# Information Security Management System (ISMS)

| Version | Date | Author | Changes |
|---|---|---|---|
| 01 | 25 July 2018 | David Howorth | New policy |
| 02 | 21 September 2018 | Eliot Benzecrit | Added versioning controls |
| 03 | 12 December 2018 | David Howorth | Added reference to our Information Security Policy and added our neighbouring businesses and landlord as interested parties. Also deleted appendix so we just have the standalone organisation chart. |
| 04 | 26 April 2019 | David Howorth | Added to communication to reflect our weekly Thursday catch-ups where ISMS concerns are raised and discussed. |
| 05 | 4 July 2019 | Eliot Benzecrit | Added quarterly training sessions |
| 06 | 26 August 2019 | Eliot Benzecrit | Updated Management Action log appraisal from biannual to quarterly |
| 07 | 15 January 2021 | Eliot Benzecrit | Updated plan-do-check model |
| 08 | 30 March 2021 | David Howorth | Updated legislation |
| 09 | 31 March 2022 | David Howorth | Added greater interested parties / external factors |
| 10 | 20 February 2024 | Eliot Benzecrit | Reviewed and updated legislation during management reviewing meeting |
| 11 | 25 February 2025 | Marharyta Mohylova | Document has been consolidated with business management system |

# Table of Contents

# 1. PLAN-DO-CHECK-ACT

1.1.1. At Avvoka, we adhere to the plan-do-check-act model when it comes to thinking about information security and business risk

## 2. Introduction

2.1.1. This document is the Information Security Management System Policy (the Policy) of Avvoka Limited, which, for the purpose of this Policy, will be referred to as 'Avvoka'.

2.1.2. The Policy is the property of Avvoka and is a controlled document.

2.1.3. The purpose of the Policy is to provide an overview of Avvoka, the activities it carries out, and the ISMS standards of operation it conforms to.

2.1.4. It is not designed to act as a procedures manual, although it does carry information about where procedures information is located and the detailed information on documentation requirements for the procedures required by the respective standards.

2.1.5. This Policy is designed to meet the requirements of ISO 27001 and applicable regulations, standards, and frameworks as regards information security and data protection defined in this document.

2.1.6. For the purposes of this Policy:

- the Managing Directors are David Howorth and Eliot Benzecrit
- the Cybersecurity Manager is Marharyta Mohylova.

## 3. The issue status

3.1.1. The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this Policy.

3.1.2. When any part of this Policy is amended, a record is made in the Amendment Log on the first page of this document.

3.1.3. The Policy can be fully revised and re-issued at the discretion of the Management Team.

# 4. Information Security Management System Policy

## 4.1. ISMS Policy

4.1.1. It is the policy of Avvoka to maintain an Information Security Management System ("**ISMS**") designed to meet the requirements of ISO 27001 in pursuit of its primary objectives, the purpose and the context of the organisation. Avvoka has also created another standalone document called the 'Information Security Policy' which provides an overview of our information security procedures, rules, and implemented controls.

4.1.2. It is the policy of Avvoka to:

- make the details of our Policy known to all other interested parties, including external, where appropriate, and determine the need for communication and by what methods relevant to the ISMS;
- comply with all legal requirements, codes of practice, security and privacy standards and best practices, and all other requirements applicable to our activities; therefore, as a company, we are committed to satisfying applicable requirements related to information security and data protection and the continual improvement of the ISMS;
- provide all the resources of equipment, trained and competent staff, and any other requirements to enable these objectives to be met;
- ensure that all employees are made aware of their individual obligations in respect of information security and data protection;
- maintain an ISMS that will achieve these objectives and seek continual improvement in the effectiveness and performance of our ISMS based on Risk Assessment results and established KPIs.

4.1.3. This ISMS Policy provides a framework for setting, monitoring, reviewing, and achieving our objectives, programmes, and targets.

4.1.4. To ensure the company maintains its awareness for continuous improvement, the ISMS is regularly reviewed by the Managing Directors and Cybersecurity Manager to ensure it remains appropriate and suitable for our business. The ISMS is subject to both internal and external annual audits.

## 4.2. The Scope of the Policy

4.2.1. The scope of this Policy relates to the use of the database and computer systems operated by the company in pursuit of the company's business of providing software services to in-house legal teams and law firms. It also relates, where appropriate, to external risk sources, including functions that are outsourced.

# 5. Context of the organisation

## 5.1. Overview of the organisation

5.1.1. Avvoka is an end-to-end contract creation, live-negotiation, and analytics tool, founded in 2016 by two former corporate solicitors to bring efficiency to the way in-house legal teams and law firms contract on standard terms. The business serves clients globally, with an emphasis on Europe, the United States, and the Asia-Pacific region.

## 5.2. Scope of registration

5.2.1. Avvoka Limited is located in London, England, and develops and licenses legal document automation software and accompanying consultancy services to companies in any industry.

## 5.3. Functions

5.3.1. Avvoka consists of the following organizational functions:

- Customer Success (Sales Development, Customer Success, Product Management, Account and Business Development)
- Customer Support
- Executive Leadership (Executive Management)
- Growth (Sales Development, Growth Executive, Creative Management)
- Information Security (Cybersecurity Management, Cybersecurity Analysis)
- Legal (In-house legal support)
- Marketing (Creative Management, Legal Content Strategy)
- People (People Operations)
- Product (Product Management)
- Quality Assurance (Quality Assurance, Software Development)
- Tech (IT Project Management, Backend Software Development, Frontend Software Development, Editor Software Development, UI/UX Design, Server Infrastructure support).

## 5.4. Products & Services

5.4.1. Avvoka offers the following products & services to its customers:

- Avvoka “Core: - its “no-code” document automation software application that’s used by lawyers and business personnel.
- Massdraft – its mass-document-generation software application, used for volume document creation exercises and those that require e-signature.
- Professional Services – on occasion, Avvoka will assist clients with the automation of their legal documents, as well as perform integration and development services, for a fee.

## 5.5. Potential impact of an information security incident or business disruption

5.5.1. The impact of any specific incident will obviously depend upon its nature and the criticality of the asset. Thus, a comprehensive risk assessment is maintained to assess and mitigate the risks that can be reasonably identified. The potential impact of an inability to perform normal business processes and/ or compromising information security will be shown in one or more of the following key areas:

- Reputation
- Financial viability
- Product or service quality
- Staff well-being
- Legal or regulatory requirements
- Contractual obligations.

Categories of potential impact, as indicated above, cover different key business activities Avvoka performs.

# 6. Objectives

## 6.1. Objectives statement

6.1.1. We aim to provide a professional and ethical service to our clients that conforms with security and privacy requirements and best practices. In order to demonstrate our intentions, the Managing Directors will analyse customer feedback data, internal performance data, financial performance data, ISMS performance data, and business performance data to ensure that our objectives are being met.

## 6.2. Information Security objectives

6.2.1. Each department is responsible for delivering its objectives, and this is monitored via individual appraisals and team meetings. Avvoka's general/ strategic ISMS and business management objectives are as follows:

- Objective 1: Existing services - Avvoka will continue to deliver its services within a secure environment, keeping the service level and product quality at the highest
- Objective 2: Development - Avvoka will conduct annual risk assessments to ensure that the risk to information in the care of Avvoka is minimised or eliminated.
- Objective 3: Reputation – Avvoka shall perform its best efforts to maintain customers' trust and the company's good reputation
- Objective 4: Finance – Avvoka adheres to minimizing loss of revenue, where possible
- Objective 5: Compliance – Avvoka follows applicable regulations and security best practices and standards to ensure its compliance with security and privacy standards.

6.2.2. Whilst the above company objectives are "high-level", we have further analysed and categorised these into our 'Context, Risk, Opportunities and Objectives' Matrix (CROO). In some cases, this may allow for specific objectives being set across different functions. Some of these other objectives are as follows:

- Continue to meet legislative requirements surrounding GDPR.
- Continue to meet ISO27001 requirements.
- Minimise the risk of hardware/software being compromised by common security threats and vulnerabilities.
- To ensure that the security documentation cycle is consistent, robust, and formal.

- To ensure that clients' data and information are maintained in the most secure way and are not compromised.
- To ensure that team training on information security and personal data protection is robust and reflects the current trends of the topic.
- To ensure we are aware of the possible business disruption scenarios, our critical business activities are identified, and a business continuity plan is duly established and tested regularly
- Conduct an efficient incident management procedure
- Address supply chain security
- Continuous improvement of security controls
- Ensure robust access control and identity management
- To ensure the secure, thoughtful, and compliant integration of AI technologies into Avvoka’s business processes, products, and services.

Where applicable, we have mapped the ISMS objectives against KPIs, and these can be found within a separate tab in the 'CROO' document.

# 7. Requirements of the Interested Parties

## 7.1. Understanding legal and regulatory requirements

7.1.1. This section of the Policy sets out the interested parties that are relevant to ISMS and the business management system, and their requirements. It also summarizes the applicable legal and regulatory requirements to which Avvoka subscribes.

7.1.2. An interested party is defined as “a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity”.

7.1.3. Applicable legal and regulatory requirements arise from the following:

| Legislation/Regulatory Compliance | Link |
|---|---|
| General Data Protection Regulation (GDPR) | https://gdpr-info.eu/ |
| Data Protection Act 2018 | https://www.legislation.gov.uk/ukpga/1998/29/contents |
| Electronic Communications Act 2000 | https://www.legislation.gov.uk/ukpga/2000/7/contents |
| Electronic Signature Regulations 2002 | http://www.legislation.gov.uk/uksi/2002/318/contents |
| Bribery Act 2010 | https://www.legislation.gov.uk/ukpga/2010/23/contents |
| Companies Act 2006 | http://www.legislation.gov.uk/ukpga/2006/46/contents |
| Employment Act 2002 | http://www.legislation.gov.uk/ukpga/2002/22/contents |
| Management of Health and Safety at Work Regulations 1999 | https://www.legislation.gov.uk/uksi/1999/3242/contents |
| The Workplace (Health, Safety and Welfare) Regulations 1992 | https://www.legislation.gov.uk/uksi/1992/3004/contents |
| Health and Safety (Display Screen Equipment) Regulations 1992 | https://www.legislation.gov.uk/uksi/1992/2792/contents |
| Provision and Use of Work Equipment Regulations 1998 | https://www.legislation.gov.uk/uksi/1998/2306/contents |
| Reporting of Injuries, Diseases and Dangerous | https://www.legislation.gov.uk/uksi/2013/1471/contents |

| Legislation/Regulatory Compliance | Link |
|---|---|
| Occurrences Regulations 2013 | |
| Employment Rights Act 1996 | https://www.legislation.gov.uk/ukpga/1996/18/contents |
| Employment Relations Act 1999 | https://www.legislation.gov.uk/ukpga/1999/26/contents |
| Working Time Directive 1999 | https://www.legislation.gov.uk/uksi/1999/3372/contents |
| National Minimum Wage Act 1998 | https://www.legislation.gov.uk/ukpga/1998/39/contents |
| The Equality Act 2010 | https://www.legislation.gov.uk/ukpga/2010/15/contents |
| The Maternity and Parental Leave etc. Regulations 1999 | https://www.legislation.gov.uk/uksi/1999/3312/contents |
| Part-Time Workers (Prevention of Less Favourable Treatment) Regulations 2000 | https://www.legislation.gov.uk/uksi/2000/1551/contents |
| The Climate Change Act 2008 (2050 Target Amendment) Order 2019 | https://www.legislation.gov.uk/uksi/2019/1056/contents/made |
| The Waste Electrical and Electronic Equipment Regulations 2013 | https://www.legislation.gov.uk/uksi/2013/3113/contents |
| EU AI Act | https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng |
| ISO 27001 | https://www.iso.org/standard/27001 |
| California Consumer Privacy Act 2018 | https://oag.ca.gov/privacy/ccpa |
| Digital Personal Data Protection Act 2023 | https://dpdpa.in/ |
| New York SHIELD Act 2019 | https://www.nysenate.gov/legislation/bills/2019/S5575 |
| Privacy Act 1988 | https://www.legislation.gov.au/Details/C2021C00139 |
| Privacy and Other Legislation Amendment Act 2024 | https://www.legislation.gov.au/C2024A00128/asmade/text |

| Legislation/Regulatory Compliance | Link |
|---|---|
| Personal Data Protection Act 2012 | https://sso.agc.gov.sg/Act/PDPA2012 |
| Data Protection (Bailiwick of Guernsey) Law 2017 | https://www.odpa.gg/information-hub/the-law/ |
| Data Protection (Jersey) Law 2018 | https://www.jerseylaw.je/laws/enacted/Pages/L-03-2018.aspx |
| Illinois personal information protection act 2006 | https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702 |
| Georgia Personal Data Protection Act, 2024 | https://www.legis.ga.gov/api/legislation/document/20232024/225826 |
| Pennsylvania Breach of Personal Information Notification Act 2005 | https://www.legis.state.pa.us/WU01/LI/LI/US/HTM/2005/0/0094..HTM |

7.1.4. The Managing Directors are both solicitors and regularly review statutory and regulatory guidance relating to the company's business activities to check for ongoing legal compliance and relevance.

## 7.2. Understanding the needs and expectations of interested parties

| Interested Parties | Interested parties' needs and expectations | Avvoka's expectations |
|---|---|---|
| Directors | Ensure that the business continues to function in a profitable manner without hindrance, bureaucracy or disruptions | All necessary resources, equipment and budgets are allocated and provided |
| Personnel (employees and contractors) | Ensure Avvoka provides safe and healthy working environment, up to date awareness trainings on information security and data | Ensure they acknowledge, understand and follow Avvoka information security and privacy policies and procedures and take responsibility to comply with |

| Interested Parties | Interested parties' needs and expectations | Avvoka's expectations |
|---|---|---|
| | protection as well as training on emergency procedures | them<br>Ensure that all necessary trainings are completed within the prescribed terms<br>Ensure timely and quality completion of the assigned tasks<br>Working safely and secure |
| Clients | Ensure they are provided with the best quality service which is timely delivered and understand the processes that Avvoka follow in delivering that service.<br>Ensure that high standard customer support is provided, and any feedback is taken into consideration.<br>Ensure they are provided with uninterrupted services and that we and our service providers have efficient business continuity and disaster recovery procedures, which cover, inter alia, disruptions due to climate change and environmental disasters | Payments for our services are conducted in a timely and agreed manner.<br>Contracts with clients are renewed at most times. |
| End users through clients | Ensure that Avvoka products and services comply with high standards for information security and personal data protection. Ensuring no data is leaked or corrupted, including, due to environmental changes events | No major complaints about Avvoka services and products are received |
| Suppliers | Ensure the suppliers are timely paid for the services/ products as well as their services/ products are | Ensure they understand the procedures and processes contained in this manual and |

| Interested Parties | Interested parties' needs and expectations | Avvoka's expectations |
|---|---|---|
| | used in accordance with terms of use and concluded contracts (including, but not limited to secure usage requirements). Ensure we adhere to and comply with applicable personal data protection requirements when processing of personal data within the service/ product takes place. | take responsibility to comply with them to the extent necessary |
| Accountants | Ensure compliance with applicable laws, regulations and accounting standards | Ensure they maintain confidentiality, integrity and availability of Avvoka financial information, adhere to applicable legal and regulatory standards, promptly notify Avvoka of any security or data breaches involving Avvoka data, and fulfil of SLAs and contractual obligations. |
| Neighbouring businesses | Ensure we understand the need for integrity when operating within a shared working space. We have mutual duties to not act upon anything we hear or see that might threaten information security policies and procedures. | Ensure they understand the need for integrity when operating within a shared working space. We have mutual duties to not act upon anything we hear or see that might threaten information security policies and procedures. |
| Landlord | Ensure we are complaint with their own information security policies and procedures, physical security rules, lease terms and safety policies. We have to use the shared facilities in a proper way. | Ensure only authorized personnel can access our space and that our information is protected from other tenants. Ensure that they provide reliable utilities and services (power, internet, etc.) within the facility, |

| Interested Parties | Interested parties' needs and expectations | Avvoka's expectations |
|---|---|---|
| | | provide physical protection to the space. |
| Avvoka PTE Ltd (Singapore marketing / sales subsidiary of Avvoka Limited) | Ensure that the working environment is safe and healthy, as well as all necessary working equipment is provided. Ensure that this subsidiary is duly aligned with the strategies and policies of Avvoka, provided with up-to-date awareness trainings on information security and data protection as well as training on emergency procedures | Ensure they acknowledge, understand and follow Avvoka information security and privacy policies and procedures and take responsibility to comply with them<br>Ensure that all necessary trainings are completed within the prescribed terms<br>Ensure timely and quality completion of the assigned tasks<br>Working safely and secure<br>Ensure new customers are engaged |
| Legal technology community | Ensure that they have a positive perception of the company as a market-leading tool that can be trusted | Ensure we follow the trends in the domain of legal technology to provide our customers and with the highly competitive solution (including, but not limited to security and privacy trends) |
| Investors and shareholders | Ensure that value of share price is duly maintained. Ensure that Avvoka has clear strategies for information security, business management, and environmental footprint reducing as well as that any identified risks associated with information security, business health and climate change are duly mitigated. | Keeping investors and shareholders aligned with our business and growth strategy<br>Involving new investors and shareholders |

| Interested Parties | Interested parties' needs and expectations | Avvoka's expectations |
|---|---|---|
| Insurance company | Insurance providers may impose certain requirements or stipulations that affect our information security policies and external contracts | Our insurance providers shall have sufficient coverage for security incidents and our business resilience |
| National or local government organizations | Remain compliant with national and local legislation requirements | Obtaining support and protection in case Avvoka's rights are infringed |
| Information Commissioner's Office | Ensure that we adhere to applicable data protection legislation when processing personal data during our business activities<br>Ensure that data breaches are reported to ICO within the prescribed timeframes (where such reporting is required by the law) | No notices/ fines are received by Avvoka |
| International Standards Organisation | N/A | Avvoka should constantly monitor and implement the latest security and personal data protection standards applicable to its activities |
| British Assessment Bureau | As our external auditor, the company's implementation of the ISO27001 make them an interested party<br>Avvoka should ensure that it provides all necessary evidence and documentation during the audit | Obtaining renewed ISO27001 certificate |

## 7.3. Internal issues

7.3.1. With regards to Avvoka's business itself, there are a number of internal issues and factors that may create uncertainty and give rise to risk. These include:

| Internal factors | Information Requirements |
|---|---|
| Avvoka expansion | Company growth and expansion of the geographies of its activities lead to the need for broadening of personnel geography. This pose additional legal obligations to Avvoka which should be duly addressed |
| Corporate changes | Rapid changes in organizational structure may make be confusing for new personnel and/ or customers as well as there can be misunderstanding in corporate functions and roles within the organization |
| Internal documentation management | Although Avvoka takes due care for maintenance of its policies, some processes within the company are formalized at a high-level lacking detail. Avvoka undertakes to improve its internal policies and procedures |
| Contractual relationships and undertaken obligations | As the quantity and quality of the Avvoka customers constantly grows, Avvoka undertook a big number of contractual obligations that should be monitored for the performance and non-breach. The customers that demand an individual approach expanding their requirements beyond standard Avvoka terms and conditions pose additional challenge to Avvoka operations, which should be duly addressed without disruptions in Avvoka's daily operations |
| Technology development | Avvoka's product and services are constantly developing having new functionalities, improvements and changes. Those should be duly maintained and addressed by the qualified personnel to ensure that the changes in the product do not disrupt its overall functionality |
| Asset management | Although Avvoka has the process for asset management and maintains asset register, fast changes and replacements of the assets are not always reflected in the register timely. Avvoka |

| Internal factors | Information Requirements |
|---|---|
| | needs to pay more attention to the maintenance of its asset register up to date |
| Energy use | The energy consumption associated with our technology infrastructure, including remote work devices, contributes to our overall environmental impact. As part of our information security practices, we aim to ensure that our use of energy is optimized, and our personnel adheres to energy-efficient practices when working remotely. |

## 7.4. Other external factors

7.4.1. In addition to the legal, regulatory factors and interested parties, the Managing Directors also consider that the following factors impact the context of the organisation:

| External factors | Information Requirements |
|---|---|
| Current political landscape and agenda | Impacts such as Brexit, data regulation and tax incentives will all impact our ability to continue to grow operations or may cause us to require more FTE to continue servicing our current client base |
| Customer demand | Our ability to continue to finance operations is directly related to customer demand for automation projects in the delivery of legal advice |
| Cyber crime | More sophisticated cyber criminals continue to pose a threat to the data held in our software and business tools. Vigilance on latest attack techniques is therefore crucial |
| Economic climate | Inflation is causing an increase in business costs across the organisation. We need to continue to invest in information security and business resilience practices despite increased running costs |
| Legal innovation | The legal industry is continuing to slowly evolve in its thinking. They are a key client of ours and therefore our business success depends on their ability to evolve |

| External factors | Information Requirements |
|---|---|
| Sustainability | Sustainability is a key driver for all businesses and individuals. We must make sure we balance sustainability with the need to be information security conscious |
| Regulatory changes | The regulatory requirements and laws are dynamic and changing constantly, especially in IT field. Avvoka should monitor the changes in applicable regulations constantly to ensure its uninterrupted compliance |
| Technology | IT trends are changing very fast, especially with the AI and quantum technologies evolving. To be a leader in the market, Avvoka must track the trends and implement the new technologies and features in its product as well as to modernise its security controls in accordance with the new risks which such technologies pose |
| Environmental risks and Climate change | Extreme weather events such as storms, floods, or heatwaves have some probability to cause disruptions to the Avvoka services, potentially leading to data loss, downtime, or service interruption. Thus, those implications should be considered in Avvoka's business continuity and disaster recovery program. |

## 7.5. Determining the scope of the ISMS (ISO 27001)

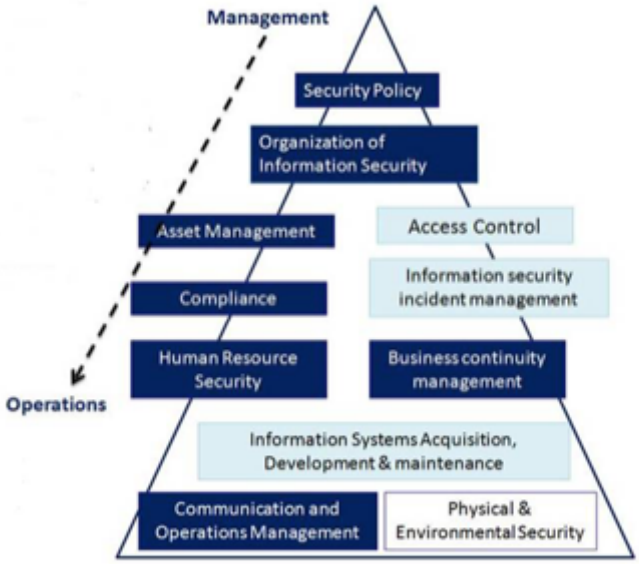
7.5.1. The scope of the system covers all the core and supporting activities of the company as well as all products and services it provides to the clients. The activities and arrangements of all personnel including any sub-contractors also fall within the scope of the system.

7.5.2. The defined scope of ISMS considers the internal and external issues listed in this document as well as requirements of the interested parties. It also reflects the needs and expectations of the interested parties as well as the legal and regulatory requirements that apply to Avvoka.

7.5.3. Our marketing subsidiary in Singapore, Avvoka PTE Limited, is excluded from the scope of ISMS, though our sole employee there has been detailed within our relevant documentation for best practice purposes.

## 7.6. Information Security Management System

7.6.1. The organisation has established, implemented, maintained, and will continually improve an ISMS in accordance with ISO 27001. This Policy provides information as to how we meet these requirements, with reference to key processes and policies, as appropriate.



# 8. Leadership

## 8.1. Leadership and Commitment

8.1.1. Avvoka's Managing Directors are committed to the development and implementation of an ISMS Policy and the ISMS, which is compatible with the organisation's strategy, and the whole system is frequently reviewed to ensure conformance to ISO 27001.

8.1.2. The Managing Directors will ensure that Avvoka staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving Avvoka's Information Security Policy and objectives, which are aligned with the organisation's strategic direction.

8.1.3. The Managing Directors are responsible for implementing this system and ensuring the system is understood and complied with at all levels of the organisation.

8.1.4. In summary, the Managing Directors will ensure that:

- The company has a designated Cybersecurity Manager who is responsible for the maintenance and review of the ISMS.
- The ongoing activities of Avvoka are reviewed regularly, assessed against possible risks and disruptions, and any required corrective action is adequately implemented and reviewed to establish an effective preventative process.
- Measurement of performance against declared ISMS objectives is undertaken.
- Resources needed for the ISMS management are assigned, and employees have the necessary training, skills, and equipment to effectively carry out their work in conformity with ISMS requirements.
- Internal audits are conducted regularly to review progress and assist in the improvement of processes and procedures.
- Objectives are reviewed and, if necessary, amended at regular Management Review meetings, and the performance is communicated to stakeholders.
- The ISMS Policy and its objectives are established in line with the strategic direction of the organisation, and that the intended outcome(s) are achieved.
- The ISMS is integrated into the organisation's business processes.
- Continual ISMS improvement is planned and performed.

- The contribution of persons involved in the effectiveness of the ISMS is achieved by engaging, directing, and supporting persons and other management roles within their area of responsibility.

## 8.2. Organisational roles, responsibilities, and authorities

8.2.1. Avvoka has an organisation chart in place, which is contained within a further standalone document, employee contracts, together with job descriptions, to ensure that the appropriate personnel are in place to cover the whole context of the organisation and strategy of the business.

8.2.2. Within ISMS, the following roles should be defined and allocated:

- Managing Directors
- Data Protection Officer
- Cybersecurity Manager
- Internal Auditor
- System and application administrators
- Emergency Management Team
- Business Process Owner

There are also particular information security, data privacy, and business continuity responsibilities that must be carried out by existing internal roles within the organization. These roles are:

- Department Heads/ Team Leads
- Users

8.2.3. The responsibilities that apply to all Avvoka personnel, including sub-contractors and other interested parties, are set out within the relevant organizational policies.

8.2.4. Overall responsibility for the management of the various sections of ISMS is shown in the following RASCI matrix. It defines the type and responsibility of each role in each area according to whether the listed role is:

- R: Responsible
- A: Accountable
- S: Supporting
- C: Consulted
- I: Informed

| ISO27001 areas | MDs | DPO | CsM | IA | Admins | EMT | BPO | DHs | Users |
|---|---|---|---|---|---|---|---|---|---|
| Context of the organization | A/R | C | C | I | I | I | I | I | I |
| Leadership | A/R | R | R | I | I | I | I | I | I |
| Planning | I | C | A/R | I | C | C | S | S | I |
| Support | R | C | A/R | I | C | S | I | I | I |
| Operation | A | C | R | I | R | C | I | I | I |
| Performance evaluation | A | C | R | R | C | I | I | I | I |
| Improvement | A | C | R | R | R | C | I | S | I |
| Annex A controls | I | R | A/R | I | R | R | S | S | I |

These responsibilities and authorities are expanded on further in this section, unless they are specifically identified in the separate dedicated document.

8.2.5. Managing Directors' responsibilities:

- Establish and maintain the information security policies, objectives, and plans
- Communicate the importance of meeting the objectives and the need for continual improvement throughout the organization
- Maintain awareness of business needs and major changes
- Ensure that the information security requirements are determined and are met, minimizing the risk for Avvoka and its customers
- Determine and provide resources for the implementation and maintenance of information security throughout the organization
- Oversee the management of risks to the organization and its products/ services
- Conduct management reviews of information security at a planned schedule to ensure continuing suitability, adequacy, and effectiveness
- Select auditors and ensure that internal audits are conducted in an objective and impartial manner

- Review major information security incidents
- Ensure that relations with any external service provider who has access to the information systems of Avvoka are based on a formal agreement that defines all necessary security requirements
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel
- Creating and distributing security incident response and escalation procedures that include a formal security awareness program for all employees, which provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).

8.2.6. Cybersecurity Manager's responsibilities:

- Reporting on all security-related matters on a regular and ad-hoc basis, when required, to the Managing Directors
- Perform all actions for mitigating incidents, along with post-incident steps
- Communicate the information security policies to all relevant interested parties (where appropriate), including customers
- Managing the implementation of the requirements of the information security policies
- Managing day-to-day maintenance of security controls
- Perform all security-related assessments according to the defined schedule
- Organize and manage regular security awareness training for all personnel
- Manage risks associated with access to Avvoka services and systems
- Ensure the security controls are in place and documented
- Define improvement plans and targets, and monitor their achievement status
- Report on ISMS efficiency and improvement activities status
- Communicate with representatives of vendors who have access to Avvoka information systems on information security-related matters

8.2.7. Data Protection Officer responsibilities:

- Inform and advise the personnel who are involved in the processing of personal data, of their obligations under applicable data protection legislation
- Monitor Avvoka compliance with data protection legislation and Avvoka policies which define the requirements for protecting personal data
- Awareness-raising and training of personnel who are involved in the processing of personal data
- Provide advice when requested regarding privacy impact assessments, and monitor their performance
- Cooperate with data protection supervisory authorities

- Act as a contact point for any interested parties on privacy-related issues

8.2.8. Internal Auditor responsibilities:

- Plan and develop an internal audit schedule
- Define the internal audit criteria and scope
- Conduct internal audits according to the planned schedule
- Ensure the audit process is objective and impartial
- Report the results of internal audits to the Managing Directors
- Retain documented information as evidence of the audit results

8.2.9. System and application administrators' responsibilities:

- Monitor and analyse security alerts and information, and distribute to the appropriate personnel
- Administer user accounts and manage authentication
- Monitor and control all access to data
- Maintain a list of service providers
- Ensure that there is a process for engaging service providers, including proper due diligence before engagement

8.2.10. Business Process Owner responsibilities:

- Maintaining the continuity of the specific business process
- Maintain and review business continuity strategies and plans for the allocated processes
- Participate in security assessments concerning their process(es)
- Review the effectiveness of actions taken

8.2.11. Department Heads/ Team Leads

- Review and manage the competencies and training needs of team members to enable them to perform their role effectively within the information security area
- Ensure that team members are aware of the relevance and importance of their activities and how they contribute to the achievement of information security objectives
- Participate in and contribute to security assessments affecting their business area

8.2.12. Users' responsibilities:

- Ensure they are aware of and comply with all information security policies of the organization
- Report any actual or potential security incidents
- Contribute to security assessments where required.

# 9. Planning for the Information Security Management System

## 9.1. Actions to address operational risk and opportunities

9.1.1. Avvoka has been identifying the risks and opportunities that are relevant to our ISMS from an operational perspective during the annual risk assessment exercise. The risk assessment results are recorded in 'Context, Risk, Opportunities and Objectives' (CROO). Within each of the areas, the risks are identified together with a rating as to the importance of the risk. The associated consequences and mitigation of the risk are also noted together with any new opportunities that we have identified.

9.1.2. The controls identified in this document feed into our Statement of Applicability, which has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions. The document identifies controls to mitigate risks following the process of identification, analysis, and evaluation. The SOA document is separate from this Policy.

**Information Security Risk Assessment**

9.1.3. In accordance with our 'CROO' matrix, we are regularly performing assessments of any typical / likely Information Security threats and vulnerabilities based on their potential effects on Confidentiality, Integrity, and Availability (CIA) attributes and matching those against the probability of occurrence and impact of the risk to Avvoka. Internal and external issues are considered during the risk assessment, too.

9.1.4. Following this analysis, we define our risk mitigation strategy taking into account the existing controls for risk decreasing and the risk appetite of Avvoka.

9.1.5. Avvoka's risk management strategy is to adhere to the principles of risk management as specified in ISO31000 standard (Risk management – principles and guidelines), so that Avvoka's risk management:

- Creates and protects value
- Is an integral part of all organizational processes
- Is part of the decision-making
- Explicitly addresses uncertainty
- Is systematic, structured, and timely
- Is based on the best available information
- Is tailored
- Takes human and cultural factors into account
- Is transparent and inclusive

- Is dynamic, iterative, and responsive to change
- Facilitates continual improvement of the organization

These principles will also be applied to the management of risk with respect to the business continuity of the organization.

**Information Security Risk Treatment**

9.1.6. The approach to our risk treatment plan has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – Control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions.

9.1.7. The document identifies controls to mitigate risks following the process of identification, analysis, and evaluation, and is directly linked to the aspects of the organisation.

9.1.8. The SOA document is separate to this Policy and conforms to the requirements as defined within clause 8.3 of the ISO 27001 standard.

9.1.9. The detailed process of Avvoka's risk management is outlined in Risk Management Methodology.

# 10. Support

## 10.1. Resources

10.1.1. Avvoka determines and provides the resources needed for the establishment, implementation, maintenance, and continual improvement of the ISMS.

10.1.2. Avvoka ensures that the following elements are taken into account when completing an evaluation:

- the capabilities of, and constraints on, existing internal resources; and
- information needed to be obtained from external providers.

## 10.2. Competence

10.2.1. All employees have the training and skills needed to meet their job requirements. All employees are monitored on an ongoing basis to identify any training and development needs. Competences and training needs are identified / satisfied by using:

- Job descriptions that set out the competencies required
- Contracts of employment that set out contractual and legal requirements
- Induction checklists to ensure / check understanding
- Appraisal reviews to monitor performance
- Development plans to set objectives
- On the job reviews to ensure / check levels of competence
- Tests of understanding

## 10.3. Awareness

10.3.1. Avvoka ensures that all employees are aware of all policies, information security, and privacy requirements, and their contribution to the effectiveness of the ISMS through:

- Induction
- Company messaging systems (Slack)
- Training sessions that cover the changes made to the Information Security Policy and processes, and refresher sessions on key policies and standards
- Annual Information security and privacy awareness online training.

## 10.4. Communication

10.4.1. For internal staff on the company's SharePoint, the Slack noticeboard is a source of information and is updated regularly to ensure that all information is correct. This is accessible to all staff.

10.4.2. For external persons, the https://avvoka.com is a source of information and is updated regularly to ensure that information is up-to-date.

## 10.5. Documented Information

### General

10.5.1. Avvoka demonstrates documented compliance with ISO 27001 through this ISMS Policy (which includes processes and procedures) and is distributed to all Avvoka employees on joining and is available in the "Information Security" sub-folder within "Compliance" on Avvoka's SharePoint folder system. All information is read-only and only accessible via the document owner for amendment.

### Creating and updating

10.5.2. The creation of documentation to support the ISMS is primarily the responsibility of the designated Cybersecurity Manager. The designated person is responsible for documents accuracy, relevance, and compliance with applicable standards and regulations.

10.5.3. When creating the information security documentation, the relevant stakeholders may be engaged based on the defined needs of Avvoka's ISMS. These include, but are not limited to, security policies, procedures, guidelines, manuals, etc.

10.5.4. When created, every ISMS document shall be clearly identified with a document title that reflects the document content, document version number, its creation date, and the author. Each ISMS document shall also include change log records that specify the date of change, its author, and a brief description of the amended content, along with the new versioning number.

10.5.5. Information security documents shall contain a clear description of their purpose and scope, as well as the intended audience.

10.5.6. Created or changed documents shall undergo a formal review and approval by the Managing Directors before the documents are finalized. To aid the approval and suitability of documents, the Managing Directors authorise the release and delegate any training required to the Information Security team.

10.5.7. Documents shall be reviewed on an annual basis or whenever there are significant changes in Avvoka processes, applicable legal or regulatory requirements, or threat landscape.

10.5.8. All ISMS documentation shall be drafted in English and stored in electronic format unless there is a critical need for having a hard copy of the document in the predefined office locations. If the document is stored in a hard copy, it should be specifically stated so in the document in question, identifying the location of such storage.

**Control of documented information**

10.5.9. All documentation is controlled by version and date and is listed on a “Master Document List”.

10.5.10. Control of documents can be seen on the Master Document List and encompasses the following elements:

- Distribution, Access, Retrieval, and use
- Storage and preservation, including preservation of legibility
- Control of changes (e.g. version control)
- Retention and disposition

10.5.11. Documents can be accessed by authorised personnel via the “Compliance” section on Avvoka’s SharePoint folder system. Customer records are identified by *customer name* within the “Customers and Partners” folder of SharePoint. By default, the access level is “view only”, and the “editing” level is provided only to the document owners/ authorized stakeholders.

10.5.12. On or after the retention period stated, the relevant records will be reviewed by the Managing Directors and will either remain in-situ, be archived, or destroyed.

10.5.13. If records are to be destroyed, they will be disposed of in a controlled manner; *sensitive hard copies will be shredded, and soft copies will be deleted from the system*. If records are to be archived, they will be identified and stored appropriately.

# 11. Operation

## 11.1. Operational planning and control

11.1.1. Avvoka has determined the requirements and controls implemented for all processes needed to meet information security requirements and has implemented the actions described in this Policy. Avvoka will also implement plans to achieve ISMS objectives, as highlighted in section 6.2 of this Policy. Avvoka retains documented information to the extent necessary to have confidence that the processes have been carried out as planned. Avvoka shall control any planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects.

11.1.2. Avvoka's regular Information Security Risk Assessment is also a part of operational planning and control, as during this exercise, Avvoka defines the mitigation strategies to be performed and/or controls to be implemented before the next cycle of the Risk Assessment starts. Documented information on the results of risk assessments, including chosen risk mitigation strategies, is retained. More detailed information on the risk assessment process is incorporated in Section 9 of this Policy.

# 12. Performance Evaluation

## 12.1. Monitoring, measurement, analysis, and evaluation

12.1.1. Avvoka is committed to regularly evaluating the performance of ISMS to make sure it remains effective, efficient, and aligned with Avvoka's business and security objectives. Evaluation is based on monitoring and measurement of ISMS objectives, assessment of the information security risks, results of performed internal audits, results of external audits, and regular management reviews.

12.1.2. Avvoka establishes measurable information security objectives, which are periodically reviewed as to their relevance and adequacy. The objectives, their key performance indicators (KPIs), and metrics are defined and recorded in the CROO document. The objectives are tracked within the information security activities performed, and their progress is monitored and reported to the Managing Directors.

## 12.2. Internal Audit

12.2.1. An internal audit schedule is prepared on an annual basis and covers the requirements of the ISO 27001 standard, Avvoka's information security policies, and other relevant applicable standards or regulations (if any). Internal audits are carried out through "risk or clause-based" auditing.

12.2.2. Appropriate personnel are allocated to complete the internal audits and must record appropriate evidence for completeness. All audits completed must be authorised by the Managing Directors as complete, provided any non-conforming areas have been dealt with (according to the defined schedule, but in any case, without any undue delay). Internal audit documentation must be kept and filed appropriately.

## 12.3. Management Review

12.3.1. Management reviews take place on an annual basis. The attendees present are the Managing Directors, Cybersecurity Manager, and any other appropriate persons of the business. During these reviews, Managing Directors will review the audit findings, risk assessment results, and KPI performance of ISMS, as well as any corrective actions, to ensure informed decision-making. During the management review, decisions will be made regarding the allocation of resources, potential adjustments to the ISMS, and improvements in the overall information security posture.

12.3.2. All inputs / outputs are fully documented and minuted in line with the requirements of ISO 27001. Any actions arising from the meeting must be completed in accordance with the agreed schedule and, in any case, without any undue delay, and appropriate evidence filed with the Management review documentation.

12.3.3. A summary of performance evaluations will also be communicated to relevant stakeholders within Avvoka to maintain awareness of the ISMS's effectiveness and alignment with security objectives.

# 13. Improvement

## 13.1. Nonconformity and corrective action

13.1.1. Should a nonconformity occur, including those arising from complaints, risk assessments, internal audits, and external third-party assessments, Avvoka will designate the appropriate Cybersecurity Manager to ensure that corrective action, including root cause analysis, is completed and implemented to avoid any further occurrences.

13.1.2. Should any non-conformances occur or be identified, then an internal audit report / non-conformance report must be completed to ensure that a full analysis of the problem is resolved. A summary of all actions will be maintained within the Management Action Log (CAPA LOG). The management action log must now be appraised quarterly as opposed to just in the biannual management reviews.

13.1.3. The corrective action plan summary must be completed, as this then forms part of the Management Review meeting.

## 13.2. Continual Improvement

13.2.1. The results of the performance evaluation will be duly taken into consideration in the framework of the continual improvement process for Avvoka's ISMS.

13.2.2. Opportunities for improvement will be identified, and action plans will be developed and implemented as the next stage of the performance evaluation process.

13.2.3. Continual Improvement will be ongoing through various elements of the ISMS, which is encompassed within this document. The list below is not exhaustive:

- CROO Document
- ISMS Policy / Objectives
- Internal Audits
- Third-Party External Audits
- Management Review