DOCUMENT TITLE	INFORMATION SECURITY
DESCRIPTION	Outlines procedures/approach for continuity of critical services
AUTHOR/OWNERSHIP	Martin Cheetham - CTO

Contents

Information Security

Purpose

The purpose of this policy is to establish a framework for protecting Verifi's information assets, including customer data, company records, and intellectual property, against unauthorized access, disclosure, modification, or destruction. This policy supports the confidentiality, integrity, and availability of information and aligns with industry-standard security practices.

Scope

This policy applies to all information and systems used by Verifi including:

- Application and customer data hosted on Bubble.io
- Cloud infrastructure provided by AWS through Bubble.io
- Company devices and accounts used by the CEO and CTO

Policy Statement

Verifi is committed to protecting information assets through a combination of platform-managed security, internal controls, and operational best practices:

1. Platform Security:
    - All infrastructure and hosting are provided and secured by Bubble.io and AWS.
    - Bubble.io manages network security, system monitoring, backups, and access controls.
2. Access Control:
    - Only authorized personnel (CEO and CTO) have access to production systems and sensitive data.
    - Strong authentication and MFA are enforced on all accounts.
    - Principle of least privilege is applied to limit access to only what is necessary for job responsibilities.
3. Data Protection:
    - Data at rest and in transit is protected by encryption provided by Bubble.io/AWS.
    - Regular application backups are maintained to ensure recoverability.
4. Logging and Monitoring:

- Security-relevant events are logged at the platform level by Bubble.io and AWS.
- Internal accounts are monitored for anomalous behaviour.

5. Incident Response:
    - Any suspected security incidents will be investigated promptly by the founders.
    - Bubble.io provides platform-level monitoring and alerting to assist in detecting potential incidents.
6. Third-Party Services:
    - Only vetted third-party services are used.
    - Security and compliance of these services are reviewed as part of the Third-Party Risk Management Policy.
7. Training and Awareness:
    - The CEO and CTO maintain awareness of security best practices.
    - Security responsibilities are embedded in daily operations.

Responsibilities

CTO	Maintain security controls, manage backups, monitor access, and review platform security updates.
CEO	Oversight of security priorities, incident response, and third-party risk.

Policy Review

- This policy will be reviewed annually or when significant operational, technological, or regulatory changes occur.

Change Notes/Comments

VER	REVIEW DATE	NEXT REVIEW (LATEST)	APPROVERS (2 MINIMUM)	COMMENTS
1.0	Jan 17, 2025	Jan 17, 2026	John Kauffman (CEO), Martin Cheetham (CTO)	Initial document following company incorporation