System Description of the Navu Services System

Prepared in Support of a SOC 2 Examination

Relevant to Security, Availability, and Confidentiality

Company Background

Navu Inc. ("Navu") is a Software-as-a-Service (SaaS) company founded in 2024 in Palo Alto, CA. Navu's mission is to help business-to-business (B2B) companies convert more of their website visitors by making their websites smarter, more helpful, and more engaging.

Navu augments B2B websites by embedding a dynamic, AI-powered sidebar that offers interactive guidance, on-site search, content summarization, live chat, lead capture forms, and promotional tools. Navu also empowers its customers with insights and analytics through a secure, customer-specific portal.

All Navu services are delivered through cloud-based infrastructure hosted in OVH data centers located in Canada, leveraging leased ("bare metal") hardware for control and compliance purposes.

Services Provided

Navu provides a cloud-based engagement platform that embeds a smart, interactive Sidebar into customer websites. Designed to enhance user experience and surface high-value content, Navu delivers intelligent, contextual support through a combination of AI capabilities and real-time interactions. Core features of the platform include:

- **AI-powered, context-aware guidance** tailored to visitor behavior and page content
- **On-site search with summarization**, enabling fast access to relevant information
- **Form-based engagement modules** for lead capture and feedback collection
- **Integrated live chat support** with real-time agent interaction
- **Automated content promotion**, surfacing contextually relevant site resources
- **Customer analytics portal** for monitoring visitor behavior, conversions, and engagement trends

Navu collects and presents behavioral analytics derived from visitor interactions, including page views and click activity, search terms and engagement flow, and logs from AI and live agent conversations. When personally identifiable information (PII) collection is enabled by the customer, Navu securely stores form submission data (e.g., names, emails, custom fields) and customer records integrated from third-party CRMs such as HubSpot or Salesforce.

Navu is designed to be secure by default. Each customer's data is siloed, ensuring no cross-domain data exposure; visitor tracking is limited strictly to domains owned by the customer; and no external tracking mechanisms (such as third-party cookies or scripts) are used.

Principal Service Commitments and System Requirements

Navu designs its processes and procedures related to its platform to meet its objectives for the Navu services. Those objectives are based on the service commitments that Navu makes to user entities, the laws and regulations that govern the provision of Navu services, and the financial, operational, and compliance requirements that Navu has established for the services. The Navu services are subject to the security and privacy requirements of applicable privacy and data protection laws and regulations in the jurisdictions in which Navu and its customers operate, including the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Security, availability, and privacy commitments to user entities are documented and communicated in customer agreements, in Navu's published Privacy Policy, and in the description of the service offering provided online. Commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the Navu platform that are designed to permit system users to access the information they need based on their role in the system, while restricting them from accessing information not needed for their role. Access to PII is limited to designated administrators within each customer organization and a small number of authorized Navu personnel.
- Use of encryption technologies to protect customer data both at rest and in transit. All data transmitted outside Navu's firewalled environment travels over TLS/SSL-encrypted channels.
- Strict tenant-level data isolation, whereby each customer's data is logically segregated using a unique site identifier so that no customer can access another customer's data.
- Collection of PII only when explicitly enabled by the customer, with collection further governed by opt-in/opt-out signals from customer-deployed Consent Management Platforms (CMPs) or, in their absence, by GDPR-based restrictions applied according to visitor geography.
- Deletion of customer data upon termination of service, and deletion of PII upon customer request at any time.
- Notification of customers without undue delay, and no later than 72 hours, after Navu becomes aware of a data breach affecting customer data.

Navu establishes operational requirements that support the achievement of these commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Navu's policies and procedures (including its Sensitive Data Management documentation), system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the

Navu platform, including production upgrade procedures, code review processes, and data disposal procedures.

Components of the System

Infrastructure

Primary infrastructure used to provide the Navu services system includes the following:

Primary Infrastructure		
Provider / Hardware	**Type**	**Purpose**
OVH	Bare metal (leased) servers – Canadian data centers (Montreal)	Physical hosting for all production and staging systems. OVH provides physical security, fire protection, power redundancy, and multiple independent network paths to the internet.
Kubernetes	Container orchestration platform	Runs Navu's containerized services in compartmentalized clusters, each serving a specific customer cohort. Provides self-healing, horizontal scale-out, and zero-downtime rolling upgrades.
MongoDB	Per-cluster document database (redundant configuration)	Primary data store for configuration, analytics, and (when enabled) PII data. Each cluster contains its own isolated MongoDB deployment.
OpenSearch	Per-cluster search database (redundant configuration)	Powers on-site search and content indexing within each cluster.
AWS	S3	Offsite storage, accessed via scoped keys; interactive AWS portal logins by Navu personnel require MFA.
Firewall / VPN	Perimeter firewall with secure VPN gateway	All administrative access to production servers requires secure VPN connectivity with limited port openings; only a small number of authorized Navu personnel are permitted VPN access.

Software

Primary software used to provide the Navu services system includes the following:

Primary Software		
Software	**Environment**	**Purpose**
Navu application services	Kubernetes (Linux containers)	Four primary compute container types, each performing a distinct function and each redundant using a load-sharing “scale-out” approach, plus shared administrative and system-wide services.
MongoDB	Kubernetes clusters	Transactional and analytics data store, deployed redundantly per cluster.
OpenSearch	Kubernetes clusters	Search and indexing engine, internal to each Kubernetes cluster.
Graphite / Grafana	Monitoring stack	Real-time collection and dashboarding of server-level and application-level KPIs, with alerting to email and Slack.
GitHub / NPM	SaaS (secure offerings)	Source code version control, package management, mandatory code review via pull requests, and structured branching workflows.
Jenkins / Playwright	CI / automated testing	Automated test execution against new code prior to production release.
Linear	SaaS	Issue and release tracking for transparency and traceability of development work.
OpenAI / Google AI services	Third-party AI providers	Generative AI answer generation, organized in a redundant pattern so that if one provider is unavailable or too slow, the platform falls back to the other.

People

Navu has a staff of employees and contractors organized into the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. Management has asserted responsibility for the design and implementation of the controls described in this report and commits to an ongoing, at least annual, review of Navu’s system and organization controls.
- **Product Development:** Product managers and software engineers, led by the VP of Products, who design and maintain the Navu platform, including the Sidebar, the AI answer engine, the customer analytics portal, and third-party integrations. This team designs and implements new functionality, assesses and remediates issues or bugs, and owns the change management controls over the codebase. Members of the product team are responsible for peer reviews of

code authored within the team: all production code is added via pull requests reviewed by an authorized developer other than the author.

- **Operations:** Led by the Operations Manager, this function monitors and maintains the deployed Navu platform, including the Kubernetes clusters, databases, firewall and VPN infrastructure, and monitoring/alerting systems (Graphite and Grafana). The operations function responds to alerts generated by the system, executes rolling ("canary-first") production upgrades, manages logical access to infrastructure, and owns physical/hosting, access, and encryption controls.
- **Commercial:** Individuals in commercial roles market, sell, and support the Navu platform and are typically the primary point of contact for Navu customers. They assist customers with onboarding, configuration of the Sidebar and integrations, and identification of issues encountered in production.

Data

There are three major types of data used by the Navu platform:

- **Configuration Data:** Data used to configure a customer's Navu deployment, including site settings, integration credentials (OAuth tokens), portal user accounts and roles, and consent management (CMP) settings.
- **Analytics Data:** Behavioral analytics derived from visitor interactions on customer websites, including page views and click activity, search terms and engagement flow, and logs of AI and live agent conversations.
- **Personally Identifiable Information (PII):** Collected only when explicitly enabled by the customer, this includes form submission data (e.g., names, email addresses, custom fields) and customer records integrated from third-party CRMs such as HubSpot or Salesforce.

All customer data is siloed on a per-customer basis. Each customer is assigned a unique identifier (a "site ID"), and all database records associated with a customer are keyed using that ID. All relevant database queries include that key to ensure strict tenant isolation. Visitor tracking is limited strictly to domains owned by the customer, and no external tracking mechanisms (such as third-party cookies or scripts) are used.

PII is treated as the most sensitive data in the Navu system. Access to PII within a customer organization is limited to members of that customer's Navu portal; configuration of PII collection, addition of members, and assignment of roles can only be performed by users holding owner or editor roles, and access/change logs provide a history of configuration changes. Access to PII by Navu staff is limited to those with Super Admin status, which is controlled via a designated field in the administrators database collection.

Where a customer has deployed a Consent Management Platform (CMP), PII collection respects the opt-in/opt-out signals determined by the CMP. Where a customer permits collection without a CMP integration, Navu unilaterally enforces GDPR-based restrictions according to the geographical location of the visitor.

All data transmitted into or out of Navu's data center travels over secure, TLS-encrypted links, and is exchanged only with trusted parties, including authorized Navu personnel and trusted third-party processors. Data at rest is encrypted and stored within a firewalled environment with access restricted to authorized administrators. Customer data is deleted within 30 days of termination of service, and PII is deleted upon customer request at any time.

Processes and Procedures

Formal policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Navu policies and procedures that define how services should be delivered, including Navu's Sensitive Data Management documentation, Code Review Process, and Production Upgrade Procedure.

Physical Security

All production and staging systems are hosted in OVH data centers located in Canada. Navu depends on OVH to provide physical security and related protection systems, including fire detection and suppression, power redundancy, and redundant network access. OVH data centers maintain multi-layer protections and hold independent security certifications, including SOC reports. OVH data centers do not allow Navu employees physical access.

Logical Access

Access to production servers is protected by a firewall requiring secure VPN access, using standard security techniques including VPN password protection and limited port openings. Only a small number of authorized Navu personnel are permitted access through the VPN. Multifactor authentication (MFA) is enforced for all privileged users: downstream and administrative services either directly require MFA (e.g., GitHub, Stripe, Grafana via SSO, the Navu administrative portal, and interactive AWS portal access) or are reachable only via the secure VPN, which serves as an independent authentication point (e.g., MongoDB, Kubernetes, and Graphite). Internal services such as OpenSearch are accessible only from within the Kubernetes cluster.

Customer access to the Navu portal is secured using Google OAuth or passwords verified via email. Within each customer organization, role-based permissions (owner, editor, member) govern who may configure PII collection, add members, and assign roles.

Third-party integrations (e.g., OpenAI, Google, HubSpot, Salesforce, Slack) are authorized using OAuth 2.0 with granular, limited scopes to minimize exposure and uphold the principle of least privilege, and are activated only with explicit customer consent.

Computer Operations – Backups and Redundancy

Navu builds physical and virtual redundancy into the system at multiple levels. The Navu service can survive the loss of multiple physical or virtual servers; all databases are deployed in redundant configurations; and the data center provides multiple separate paths to the internet to ensure network

redundancy. There is no single point of failure in the system: if any one pod, server, or database fails, the system continues operating uninterrupted.

Computer Operations – Availability and Monitoring

Navu uses Graphite for data collection and Grafana as a dashboard of key performance indicators covering both server-level and application-level metrics, including CPU and memory usage, pageview processing rates, worst-case pageview processing durations, sidebar question rates, AI generation fallback, AI processing speeds, and AI failures. Navu employs extensive logging using standard text logging systems as well as logging into its databases to review current and recent operations. Servers notify Navu personnel via email and/or Slack messages about notable events, and a public status page provides availability transparency to customers.

At the application level, Navu's primary function of generating AI-powered answers is implemented by calling downstream services at OpenAI and Google, organized in a redundant pattern so that if one service is unavailable or too slow, the platform falls back to the other.

Navu commits to transparent notification procedures for data incidents: in the event of a data breach, Navu will notify affected customers without undue delay and no later than 72 hours after becoming aware of the breach.

Change Control

Navu maintains multiple codebases covering different parts of the service, stored and managed using the secure service offerings of GitHub and NPM. Standard versioning and branching techniques ensure that code is properly reviewed before release. Except in emergency situations, all code running in the production environment comes from branches designated as production, and all code in production branches is added via pull requests that have been reviewed by an authorized developer other than the author.

Navu uses a combination of manual and automated testing to ensure the integrity of its code. A complete mirror of the production systems is implemented separately in a staging environment, hosted in the same data center, which is used to verify new code before it is promoted to production. Automated tests are executed via Jenkins, and Linear is used to maintain a list of open issues and bugs, which are reviewed before each release.

Kubernetes is used to upgrade software by replacing containers on the fly, resulting in a zero-downtime rolling deployment design. Navu typically upgrades one cluster as a "canary" first and confirms correct operation before upgrading the remaining clusters.

Data Communications

All data transmitted outside Navu's firewalled environment travels over SSL/TLS-encrypted channels (HTTPS), ensuring protection during transmission. Ingress to the production environment is limited to designated service endpoints, and administrative ingress is restricted to the secure VPN. Sensitive data

arriving at or leaving the data center is exchanged only with trusted parties, including authorized Navu personnel and trusted third-party processors.

Boundaries of the System

The scope of this report includes the Navu services system performed by Navu Inc. This report does not include the data center hosting services provided by OVH, nor the services provided by third-party processors such as OpenAI, Google, Amazon Web Services (S3), HubSpot, Salesforce, Slack, or Stripe.

The applicable trust services criteria and the related categories are described below.

Common Criteria (to the Security, Availability, Processing Integrity, Confidentiality, and Privacy Categories)
Security refers to the protection of (i) information during its collection or creation, use, processing, transmission, and storage, and (ii) systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing Integrity
Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Privacy

The privacy criteria are organized as follows: (I) Notice and communication of objectives – the entity provides notice to data subjects about its objectives related to privacy. (II) Choice and consent – the entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects. (III) Collection – the entity collects personal information to meet its objectives related to privacy. (IV) Use, retention, and disposal – the entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy. (V) Access – the entity provides data subjects with access to their personal information for review and correction to meet its objectives related to privacy. (VI) Disclosure and notification – the entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy; notification of breaches and incidents is provided to affected data subjects, regulators, and others. (VII) Quality – the entity collects and maintains accurate, up-to-date, complete, and relevant personal information. (VIII) Monitoring and enforcement – the entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Navu's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Navu's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts, as well as the communication of entity values and behavioral standards to personnel through policy statements and by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally documented organizational policies, including Navu's Sensitive Data Management documentation, communicate entity values and behavioral standards to personnel.
- Access to sensitive customer data by Navu staff is limited to a small number of personnel with explicitly designated Super Admin status, reinforcing accountability for the handling of confidential information.

Commitment to Competence

Navu's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Each documented control has a designated control owner (e.g., the VP of Products or the Operations Manager) with the skills and authority required to operate and maintain that control.
- Code contributed to production must be reviewed by an authorized developer other than the author, ensuring that competent oversight is applied to all changes.

Management's Philosophy and Operating Style

The Navu management team must balance two competing interests: continuing to grow and innovate in a rapidly changing AI technology space while remaining excellent and conservative stewards of the data and website experiences its customers entrust to it. Management is briefed on technology changes that affect how Navu delivers AI-powered engagement, on new security technologies, and on regulatory changes (such as GDPR and CCPA developments) that may require Navu to alter its software or practices to maintain legal compliance.

Specific control activities that the service organization has implemented in this area are described below:

- Management has documented its assertion of responsibility for the design and implementation of controls addressing the AICPA Trust Services Criteria.
- Management commits to an ongoing, at least annual, review of the system and organization controls, including an assessment of controls requiring improvement in light of incidents occurring in the review period.

Organizational Structure and Assignment of Authority and Responsibility

Navu is organized in a simple structure appropriate to its size, in which control ownership is explicitly assigned to named roles. The Operations Manager owns physical/hosting security, logical access for Navu staff, data-in-transit, data-at-rest, and system resilience controls; the VP of Products owns change management, data retention and disposal, confidentiality, and privacy controls. As the team grows, management will evolve the organizational structure to ensure that employees clearly understand their roles and reporting channels.

Specific control activities that the service organization has implemented in this area are described below:

- Every documented control is assigned a named control owner responsible for its operation and evidence.
- Access rights to production infrastructure are aligned with role: only personnel whose responsibilities require it are granted VPN access or Super Admin status.

Human Resource Policies and Practices

Navu's success is founded on sound business ethics reinforced with a high level of efficiency, integrity, and ethical standards. Navu's human resources policies and practices relate to employee hiring, orientation, training, evaluation, promotion, compensation, and disciplinary activities.

Risk Assessment Process

Navu's risk assessment process identifies and manages risks that could potentially affect Navu's ability to provide reliable and secure services to its customers. Navu commits to an ongoing, at least annual, review of the system and organization controls documented in this description. This review includes an assessment of controls that require improvement in light of incidents occurring in the review period. Identified improvements are tracked as issues in Linear and incorporated into the regular Navu product development process so they can be addressed predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Navu's system; and the nature of the components of the system result in risks that the criteria will not be met. Navu addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Navu's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Navu's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Navu uses several information and communication channels internally to share information with management, employees, contractors, and customers. Navu uses Slack and email as the primary internal communication channels, including automated alerting from production systems. Development work and releases are communicated and tracked via Linear and GitHub. Monitoring information is communicated via Grafana dashboards, and service availability is communicated to customers via a

public status page. Customers interact with Navu through the customer analytics portal, through their designated commercial contacts, and through the integrated live chat capability.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Navu's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Navu's production systems are monitored in real time using Graphite and Grafana, with automated notifications delivered via email and Slack for notable events. Extensive text and database logging supports the review of current and recent operations. Management's close involvement in Navu's operations helps to identify significant variances from expectations regarding internal controls. Management evaluates the facts and circumstances related to any suspected control breakdown and decides whether the incident was isolated or requires a change in the company's procedures or personnel.

Reporting Deficiencies

Linear is utilized to document and track the results of ongoing monitoring procedures, including issues and bugs identified through automated testing, staging validation, and production monitoring. Open issues are reviewed before each release. Risks and deficiencies identified through the annual controls review are documented, and corrective actions are tracked to completion through the same issue-tracking process.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date. Navu has not experienced a data breach. Should a breach occur, Navu will notify affected customers without undue delay and no later than 72 hours after becoming aware of the breach.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to the Navu services system.

Subservice Organizations

Navu's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Navu's services to be solely achieved by Navu control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Navu.

Navu's primary subservice organization is OVH, which provides the physical data center facilities in Canada where Navu's leased ("bare metal") servers are hosted. Navu depends on OVH to provide physical security and related protection systems, such as fire protection, power redundancy, and network access and redundancy. The following subservice organization controls should be implemented by OVH to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – OVH		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is restricted to authorized individuals and managed by electronic access control devices. Physical access points to server locations are monitored, and intrusion detection mechanisms alert appropriate personnel of security incidents. Multi-layer physical protections are maintained across OVH Canadian data centers.
Availability	A1.2	Data centers are protected by fire detection and suppression systems. Data centers maintain appropriate environmental controls, including cooling and atmospheric monitoring. Redundant power supplies and backup power provisions protect against electrical failure. Multiple independent network paths to the internet provide network redundancy.

In addition to OVH, Navu relies on an array of downstream third-party processors, including OpenAI and Google (AI processing), Google (authentication and site search enhancements), Amazon Web Services (S3 offsite storage), HubSpot and Salesforce (CRM synchronization), Slack (alerting and messaging), and Stripe (payments). Some of these services process sensitive information by the nature of the service, and each is deemed by Navu to be secure appropriate to the nature of the information shared with it. All such integrations are authorized using OAuth 2.0 with granular, limited scopes, and these services either

directly require MFA or are accessible only via Navu's secure VPN, which serves as an independent authentication point.

Navu management, along with its subservice organizations, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts and service agreements. In addition, Navu performs monitoring of subservice organization controls, including the following procedures:

- Reviewing publicly available security documentation, certifications, and attestation reports (including SOC reports) over services provided by OVH and other third-party processors.
- Maintaining a documented list of third-party processors, their accreditations, and available customer access controls in Navu's Sensitive Data Management documentation.
- Monitoring the operational health of downstream AI services in real time and automatically falling back to a redundant provider when a service is unavailable or degraded.

Complementary User Entity Controls

Navu's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Navu's services to be solely achieved by Navu control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Navu.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Navu.
2. User entities are responsible for notifying Navu of changes made to technical or administrative contact information.
3. User entities are responsible for managing membership of their Navu portal, including the assignment of owner, editor, and member roles, and for restricting owner and editor roles to appropriate personnel.
4. User entities are responsible for determining whether to enable PII collection and for ensuring that such collection complies with the laws and regulations applicable to their business.
5. User entities are responsible for managing visitor disclosures and consent, including the deployment and configuration of a Consent Management Platform (CMP) where required.

6. User entities are responsible for authorizing, scoping, and reviewing third-party integrations (e.g., HubSpot, Salesforce, Slack) connected to their Navu deployment.
7. User entities are responsible for ensuring the supervision, management, and control of the use of Navu services by their personnel.
8. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Navu services.
9. User entities are responsible for immediately notifying Navu of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations.
10. User entities are responsible for requesting deletion of PII where required, and for notifying Navu upon termination of service so that data disposal timelines can be met.