Security Exhibit / Security Whitepaper

Document ID: VC-LEGAL-004 **Title**: Security Exhibit **Version**: 1.0-draft **Last updated**: 2026-05-15 **Publisher**: Algoshred Technologies Private Limited (Burdenoff Group) **Canonical location**: https://burdenoff.com/contracts/vibecontrols/VC-LEGAL-004 **Burdenoff Group Contract Registry** — root at https://burdenoff.com/contracts (one subgroup per product). The contracts referenced in this document belong to the **VibeControls subgroup** at https://burdenoff.com/contracts/vibecontrols/. Every referenced contract is identified by its Document ID (`VC-LEGAL-###` / `VC-PRICING-###`) and incorporated by reference.

Status: TEMPLATE / DRAFT — to be reconciled with the live Algoshred's internal security findings tracker and infra-specs before customer publication. See **VC-LEGAL-REG** — Open Questions & Risks Register (Q-SEC-*). **Incorporated by reference** into the MSA, DPA, and Order Forms unless explicitly varied.

---

1. Overview

VibeControls is a multi-tenant SaaS developer control plane. Algoshred designs and operates the Service following defence-in-depth principles across (a) cloud infrastructure, (b) Kubernetes platform, (c) service mesh, (d) application code, (e) data layer, (f) operator access, and (g) supply chain.

Operating model. Algoshred is the contracting party. The Burdenoff Group's manpower house — **Burdenoff Consultancy Services Private Limited** — employs the engineering, support, security, and operations personnel that operate the Service under Algoshred's instructions and the Group's intra-group confidentiality and data-protection arrangements. **Data and compute** run on managed cloud services (AWS, Microsoft Azure, Google Cloud) acting as Subprocessors per the DPA Annex 3.

Current security state. Algoshred maintains a tracker of open security findings (Algoshred's internal security findings tracker). The known critical items SEC-001 (hardcoded demo workspace IDs in the VibeControls microfrontend) and SEC-002 (committed credentials in the VibeControls workspace-service environment file) have been addressed: SEC-001 by routing the five affected form components through the VibeControls workspace context workspace context, and SEC-002 by confirming environment file is gitignored / untracked, with secret rotation and re-encryption-of-encrypted-at-rest fields routed to operations via OpenBao. See the project SEC tracker for current status of all findings.

This Exhibit describes the controls in force. Specific commitments (e.g., RPO/RTO, retention, residency, customer-managed keys) are set on the Order Form. **No certification beyond what is expressly listed here is claimed**; ISO/IEC 27001 and SOC 2 Type II are on the roadmap and not in force at the date of this Exhibit.

2. Organisational controls

- ISO/IEC 27001-aligned ISMS (certification roadmap — see Risks).
- Information Security Lead reporting to senior management.
- Security risk register reviewed quarterly.

- Documented policies for access control, asset management, change management, incident response, business continuity, vendor management, secure development, acceptable use.
- Mandatory annual security and privacy training; phishing simulations.

3. Personnel

- Confidentiality undertakings on all employees and contractors.
- Background checks for roles with production access, subject to local law.
- Access revocation within 24 hours of offboarding.
- Separation of duties for production change deployment vs. approval.

4. Identity and access management

Layer	Control
Internal SSO	SSO with MFA mandatory; no shared accounts
Cloud admin	MFA enforced on AWS / Azure / GCP root and admin
Production K8s	RBAC, Cloudflare Zero Trust + bastion; just-in-time elevation
Secrets	OpenBao self-hosted vault; per-environment paths (`boff/*`); access scoped by role
Customer-facing	RBAC enforced at the gateway via @requiresPermission GraphQL directives; SSO/SAML/OIDC and SCIM available on Enterprise

5. Encryption

Data state	Mechanism
In transit	TLS 1.2+ on all public endpoints; HSTS; mTLS via Istio between internal services
At rest	AES-256 for primary databases (PostgreSQL), Valkey/Redis (where supported), object storage (S3/Azure Blob with provider-managed keys)
Application-layer	Webhook signing keys and other tenant secrets encrypted with AES-256-GCM
Key management	OpenBao KMS; rotation policies; customer-managed keys available on Enterprise

6. Network architecture

- Production runs on managed Kubernetes per-environment (alpha, prod) with namespace segregation (`svc` , `state` , `public` , `internal`).
- Service mesh: Istio with mTLS, egress gateway, cert-manager.
- Public traffic: Cloudflare WAF → provider load balancer → API gateways.

- Internal-only traffic: internal API gateways behind private ingress; M2M via `wspace-int-gateway` and `global-int-gateway`.
- Default-deny network policies; egress restricted to approved destinations.

7. Application security

- Secure SDLC: PR review, signed commits encouraged, GitHub Actions on self-hosted ARC runners.
- Static analysis on CI; dependency scanning; secret scanning.
- Build-time container scanning with **Trivy** (CVEs, IaC misconfig, SBOM).
- Deploy-time policy enforcement with **OPA / Gatekeeper**.
- Runtime threat detection with **Falco** (eBPF).
- Strict input validation; GraphQL query depth/cost limits at gateway; parameterised DB access via Prisma parameterised SQL via Prisma.
- Strict TypeScript; no `any`, no `eslint-disable`, no `@ts-ignore` in repo standards.

8. Multi-tenancy and data isolation

- Logical tenant isolation by workspace ID; RBAC enforcement at the resolver layer.
- Storage and API request quotas applied per account.
- Dedicated tenant deployment available on Enterprise (single-tenant cluster / namespace).
- Self-hosted / air-gapped option available on Enterprise.

9. Logging, monitoring, audit

- Centralised logs (Loki), metrics (Mimir / Prometheus), traces (Tempo) with Grafana dashboards.
- Customer-visible audit history per Plan; longer retention for Enterprise.
- Security event monitoring 24×7 (best-effort outside business hours for non-Enterprise tiers).
- Burdenoff Group status page at **https://status.burdenoff.com** (Gatus) publishes uptime and incident status for **all Burdenoff Group products**, including VibeControls.

10. Vulnerability and patch management

- Continuous CVE scanning of base images and dependencies.
- Patch SLO: critical within 7 days, high within 30 days, medium within 90 days, subject to operational risk.
- Annual third-party penetration test (target — see Risks).
- Coordinated vulnerability disclosure programme at security@burdenoff.com (TBC).

11. Backup and disaster recovery

Item	Detail
Database backups	Automated, encrypted; hot tier rolling 30 days
Long-term backups	Cold tier up to 90 days

Item	Detail
BCP / DR test	At least annually
Default RPO / RTO	RPO 24 hours / RTO 24 hours
Enterprise commitment	RPO 1 hour / RTO 8 hours (subject to deployment mode)

Agent-local data (sessions cached on Customer machines) is **not** backed up by Algoshred.

12. Incident response

- Documented IR playbooks with severity classification (SEV-1 to SEV-4).
- 24×7 on-call rotation.
- Customer notification within 72 hours of confirmed Personal Data Breach.
- Post-incident review and root-cause analysis shared with affected Customers under NDA.

13. Compliance and certifications

Item	Status
ISO 27001	Roadmap
SOC 2 Type II	Roadmap
GDPR / DPDP Act readiness	DPA available
PCI-DSS	Out of scope (payment processing delegated to Stripe / Razorpay)
HIPAA / BAA	Not supported by default; case-by-case Enterprise review
Cert-In directives (CERT-In 2022)	Algoshred complies with applicable Indian CERT-In reporting requirements

14. Subprocessors

See **VC-LEGAL-003C** — DPA Annex 3 (Subprocessors). The live, authoritative list is published at https://burdenoff.com/contracts/subprocessors.

15. Customer responsibilities (shared responsibility)

Algoshred	Customer
Service infrastructure and platform	OS hardening on Customer-controlled Agent hosts
Service-level RBAC primitives	Customer's RBAC / SSO configuration and access reviews
Encryption of Customer Data at rest/in transit in the Service	Encryption / control of Customer Data **outside** the Service (local files, source code repos, target hosts)
Plugin runtime and review	Customer's choice of plugins and trust in plugin authors
Tenant isolation in multi-tenant SaaS	Workspace-level access management within the tenant

Algoshred	Customer
AI gateway and limits	Choice and security of BYO AI providers, prompt content review
Backups of Service data	Backups of Customer-side data (source code, local config)

16. Reporting

- Status page (group-wide): https://status.burdenoff.com — publishes status for all Burdenoff Group products including VibeControls
- Security contact: security@burdenoff.com (Burdenoff Group security mailbox; monitored by the Burdenoff Consultancy security personnel that operate the Service on Algoshred's behalf)
- Vulnerability disclosure: same address; PGP key on request
- DPO / Grievance Officer (DPDP Act): **Vignesh T.V.**, Founder, CEO & CTO of Algoshred — contact@vibecontrols.com

17. Changes

This Security Exhibit may be updated provided the overall level of security is not materially diminished. Material changes will be notified through standard channels.

Reference and incorporation

All Burdenoff Group contracts, addenda, exhibits, policies and registers referenced in this document are identified by their **Document ID** (`BOFF-LEGAL-###` or `BOFF-PRICING-###`) and are published at **https://burdenoff.com/contracts**. Each such referenced document is incorporated into this document by reference. The version of a referenced document that applies is the version published at https://burdenoff.com/contracts as at the Effective Date of the applicable Order Form (or, where no Order Form exists, the version current at the date of acceptance), unless an executed Order Form specifies a frozen version.

CERT-In Incident Reporting — Customer-facing Summary

Document ID: VC-LEGAL-004A **Title**: CERT-In Incident Reporting Summary **Version**: 1.0-draft **Last updated**: 2026-05-15 **Publisher**: Algoshred Technologies Private Limited (Burdenoff Group) **Canonical location**: https://burdenoff.com/contracts/vibecontrols/VC-LEGAL-004A **Burdenoff Group Contract Registry** — root at https://burdenoff.com/contracts (one subgroup per product). The contracts referenced in this document belong to the **VibeControls subgroup** at https://burdenoff.com/contracts/vibecontrols/. Every referenced contract is identified by its Document ID (`VC-LEGAL-###` / `VC-PRICING-###`) and incorporated by reference.

This is a customer-facing summary of Algoshred's compliance with the **CERT-In Cyber Security Directions dated 28 April 2022** under Section 70B(6) of the Information Technology Act, 2000.

For the internal operational procedure, see SOP **BUR-SOP-027** in BUR-SOP-027 (CERT-In Incident Reporting).

Commitments

- **6-hour reporting**: Algoshred reports qualifying cyber security incidents to CERT-In (incident@cert-in.org.in) within **6 hours** of noticing or being notified, using the prescribed format and via the prescribed channel.
- **180-day log retention in India**: Algoshred retains ICT system logs relevant to incident investigation for at least **180 days** within Indian jurisdiction.
- **Time synchronisation**: production systems synchronise clocks with NPL / NIC time servers (or an equivalent stratum source) to ensure consistent timestamps across incident timelines.
- **Coordinated disclosure**: where an incident impacts Customer Personal Data, Algoshred will additionally notify the affected Customer per DPA §4.8 (within 72 hours of confirmation) and provide a post-incident report.

Indian public-sector customers

For public-sector Customers, additional commitments under the Public Sector Addendum §5 apply, including support for MeitY auditor-empanelled security audit.

Reference and incorporation

All Burdenoff Group contracts, addenda, exhibits, policies and registers referenced in this document are identified by their **Document ID** (`BOFF-LEGAL-###` or `BOFF-PRICING-###`) and are published at **https://burdenoff.com/contracts**. Each such referenced document is incorporated into this document by reference. The version of a referenced document that applies is the version published at https://burdenoff.com/contracts as at the Effective Date of the applicable Order Form (or, where no Order Form exists, the version current at the date of acceptance), unless an executed Order Form specifies a frozen version.