TaskUs Security & Compliance

October 2017

WHITE PAPER

Next Generation Customer Experience

CX Consulting | Digital Transformation | Outsourcing

TaskUs

Keeping Your Data Secure

TaskUs' culture embraces having a robust, nucleus-focus on security and privacy. Nothing less is acceptable in today's modern business world. Our team is proud to announce that we have again heightened our security procedures. TaskUs has attained SOC 2 Type II audit certification for three Manila Metro-based sites, plus our newest San Antonio, Texas site. We also now hold the prestige of PCI DSS Level 1 certification for a total of five sites. TaskUs first attained PCI compliance in 2015 from our external Qualified Security Assessor (QSA), Control Case. Additionally, in August 2016, we became one of the first companies to certify compliance with the EU-US Privacy Shield Framework. TaskUs is fully committed to security!

We believe that it is mission-critical for our teammates to be top-tier guardians of our partners' data, so we handle the confidentiality, integrity and availability of customer data with the same degree of stewardship that we would expect of our data. Our aim is to ensure that our partners are confident that its customer's data is safe and secure with us.

We strive to protect your data as it is our own, and our aim is to deliver confidence and assurance to all clients that their data is secure.

TaskUs genuinely understands – and appreciates – the critical importance of being able to trust that service levels are stable when a partner makes the strategic choice to outsource components of its business. A contact center often presents as "the face of the company" to users and, thus, must respect both the partner's business with seamless continuity and become an extension of it.

Fraud detection and regulatory compliance are crucial to any program's success, regardless of where the work takes place. More so, mitigating the significant risks of noncompliance, fraud and privacy breach is a critical responsibility and customer service obligation in industries such as technology, retail and financial services to list a few.

TaskUs has built a robust set of controls that are designed to address each of these risks. Controls include:

- Employee Training & Awareness
- Information Security Policies
- Vendor Management & Background Checks
- Physical Security
- Incident Response
- Network Security
- Data Protection
- Configuration Standards
- Access Control Measures
- Security Monitoring and Management
- Vulnerability Management
- Audit and Assessment

Our Approach: People, Process and Technology

Fostering and delivering a "security culture" is neither instinctive nor is it built overnight. Further, it not a forgotten one-off event once implemented. A security culture should be rooted in an organization's ethos. At TaskUs, it is. TaskUs CEO Bryce Maddock frequently states that "Security is the most important aspect of our operations and is everyone's responsibility." Logically, security does not exist within a silo – it is the organic end result of hiring the right people who are committed to serving our partners' best interests and protecting their data.

> "Security is the most important aspect of our operations and is everyone's responsibility."
>
> Bryce Maddock, CEO

People

We promote our security culture to each teammate from day one. This importance of this type of culture is communicated during the hiring and employee onboarding and continues throughout each employee's tenure to drive awareness and adoption. As such, a core TaskUs strength resides in our people.

Process

TaskUs is hyper-focused on process to ensure that all operational and security procedures are well-defined, documented and repeatable. We align our informational security program with enterprise goals and priorities to deliver genuine value for our partners. Additionally, we support the ability of our leaders to innovate when it helps to further control risk for our partners.

Technology

Information security is not simply a technical discipline at TaskUs. While we believe that IT teams provide useful tools for safeguarding information, we know that technology alone is not the solution. In support of our investment in leading security technologies, TaskUs believes in thorough solution implementation efforts, enforcement of effective technical controls and continual system management.

Employee Training and Awareness

Simply put, we train our employees early and often. Training is a core operational strength at TaskUs. Our teammates receive new and revised partner-specific training programs regularly to keep pace with our partners' evolving processes.

New teammates' formal security awareness training begins on the first day during New Employee Orientation (NEO). This training session teaches new hires all aspects of TaskUs, including their duties and responsibilities that pertain to security and keeping our customers' (and their users') data safe.

Information security training is provided through a learning management system (LMS) to ensure full coverage of all internal security policies and guidelines for respecting the confidentiality of all data handled. TaskUs provides a variety of content on security best practices which are posted to our popular employee intranet website. Security alerts and other advisories are distributed via email. Town hall sessions are also hosted by our information security team to further support awareness and to reinforce security as a core value.

All teammates undertake mandatory security fundamentals training on an annual basis. Specialized security training is also required of the IT and incident response teams to ensure technical security proficiency. We conduct regular phishing simulation exercises to assess teammates' vigilance, and follow-up training is provided to those who fail this simulation.

To better secure our teammates' email experience (and by extension to safeguard our partners' data), TaskUs has deployed DMARC email sender identity and authentication policies to mitigate spoofed email spam and phishing attacks.

Last, but not least, teammates are urged to report suspicious behavior and potential security events to the Information Security team at infosec@taskus.com.

Information Security Policies

TaskUs has implemented policies, standards and guidelines that define security controls across all assets, resources and data to protect their confidentiality, integrity, and availability to the organization. TaskUs aligns our policies with the ISO 27001 Information Security Management System standards as well as ITILv3 IT Service Management best practices. Our policies are reviewed periodically on an at-least annual basis for necessary updates. Policies are also communicated to all employees when starting employment and annually reintroduced during security awareness training.

> "TaskUs has deployed email sender identity and authentication practices to mitigate spoofed email spam and phishing attacks."

Vendor Management & Background Checks

TaskUs ensures that only well-vetted candidates are in a trusted position to handle partners' customer support programs and potentially sensitive data. We conduct comprehensive background checks for all new employees and contractors via trusted (and verified) third-party vendors. Our standard background checks include an identity check, education and work history verification, and criminal records verification.

TaskUs also takes special care to ensure that third party vendors who have access to TaskUs' sensitive data or networks are thoroughly vetted. Prospective vendors are required to complete a comprehensive security questionnaire, which is used by the TaskUs information security team to perform a vendor risk assessment prior to allowing access to any data or networks. We also actively contribute to, and maintain membership in, the Vendor Security Alliance – a coalition of companies committed to improving Internet security by standardizing security and compliance assessment of their peers.

Physical Security

The physical security of all TaskUs contact center sites is of critical importance to us, as our layered security model demonstrates. Blind-spot free CCTV video monitors are present at every entrance and throughout production floors. Security guards are positioned at every entrance and may also roam on production floors throughout shifts. Employee ID badges are required for initial building/suite entrance and are also required for production floor access.

In addition, facial image recognition or fingerprint scanners are present at all doors for production floor access, and only upon successful biometric read will the doors unlock for entrance to an authorized employee. Employees must also submit to biometric read upon exit to discourage tailgating and further enforce the biometric authorization checks.

Visitors must be signed in by an authorized employee, badged with a visitor ID, and must remain escorted at all times. Personal bags are checked at building and production floor entrances to record the movement of laptops and other IT equipment. Mobile devices are not permitted on the production floor, with noted exceptions for MDM locked-down devices required by our mobile app campaigns. Server rooms are also protected with biometric-restricted access control, fire suppression and smoke detection. Further, uninterruptible power supply and backup power generation is present in the event of power outage.

Network Security

TaskUs believes strongly in the benefit of a layered security model. We consider network security to be a foundational element of our security. We also understand it's criticality to our partners, and as such, we take the task of securing our perimeter very seriously.

Each of our locations have redundant Palo Alto Networks (PAN) next-generation firewalls that are deployed for enterprise-grade protection and high availability. All traffic from untrusted networks and hosts are denied by default.

> "We consider network security to be a foundational element of our security."

Deep VLAN segmentation is also applied to isolate each partner campaign from every other, with constant focus to keep trusted networks isolated from untrusted networks. Further, micro-segmentation is applied to prevent workstation host-to-host communications, thus thwarting potential attacker lateral movement and worm-like malware infections. PAN Threat Prevention blocks perimeter threats with intrusion detection and prevention (IDPS) controls, and URL web content filtering is enabled to protect users from malicious and non-work related websites (customized per partner campaign needs and preferences).

PAN Wildfire protection provides cloud-based malware analysis of all network traffic to dynamically detect and prevent unknown threats. PAN Data Filtering is deployed to block sensitive data (including personally identifiable information and payment card information) from unauthorized transfer outside of the network.

Lastly, careful change management and configuration reviews are implemented to ensure that TaskUs' network remains operational and secure at all times to the best of our ability.

Data Protection

The protection of partner data is of paramount concern to everyone at TaskUs. As such, we employ rigorous technical controls to ensure it remains protected at all times. Antivirus is deployed to all endpoints (servers, workstations and laptops) and is centrally managed with the management console server to ensure enterprise coverage and comprehensive compliance reporting. We use full-disk encryption to protect all workstations and laptops to negate the impact of system loss or theft. Sensitive data is also always encrypted when transmitted over any network, whether internal or external. We deploy host data loss prevention (DLP) on all workstations to identify sensitive content and apply blocking/alerting policies to protect against the risk of unauthorized transfer of data from within or outside of the network.

> "The protection of partner data is of paramount concern."

Google mobile device management (MDM) is enforced upon all mobile devices that have access to TaskUs Google Apps, requiring minimum passcode length, device encryption, device idle lock, incorrect passcode auto-wipe, and enabling remote wipe of data for lost or stolen devices. An alternative MDM solution is deployed to laptops to enable geolocation and to allow remote lock and wipe of data on lost or stolen devices.

Configuration Standards

TaskUs implements secure system build standards on all endpoints, servers and network devices to enforce a consistent security baseline across our organization. The includes the management of default configurations, encryption of administrative access, and robust systems hardening to reduce attack surface to only necessary, secure services. We manage all assets in line with ITILv3 standards by adhering to centralized change control and asset management systems.

Identity Management and Access Controls

At TaskUs, all user accounts are managed by centralized access controls. Users are assigned unique IDs to which roles are defined by job functions and rights are provisioned based upon the principle of least privilege. Password complexity, expiration and account lockout controls are enforced with centralized Active Directory Domain Services. Two-factor authentication (2FA) is enforced for all remote access to our network, and 2FA is required for the use of privileged administrator accounts to ensure secure access to corporate networks and critical system administration consoles beyond ordinary passwords alone.

We employ robust procedures for identity and access management to document a comprehensive account lifecycle. Single sign-on using the Bitium IdaaS (Identity as a Service) portal is employed to centralize identity management and cloud application access, as well as to enforce 2FA and ensure robust account provisioning. Further, we perform frequent reconciliation of accounts and periodic access reviews to ensure that user rights reflect current job duties.

> “Two-factor authentication is enforced...to ensure secure access to corporate networks and critical systems beyond ordinary passwords alone.”

Security Monitoring and Management

At TaskUs, security monitoring is focused on information that is gathered from internal network traffic, teammates' actions on our systems and external knowledge of vulnerabilities. Our Security Information & Event Management (SIEM) system maintains and centrally stores security and audit logs from all critical systems for analysis and reporting. We implement automated audit trails to reconstruct information such as: data access, actions taken with root or administrative privileges, access to audit logs, invalid logical access attempts, use of identification and authentication mechanisms, and modification of system-level objects. System file integrity monitoring (FIM) is implemented on all critical servers in the production environment to monitor for unexpected changes, which is also tracked by the SIEM. Further, we understand the imperatives of cloud security governance and look to cutting edge technologies to address the risks of operating in the cloud. We employ Skyhigh cloud access security broker (CASB) to provide full visibility, risk assessment and control of cloud applications usage.

Vulnerability Management

TaskUs conducts internal and external vulnerability assessments for all systems on a bi-monthly basis. The Information Security team is responsible for tracking and following up on vulnerabilities which require remediation as per documented risk methodology. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. We track and require regular follow-up on these vulnerabilities until we can verify that all issues have been remediated. Lastly, operating system and application patches are risk assessed and deployed to all endpoints and network gear by a centralized patch management system on a monthly basis, or as necessary in the event of critical security patches.

> "...We understand the imperatives of cloud security governance..."

Incident Response

TaskUs has a rigorous incident management process for security events that may affect the confidentiality, integrity and/or availability of systems or data. If an event occurs, the security team logs and prioritizes it according to its severity for incident classification. Incidents that directly impact partners are assigned the highest priority. Our incident response and breach notification process is detailed at length within the TaskUs Incident Response Plan, and includes seven primary stages of response: preparation, identification, containment, eradication, recovery/closure, breach notification, and after-incident-review follow-up. In the unlikely event that a security incident results in the breach of partner data - or upon the discovery of any data breach - TaskUs will promptly notify affected customers to identify any customer data that may have been impacted by the breach. Incident response plan testing is conducted periodically and considers a variety of scenarios in order to ensure swift and appropriate resolution of any and all security incidents.

TaskUs Incident Response Process

Audit and Assessment

TaskUs' systems are routinely tested for compliance with configuration standards, and annual audits are performed by a Qualified Security Assessor (QSA) to validate Payment Card Industry Data Security Standards (PCI DSS) compliance. This QSA review includes both internal and external network penetration testing which is conducted several times throughout the year. TaskUs also annually engages an independent auditor to perform an audit based upon the American Institute of Certified Public Accountants (AICPA) Trust Services Principles, and then issue a SOC 2 Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy. Health Insurance Portability and Accountability Act (HIPAA) compliance is another domain that TaskUs has expertise, as we have attained 3rd party attestation of HIPAA compliance for campaign-specific requirements, thus allowing us to sign a business associate agreement.

TaskUs utilizes the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as a risk-based methodology for information security program management and measurement. Additionally, it creates a common language for internal and external communication of cybersecurity issues. The NIST CSF process

model of identify, protect, detect, respond, and recover is central to the TaskUs information security program, so semi-annual assessments are performed to gauge maturity growth and to support continued investments in security. Additionally, we work with leading security consulting firms for the assessment of security posture and infrastructure controls so that we may continuously improve our protection levels.

At TaskUs, fraud and operational risks are also a critical component of our comprehensive security strategy. Our Fraud Prevention & Audit team is focused on reducing fraud risks within all active operations. The cornerstone of that effort is proactively identifying risks during new campaign implementations to ensure well-controlled systems and processes are in place from day one. In the unlikely event that there should be any incident requiring examination, our seasoned team of fraud analysts and attorneys bring years of such experience to the table to ensure a prompt and exhaustive investigation.