Security Overview

Tallyfy

Strike Graph

Prepared on Nov 08 2022

Company Overview

Tallyfy is a workflow automation platform. We believe in workflow made easy for our customers and partners.

Tallyfy, Inc was founded as a company in 2014 and has been growing and active ever since. It's located in St. Louis, Missouri.

We serve a diverse range of business sizes, teams and sectors - all which which utilize some or all of the 3 core features of our product:

Building blueprints of document templates, policies, procedures, playbooks, business processes, approvals and more. We also have a feature to enable an organization to share a blueprint in public to anyone with the link.

Launching processes using blueprints. This feature enables you to take a blueprint definition and launch a running process (instance) - to track a specific workflow being executed amongst a group of people. It eliminates the need for manual status updates (because you can track any workflow in real-time) and also reduces/eliminates meetings and emails about the status of workflows, handovers or approvals. A blueprint-driven approach ensures work is systemized and standardized, and outcomes are always consistent.

Tasks, auto-reminders and updates. The core feature in Tallyfy is a task, which includes the ability to share comments with internal and external people - and the ability to auto-remind any assignees of a task due.

Risk Posture & Security Controls

To mitigate cyber security and information security risks, Tallyfy has established the following security posture which is composed of security controls unique to Tallyfy's environment. This posture is aligned to common risk categories for ease of use.

Access

The following controls mitigate risks related to logical access, including concepts like authentication and the appropriateness of access to information and data.

Mitigated and monitored by 16 control(s)

Firewall Rules

Firewall rulesets are configured and in place to help prevent unauthorized access threats from outside the application and infrastructure environment.

Covered Security Criteria: SOC2.CC.6.6.1,

Logical Access

Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually.

Covered Security Criteria: SOC2.CC.5.2.3, SOC2.CC.5.3.1, SOC2.CC.6.1.2, SOC2.CC.6.1.3, SOC2.CC.6.1.5, SOC2.CC.6.3.1,

User Access Review

Management performs at least an annual review of user access to systems based on job duties. Inactive users are removed and removal is documented. The review is formally documented including system generated user listings and sign off by management.

Covered Security Criteria: SOC2.CC.5.2.3, SOC2.CC.6.2.1, SOC2.CC.6.2.2, SOC2.CC.6.2.3,

User Authentication

Unique usernames and passwords are required to authenticate all users. Exceptions are approved by the CEO.

Covered Security Criteria: SOC2.CC.6.1.3, SOC2.CC.6.1.7,

Termination of Access

A user's physical and logical access to IT systems is revoked within 48 hours when employment or contract terminates. Exceptions are documented in the checklist and/or offboarding ticket.

Covered Security Criteria: SOC2.CC.6.2.2, SOC2.CC.6.3.2, SOC2.CC.9.2.8,

Role Based Access

Role based security is utilized to grant user access and to segregate access to sensitive data in production and supporting tools.

Covered Security Criteria: SOC2.CC.6.1.2,

Provisioning

Logical user access requests are documented and require approval prior to access being provisioned for cloud and server systems.

Covered Security Criteria: SOC2.CC.6.1.2,

Password Requirements

Authentication for the network, databases and applications adheres to the company password setting requirements.

Covered Security Criteria: SOC2.CC.6.2.1,

Encryption in Transit

Any sensitive data that's transmitted over public networks, and data in transit is encrypted. HSTS compliance is maintained.

Covered Security Criteria: SOC2.CC.6.1.9, SOC2.CC.6.7.2, SOC2.PI.2.4.1,

Virtual Private Network Encryption

Remote access virtual private network sessions are encrypted.

Covered Security Criteria: SOC2.CC.6.6.3, SOC2.CC.6.7.2,

Encrypted Server Access

Production system access is encrypted to ensure communications with servers are secured.

Covered Security Criteria: SOC2.CC.6.6.1,

Encryption at Rest

All data at rest in the cloud is encrypted using industry standard algorithms.

Covered Security Criteria: SOC2.CC.6.1.9, SOC2.PI.2.5.1,

Separation of Duties: Developers

Access to the source code repository is restricted to authorized employees.

Covered Security Criteria: SOC2.CC.5.1.6, SOC2.CC.6.3.3,

Review Privileged Access

Administrative and privileged access, as defined by policy, is reviewed at least quarterly.

Covered Security Criteria: SOC2.CC.6.2.3, SOC2.CC.6.3.2,

Separation of Duties: IT Operations

Developers do not have access to IT infrastructure tools or the production environment. Exceptions are documented and approved by the CEO.

Covered Security Criteria: SOC2.CC.5.1.6, SOC2.CC.6.3.3,

Administrator Access

Administrator access to the application, database, network, VPN, and operating system is restricted to authorized users.

Covered Security Criteria: SOC2.CC.6.2.1, SOC2.CC.6.3.1,

Fraud

The following controls mitigate risks related to fraud, specifically as it relates to the legal concept of inappropriate action that leads to financial or personal gain.

Legal

The following controls mitigate risks related to the application (or lack of application) of laws, regulations, and contractual requirements applicable to Tallyfy.

Mitigated and monitored by 8 control(s)

Contracts

The organization utilizes a standard contractual agreement that defines relevant security (and privacy) commitments and requirements for both its customers as well as third party providers; scope, responsibilities, compliance requirements, and service levels are included in the contract. The agreement template is periodically reviewed to align with business requirements.

> **Covered Security Criteria:** SOC2.CC.2.2.10, SOC2.CC.2.3.10, SOC2.CC.2.3.6, SOC2.CC.2.3.8, SOC2.CC.2.3.9, SOC2.CC.9.2.1, SOC2.CC.9.2.11, SOC2.CC.9.2.3, SOC2.CC.9.2.4, SOC2.CC.9.2.7, SOC2.CC.9.2.8, SOC2.CC.9.2.9, SOC2.P.6.1.3, SOC2.P.6.4.1,

Non Disclosure Agreement

Employees and contractors are required to sign a confidentiality policy upon hire. A non disclosure agreement is required for third parties that may have access to personal information. The non disclosure agreement includes the signee's and the company's responsibility with respect to information security. The template is periodically reviewed to align with business requirements.

> **Covered Security Criteria:** SOC2.CC.9.2.9,

Third Party SOC2

Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.

> **Covered Security Criteria:** SOC2.CC.3.1.9, SOC2.CC.3.2.1, SOC2.CC.3.4.5, SOC2.CC.9.2.10, SOC2.CC.9.2.12, SOC2.CC.9.2.2, SOC2.CC.9.2.6,

Vendor Management Expectations

The organization clearly defines and documents vendor management roles, contract expectations, and vendor risks.

> **Covered Security Criteria:** SOC2.CC.1.1.5, SOC2.CC.1.3.5, SOC2.CC.2.3.6, SOC2.CC.9.2.1, SOC2.CC.9.2.5, SOC2.CC.9.2.6, SOC2.CC.9.2.7, SOC2.P.6.1.1,

Data Disposal Process

Data is disposed of according to the Data Retention and Disposal Policy and customer contract.

> **Covered Security Criteria:** SOC2.C.1.2.1, SOC2.C.1.2.2, SOC2.CC.6.5.2,

Data Retention/Deletion

Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place.

> **Covered Security Criteria:** SOC2.C.1.1.2, SOC2.C.1.2.1, SOC2.C.1.2.2, SOC2.CC.6.5.2, SOC2.P.4.3.1,

Risk Assessment Methodology

An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.

Covered Security Criteria: SOC2.CC.2.1.1, SOC2.CC.3.1.11, SOC2.CC.3.1.15, SOC2.CC.3.1.2, SOC2.CC.3.2.1, SOC2.CC.3.2.2, SOC2.CC.3.2.3, SOC2.CC.3.2.4, SOC2.CC.3.2.6, SOC2.CC.3.2.7, SOC2.CC.3.2.8, SOC2.CC.3.3.1, SOC2.CC.3.3.2, SOC2.CC.3.3.3, SOC2.CC.3.3.4, SOC2.CC.3.3.5, SOC2.CC.3.4.1, SOC2.CC.3.4.2, SOC2.CC.3.4.4, SOC2.CC.3.4.5, SOC2.CC.5.1.3, SOC2.CC.9.2.2, SOC2.CC.9.2.3,

Tech Competence

The new hire screening process includes a consideration of skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Reference checks are also performed prior to hire.

Covered Security Criteria: SOC2.CC.1.4.1, SOC2.CC.1.4.5, SOC2.CC.1.4.6, SOC2.CC.4.1.4,

People

The following controls mitigate risks related to Tallyfy's employees and other staff. Examples include dissatisfaction, attrition, and HR related events.

Mitigated and monitored by 10 control(s)

Acceptable Use Policy

All employees are required to acknowledge the Acceptable Use Policy upon hire. The policy outlines rules for the acceptable use of information associated with information and information processing, as well as, appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services. The policy is updated by management as needed and available to employees.

Covered Security Criteria: SOC2.CC.2.2.9,

Code of Conduct

A code of conduct exists and is required to be signed by all employees upon hire. The code of conduct is updated by management as needed, and available to employees via the human resources site.

Covered Security Criteria: SOC2.CC.1.1.2, SOC2.CC.1.1.3,

Deficiency Monitoring

Control deficiencies and results of separate evaluations are communicated to, and monitored by the CEO and other senior management, as appropriate. Security and IT operational issues are tracked and monitored.

Covered Security Criteria: SOC2.CC.2.1.4, SOC2.CC.4.2.2, SOC2.CC.4.2.3,

Employee Shared Drive

A centralized drive is in place for employees to access all corporate policies and procedures in PDF format as well as job descriptions.

Covered Security Criteria: SOC2.CC.2.2.1,

Job Descriptions

Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.

Covered Security Criteria: SOC2.CC.1.3.3, SOC2.CC.1.4.1, SOC2.CC.1.4.3, SOC2.CC.2.2.1, SOC2.CC.2.2.9, SOC2.CC.5.3.5,

Tech Competence

The new hire screening process includes a consideration of skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Reference checks are also performed prior to hire.

Covered Security Criteria: SOC2.CC.1.4.1, SOC2.CC.1.4.5, SOC2.CC.1.4.6, SOC2.CC.4.1.4,

Employee Performance

A formal performance evaluation procedure is in place and employees are evaluated at least annually.

Covered Security Criteria: SOC2.CC.1.1.3, SOC2.CC.1.1.4, SOC2.CC.1.4.2, SOC2.CC.1.5.1, SOC2.CC.1.5.5,

Internal Controls

Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.

Covered Security Criteria: SOC2.CC.1.5.1, SOC2.CC.2.2.1, SOC2.CC.2.2.5, SOC2.CC.2.3.10, SOC2.CC.4.1.3, SOC2.CC.5.1.2, SOC2.CC.5.1.5, SOC2.CC.5.3.2, SOC2.CC.5.3.3, SOC2.CC.5.3.5, SOC2.P.8.1.8,

Security Training

Employees complete security related training, as relevant to their duties, upon hire and on an annual basis. The annual security training includes information on how to report security incidents and concerns.

Covered Security Criteria: SOC2.CC.1.5.1, SOC2.CC.2.2.1, SOC2.CC.2.2.5, SOC2.CC.2.2.6, SOC2.CC.2.2.8, SOC2.CC.5.3.1,

Incident Response: Employee Responsibility

A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.

Covered Security Criteria: SOC2.CC.2.2.3, SOC2.CC.2.2.6, SOC2.CC.2.3.5, SOC2.CC.7.3.2, SOC2.CC.7.3.4, SOC2.CC.7.4.1, SOC2.CC.9.2.4, SOC2.P.6.3.1, SOC2.P.6.5.1, SOC2.P.8.1.6, SOC2.P.8.1.7,

Physical

The following controls mitigate risks related to physical access, such as doors, loading docks, copy rooms, server rooms. This also includes any environmental risks, such as fires, floods, or earthquakes.

Policy

The following controls mitigate risks related to how information security is governed at Tallyfy. This includes policy, procedures, work instructions, and how they are communicated throughout the organization.

Mitigated and monitored by 18 control(s)

Risk Assessment Action Plans

Risks identified through the risk assessment process are addressed by management and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion. Risk assessment

results are shared with the leadership team and the board annually, and risk treatment activities are documented accordingly.

Covered Security Criteria: SOC2.CC.3.1.11, SOC2.CC.3.1.16, SOC2.CC.3.2.3, SOC2.CC.3.2.5, SOC2.CC.5.1.1, SOC2.CC.5.1.2,

Risk Assessment Methodology

An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.

Covered Security Criteria: SOC2.CC.2.1.1, SOC2.CC.3.1.11, SOC2.CC.3.1.15, SOC2.CC.3.1.2, SOC2.CC.3.2.1, SOC2.CC.3.2.2, SOC2.CC.3.2.3, SOC2.CC.3.2.4, SOC2.CC.3.2.6, SOC2.CC.3.2.7, SOC2.CC.3.2.8, SOC2.CC.3.3.1, SOC2.CC.3.3.2, SOC2.CC.3.3.3, SOC2.CC.3.3.4, SOC2.CC.3.3.5, SOC2.CC.3.4.1, SOC2.CC.3.4.2, SOC2.CC.3.4.4, SOC2.CC.3.4.5, SOC2.CC.5.1.3, SOC2.CC.9.2.2, SOC2.CC.9.2.3,

Risk Assessment Policy

Risk assessment policy and procedures are in place and include how to identify risks, to evaluate risks, and how to address and mitigate those risks.

Covered Security Criteria: SOC2.CC.3.1.11, SOC2.CC.3.1.15, SOC2.CC.3.1.2,

Incidents External

External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organizations support webpage. The incident is documented in accordance with the Incident Response Plan, if required.

Covered Security Criteria: SOC2.CC.2.2.3, SOC2.CC.2.3.11, SOC2.CC.2.3.2, SOC2.CC.2.3.4, SOC2.CC.9.2.4, SOC2.P.6.5.2,

Incident Response: Employee Responsibility

A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.

Covered Security Criteria: SOC2.CC.2.2.3, SOC2.CC.2.2.6, SOC2.CC.2.3.5, SOC2.CC.7.3.2, SOC2.CC.7.3.4, SOC2.CC.7.4.1, SOC2.CC.9.2.4, SOC2.P.6.3.1, SOC2.P.6.5.1, SOC2.P.8.1.6, SOC2.P.8.1.7,

Incident Response: Process

The incident response process includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security, confidentiality, or privacy.

Covered Security Criteria: SOC2.CC.7.3.1, SOC2.CC.7.3.2, SOC2.CC.7.3.3, SOC2.CC.7.3.4, SOC2.CC.7.4.11, SOC2.CC.7.4.2, SOC2.CC.7.4.3, SOC2.CC.7.4.4, SOC2.CC.7.4.5, SOC2.CC.7.4.6, SOC2.CC.7.4.7, SOC2.CC.7.5.1, SOC2.CC.7.5.2, SOC2.CC.7.5.3, SOC2.CC.7.5.5,

Incident Response: Responsibility

The design, implementation, maintenance, execution, and periodic testing of the security incident response program and data breach response procedures are the responsibility of the CEO.

Covered Security Criteria: SOC2.CC.2.2.6, SOC2.CC.7.4.1,

Policy Review

IT security related policies are reviewed and approved annually or as business needs change.

Procedure documents related to access control, change management, and incident management are updated as processes change.

Covered Security Criteria: SOC2.CC.5.3.3, SOC2.CC.5.3.6,

Internal Controls

Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.

Covered Security Criteria: SOC2.CC.1.5.1, SOC2.CC.2.2.1, SOC2.CC.2.2.5, SOC2.CC.2.3.10, SOC2.CC.4.1.3, SOC2.CC.5.1.2, SOC2.CC.5.1.5, SOC2.CC.5.3.2, SOC2.CC.5.3.3, SOC2.CC.5.3.5, SOC2.P.8.1.8,

Disaster Recovery Plan

A Disaster Recovery Plan is maintained and tested annually.

Covered Security Criteria: SOC2.A.2.1.10, SOC2.CC.9.1.1,

Business Continuity

A Business Continuity Plan has been developed and reviewed in the event of a catastrophic event. The plan identifies a process, roles, and milestones for maintaining business continuity and restoring system functionality.

Covered Security Criteria: SOC2.A.2.1.3, SOC2.A.2.2.1, SOC2.CC.3.2.1, SOC2.CC.5.1.2, SOC2.CC.5.2.1,

Restore

Documented backup and restoration procedures for the network are maintained and reviewed annually.

Covered Security Criteria: SOC2.A.2.2.2, SOC2.CC.7.5.1,

Data Flow Diagram

The data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level.

Covered Security Criteria: SOC2.CC.2.2.9, SOC2.CC.3.2.6, SOC2.CC.5.1.3, SOC2.CC.6.1.5,

Data Classification Policy

A defined information classification scheme has been established to label and handle data. Classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information. Data is classified into three levels: public, confidential, sensitive.

Covered Security Criteria: SOC2.A.2.1.7, SOC2.C.1.1.1, SOC2.CC.3.2.6, SOC2.CC.6.1.6,

Asset Inventory

An inventory of information assets, including hardware, software, processing facilities and data, is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention.

Covered Security Criteria: SOC2.C.1.1.1, SOC2.CC.3.2.6, SOC2.CC.6.1.1,

Data Retention/Deletion

Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a

data disposal process is in place.

Covered Security Criteria: SOC2.C.1.1.2, SOC2.C.1.2.1, SOC2.C.1.2.2, SOC2.CC.6.5.2, SOC2.P.4.3.1,

Data Management Policy

A defined Data Management Policy provides guidance on information categories, usage, storage, and transmission of data.

Covered Security Criteria: SOC2.C.1.1.1, SOC2.C.1.2.1, SOC2.C.1.2.2, SOC2.CC.6.5.2, SOC2.P.4.2.2, SOC2.P.4.3.1,

Backup Schedule

Data is backed up following a set schedule and staff is notified of back up failures; access to backups is restricted to privileged users. Backup schedules adhere to the Backup Policy.

Covered Security Criteria: SOC2.A.2.1.8, SOC2.A.2.1.9, SOC2.PI.2.5.2, SOC2.PI.2.5.3,

Privacy

The following controls mitigate risks related to any of Tallyfy's operations that can be tied to or attributed to the personal or protected data of an individual.

Mitigated and monitored by 2 control(s)

Incidents External

External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organizations support webpage. The incident is documented in accordance with the Incident Response Plan, if required.

Covered Security Criteria: SOC2.CC.2.2.3, SOC2.CC.2.3.11, SOC2.CC.2.3.2, SOC2.CC.2.3.4, SOC2.CC.9.2.4, SOC2.P.6.5.2,

Incident Response: Employee Responsibility

A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.

Covered Security Criteria: SOC2.CC.2.2.3, SOC2.CC.2.2.6, SOC2.CC.2.3.5, SOC2.CC.7.3.2, SOC2.CC.7.3.4, SOC2.CC.7.4.1, SOC2.CC.9.2.4, SOC2.P.6.3.1, SOC2.P.6.5.1, SOC2.P.8.1.6, SOC2.P.8.1.7,

Software

The following controls mitigate risks related to the use of protection of any applications or code, whether proprietary or provided by others.

Technical

The following controls mitigate risks related to anything having to do with how the network operates. This includes firewalls, data loss prevention, and network operations.

Mitigated and monitored by 15 control(s)

Change Management: Application/Software

All application changes are developed, tested, reviewed, and approved prior to implementation.

Covered Security Criteria: SOC2.CC.8.1.2,

Change Management: Emergency Process

An emergency change process is followed for changes required in urgent situations.

Covered Security Criteria: SOC2.CC.8.1.13,

Vulnerability Scan

Vulnerability scans are performed on a periodic basis to help identify security risks and results are triaged and actioned per Service Level Agreement.

Covered Security Criteria: SOC2.CC.4.1.1, SOC2.CC.5.3.4, SOC2.CC.6.1.5, SOC2.CC.6.8.2, SOC2.CC.7.1.2, SOC2.CC.7.1.4, SOC2.CC.7.1.5, SOC2.CC.7.2.2, SOC2.CC.7.2.4,

Change Management: Ticketing System

A centralized ticketing and workflow tool tracks software change activity, including development, approvals and testing.

Covered Security Criteria: SOC2.CC.8.1.4, SOC2.CC.8.1.8, SOC2.CC.8.1.9,

Antivirus

Antivirus is installed on workstations and servers to help protect against viruses and malicious software on the systems.

Covered Security Criteria: SOC2.CC.6.8.4,

Change Management Policy

A Change Management Policy and Procedures are in place to request, document, test, and approve changes.

Covered Security Criteria: SOC2.CC.8.1.1, SOC2.CC.8.1.2, SOC2.CC.8.1.3,

Separation of Environments

Production, testing, and development environments are logically and physically separated.

Covered Security Criteria: SOC2.CC.8.1.15,

Change Management: Segregation of Duties

Segregation of duties exist during the infrastructure and application change process, enforced in the source control system (GitHub).

Covered Security Criteria: SOC2.CC.5.1.6, SOC2.CC.6.3.3,

Patch Management

A formal process is followed in order to identify, review, install, and monitor patches for servers and network devices. Server patching scans occur and patches are applied as needed. Management is notified of any down time to apply updates. Acceptance testing is documented for new information systems, upgrades, and new versions.

Covered Security Criteria: SOC2.CC.5.2.2,

Change Management: Infrastructure

Infrastructure changes are tested, reviewed, and approved by authorized personnel prior to implementation.

Covered Security Criteria: SOC2.CC.8.1.10, SOC2.CC.8.1.7,

Pen Test

An independent, third party provider is contracted to perform penetration tests at least annually. Test results are reviewed and tracked to resolution.

Covered Security Criteria: SOC2.CC.2.3.3, SOC2.CC.4.1.1, SOC2.CC.4.1.5, SOC2.CC.4.1.6, SOC2.CC.4.1.8, SOC2.CC.4.2.1, SOC2.CC.5.3.4, SOC2.CC.7.2.4,

Configuration Standards

A baseline security configuration is maintained by the information technology team and is deployed to all systems; the baseline settings are reviewed annually or as business needs change. This can be in the form of AWS deployment recipes.

Covered Security Criteria: SOC2.CC.7.1.1, SOC2.CC.8.1.12,

Intrusion Detection

Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.

Covered Security Criteria: SOC2.CC.4.1.1, SOC2.CC.5.3.4, SOC2.CC.6.6.4, SOC2.CC.7.1.2, SOC2.CC.7.2.1, SOC2.CC.7.2.2, SOC2.CC.7.2.3,

Monitoring Infrastructure

IT infrastructure monitoring tools are configured to monitor IT infrastructure availability and performance, generate alerts when specific predefined thresholds are met, and forecast capacity requirements to ensure system performance.

Covered Security Criteria: SOC2.A.1.1.1, SOC2.A.1.1.2, SOC2.A.1.1.3, SOC2.A.2.1.2, SOC2.A.2.1.3, SOC2.A.2.1.4, SOC2.A.2.1.5, SOC2.A.2.1.6, SOC2.CC.4.1.3,

Network Diagram

Service boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.

Covered Security Criteria: SOC2.CC.2.2.9, SOC2.CC.3.2.6, SOC2.CC.5.1.3,

Vendor

The following controls mitigate risks related to any supplier or service provider, including contractors, consultants, and cloud providers.

Mitigated and monitored by 3 control(s)

Vendor Management Expectations

The organization clearly defines and documents vendor management roles, contract expectations, and vendor risks.

Covered Security Criteria: SOC2.CC.1.1.5, SOC2.CC.1.3.5, SOC2.CC.2.3.6, SOC2.CC.9.2.1, SOC2.CC.9.2.5, SOC2.CC.9.2.6, SOC2.CC.9.2.7, SOC2.P.6.1.1,

Vendor Due Diligence

Due diligence activities are performed over new vendors prior to contract execution, and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.

Covered Security Criteria: SOC2.CC.1.1.5, SOC2.CC.1.4.6, SOC2.CC.9.2.1,

Third Party SOC2

Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.

Covered Security Criteria: SOC2.CC.3.1.9, SOC2.CC.3.2.1, SOC2.CC.3.4.5, SOC2.CC.9.2.10, SOC2.CC.9.2.12, SOC2.CC.9.2.2, SOC2.CC.9.2.6,