IS000-Infinigate Information Security Mandate

Document type: Policy	
Author: Head of Information Security	Annual Review date: 03/06/2026
Review: Head of Information Security	Version: 1.2
Owner/Approval: CEO	

Signed: DocuSigned by: E2D3DED5C40F4CE... Klaus Schlichtherle 03-Jun-2025 | 04:12 PDT

Version	Date DD-MM-20YY	Amends	Author
0.1	14-Aug-2023	Draft for review	Bright Cyber
0.2	29-Sep-2023	Revised draft	Bright Cyber
1.0	18-Oct-2023	Baselined version	Simon King
1.1	21-NOV-2023	Update Changes	Simon King
1.2	03.06.2025	Review + Resign	Head of Information Security

Classification:

Sensitivity label

Public

Content

1. Mandate Scope and Purpose 3
1.1 Senior Management Statement 3
1.2 Scope 4
1.3 Purpose 4
1.4 Mandate Availability 4
1.5 Mandate Review 4
1.6 Mandate Violations 4
2. Mandate Statements 5
2.1 Information Security Strategy 5
2.2 Information Security Management System (ISMS) 5
2.3 Roles and responsibilities 5
2.4 Planning and Risk Management 6

1. Mandate Scope and Purpose

1.1 Senior Management Statement

Our information security policies and the associated document framework are the cornerstone of Infinigate's ongoing commitment to develop and continually enhance and improve our information security posture and practices. It has, in consequence, my full support and I ask that all Infinigate employees ensure they read and adhere to all policies, and any supporting standards and/or guidelines.

As a cyber security powerhouse with vast ambition and potential, our approach to information security demonstrates to our clients and broader stakeholders the professionalism and corporate values by which we conduct ourselves. We therefore have both a legal and professional duty to ensure that the information we hold conforms to the core security principles of confidentiality, integrity and availability.

As such Infinigate will ensure that our information, or that for which we are custodians are safeguarded from unauthorized disclosure, are kept accurate and are available to those authorized to access it.

1.2 Scope

This Information Security Mandate and the Information Security Management System (ISMS) is applicable to all employees, partners, vendors and contractors working in, or on behalf of Infinigate.

1.3 Purpose

This Information Security Mandate describes the requirements by which Infinigate will develop, implement and maintain its Information Security Management System (ISMS) in line with all applicable legislation, regulation or in line with any relevant industry best practice or certification.

1.4 Mandate Availability

This Policy will be made available to all relevant parties.

- Internally: Electronic copies will be made available to all employees.
- Externally: Electronic copies will be made available to external parties ONLY on a need-to-know basis.

1.5 Mandate Review

This Policy will be reviewed at least yearly or upon significant change to business processes and procedures.

1.6 Mandate Violations

Violations of this Policy will be subject to disciplinary action, up to and including termination of employment subject to local jurisdiction and regulations. In all cases, any use of information systems must be carried out in accordance with the law of the country from where the information is owned.

2. Mandate Statements

2.1 Information Security Strategy

Senior management will make available an Information Security Strategy which:

- demonstrates leadership and commitment to the ISMS. The strategy will demonstrate that information security objectives are established and complement the strategic direction of the organisation;
- makes available resources needed for the ISMS to operate effectively;
- ensures that the information security management system can achieve its intended outcomes;
- establishes information security objectives;
- prevents, or reduces, undesired effects;
- achieves continual improvement.

2.2 Information Security Management System (ISMS)

Infinigate will establish, implement, operate, monitor, review, maintain, and update, as needed, an ISMS to protect its Information.

The ISMS will include a comprehensive set of policies, procedures, standards and guidelines to support the information security requirements, with a focus on the most critical assets. These will be appropriate to Infinigate's business objectives; be made available as documented information; be communicated within the organization and made available to interested parties as appropriate.

The ISMS will be developed to allow flexibility to ensure adherence to local legislation, regulation and client requirements where necessary.

The ISMS is based on the relevant elements of the ISO/IEC 27001 Standard, which: embodies internationally recognized set of security Controls.

Where applicable, other security standards or standardized security controls will be incorporated based upon business requirements whilst maintaining the effectiveness of the ISMS.

Provision will be made for reporting the performance of the ISMS to senior management and the reporting of information security risks.

2.3 Roles and responsibilities

Infinigate Senior Management will:

- remain accountable for information security within the business;
- act as the highest business authority for information security decision making and risk acceptance;
- establish a cross-functional, Information Security Forum (ISF) or its equivalent to oversee the Information Security Management System and its effectiveness;

- ensure that person(s) undertaking work that affects Infinigate's information security performance:
    - have their necessary competence reviewed;
    - are competent on the basis of appropriate training, education and/or experience;
    - take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;
    - retain appropriate documented information as evidence of competence.

Infinigate's Information Security Function

- shall determine:
    - the boundaries and applicability of the Information Security Management System to establish its scope;
    - interested parties (internal and external) that are relevant to the information security management system;
    - the requirements of these parties relevant to the information security;
    - information security risks relevant to Infinigate, record and continue to monitor these risks;
    - the control design and effectiveness of current operational security controls in order to assess their ability to manage risk in line with Infinigate's information security risk appetite.

2.4 Planning and Risk Management

Infinigate will determine the information security risks and opportunities by;

- establishing and maintaining an information security risk criteria that:
    - includes risk acceptance criteria; and criteria for performing information security risk assessments;
    - ensures repeated information security risk assessments produce consistent, valid and comparable results;
    - identifies the information security risk owners;
    - analyses the information security risk along with potential consequences and probability of the risk materialization;
    - prioritizes analysed risks for risk treatment.

- defining information risk and applying an information security risk treatment process to:
    - select appropriate information security risk treatment options;
    - determine controls necessary to implement the chosen risk treatment option;
    - identify owners responsible for risk treatment.