Baringa

Security Addendum

Version 1 | September 2024

Contents

Review of the Security Addendum

Baringa will review and update the Security Addendum on an annual basis to ensure that the information remains accurate. Any major changes will be updated immediately.

Confidentiality and limitation statement

This document: (a) is proprietary and confidential to Baringa Partners LLP ("Baringa") and should not be disclosed to third parties without Baringa's consent; (b) is subject to contract and shall not form part of any contract nor constitute an offer capable of acceptance or an acceptance; (c) excludes all conditions and warranties whether express or implied by statute, law or otherwise; (d) places no responsibility on Baringa for any inaccuracy or error herein as a result of following instructions and information provided by the requesting party; (e) places no responsibility for accuracy and completeness on Baringa for any comments on, or opinions regarding, the functional and technical capabilities of any software or other products mentioned where based on information provided by the product vendors; and (f) may be withdrawn by Baringa within the timeframe specified by the requesting party and if none upon written notice. Where specific Baringa clients are mentioned by name, please do not contact them without our prior written approval.

Copyright

1. Introduction

1. Introduction

Baringa maintains a comprehensive security program and implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability of our client data. Baringa regularly tests and evaluates its security programme to ensure all controls are effectively managed and maintained.

1.1 Baringa's audits and certifications

Baringa's information security management system is assessed by independent third-party auditors on a regular basis as well as the Cyber team operating a robust internal audit programme for:

- ISO 27001 scope include Baringa London and Baringa Australia Sydney offices
- Cyber Essentials Plus

These certifications demonstrate our continued commitment to keeping client data safe and secure. The certifications can be found on Baringa's website here.

1.2 Information security policies

Baringa maintains information security, use and management policies (collectively "Security Policies") designed to educate our employees and contractors regarding appropriate use, access to and storage of client data, including (but not exclusively) acceptable use of their equipment. All employees must read and confirm that they have read the Acceptable Use policy as part of their induction training. Baringa monitors employee behaviour and adherence to the security policies and can implement disciplinary measures if failures/security incidents are found.

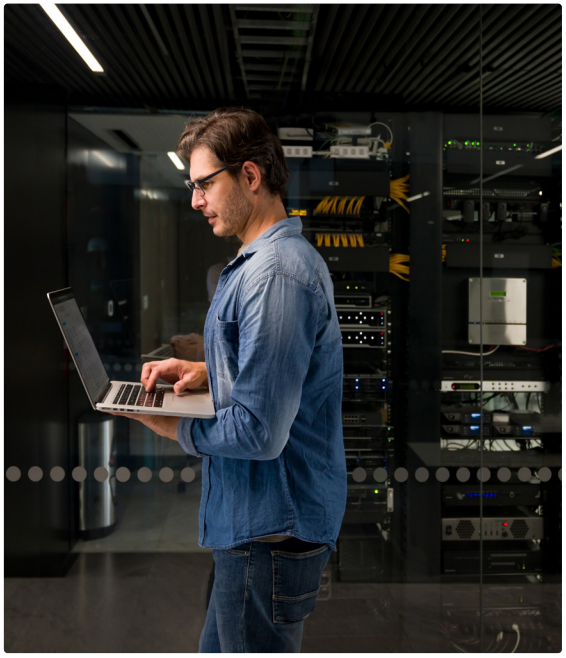
1.3 Awareness and training

New employees are required to complete security training as part of the new hire process, this includes cyber and data privacy. All existing employees receive quarterly security training and, in some instances, targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Security Policies, as well as other corporate policies, such as the Baringa Code of Conduct. Baringa conducts periodic security awareness campaigns to educate employees about their responsibilities and provide guidance to create and maintain a secure workplace.

2. Physical and Environment Controls

2. Physical and environment controls

The hosting location of our client data is in a production cloud environment and is held within the EU, East US or Australia East.



2.1 Cloud environment and data centres

To ensure that Baringa's Cloud Provider has appropriate physical and environmental controls for its data centres. Baringa regularly reviews external audit reports to confirm controls are effective. Each cloud Provider must have a SOC 2 Type ll annual audit and ISO 27001 certification, or alternative industry recognised equivalent frameworks. Such controls, shall include but are not limited to, the following:

- Physical access to the facilities are controlled at building ingress points;
- Visitors are required to present ID and are signed in;
- Physical access to servers is managed by access control devices;
- Physical access privileges are reviewed regularly;
- Facilities utilise monitor and alarm response procedures;
- Use of CCTV;
- Fire detection and protection systems;
- Power back-ups and redundancy systems; and
- Climate controls systems.

Our offices will have technical, administrative and physical controls and shall include, but not limited to, the following:

- Physical access to the office is controlled at office ingress points;
- Badge access is required for all personnel and badge privileges are reviewed regularly;
- Visitors are required to sign in;
- Use of CCTV at building ingress points;
- Tagging and inventory of Baringa issued laptops and network assets;
- Fire detection and sprinkler systems; and
- Climate control systems.

3. Technical controls

3. Technical controls

Baringa has various technical safeguards in place to protect the confidentiality, integrity and availability of client data. These controls are summarised below, this is not an exhaustive list.

3.1 Encryption

Baringa encrypts client data at rest and in transit by using industry standard encryption.

Encryption key management is in place and involves regular rotation of encryption keys. Baringa logically separates encryption keys from client data.

3.2 Access controls

All Baringa employees have a unique user ID and password, as well as multi-factor authentication to be able to access Baringa systems. Access is via a secure VPN. Additional training is provided to users who are given privilege access levels. Access reviews are performed at least quarterly for privilege access.

3.3 Endpoint controls

For all access to the cloud environment or Baringa systems employees are issued with dedicated Baringa laptop devices which utilise security controls that include, but not limited to: Disk encryption, endpoint detection and response (EDR) tools to monitor and alert to suspicious activities and malicious code remediation and vulnerability management.

3.4 Hardening

Baringa systems are hardened using industry best practices to protect it from vulnerabilities, including changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regularly patches as described in this Security Addendum.

3.5 Firewalls and security groups

Baringa protects its cloud environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business required.

3.6 Monitoring and logging

Monitoring tools or services, such as host-based intrusion detection tools, are utilised to log certain activities and changes within the Cloud Environment. These logs are further monitored, analysed for anomalies, and are securely stored to prevent tampering for at least one year.

3.7 Penetration testing

Baringa performs an annual penetration test by an accredited penetration testing company. Any new applications/systems will be penetration tested during development.

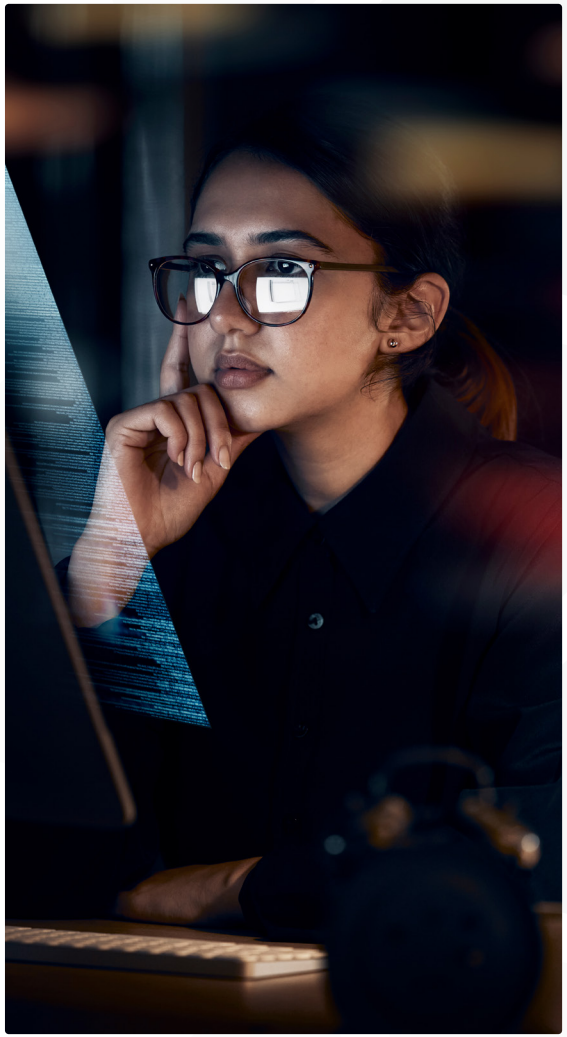
3.8 Secure disposal

Baringa has appropriate measures in place to securely dispose of its equipment via an accredited third-party supplier.

3.9 Vulnerability detection and management

Antivirus and anti-malware is updated on regular intervals. Detection tools monitor and provide alerts for suspicious activity, potential malware, and viruses.

Vulnerability scans are performed within the environment to determine potential vulnerabilities in accordance with then-current security operating procedures, which will be at least quarterly. When software vulnerabilities are revealed and addressed by a vendor patch, the patch will be obtained from the applicable vendor and applied within an appropriate risk-based timeframe in accordance with the then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in production systems.



4. Administrative controls

4. Administrative controls

This section includes aspects such as personnel security, risk management, vendor management and change management.

4.1 Personnel security

Baringa requires criminal background screening, references, proof of identity/address, right to work, credit checks and education certificates for all personnel as part of its hiring process. Where Baringa is working with the government, Baseline Personnel Security Standard Checks (BPSS) are performed. Any additional checks required by our client are considered when signing the agreement.

Personnel are asked to sign a confidentiality agreement and are provided with an Employee Handbook which includes cyber security and data protection responsibilities.

4.2 Risk management

Baringa has a Risk Management Framework which is adhered to by all areas of the business. The Risk Committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies in order to make recommendations for new and improved controls and threat mitigation strategies.

4.3 Vendor management

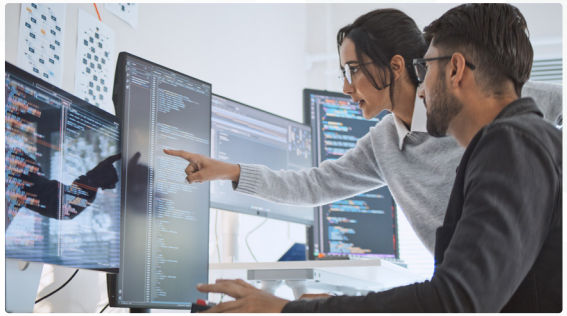
Third-party vendors with access to Confidential Information are subject to contractual obligations of confidentiality and risk assessments to gauge the sensitivity of information shared. Vendors are expected to comply with any pertinent contract terms relating to the security of data, as well as any applicable Baringa policies or procedures. Periodically, Baringa may as the Vendor to re-evaluate its security posture to help ensure compliance.

4.4 Deletion of client data

Baringa securely disposes of any client data as requested and in line with regulatory, legislative and contractual arrangements.

4.5 Business continuity

Baringa maintains a business continuity plan for responding to emergency or other critical situations that could adversely impact services. Baringa will review and update, if necessary, its business continuity plan at least once a year.



5. Incident response and reporting

5. Incident response and reporting

This section confirms how Baringa manages its security incidents and reporting to its clients.

5.1 Security incidents

If Baringa becomes aware of a security breach Baringa shall notify the client without undue delay, and in any case, where feasible, notify the client within 72 hours after becoming aware. The Information Security Incident Management process requires (i) an incident response team to be set up with a response leader, (ii) an investigation team to contain and perform root cause analysis and identifying any affected parties, (iii) internal reporting and notification processes; documenting responsive actions and remediation plans; and (iv) a post incident review of the event.

Baringa

At Baringa, protecting the information of our clients is taken very seriously and security is integrated throughout our consulting business. Baringa has integrated security awareness embedded throughout our business and ensures we remain highly diligent, compliant with industry best practice and adaptive to changing threats. We operate a defence in depth strategy to protect all information.

Find out more about how we secure our clients' data »

We'd love to hear from you at enquiries@baringa.com or visit our website at baringa.com