Information Security Policy

Version: 1.0

Status: Formal Policy

1. Purpose

This Information Security Policy establishes the principles, responsibilities, and controls that 2BrightSparks Pte. Ltd. applies to protect the **confidentiality**, **integrity**, and **availability** of its systems, data, products, and services.

2. Scope

This policy applies to all employees, contractors, and third parties who access, manage, store, transmit, or otherwise handle company systems or data. It includes:

- Internal business systems (licensing, website, support portal, financial systems)
- Source code repositories and development environments
- Communication and collaboration platforms
- Endpoints used for company operations (workstations, laptops, mobile devices)

2.1. Customer Data Exclusion

This policy covers the security of 2BrightSparks' internal systems and data. **Customer backup data created using SyncBack software is stored in locations chosen and controlled exclusively by the customer.** 2BrightSparks does not store, access, or manage this customer data as part of its services.

3. Security Principles

- **Protect Data:** Protect personal and operational data according to all applicable legal and regulatory requirements.
- **Least Privilege:** Limit system and data access to only those with an authorized and necessary business need.
- **Secure Development:** Maintain secure software development and deployment practices.
- **Respond & Improve:** Monitor, respond to, and learn from security incidents promptly.

4. Roles & Responsibilities

Role	Responsibility
Management	Approves security policies, provides necessary resources, and ensures overall company compliance.
Security Lead	Oversees day-to-day security practices, risk management, and the implementation of security controls.
IT / System Admins	Implement and maintain technical safeguards, patch management, and operational security.
All Employees & Contractors	Adhere to all policies, report security concerns, protect company-issued credentials, and secure their devices.

5. Access Control

- Access to systems and data must follow the principle of least privilege.
- Role-based permissions are required for all production systems.
- Strong authentication (e.g., MFA) is required for all administrative access and critical systems.
- User accounts must be reviewed regularly. Access must be removed promptly when no longer required (e.g., upon termination or change of role).

6. Data Protection & Privacy

- Personal and business data must be collected and processed only for legitimate, specified business purposes.
- Sensitive data must be protected using encryption at rest and in transit where applicable.
- Data retention is limited to the minimum time required for operational, legal, and business needs.
- Personal data may be accessed, corrected, or deleted upon a validated request as required by law.

7. Software Development Security

- Source code must be version-controlled and stored in approved, secured repositories.

- Code changes must be reviewed by a qualified individual (other than the author) before deployment to production.
- Software dependencies must be monitored for vulnerabilities, and patches must be applied in a timely manner.
- Releases must be tested, documented, and distributed to customers through trusted, secure channels.

8. System & Network Security

- Production systems must be protected using firewalls, and networks must be segmented to limit potential lateral movement.
- Systems must be monitored for security events, and logs must be retained.
- Administrative interfaces must not be publicly exposed unless specifically required and secured.
- Backups of critical operational systems must be taken periodically and stored securely. **Recovery procedures are detailed in the *Business Continuity & Disaster Recovery (BC/DR) Plan*.**

9. Incident Response

2BrightSparks maintains a dedicated **Incident Response Plan (IRP)** to manage security incidents.

- All personnel must report suspected security incidents immediately, according to the procedures defined in the IRP.
- The IRP details the specific phases of response: Identification, Containment, Eradication, Recovery, and Post-Incident Review.
- The IRP also defines the specific roles and responsibilities of the incident response team.

10. Third-Party Services & Vendors

- Only approved providers may be used for hosting, payments, and other critical business functions.
- Vendors must be vetted to ensure they provide adequate data protection and security assurances.
- Access provided to third parties must be restricted to the minimum necessary and must be time-limited.

11. Remote Work & Device Security

- Devices used for company operations must use supported, patched operating systems.
- Full-disk encryption and an automatic screen lock must be enabled on all company laptops.
- Use of public or untrusted Wi-Fi requires a secure tunnel (e.g., VPN) when accessing

internal, non-public systems.

12. Training & Awareness

- Guidance on common threats, such as phishing prevention, social engineering, credential hygiene, and secure communication is detailed in the ***Security Awareness Guidance*** document.

13. Compliance & Review

13.1. Policy Compliance

- All employees, contractors, and third parties are required to read, understand, and adhere to this policy.
- Violations of this policy may result in access restrictions or disciplinary actions, up to and including termination of employment or contracts.

13.2. Policy Review

- This Information Security Policy will be reviewed at least annually, or upon any significant infrastructure, business, or regulatory change, to ensure its continued relevance and effectiveness.

14. Contact

Questions regarding this policy or requests for security guidance should be directed to the **Security Lead** or **Management**. Security incidents must be reported per the **Incident Response Plan**.

15. Document Maintenance & Control

Document Version History

Version	**Date**	**Approver**	**Summary of Changes**
1.0	11 Nov 2025	Michael Leaver	Initial formal policy. Links to IRP and BC/DR plans.