BuildOps Security Policy

This document describes the safeguards, controls, and practices BuildOps maintains to protect the information you entrust to us through our use of the BuildOps platform, our cloud-based operations management system. This Security Policy is incorporated into and subject to the BuildOps Terms of Service (the "Agreement"). Capitalized terms not defined herein have the meanings set forth in the Agreement.

Platform and Infrastructure

BuildOps, a SOC 2 Type I certified program runs our operations on **Amazon Web Services (AWS)**. This means your data benefits from enterprise-grade cloud infrastructure with the following protections:

- **Encryption** of all data at rest and in transit
- **Unique authentication** required for every user accessing the system
- **Restricted encryption key access**, limited to authorized personnel
- **Continuous vulnerability and system monitoring** to detect and address threats proactively
- **Regular penetration testing** conducted by annually and after major platform changes by independent assessors

Access Controls

We enforce strict controls over who can access your information:

- This policy applies to subprocessors, contractors, partners, consultants, and any other third party who has access to Customer Data. We review critical providers on periodic basis and take action where risk is no longer acceptable
- Every team member uses a unique, individually assigned account with Multi-Factor Authentication enforced across the tenant and all applications. Shared credentials are prohibited."
- Access is granted on a **least-privilege basis**, meaning each person can only view and interact with the data necessary for their role.
- Company-managed devices are configured, updated, and monitored in line with industry-leading security standards
- Access rights are reviewed quarterly and revoked immediately upon role change, transfer, or departing the company.
- All access activity is **logged and auditable (within applicable retention periods)**.

Incident Response

We maintain a formal Incident Response Plan that includes:

- Immediate identification, containment, evidence preservation, and chain-of-custody requirements of security event
- **Root cause analysis** and remediation in coordination with our platform provider
- **Timely notification** to affected customers if an incident involves their data, as well as regulators and law enforcement as applicable
- **Post-incident review** to strengthen controls and prevent recurrence

Business Continuity

We maintain Business Continuity and Disaster Recovery plans to minimize disruption to the services you depend on. These plans cover:

- Identification of critical workflows and recovery priorities
- Defined recovery point objectives to mitigate data loss
- Regular backups of critical data tested for integrity and availability on an annual basis
- Manual fallback procedures for essential operations
- Annual and regular testing of business continuity/disaster recovery plans through tabletop, walkthroughs, or full-scale simulations
- A communication plan to keep you informed during any service disruption

Our People

Security is part of our culture, not just our technology:s

- All team members complete **annual security awareness training**.
    - Training covers topics such as phishing, social engineering, secure use of passwords, multi-factor authentication, appropriate handling of data, and how to report security concerns..
- Physical visitor procedures are enforced at all of our locations.

Privacy

Your personal data is handled in accordance with applicable privacy laws and our Privacy Policy. We maintain formal data retention and data classification procedures, and we regularly review the privacy practices of our platform and third-party providers to confirm ongoing alignment with our obligations.

Continuous Improvement

We review and update our security program at least annually, and more frequently in response to security incidents, changes in technology, regulatory developments, or changes in our business operations. Our goal is to ensure that the protections described here keep pace with evolving threats and your expectations.

Questions

If you have questions about our security practices or want to report a concern, please contact us at **security@buildops.com**