TRANSACT

Security & Trust Center

Table of Contents

Transact recognizes the importance of maintaining the confidentiality, integrity, and availability of our customers' information and the protection of its valuable business assets and applications. Transact's Security & Trust Center reflects our commitment to providing a secure environment and adopting effective security standards that exceed industry best practices in the areas of information security and compliance.

With the use of a variety of reliable security technologies as well as a unique combination of trained personnel, mature business processes, and regular third-party audits measured against several international and U.S. standards, Transact delivers a high level of security and confidence that is unmatched in the industry.

Transact's Security & Trust Center describes each layer of this assurance approach to provide an overview of the compliance, data protection, and cybersecurity that Transact provides.

Transact's Information Security Program

Transact protects the confidentiality, integrity, and availability of customer data and systems, regardless of how the data is created, distributed or stored. Transact's security controls are tailored accordingly so that effective controls are applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal and contractual obligations.

Management Direction for Transact's Information Security Program

The objective of Transact's Information Security Program is to provide direction for information security and privacy requirements that are in accordance with Transact's business requirements, as well as relevant laws and other legal obligations for data security and privacy.

Transact is committed to protecting its employees, partners and clients from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every team member and vendor that interacts with Transact data and/or systems. Therefore, it is the responsibility of Transact to be aware of and adhere to the information security and privacy requirements.

Protecting Transact and customer data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems, applications and services include controls and safeguards to offset possible threats. Commensurate with risk, information security and privacy measures are implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction.

The security of systems, applications and services include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety.

Security & Trust Center Scope

The requirements of the Information Security Program in conjunction with the scope of Transact's Security & Trust Center apply to all team members and vendors that support Transact operations. This includes all stakeholders involved in transmitting, processing and storing Transact and customer data.

Intent

Transact's information security requirements are comprehensive. Therefore, Transact maintains a comprehensive set of information security and privacy policies, standards, procedures and controls to protect Transact's data, as well as its systems, applications and services.

Transact's information security program is reasonably designed to achieve the following objectives:

- Ensure the Confidentiality, Integrity, Availability and Safety of Transact systems, applications, services and data;
- Perform ongoing risk management practices to maintain situational awareness of risk; and
- Reasonably protect against any anticipated threats or hazards.

Information Security Practices Alignment

Transact's information security program is represented by industry best practices for information security. Therefore, Transact's information security requirements internally and for our vendors aligns with Transact's controls to ensure due care and due diligence in maintaining our information security program.

Information Security Documentation

In order to limit confusion, Transact follows a standard framework for information security documentation:

1. Core organizational policies that establish management's intent;
2. Control objectives that identify desired outcomes and leading practices;
3. Standards that provides quantifiable, measurable or qualified requirements;
4. Controls identify desired conditions that are expected to be met;
5. Procedures and Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
6. Guidelines and enhancements which are recommended, but not mandatory.

Transact's Information Security Responsibilities

Transact maintains controls that support an industry recognized framework to ensure Transact's due care and due diligence in maintaining its information security program.

Transact's information security framework is detailed into five (5) categories of controls that include:

- Identify
- Protect
- Detect
- Respond
- Recover

Identify

Transact considers these controls as foundational for effective information security and privacy. Understanding the business context, resources that support critical functions and the related information security risks Transact focuses its efforts and resources to properly secure the network and cloud resources.

Transact focuses on the following categories:

- Business context;
- Resources that support critical functions; and
- Related information security risks.

Asset & Resource Management

The Asset Management section of the information security program addresses the data, personnel, devices, systems and facilities that enable an organization to achieve business goals and objectives that are identified and managed consistent with their relative importance to Transact's objectives and risk strategy.

Hardware Management
Transact maintains accurate inventories of its information systems and components.

Software Management
Transact maintains accurate inventories of its approved operating systems and applications.

Data Flow Management
Transact documents its data flows by maintaining network diagrams and Data Flow Diagrams (DFDs).

External Information Systems
Transact identifies and documents information systems and services hosted or maintained by 3rd parties.

Resource Value Categorization
Transact assigns assets and resources a classification based on the business value and criticality in accordance with Transact's policies and standards.

Information Security Roles & Responsibilities
Transact establishes and documents information security specific roles and responsibilities for the workforce, including third-party stakeholders.

Business Environment

The Business Environment section of Transact's information security program addresses Transact's mission, objectives, stakeholders and activities. This information is used to inform information security roles (people and teams), responsibilities and prioritize risk management decisions.

Mission & Objectives
Transact establishes and communicates its mission and objectives to ensure organizational awareness of its critical business functions and how that impacts clients.

Dependencies Analysis
Transact identifies and documents dependencies and critical functions within its business processes that impact the delivery of critical services.

Resiliency Analysis
Transact identifies and documents resilience requirements to support the delivery of services to customers.

Governance

The Governance section of Transact's information security program addresses the policies, standards, procedures and processes to manage and monitor Transact's statutory, regulatory and contractual requirements. These external and internal influencers are understood to properly manage information security risk.

Information Security Policy & Standards
Transact documents formal information security policies, standards and procedures. This information security-related documentation is clearly made available to Transact's workforce via Atlassian Confluence and Microsoft SharePoint.

Information Security Functions
Transact coordinates and aligns designated information security roles with internal and external stakeholders to ensure all applicable information security and privacy responsibilities are properly addressed.

Statutory, Regulatory & Contractual Obligations
Transact adheres to all applicable information security and privacy-related statutory, regulatory and contractual obligations.

Information Security & Privacy Program
Transact maintains a documented program to govern information security and privacy risks.

Risk Assessment

The Risk Assessment section of Transact's information security program addresses the organization's understanding of information security risk to organizational operations, organizational assets, individuals and teams.

Vulnerability Identification
Transact identifies, documents and remediates vulnerabilities as part of a formal Vulnerability and Patch Management Program.

Threat & Vulnerability Intelligence
Transact receives threat and vulnerability information from information sharing forums and sources via RSS and vendor feeds.

Threat Assessments
Transact maintains a process to identify and assess both internal and external threats.

Business Impact Assessment
Transact performs Business Impact Assessments to assess the likelihood and potential impact associated with inherent and residual risk, considering all available risk sources.

Risk Determination

Transact assesses threats, vulnerabilities, likelihoods, impacts and compensating controls to determine overall risk.

Risk Responses
Transact identifies and prioritizes risk responses via the Transact Compliance Committee.

Risk Management

The Risk Management Strategy section of Transact's information security program addresses the organization's priorities, constraints, risk tolerances and assumptions that are established and used to support operational risk decisions.

Risk Management Framework

Transact maintains an enterprise-wide Risk Management Program to manage risk to an acceptable level.

Risk Tolerance Level

Transact's determines and documents the organization's risk tolerance level.

Risk Thresholds

Transact determines and documents thresholds for incident alerts.

Supply Chain Risk Management

The Supply Chain Risk Management section of Transact's information security program addresses the organization's priorities, constraints, risk tolerances and assumptions that are used to support risk decisions associated with managing supply chain risk.

Supply Chain Risk Management

Transact's supply chain risk management processes are identified, established, assessed, managed, and agreed to by Transact's stakeholders.

Supply Chain Risk Assessments

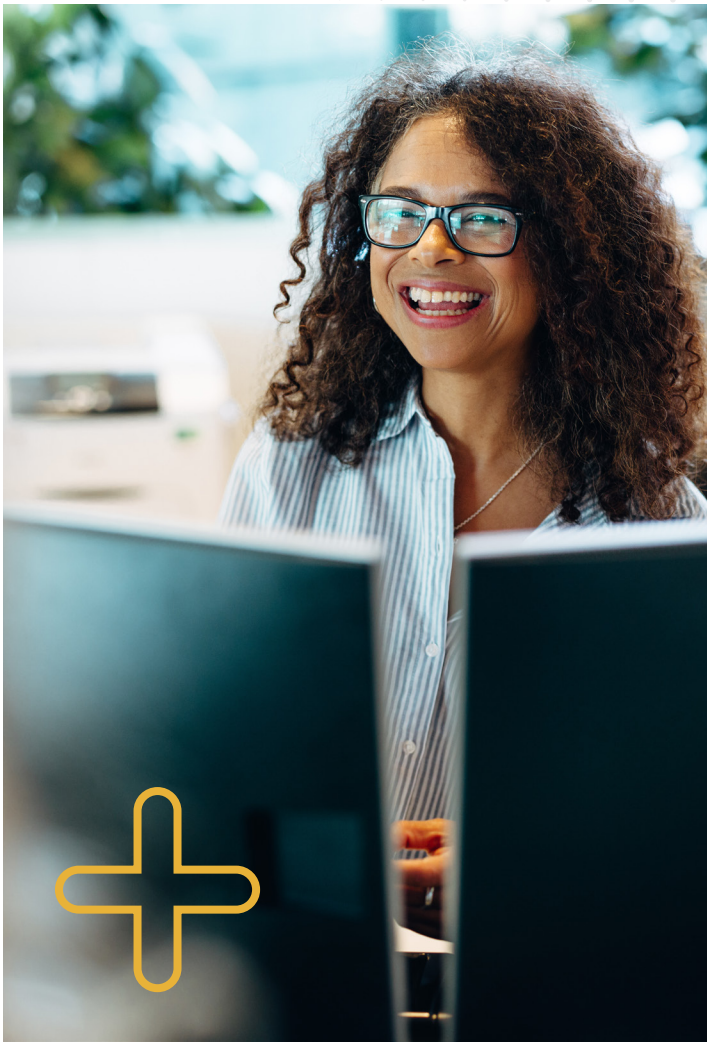
Transact's suppliers and third-party service providers of information systems and services are identified, prioritized, and assessed using a risk assessment process that takes both information security and privacy into consideration.

Third-Party Contracts

Transact's contracts with its suppliers and third-party service providers are used to implement appropriate measures designed to meet the objectives of Transact's information security and privacy program.

Third-Party Assessments

Transact's suppliers and third-party service providers are routinely assessed using audits, test results, or other forms of evaluations to confirm those parties are meeting their contractual obligations.



Protect

Transact's information security controls focus on implementing the appropriate safeguards to ensure the safe functionality of systems, applications and services. These activities are performed consistent with Transact's risk strategy and support the ability to limit or contain the impact of a potential information security event.

Controls in this category focus on helping Transact understand the following:

- How user accounts are being managed;
- Established maintenance plans to keep the system patched and secure;
- Change control processes;
- End user security training & awareness; and
- Baseline configuration hardening that is in place.

Access Control

The Identity Management, Authentication and Access Control section of Transact's information security program addresses the access to physical and logical assets and associated facilities that are expected to limited access to authorized users, processes and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Logical Access Control

Transact manages logical access controls (User IDs and credentials) to ensure access is limited to authorized users and devices.

Physical Access Control

Transact implements mechanisms to limit physical access to assets and resources to authorized users.

Remote Access Control

Transact implements mechanisms to limit remote network access to authorized users and devices.

Least Privilege

Transact manages logical and physical access permissions that incorporate the principles of least privilege and separation of duties.

Network Segmentation

Transact implements network segregation and segmentation for both security and compliance.

Non-Repudiation

Transact verifies the identities of its users and implements technologies to ensure non-repudiation of user activities by binding all user accounts to specific individuals, including privileged users.

User Authentication

Transact implements technologies to authenticate its users, devices, and other assets commensurate with the risk of the transaction. Transact uses Multi-Factor Authentication for privileged accounts and customer environments as needed to address statutory, regulatory or contractual obligations for enhanced user authentication.

Awareness & Training

The Security Awareness and Training section of Transact's information security program addresses the organization's information security awareness education to ensure users are properly trained to perform their information security-related duties and responsibilities consistent with related policies, standards, procedures and agreements.

Awareness & Training

Transact maintains an information security awareness and training program to provide information security training and awareness for all users.

Privileged User Training

Transact provides its privileged users adequate training prepared them for their specific information security roles & responsibilities.

Management Training
Transact implements processes to ensure its management and executives are trained and adequately prepared for their specific information security roles & responsibilities.

Security Personnel Training
Transact implements processes to ensure its security personnel are trained and adequately prepared for their specific physical and information security roles & responsibilities.

Data Security

The Data Security section of Transact's information security program addresses the management of information and records (data) consistent with Transact's risk strategy to protect the confidentiality, integrity, availability and safety of information systems and data.

Protecting Data At Rest
Transact protects sensitive data at rest with appropriate encryption and physical security protections.

Protecting Data In Transit
Transact protects sensitive data being transmitted with appropriate encryption.

Removal of Assets & Data
Transact implements processes to manage the removal, transfer and disposal of assets and resources.

Availability Protections
Transact implements processes to ensure adequate availability capacity is maintained.

Data Leakage
Transact implements processes to protect against data leakage and data loss.

Software Integrity
Transact uses integrity checking mechanisms to verify software and information integrity.

Separate Environments
Transact separates production and non-production environments.

Information Protection Processes & Procedures

The Information Protection Processes and Procedures section of Transact's information security program addresses the information security policies standards, processes and procedures used to manage the protection of information systems and data.

Baseline Configuration Requirements
Transact maintains baseline configurations for its technology assets that are based on industry-recognized secure practices and implements these baselines uniformly to ensure least functionality is enforced.

System Development Life Cycle (SDLC)
Transact operates a System Development Life Cycle (SDLC) process to ensure information security and privacy principles are identified and implemented by design.

Configuration Change Control
Transact operates a configuration change control process that considers information security and privacy implications for proposed changes.

Data Backup
Transact conducts, maintains and tests data backups and redundancy in accordance with its business obligations.

Workplace Security
Transact ensures technical and physical controls are effective regardless of an end user's workplace.

Secure Disposal of Information
Transact ensures physical and digital assets are destroyed in a manner that prevents the disclosure information to unauthorized entities.

Protection Effectiveness Review
Transact implements processes to review and continuously-improve its protection processes.

Incident Response & Business Continuity Plans
Transact maintains documented Incident Response Plans and Business Continuity Plans in tandem with tactical playbooks.

Response & Recovery Plan Testing
Transact tests its recovery plans on at least an annual basis and in some cases monthly to ensure the validity of the plans and applied lessons learned from the test to improve the plans.

Human Resources Security
Transact's People Operations processes incorporate information security considerations for hiring and employment termination activities for employees and contractors.

Vulnerability Management Plan
Transact maintains a formal Vulnerability Management Program to proactively identify and remediate technical vulnerabilities in its systems, applications and services.

Maintenance

The Maintenance section of Transact's information security program addresses the maintenance and repair of systems and components that are performed consistent recommended practices.

Maintenance Support
Transact performs timely maintenance of its systems, applications and services using secure practices.

Remote Maintenance
In some cases, Transact performs remote maintenance of its assets and resources in an approved manner that prevents unauthorized access.

Protective Technology
The Protective Technology section of Transact's information security program addresses the management of technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.

Audit & Log Records
Transact ensures log files are created, protected and retained in accordance with Transact's policies and standards.

Removable Media
Transact restricts the use of removable media and enforces encryption through administrative and technical measures.

Least Functionality Protections
Transact uses secure baseline configurations to enforce the principles of least functionality.

Network Communications Protections
Transact implements appropriate technical solutions to protect the confidentiality and integrity network communications.

Availability Protections
Transact configures its systems to operate in pre-defined functional states to achieve availability in a fail-safe mode.

Detect

These controls focus on situational awareness to ensure the timely identification and response to potential information security or privacy incidents. By decreasing response time, Transact increases its ability to limit or contain incidents with the least amount of negative consequences.

Controls in this category focus on helping Transact understand the following:

- How incidents are detected;
- What constitutes or defines anomalous behavior; and
- How the systems are being logged & monitored.

Anomalies & Events

The Anomalies and Events section of Transact's information security program addresses the detection of anomalous activity and the understanding of potential event impacts.

Network Traffic Baselines
Transact establishes baselines of network traffic and expected data flows to identify what activities that would be considered anomalous behavior.

Event Log Reviews
Transact analyzes detected events to understand the target(s) of attack and the methods used.

Event Correlation
Transact correlates events logs to improve detection and escalation by bringing together information from different sources to better understand what occurred.

Event Impact Assessment
Transact assesses events to determine appropriate response & recovery activities based on the potential impact.

Incident Alerting Thresholds
Transact establishes thresholds to manage incident alerting and escalation.

Continuous Monitoring

The Security Continuous Monitoring section of Transact's information security program addresses the monitoring of information systems to identify information security events and verify the effectiveness of protective measures.

Network Monitoring
Transact monitors network traffic to detect potential information security events.

Physical Monitoring
Transact monitors the physical environment to detect potential information security events.

Personnel Monitoring
Transact monitors individual user activities to detect potential information security events.

Malicious Code Detection Mechanisms
Transact deploys malicious code detection mechanisms to detect and remove malicious code.

Service Provider Monitoring
Transact monitors its third-party service providers to ensure their compliance with Transact's policies, standards, procedures and contractual obligations during the procurement phase and annually thereafter.

Periodic Checks
Transact performs periodic checks for unauthorized personnel, network connections, devices and software.

Production Vulnerability Scanning
Transact performs internal and external vulnerability assessment scans on a recurring basis.

Detection Processes

The Detection Processes section of Transact's information security program addresses the maintenance and testing of detection processes and procedures to ensure awareness of anomalous events.

Roles & Responsibilities for Event Detection & Response
Transact assigns roles and responsibilities for the detection and response to information security and privacy-related incidents.

Detection Procedures
Transact takes appropriate response actions in accordance with its Incident Response Plan.

Response Exercises
Transact tests its detection processes to ensure that the process is valid and applicable personnel understand their assigned roles and responsibilities.

Information security Event Coordination
Transact communicates event detection information among appropriate stakeholders.

Detection Process Improvement
Transact implements processes to continuously-improve its detection processes.

Respond

These controls focus on the processes used to act when an information security or privacy event is detected. These controls support Transact's ability to contain the impact of a potential incident.

Controls in this category focus on helping Transact understand the following:

- What response plans are in place;
- Roles and responsibilities for incident response;
- What the options are for mitigating risks from an information security incident.

Response Planning

The Response Planning section of Transact's information security program addresses the response processes and procedures that are executed and maintained to ensure response to detected information security incidents.

Response Plan Execution
Transact uses its documented Incident Response Plan when responding to information security and privacy-related incidents.

Communications
The Communications section of Transact's information security program addresses response activities that are coordinated with internal and external stakeholders (including external support from law enforcement agencies as needed).

Responder Roles & Responsibilities
Transact assigns roles and responsibilities for incident responders to ensure a successful response to information security and privacy-related incidents.

Incident Reporting
Transact reports information security and privacy-related incidents consistent with established reporting criteria as mandated by statutory, regulatory and contractual obligations.

Incident Information Sharing
Transact shares pertinent incident information with affected stakeholders.

Stakeholder Coordination
Transact coordinates incident response activities with stakeholders that are consistent with documented plans.

Situational Awareness
Transact voluntarily shares information security and privacy-related incident information with external stakeholders to achieve broader situational awareness.

Analysis

The Analysis section of Transact's information security program addresses the analysis that is conducted to ensure effective response and support recovery activities.

Alert Analysis
Transact investigates notifications from detection systems in a timely manner.

Impact Understanding
Transact evaluates the potential damage and scope of the incident to understand the potential impact of an incident.

Forensics
Transact utilizes proper forensic procedures for information security and privacy-related incidents that have the potential for legal action or data breach reporting. This is provided by either an approved Transact forensic partner or an insurance company provided entity.

Incident Classification
Transact classifies and documents incidents consistent with established response plans.

Incident Classification
Transact maintains processes to receive, analyze and respond to vulnerabilities disclosed from internal and external sources (internal testing, RSS, or security researchers).

Mitigation

The Mitigation section of Transact's information security program addresses the activities to prevent the expansion of an event, mitigate its effects and resolve the incident.

Contain Incidents
Transact implements mechanisms to contain the scope of information security incidents.

Mitigate Incidents
Transact implements mechanisms to mitigate the ramifications of information security incidents.

New Vulnerability Response
Transact identifies, documents and mitigates (new) identified vulnerabilities in a timely manner.

Improvements

The Improvements section of Transact's information security program addresses organizational response activities that are improved by incorporating lessons learned from current and previous detection/ response activities.

Incident Response Lessons Learned
Transact updates its Incident Response Plan based on lessons learned following incidents or tabletop exercises.

Incident Response Strategy Update
Transact's management and cross-functional teams update its incident response strategy.

Recover

These controls focus on restoring capabilities or services that were impaired during an incident. These controls support Transact's ability to recover to "normal" operations as rapidly as possible and with as minimal disruption as possible.

Controls in this category focus on helping Transact understand the following:

- Plans that are in place to recover systems and data; and
- How recovery will be communicated to impacted or potentially impacted parties.

Recovery Planning

The Recovery Planning section of Transact's information security program addresses the recovery processes and procedures that are executed and maintained to ensure restoration of systems or assets affected by information security incidents.

Recovery Plan

Transact uses its documented recovery plan when responding to information security and privacy-related incidents when recovery is necessary.

Improvements

The Improvements section of Transact's information security program addresses the recovery planning and processes that are improved by incorporating lessons learned into future activities.

Recovery Lessons Learned

Transact documents lessons learned from recovery operations and incorporates that knowledge into future recovery plans.

Recovery Strategy Update

Transact uses lessons learned from recovery operations to update its response strategies.

Communications

The Communications section of Transact's information security program addresses the restoration activities that are coordinated with internal and external parties.

Public Affairs

Transact implements mechanisms to manage public affairs activities associated with recovery operations.

Recovery Activities

Transact communicates recovery activities to applicable stakeholders.

Compliance

To assure that our customers' data confidentiality, integrity, and availability are maintained, Transact conducts multiple internal audits and third-party audits on a scheduled basis. The written results of many of these audits are available on request.

The following table shows the types of audits and scans, plus the frequency in which they are conducted:

Audit	Type	Frequency
SOC2 2 Type II	External	Annual
PCI DSS	External	Annual
Secure SDLC	Internal	Continuous
Risk Assessment	Internal	At Least Annual
NIST and ISO 27001 Control Review	Internal	Continuous
ISO 27001 Statement of Applicability	Internal	Annual
Vulnerability Scanning	Internal	Quarterly
Vulnerability Assessment	External	Quarterly
Penetration Testing	External and Internal	Annual

Privacy Policies & Practices

Transact privacy policies and practices may be found at:

https://transactcampus.com/privacy-policy

https://transactcampus.com/cookie-policy

Application Security

Secure Software Development Lifecycle

Transact has implemented a secure software development lifecycle (secure SDL), requiring our product teams to include security training, tools, and processes that are in alignment with the Open Web Application Security Project (OWASP) and NIST. These guidelines include secure coding implementation in application architecture, authentication, session management, access controls and authorization, event logging, and data validation.

Required processes for Transact's product teams include threat modeling, inline and continuous security scanning and monitoring, and security reviews that enable product teams to deliver security by design.

Transact applications and services are designed to ensure that only authorized users can perform allowed actions within their privilege level, to control access to protected resources using decisions based on role or privilege level, and to prevent privilege escalation attacks.

Network Security

Transact's network architecture ensures that sensitive data is protected through best business practice security policies and procedures.

Hardened router configurations. Router configurations correctly route packets to their proper destinations and restrict traffic. Access Control Lists (ACLs) on the front-end routers stop common attacks. ACLs include implicit default deny clauses.

Network segmentation. Transact's segmented network architecture prevents direct public contact or connection to Transact's private network segment.

Distributed denial-of-service (DDoS) protection. A service protects the availability of Transact services, even when they are under a distributed denial-of-service (DDoS) attack.

Activity log aggregation. Log activities from network devices and systems are aggregated through an activity log collection system. Logs are fed to a SIEM, where alarms are generated for those events that warrant immediate attention.

Proactive monitoring. Security and Risk Management continuously monitor industry communities for news of security alerts, as well as vendor and partner security changes.

Active vulnerability assessment. Security scans of Transact applications and infrastructure are performed on a routine basis by approved third-party assessment vendors, Transact Security Engineers, and internal scanning solutions. These scans check for vulnerabilities in both our external (public facing) web applications and our internal (private) networks. Discovered vulnerabilities are managed through Transact's vulnerability and patch management program and the risk is treated per Transact's risk management program.

VPN. Transact personnel use a best-in-class VPN when connecting and processing from outside the trusted network. The VPN secure tunnel offers personnel highly secure remote connectivity to perform after-hours maintenance or trouble- shooting. Multifactor authentication is required for all Transact personnel with direct access to production systems.

Digital certificates and TLS. Digital certificates are used to encrypt all internet web traffic between clients and servers.

Host Based Security

Information Services employs a hardened, approved, and standardized build for every type of server used within the production infrastructure. This procedure disables unnecessary default user IDs, closes unnecessary or potentially dangerous services and ports, and removes processes that are not required.

Servers are built, scanned for vulnerabilities, and remediated before being put into production.

All patches are tested using a standard process to ensure proper functioning within the operating environment before they are applied to the servers.

The same process is used for Transact's cloud service providers – we control the server builds.

Transact uses dedicated engineers to continually update, optimize, and secure the standard build procedures, while adhering to industry best practices and regulatory requirements.

Centralized logging. Events from all systems are collected and aggregated, and alerts are sent, via a centralized log collection engine (SIEM) that is monitored by the Transact's security teams.

Standard change control process. All changes to any part of Transact's infrastructure must pass a strict Change Control Process to ensure best practices and minimal service interruption for our clients.

Security information and event management. Transact receives real-time alerts for a variety of activities that may indicate malicious activity.

Vulnerability Management

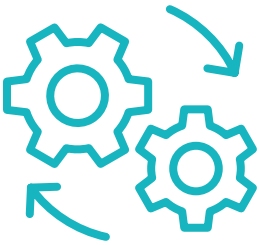
Transact regularly tests application code and scans the network and systems for security vulnerabilities. Third-party assessments are also conducted regularly (see table of audits and scans above), including:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Continuous integrated application security testing of each release
- Security control framework review and testing

Transact Personnel

Background checks are performed on all candidates before hiring, including screening of education, past employment, criminal record, and other checks consistent requirements and local laws.

Transact personnel are provided training regularly on security policies and procedures, including company policies and procedures, corporate ethics and business standards, and secure development training based on OWASP.



Disaster Recovery

Disaster Recovery, Business Continuity and Incident Response

Transact maintains a comprehensive continuity of operations strategy complete with tactical playbooks for Disaster Recovery, Business Continuity and Incident Response.

Transact uses a high-availability architecture to ensure that, in the event of a failure, service performance continues to meet client expectations.

Transact also maintains SOC 2 Type II, which requires the production, maintenance, and testing of a Disaster Recovery Plan (DRP). The current DRP is a formal recovery procedure for recovering the entire application suite in a different region. The DRP is tabletop tested annually and Transact also performs disaster simulations to test failover to secondary systems.

TRANSACT

Transact is the leading innovator in customizable, mobile-centric payment, commerce, and credentialing solutions for streamlining administration and creating one connected campus experience. Transact delivers integrated solutions for tuition, room and board, and retail transactions along with mobile-centric campus IDs, access credentials, and stored value applications. With a long-standing reputation in the education community, Transact proudly serves over 12 million students across more than 1,800 client institutions. Its fintech solutions facilitate $49 billion in payments annually and have enabled more than 178 million contactless mobile wallet transactions and $293 million in mobile orders since inception.

TransactCampus.com

Last Updated: 5/18/2023