Navu Access Control Policy

Purpose

The purpose of this policy is to ensure that access to Navu systems and data is appropriately controlled, limited to authorized personnel, and consistent with the principles of least privilege, confidentiality, integrity, and availability.

Scope

This policy applies to:

- All Navu employees, contractors, and third-party vendors with system access.
- All systems, applications, databases, and cloud infrastructure supporting Navu services.
- Customer data and personally identifiable information (PII) stored or processed by Navu.

Roles and Responsibilities

Chief Executive Officer (CEO) – Ensures executive-level accountability for access control measures.

VP of Products – Owns logical access control policies for staff.

Operations Manager – Responsible for operational enforcement of access restrictions, MFA, VPN configuration, and security monitoring.

System Administrators – Manage user provisioning and permissions in line with this policy.

Employees & Contractors – Must adhere to assigned access privileges and security requirements.

Access Control Principles

Principle of Least Privilege

- Access is granted strictly based on job function and minimum necessary permissions.
- Privileged access is restricted to designated administrators.

Authentication Controls

- **Multifactor Authentication (MFA)** is mandatory for all privileged accounts and critical systems (e.g., GitHub, AWS, Grafana, Stripe).
- **VPN-Secured Access** is required for administrative access to servers and Kubernetes environments.
- **Super Admin Access** to PII is restricted to designated Navu staff and set via MongoDB admin records.

Access Provisioning and Deprovisioning

New Employees

Access for new employees is requested by their supervisor and approved per the Roles and Responsibilities outlined above.

Role Changes

Access changes driven by changes in role are initiated by the employees supervisor and approved per the Roles and Responsibilities outlined above.

Termination of Access

Access is revoked upon termination of employment.

Related Documents

Navu Sensitive Data Management