enforced

✓ COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

1 TEST

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Configuration management system established

✓ COMPLETE

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

3 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Standard production images: This feature is built into Heroku. ✓

Standard production image updated: This feature is built into Heroku. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

Vulnerability and system monitoring procedures established

✓ COMPLETE

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

- vulnerability management;
- system monitoring.

1 TEST

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

CC 7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

7 CONTROLS

Infrastructure performance monitored

✓ COMPLETE

An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

4 TESTS

Load balancer used (Azure): Verifies that there is at least one active load balancer in the linked Azure account. ✓

Load balancer used (Heroku): This feature is built into Heroku. ✓

Azure virtual machine CPU monitored: Verifies that all Azure virtual machines have a "Percentage CPU" monitor configured. ✓

Virtual machine scale set CPU monitored (Azure): Verifies that all Azure Scale Set virtual machines have a "percentage cpu" monitor configured. ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

4 TESTS

Blob containers used to hold Activity Logs have access logs enabled (Azure): Verifies that the insights-activity-logs Azure blob container has access logging enabled. ✓

Subscription Activity Logs are being archived to a storage account (Azure): Verifies that all linked Azure subscriptions have activity logging enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

Log management utilized

✓ COMPLETE

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

5 TESTS

Blob containers used to hold Activity Logs have access logs enabled (Azure): Verifies that the insights-activity-logs Azure blob container has access logging enabled. ✓

Heroku logs archived for 365 days: Verifies that all Heroku apps are using a plugin that stores logs for 365 days, or are using a custom log drain. ✓

Subscription Activity Logs are being archived to a storage account (Azure): Verifies that all linked Azure subscriptions have activity logging enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Records of penetration testing: Verifies that a penetration test has been conducted within the last 12 months and that evidence of that test has been uploaded to Vanta. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

5 TESTS

Server configuration tool used: This feature is built into Heroku. ✓

Servers patched within 30 days: This feature is built into Heroku. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

Vulnerability and system monitoring procedures established

✓ COMPLETE

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

- vulnerability management;
- system monitoring.

1 TEST

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

CC 7.3

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

2 CONTROLS

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

4 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

CC 7.4

The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

5 CONTROLS

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

4 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Incident response plan tested

✓ COMPLETE

The company tests their incident response plan at least annually.

1 TEST

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

1 DOCUMENT

Incident report or root cause analysis ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

5 TESTS

Server configuration tool used: This feature is built into Heroku. ✓

Servers patched within 30 days: This feature is built into Heroku. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

CC 7.5

The entity identifies, develops, and implements activities to recover from identified security incidents.

4 CONTROLS

Continuity and disaster recovery plans tested

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

2 TESTS

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

4 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Incident response plan tested

✓ COMPLETE

The company tests their incident response plan at least annually.

1 TEST

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

1 DOCUMENT

Incident report or root cause analysis ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

CC 8.0

Change Management

CC 8.1

The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

7 CONTROLS

Change management procedures enforced

✓ COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

1 TEST

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Development lifecycle established

✓ COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Network and system hardening standards maintained

✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

7 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Infrastructure accounts removed when employees leave: Verifies that AWS and Heroku accounts linked to removed users are deactivated within the specified SLA. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Public SSH denied (Azure): Verifies that no Azure security groups allow unrestricted access to TCP port 22. ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Records of penetration testing: Verifies that a penetration test has been conducted within the last 12 months and that evidence of that test has been uploaded to Vanta. ✓

Production deployment access restricted

✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

3 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

5 TESTS

Server configuration tool used: This feature is built into Heroku. ✓

Servers patched within 30 days: This feature is built into Heroku. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Workstation security vulnerabilities monitored: Verifies that there is at least one Vanta Agent installed on a laptop if there is at least one installed on a server. ✓

CC 9.0

Risk Mitigation

CC 9.1

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

2 CONTROLS

Continuity and Disaster Recovery plans established

✓ COMPLETE

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.

2 TESTS

Company has an approved Business Continuity and Disaster Recovery Plan: Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

Employees agree to Business Continuity and Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

Risk management program established

✓ COMPLETE

The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Company has an approved Risk Management Policy: Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

Employees agree to Risk Management Policy: Verifies that all relevant employees have agreed to the Risk Management Policy. ✓

CC 9.2

The entity assesses and manages risks associated with vendors and business partners.

2 CONTROLS

Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

1 TEST

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

2 DOCUMENTS

Publicly available privacy policy ✓

Publicly available terms of service ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

4 TESTS

Company has an approved Third-Party Management Policy: Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

Employees agree to Third-Party Management Policy: Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

Compliance reports for critical vendors: Verifies that all vendors marked as "High Severity" within Vanta have associated security assessment documents. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

Appendix A: Definitions

Bug bounty program: A crowdsourcing initiative that rewards individuals for discovering and reporting software bugs, especially those that could cause security vulnerabilities or breaches.

DDoS: Distributed denial of service. A DDoS attack is attack in which multiple compromised computer systems flood a target—such as a server, website, or other network resource—with messages or requests to cause a denial of service for users of the targeted resource.

Multifactor authentication (MFA): A security system that requires multiple methods of authentication using different types of credentials to verify users' identities before they can access a service.

Penetration test: The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker might exploit.

Principle of least privilege: The principle of giving a user or account only the privileges that are required to perform a job or necessary function.

Protected data: Data that is protected from public view or use; includes personally identifiable information, sensitive data, HIPAA data, or financial data.

Sensitive data: Any information a reasonable person considers private or would choose not to share with the public.

SSH: Secure shell. A cryptographic network protocol for operating network services securely over an unsecured network.

SSL: Secure sockets layer. The standard security technology for establishing an encrypted link between a web server and a browser.

Appendix B: Document history

Vanta continuously monitors the company's security and IT infrastructure to ensure the company complies with industry-standard security standards. Vanta tests the company's security posture continuously, and this report is automatically updated to reflect the latest findings.

About Vanta

Vanta provides a set of security and compliance tools that scan, verify, and secure a company's IT systems and processes. Our cloud-based technology identifies security flaws and privacy gaps in a company's security posture, providing a comprehensive view across cloud infrastructure, endpoints, corporate procedures, enterprise risk, and employee accounts.

Vanta is based in San Francisco, California.