ISMS Information Security and Privacy Manual

Taboola

Table of Contents

1. Introduction..... 3
2. Scope..... 3
3. Terms and definitions..... 4
4. Context of the organization..... 5
5. Leadership..... 9
6. Planning..... 12
7. Support..... 18
8. Operation..... 22
9. Performance evaluation..... 23
10. Improvement..... 25
11. Asset management..... 27
12. Secure area..... 27
13. Information security incident management..... 28
14. Business continuity management..... 29
15. Compliance..... 29
16. Security in development and support processes..... 30

1. Introduction

The upper management of Taboola has adopted a framework for the implementation of policies and procedures relating to the Information Security and Privacy Management System based on ISO27001 and ISO27701.

This manual explains Taboola's approach to information security and privacy and contains the relevant Management Policy Statement applicable per Annex A of ISO 27001:2022 and as identified in Taboola's Statement of Applicability, which is contained in a separate document.

2. Scope

Taboola management will maintain its competitive edge through a commitment to preserving the confidentiality, integrity and availability of all the physical and logical information assets throughout its IT operations. Information security requirements are aligned continually with management goals, and the ISMS provides an enabling mechanism for information sharing, IT operations, and the reduction of information-related risks to acceptable levels.

Every Taboola employee is expected to comply with this policy and with the Information Security Management System (ISMS) that implements this policy. This includes external parties.

The following material describes the foundation of information security policy:

Preserving

Management, all full-time or part-time staff, sub-contractors, project consultants, and any external parties, must be made aware of their responsibilities as defined in their job descriptions or contracts to preserve information security, report security breaches, and act in accordance with the requirements of the ISMS. All staff will receive information security awareness training, and more specialized staff will receive appropriately specialized information security training based on their job description and function. The Human Resources (HR) department is tasked with responsibility for security policy violations.

The physical assets

The physical assets of the organization include but are not limited to computer hardware, PCs, laptops, mobile phones, telephone systems, Wi-Fi routers, physical data files, and hosting facilities. All Taboola-managed offices are also considered physical assets. These include

- Israel, UK, US, India and Bangkok offices;
- Data centers, primarily located in Israel, Los Angeles, Chicago, New Jersey, Amsterdam, Hong Kong, and Singapore. These data centers additionally serve as data recovery sites.

Logical information assets

The logical information assets, including information transmitted, stored electronically on servers, website(s), access permissions to applications and networks, supporting organization applications, and products, are classified according to documentation.

The organization

The security overview procedure refers to all Taboola offices, data centers and employees.

3. Terms and definitions

- **Asset**
  Anything that has value to the organization.
- **Availability**
  The property of being accessible and usable upon demand by an authorized entity.
- **Business Continuity Plan (BCP)**
  A plan to build-in proper redundancies and avoid contingencies to ensure continuity of Business.
- **Confidentiality**
  Ensuring that information is accessible only to those authorized to have access.
- **Information Security Event**
  An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be involved.
- **Information Security Incident**
  A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- **Statement of Applicability**

Document describing the control objectives and controls that are relevant and applicable to Organization Name's ISMS, based on the results and conclusions of the Risk Assessment and Risk Treatment Processes. It should clearly indicate exclusions with appropriate reasons.

4. Context of the organization

4.1. Understanding the organization and its context

Taboola determines all relevant external and internal issues affecting its ability to achieve the intended outcomes of its ISMS.

Internal issues relevant to Taboola include:

- Any change in organizational structure, particularly in C-level roles and above.
- Any disparity regarding the number of users of Taboola's information systems and the number of people who manage them.
- Changes in customers contracts affecting Taboola work methods.
- Risk management, including risk assessments and penetration testing results.
- Merger with another company.
- Acquisition of a new company.
- Change in goals and processes of processing of information as a controller.
- Privacy incidents pose a risk to PII data.
- Resource availability, resource competence, training, background verification etc.

External issues relevant to Taboola include:

- New market and customer needs.
- Applicable laws and regulations – e.g. EU GDPR, CCPA.
- Taboola's competitors.
- Stock market changes.
- Natural and competitive environment, key drives and trends having impact on the objectives of the organization, political, financial status of the country.

4.2. Understanding the needs and expectations of parties

Taboola management's commitment to all parties influenced or affected by its continuous information security/business includes auditing ISMS performance. Security will be provided to the following interested parties:

- Employees
- Shareholders/Stakeholders
- Clients
- Consumers / Users
- Suppliers and Partners
- Cyber insurance company
- Investors
- Privacy legislation authorities
- PII processors / third party processors

Taboola's process contains built-in security controls to satisfy all interested parties' requirements. These security controls include:

- Mandatory encryption of all transferred information through the network (emails or traffic).
- Limited need-to-know or least-privileged access to information.
- Security built into all phases of the development process .
- On-going risk assessment.

Taboola will comply with all relevant data-related legislation as requested by the interested parties, such as ISO and required privacy laws. Taboola will also ensure that customers who request data integrity and confidentiality in its processes will have that requirement met.

The Vice President of Information Technology and Cyber (VP IT and Cyber) manages and audits all ISMS controls to maintain security in the business's usual flow.

4.3. Determining the scope of the ISMS

The ISMS of Taboola encompasses the storage, access, and transmission of information in the course of its commission business.

Consequently, Taboola's ISMS scope applies to the conduct of staff, contractors, suppliers, and others with access to that information (wherever the information or the stakeholders are located), as well as the applications, systems, equipment, and premises that create, process, transmit, host, or store information, whether in-house, personally owned, or provided by external suppliers. The scope includes all of Taboola offices, including: Israel, London, Los-Angeles, New-York, Bangkok and India. The scope applies to Taboola's main service (providing recommendation platform for its customers) and any data being collected, received, stored or transmitted as part of it.

4.4. Information Security Management System

The ISMS committee reviews Information Security policies and procedures on a yearly basis, or in any significant change within the company, and may amend them to ensure its continuing viability, applicability, and legal compliance, together with a view to achieving continual improvement in the information security systems.

4.5. Privacy in Taboola (ISO27701)

Taboola is defined as a controller. Taboola collects, processes and protects PII information for 3 main purposes:

1. Consumer (aka User) data - Taboola automatically collects User Information when Users interact with its Services that appear on our Customers' websites and digital properties. Taboola collects only pseudonymized data, which means we do not know who the user is because we do not know or process its name, email address, or other identifiable data. User Information that we collect includes, but is not limited to, Information about a User's device and operating system, IP address, the web pages accessed by Users within our Customers' websites, the link that led a User to a Customer's website, the dates and times a User accesses a Customers' website, event information, general location information, hashed email addresses

(when made available by the User), and gender (when made available by the User).
This data is collected by the lawful basis of consent and Legitimate Interest.

2. Employee data - for the purpose of providing its core activities, Taboola collects data of its employees. Data can be, but not limited to, personal data contained in: Resumes and applications; References and interview notes; Letters of offer and acceptance of employment; Wage and payroll information; Benefit information; Beneficiary and emergency contact information; Access card entry and surveillance footage; Employee photographs and video footage;
   Personal data also includes information such as your name, home address, telephone number, personal email address, date of birth, Employee identification number, marital status, and any other information necessary for Taboola's business purposes, that the Employee or candidate voluntarily discloses during an application for and employment with Taboola.
   This data is collected by the lawful basis of a contract.
3. Customer data - We collect Customer Information directly from our Customers. This information can be contact details, username and password, email address, full name, phone number and other Information that Customers choose to provide to us, such as the contents of a message or form that a Customer submits through our Sites or via email.
   This data is collected by the lawful basis of a contract.

More information regarding the purposes of collecting and processing information can be found in Taboola privacy policy (https://www.taboola.com/policies/privacy-policy) or in the employee's data privacy policy.

All privacy laws, regulations, judicial decisions, contract obligations and management decisions which are applicable to the company and which it shall adhere to, are recognized, mapped and maintained by the legal department.
Taboola is committed to comply with all privacy requirements and maintain security of privacy and data of its employees, users, clients and vendors.

Taboola's management is being updated on privacy manners as part of quarterly management meetings.

5. Leadership

5.1. Leadership and commitment

The VP IT and Cyber and Director of Global IT demonstrate upper management's leadership & commitment to the ISMS by periodically conducting meetings to identify and track all ISMS-related risks.

Management commitment to information security

Taboola management is committed to each of the following:

- Approving and updating the scope of ISMS based on strategies and roadmap.
- Reviewing and approving the Information Security Policy.
- Monitoring significant changes in exposure of information assets to major threats.
- Reviewing security incidents together with the results of respective investigations.
- Approving the resources required for the security roles and responsibility.
- Assigning responsibility for each information asset and its day-to-day security.
- Arranging independent review of the implementation of the security policy.

The VP IT and Cyber shall report on any security-related issues to upper management. Any such discussions should be recorded, along with any actions taken. All management team actions related to the list above will be documented.

Allocation of information security responsibilities

Overall responsibility of the ISMS management team rests with the VP IT and Cyber who, or someone on his behalf, shall personally conduct and document the following tasks:

- Analyze security incidents.
- Review server logs for production servers.
- Review logs with access to critical applications.

- Define a global work plan of information security.
- Prioritize tasks based on risk assessments and organizational needs.

Confidentiality agreement

Requirements for confidentiality/non-disclosure agreements reflect the organization's need for protection of information, and shall be identified. The legal department, together with the security team in Taboola, have the responsibility for confidentiality agreements with vendors. The HR department is responsible for confidential agreements with regular and hired employees.

The requirements shall be reviewed by the VP IT and Cyber annually, at a minimum.

Contacts with authorities

The VP IT and Cyber, together with the legal advisor, shall maintain contacts with any relevant law enforcement authorities, regulatory bodies, information service providers, and telecommunications service providers, depending on the service required. A yearly review of the contact list is required for assistance and guidance in handling security incidents and maintaining updated security infrastructure.

Contact with special interest groups

The VP IT and Cyber and his team, shall be in contact with information security consultants, track internet resources, and keep watch for the early warnings of alerts, advisories, or patches related to Taboola's information system.

Independent review of information security

An internal auditor (not directly connected with the areas under audit) or an outsourced auditing agency shall conduct an internal audit of the ISMS when any significant changes are made to the security implementation. The VP IT and Cyber shall plan and coordinate this.

5.2. Policy

Taboola is committed to the development and maintenance of an Information Security Management System based upon the International Standard. The Information Security Policy is based on the ISO/IEC 27002:2022 implementation guidance controls. This Information Security Policy is designed to:

- Provide direction and support for information security according to business requirements, regulations, and legal requirements.
- Stipulate the responsibilities of staff, partners, contractors, and any other individual or organization having access to the organization information assets.
- Disseminate management intent to support the goals and principles of security in line with business strategy and objectives.
- Provide a framework to maintain the confidentiality, integrity, and availability of the organization's information assets.
- Optimize the management of risks by preventing and minimizing the impact of information security incidents.
- Ensure that all breaches of information security are reported and investigated, and that appropriate action is taken.
- Yearly review supporting ISMS policies and procedures, thus maintaining continual improvement, and ensuring progressive work practices and procedures are in place.
- Communicate information security requirements upon contract, to all relevant parties.

This document contains the Information Security Policy for Taboola; it describes the company's corporate approach to information security and details how the Company addresses responsibilities relating to the vital areas of our business. Taboola is fully committed to satisfying applicable requirements related to information security and the continual improvement of the ISMS.

All members of Taboola's staff share responsibility for Information Security with the senior management team. Therefore all staff should achieve an awareness of this policy and its contents, while demonstrating a practical application of its key objectives where appropriate in their daily duties.

Additionally, the company shall make the details of this policy known to all interested parties, including external parties, where appropriate. The Company will determine any need for communication and the methods to accomplish it, as relevant to the ISMS. *Inter alia* interested parties include customers and clients, with their requirements documented in contracts, purchase orders, specifications, etc.

Verification of compliance with the policy will be accomplished through a continuous program of internal audits.

5.3. Organizational roles, responsibilities and authorities

Taboola's Top Management provides evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the information security management system as defined in the roles and responsibilities.

- Establishing an information security policy;
- Ensuring that information security objectives and plans are established;
- Establishing roles and responsibilities for information security;
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
- Deciding the criteria for accepting risks and the acceptable level of risk;
- Ensuring that internal ISMS audits are conducted;
- Conducting management reviews of the ISMS

List of organizational roles, responsibilities and authorities within the ISMS are mapped and detailed in the *Roles and Responsibilities mapping* document, maintained by the security team.

6. Planning

6.1. Actions addressing risks and opportunities

6.1.1. General

Taboola has identified the process for conducting regular risk assessments related to information security issues. Within the information security area, risks are identified and assigned a rating, indicating their importance. The rating is obtained by assessing the associated consequence or severity of the risk together with its probable likelihood.

The company collects and analyzes the risks identified in the following assets/asset groups:

- Buildings, offices, secure rooms, security
- Hardware – desktops, laptops, removable media
- Software applications
- Infrastructure/servers and related services
- Paper records
- People and reputation
- Key contacts
- Critical third-party suppliers
- Utilities

6.1.2. Information security risk assessment

All typical/likely threats are assessed based on their potential effects on Confidentiality, Integrity, and Availability (CIA attributes) using a rating scale of;

1. Low
2. Medium
3. High
4. Critical

Following analysis, the most appropriate action is determined, along with the estimated cost of implementation and a cost estimation cost of accepting the risk. Key evaluation criteria used are:

1. Accept risk.
2. Apply controls.
3. Avoid risk.
4. Transfer risk.

The risk assessment process includes 2 stages:

6.1.2.1. Risk assessment

A yearly process (at least) conducted by Taboola's security team that includes a review of the existing risk register mapping, dedicated audit committee for reviewing and discussing about our risks, Cyber insurance risks review and assessment and quarterly internal security meetings of the security team to discuss new and potential risks. During all the above, the team assess the risk descriptions, existing control measures, and residual risks. The team's primary objective is to confirm the absence of any supplementary controls, validate the stability of the existing processes, and ascertain that there are no opportunities for risk reduction. During this process the team also validates that there are no new risks that were not identified by the company.

6.1.2.2. Risk register creation and update

The risk register is an excel table, held and maintained by the security team in Taboola, and includes all known risks (scored as low – high). The table includes:

- The risk area
- Vulnerability
- Risk description
- Likelihood and impact
- Inherited risk
- Implemented controls
- Risk following control implementation
- Action items
- Etc.

The risk creation process is by identifying first all main processes Taboola owns, identify the asset per process and then find all related risks per process and asset.

The table should be reviewed at least once a year and validate that no new risks are identified and that the company accepts current risks level.

Risks ranked as "moderate" level and above, should include an action item for Taboola to handle the current risk level. Medium risks are acceptable by the security team by the time they will be identified as "low".

Risks will be reviewed in a sampling method and review sampling will be based according to the risk level. All risks ranked as "moderate" and above will be reviewed, examined and compared on a yearly basis by the security team, together with 3 randomly chosen "low" risks.

Moreover, all other risks ranked as low will be reviewed, examined and compared in the next year of the ISO certification cycle (that means the next recertification audit).

Controls will be assessed together with the likelihood on yearly basis.

The risk register table shall be approved by the VP IT and Cyber on a yearly basis (at least).

6.1.3. Information security risk treatment

The security team is responsible for maintaining security controls for all Taboola assets, locations, employees, risk management, and processes. A Risk Treatment Plan will be created for each risk, including required resources, responsibilities, and priorities, along with action taken by Taboola management. These are to be documented, implemented, and reviewed periodically.

A risk treatment plan stipulates the technology, the process controls that are needed to control the risk, as well as the steps taken to mitigate a particular risk.

This plan is presented to the management team for approval. Senior management reviews the approach as well as the solution, and then approves the Risk Treatment Plan.

Taboola employees sign an agreement maintaining security and confidentiality at the time of appointment.

Taboola's VP IT and Cyber is knowledgeable regarding implementation of the required controls with their desired effect.

The ISMS operations are led by the security team, assisted and supported by other Taboola departments, such as IT team members.

The effectiveness of all security controls is measured periodically. Analysis of relevant logs and records, such as an incident report, access logs, network logs, BCP tests, formal risk assessments, and penetration tests based on the annual work plan, is performed to assess effective

implementation of security objectives. Appropriate actions will be taken when and if effectiveness is found to be lacking.

6.2. Information security objectives and planning to achieve them

The security objectives for Taboola are identified and managed so as to provide the required security needed to maintain a high level of security for Taboola management and interested parties. This consists of the following:

Availability

Information and associated assets should be accessible to authorized users when required. The computer network (identified as part of the scoping) must be resilient, and the organization must be able to detect and respond rapidly to incidents (such as viruses and other malware) threatening the continued availability of assets, systems, and information.

Confidentiality

Information shall be only accessible to authorized parties. Both deliberate and accidental unauthorized access to the organization's information and its systems, including its network(s) and website(s) shall be prevented.

All traffic to and from Taboola identified in the risk assessment process with a data classification as "sensitive" will be encrypted to protect the confidentiality of our clients.

Integrity

The accuracy and completeness of information and processing methods must be safeguarded. Therefore destruction, whether deliberate or accidental, partial or complete, or any unauthorized modification of electronic data shall be prevented.

Integrity will consist of the following:

- The information is protected against unauthorized access.
- The confidentiality of the information is assured.
- The integrity of the information is maintained.
- The information is available at the times and places required.

- The information is accessible to the employees on a "need-to-know" and "need-to-do" basis.
- The applicable laws and contractual arrangements are identified and complied with at all times.
- Business continuity with minimum impact from security incidents, if any, is maintained.

All security objectives will be analyzed and evaluated on an ongoing basis with a formal work plan for mitigating risks determined by management to be at high risk level.

6.3. Planning of changes

A change to the ISMS may be identified by any one (or more) of a number of interested parties.

When a change is proposed, it must be communicated to the security team (led by the VP IT and Cyber) via any appropriate method, including email, verbally or using collaboration tools. It will then be added to the ISMS Change Log.

The following information must be provided so that the change may be accurately assessed:

- Name and contact details of the person proposing the change
- A description of the nature of the change
- The reason for the change
- A description of which aspects of the ISMS may be affected by the change
- The urgency of the change (High, Medium or Low)

The security team will review the change to decide whether it can be approved or it needs to be referred to the higher management. Changes that need to be referred to will be those that have significant implications for the ISMS, or fundamentally affect the way in which it operates.
Changes that do not need to be referred will be assessed by the information security manager. If necessary, further detail should be requested and if the change is acceptable, it will be recorded as approved. If not, the change will be rejected, and the decision, together with the reasons for it, communicated to the person who proposed it.

7. Support

7.1. Resources

Management commitment

Taboola upper management maintains responsibility for consistent and effective information security operations across all Taboola offices and locations.

All required resources will be allocated according to a formal risk assessment process and ongoing information security assessments. Taboola upper management will:

- Ensure the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.
- Communicate the importance of effective information security management.
- Confirm that the requirements of the information security management system are met.

Provision of resources

Taboola management reviews the annual work plan and allocates resources, including personnel, technology, and training. This also includes training, awareness, and competence required for each identified role.

This ensures that a structured approach to information security resource management is built into Taboola operations.

The organization will determine the necessary competence required of personnel working under its authority who affect its information security performance. Additionally, it will ensure personnel are competently and appropriately trained or experienced.

Where applicable, Taboola will acquire the necessary competence, evaluate the effectiveness of the actions taken, and retain appropriate documentation demonstrating competence.

7.1.1. Human resources security

Roles and responsibilities

The HR department shall ensure that all employees and third-party users within the scope of this manual, and having access to information assets, sign the non-disclosure agreement and Acceptable

Usage Policy. Security roles and responsibilities of employees, contractors, and third-party users shall be defined. Each shall be made aware of their specific security roles & responsibilities as per the Taboola information security policy.

As for privacy, Taboola is considered both as a controller and in limited instances as a processor.

The HR department manages role definitions in the company, along-side with the employees manager.

Screening

Background verification checks for integrity, competence, knowledge, and conduct of all candidates selected for employment shall be carried out by the HR department as per the HR process. The VP IT and Cyber, and the relevant employee manager, shall ensure that the third-party users are properly screened before employment for specific tasks requiring privileged access to the Taboola information system. Screening will be conducted only for Finance / Office IT / Legal and only the relevant VP can provide waiver to this process, with the confirmation of the security team.

Terms and conditions of employment

All employees and third-party users shall agree and sign the terms and conditions of their employment. This shall be ensured by the HR department.

During employment

All Taboola employees, contractors, and third-party users are made aware of information security threats and concerns, as well as their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work and to reduce the risk of human error.

Management responsibilities

Upper management shall require employees and third-party users to maintain security in accordance with established policies and procedures of Taboola. Upper management shall communicate the security roles & responsibilities to the employees by providing them with relevant documents and shall motivate them to adhere to security procedures by communicating their advantages.

Termination responsibilities

Responsibilities for change of employment and/or termination will be clearly defined and assigned by the HR department, per the Taboola HR process.

Return of assets

The ITOps team will ensure that all employees and third-party users shall return all Taboola assets in their possession upon termination of their employment, contract, or agreement.

Removal of access rights

The ITOps team and the Production IT team shall ensure that access rights of all the employees and third-party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

7.2. Competence

Personnel who have experience and expertise in information security concepts are assigned to manage ISMS. Whenever feasible, experienced individuals are available and allocated appropriate responsibilities. When the required levels of skill and expertise are not available, training is provided to ensure skill/knowledge enhancement as per the Taboola training process.

7.3. Awareness

Information security awareness, education, and training

Managers should ensure staff and external parties working with systems and data are formally made aware of and are educated about the policies and procedures they must be compliant with. This is a fundamental step to establishing an individual's accountability.

The Cyber Security Compliance Lead shall ensure that all users within the scope of this manual receive appropriate awareness and training, as well as regular updates about Taboola policies and procedures, as relevant for their job function. The security team shall identify specialist training needs for employees and arrange the training through HR.

7.4. Communication and operations management

Users shall be made aware about the risk of information security while exchanging information through voice, email, chat, video communication, etc.

Taboola will use a variety of communication methods to ensure effective distribution of information security-related information, including but not limited to:

- Email: For formal communication of policies, procedures, classification and labeling and updates.
- Brain platform: A centralized platform for accessing information security policies and procedures.
- Meetings: Regular team meetings to discuss information security issues and updates. The communication can be viral and through email post meetings.
- Training Sessions: Interactive sessions to educate employees on information security policies and best practices, can be done oral or through video sessions.
- Incident Reports: Formal reports detailing information security incidents and response actions.

7.5. Documented information

7.5.1. General

All documents are maintained and controlled by the security team. Policy and procedure documents are reviewed annually. Any documents requiring amendment are updated, authorized, and completed. All updates to documents are signed and dated by the VP IT and Cyber. Electronic copies of all past versions are kept. All managers are responsible for cascading information to staff.

7.5.2. Creating and updating

User access management

To ensure authorized user access and to prevent unauthorized access to information systems, security controls are implemented.

User registration

User registration and de-registration to the system and services are carried out in a controlled manner. User/e-mail account creation and deletion are carried out only after formal authorization by the appropriate manager.

Privilege management

Allocation of system administration privileges is granted to administrators only. The administration account shall not be used for other purposes than administrative. Administration accesses shall be logged, and the logs shall be reviewed by the VP IT and Cyber.

Review of user access rights

The IT department conducts an annual formal review of the user access rights for normal and privileged user accounts.

7.5.3. Control of documented information

All the documented information required by the information security management system and by ISO 27001:2022 International Standard are protected and controlled as per documented procedure to ensure it is available and suitable for use, where and when it is needed.

8. Operation

8.1. Operational planning and control

Taboola adopts a unique risk management approach for its information assets. This approach is based on a qualitative risk analysis model for assessing and maintaining the risk framework; all risks have both probability and impact. Probability refers to the likelihood that a risk event will occur, and impact refers to the significance of the consequences of the risk event.

Risk may impact the following project elements: schedule, budget, resources, deliverables, costs, quality, scope, or performance.

The VP IT and Cyber maintains responsibility for global risks and will conduct a weekly meeting to audit the work plan prepared for mitigating and managing the risks based on priority.

Taboola security team is using dedicated documents to elaborate, implement, validate and monitor ISMS goals and objectives. Furthermore, changes are planned, controlled and reviewed by the team and any supporting resources. Changes are recorded.

8.2. Information security risk assessment

Taboola conducts a risk assessment for all the information assets to ensure that there are no unidentified risks and that all major risks are mitigated by implementing a timely solution. The owners of the information assets will carry the responsibility of managing the respective assets.

The risk assessment shall be triggered by events such as:

- **A significant change in the information environment**: This ensures that whenever any assets are added, or existing assets undergo change, the associated risks are identified and documented, and a risk mitigation/acceptance plan is prepared.
- **Periodic assessment**: Periodic Assessment will be conducted on an annual basis to ensure that existing assets that have not undergone any change are nevertheless revisited to prevent the introduction of any new risks.

8.3. Information security risk treatment

Risks will be addressed in order of importance as determined by management. In addition, the management must approve all risk residues in the company and declare them in writing. In the case that the risk residue contradicts the organization's compliance standard, the above statement will not be valid, and the risk mitigation must be carried out as per process.

9. Performance evaluation

9.1. Monitoring, measurement, analysis, and evaluation

The VP IT and Cyber is responsible for convening all aspects of information security either after significant changes in the organizational environment or prior to planned changes. This includes business circumstances, legal conditions, or technical environment changes that are likely to impact on information security, and must be undertaken annually at a minimum.

Monitoring activities are divided into categories such as daily, weekly, and monthly. These monitoring activities help track and measure the security compliance in various aspects of information security.

Management review of ISMS

Management conducts a management review of the ISMS operations in Taboola through a formal meeting each quarter.

The following reports are scrutinized during the management review:

- Status of various corrective & preventive actions initiated as non-conformities.
- Reports on internal audits.
- Incident reports.
- Any changes to ISMS documentation/operation based on the incidents or feedback received during operations, or from the interested parties mentioned above.
- The continued suitability, adequacy, and effectiveness security policy.
- Results of the measurement of effectiveness.
- Business Continuity Review.
- Compliance with organization goals.
- SOA review.

9.2. Internal audit

Taboola reserves the right to monitor the use of IT systems and information, including email and internet usage, to protect the confidentiality, integrity, and availability of organizational information assets and ensure compliance with company policies. The company may, at its discretion, or where required by law, report security incidents to the relevant authorities for further investigation.

As part of the standard audit review process, Internal Audit will routinely assess compliance with the company's Information Security Policy and relevant ISO27001:2022 and ISO27701 controls and report issues to senior management or the Information Governance Group where appropriate. Security incidents reported through the Security Incident Management Policy and Procedures will help determine the effectiveness of ISO27001:2022 controls and assist in identifying training and awareness requirements and improvements.

An internal audit of the ISMS, shall be conducted once a year and when any significant changes are made to the security implementation. The audit will be in accordance with the audit plan set in advance. This shall be done by an internal auditor (not directly connected with the areas under audit) or an outsourced auditing agency.

9.3. Management review

Information security policy

Information security provides the foundation of management direction and support for information security with business requirements and relevant laws and regulations.

Information Security Policy document

The Information Security Policy is approved by Taboola management. The origin of the document will be managed by the security team and a copy will be accessible to all employees either via a Brain platform or a dedicated online link.

Information security policies shall be made available to all other third parties, interested parties, etc. upon request.

Review of information security policy

The Information Security Policy will be overseen by the VP IT and Cyber and reviewed by the management at least annually. A review shall also be performed in the case of a major security incident or organizational and business process change.

10. Improvement

10.1. Continual improvement

Continual improvement

Taboola recognizes the need to keep the information security environment current on an on-going basis, and to achieve this it has implemented the following:

- Periodic review of the security policy (yearly basis at least).
- Periodic updates regarding the versions and patch levels.
- Periodic penetration tests and vulnerability assessments.
- Ongoing tracking of security-related tasks to closure.
- Building education and awareness through new channels.
- Improving software security related to client's connection and information transfer

10.2. Nonconformity and corrective action

Corrective action

Taboola oversees compliance on standards and procedures; this is done through various reviews by the internal team and also by the external team, if required. These reviews identify vulnerabilities and nonconformities to ensure that areas of improvement are identified and addressed. Apart from the corrective actions that are taken, a root-cause analysis of the issue is performed and proper measures are implemented to ensure that there is no recurrence of the issue. Issues identified through these reviews are tracked on a continual basis to ensure compliance. Suitable corrective controls, both process controls and technical controls, are implemented to ensure that the security position of Taboola is maintained. There is a possibility that non-conformities may lead to risks, which will be defined and managed. This process will be supervised by the VP IT and Cyber.

Preventive action

Various conclusions may emerge from reviews that are conducted as part of the information security controls put in place in Taboola. Industry best practices are integrated into the information security framework adopted by Taboola on an ongoing basis to ensure constant improvement in processes. Results of preventive action are analyzed to determine if the preventive controls have met expectations and have addressed the business/security issue that was identified.

These preventive steps include constant monitoring of threat scenarios, identifying the applicability of the same in Taboola's information context, and implementing the controls for identified threat and compliance to ISO 27001-annexure control.

Several controls and the objectives are described in the sections below.

11. Asset management

Inventory of assets

An inventory of all information assets of Taboola shall be identified, and maintained in the asset register by Taboola. The asset register shall be verified yearly.

Ownership of assets

The VP IT and Cyber is responsible for all information and assets associated with information-processing facilities within the scope of the ISMS. The VP IT and Cyber shall assign management responsibility of the assets. The asset manager shall perform:

- Initial classification of the assets.
- Initial asset allocation to the user/custodian of the assets.
- A review of any discrepancies/exceptions during the stock verification, which shall be reported to the owner.

Acceptable use of assets

Rules for the acceptable use of information and assets associated with information-processing facilities shall be communicated to all concerned users by suitable means, such as awareness program, publishing on the file server, etc.

Classification guidelines

All information assets within the scope shall be classified based on their impact value in case of loss of Confidentiality/Integrity/Availability, in accordance with Taboola's information classification matrix.

12. Secure area

To prevent unauthorized physical access to, damage to, or interference with Taboola's premises, the following controls are put in place:

Physical entry controls

An access restriction mechanism controls entry to the office, providing access rights to authorized persons only.

Securing offices, rooms, and facilities

The scope of the ISMS is Taboola's information security. Taboola's data and information are managed by a cloud-based service provider that complies with ISO 27K.

Office entry is limited solely to employees. All visitors shall be escorted by their hosts at all times during their visit.

Sustainable Energy

Taboola supports the use of Green Energy and sustainable data centers and offices, where possible.

Taboola aims to maintain sustainable energy and to support the use of Green Energy in its processes, secure environment as well as in its contact with relevant suppliers (e.g. data centers).

13. Information security incident management

Reporting information security events

Information security events shall be reported through appropriate management channels as soon as possible. Employees shall report information security events to security@taboola.com or to their direct manager. The VP IT and Cyber may refer the matter to upper management, if necessary.

Reporting security weaknesses

All employees, contractors, and third-party users of Taboola shall be informed that they are required to note and report security weaknesses (if any), to the security team or to the VP IT and Cyber.

Responsibilities and procedures

Whenever a severe or unprecedented security incident which calls for special attention comes to the knowledge of the VP IT and Cyber, this shall be communicated to the higher authority directly or through the management team. An appropriate remedial procedure shall be adopted with management's approval.

Collection of evidence

A follow-up action may involve legal action (either civil or criminal) against a person or organization after an information security incident is reported. Where legal action is required, evidence shall be collected, retained, and presented in conformity with the rules of evidence laid down in the relevant jurisdiction(s). Depending upon the type of security incident, physical or technical evidence shall be retained for any future legal purpose and provided to the operational staff for further action.

14. Business continuity management

Information security aspects of business continuity management

Business Continuity Management counteracts interruptions to business activities and protects critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.

Business continuity and risk assessment

Risk assessment is carried out for the Taboola application and databases per the Risk Assessment Procedure.

Developing and implementing continuity plans, including information security

Business Continuity Plans (BCP) shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following an interruption to, or failure of, critical business processes.

Business continuity planning framework

A single framework for business continuity plans shall be maintained to ensure consistency between plans and to address information security requirements in a uniform manner. The business continuity plans also identify priorities for testing and maintenance.

Testing, maintaining, and reassessing business continuity plans

Business continuity plans shall be tested and updated at least yearly, to ensure that they are up to date and effective.

15. Compliance

Applicable laws and regulations

Taboola is subjected to the following laws and regulations:

- Israeli Computer Law, 1995
- Israeli Privacy law, 1981
- Commercial Torts Law (Intellectual property rights), 1999
- Financial laws

- CCPA (California Consumer Privacy Act)
- GDPR (General Data Protection Regulation)
- State Laws in which Taboola operates under the contract with is customers

Taboola is also aware that laws and regulations might be added or changed as a result of its activity and geographical operation location.

Taboola is also made aware of additional laws or regulations and the applicable level of each law or regulation to Taboola, via its legal and privacy departments and 3rd party legal vendors which are reporting on every new standard or regulation which is applicable for Taboola.

This information security policy has been developed while thinking of privacy, privacy laws and regulations and relevant requirements.

Intellectual property rights

The VP IT and Cyber shall ensure compliance with legislative, regulatory, and contractual requirements on the use of the material where intellectual property rights may apply. Only software with valid licenses shall be used. The VP IT and Cyber shall be custodian of all paper licenses.

Protection of organizational records

Important records shall be protected from loss, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements. Organizational records will be categorized into record types, e.g. database records, transaction logs, audit logs, and operational procedures, each with details of retention period and type of storage media (e.g. paper, optical media, magnetic media, etc.).

16. Security in development and support processes

To maintain the security of application system software and information, the following procedures are followed:

Change control procedures

All changes to the application systems and the support environments shall be implemented in a controlled manner.

Technical review of applications after operating system changes

When operating systems are changed, business-critical applications shall be reviewed and tested to ensure against adverse impact on Taboola operations or security.

Secure development process

Taboola works according to Secure development lifecycle policy which provides guidance on how to develop and write code in a secure manner.

16. Document owner and approval

The VP IT and Cyber is responsible for this document and for ensuring that this policy is reviewed in line with the review requirements of the ISMS.

Changes History Record:

Issue	Description of Change	Approval	Date of Issue
1	Initial version in accordance with ISO27001:2022 requirements	VP IT and Cyber	Jun 30, 2024
2			
3			
4			