OutThink

Information Security Policy

1. Purpose

OutThink's Information Security Policy ("the Policy") is a key element of its Information Security Risk Management. This Policy documents OutThink's direction and commitment to information and cyber security while outlining key principles that must be followed when dealing with information to ensure the protection of our information, the resilience of the supporting information systems, continual improvement, compliance with relevant data protection legislation and all regulations to which OutThink is subject.

Information Security Risk is inherent in all administrative and business activities and everyone working for or on behalf of OutThink continuously manages information risks.

Within OutThink, Information Security Risk is defined as the risk that the Confidentiality (property that information is not made available or disclosed to unauthorized individuals, entities, or processes), Integrity (property of accuracy and completeness) and Availability (property of being accessible and usable on demand by an authorized entity) of information are not protected from internal (e.g. negligence, malicious insiders) and external threats (e.g. cyber threats), deliberate or accidental in nature, causing material business impact.

The external threats referenced as cyber threats include Cyber Crime which is defined as criminal activities carried out by means of computers, over interconnected networks (e.g., the Internet). This involves the use of sophisticated and tailored techniques to infiltrate enterprises and social networks.

There is need to understand the cyber threats and safeguard against them; these include:

- Opportunistic or unsophisticated attacks from individuals or organisations
- Organised criminals striving to extort money from OutThink and its customers
- Malicious activism/hacktivism and politically motivated threat actors
- Social engineering and data harvesting
- Sophisticated nation-state-sponsored attacks.

For the purpose of this Policy Standard; Information Assets are defined as:

A. **OutThink Information** (incl. all records and personal or non-personal data) in all formats - digital (information created, processed, stored or transmitted using information technology), spoken (ideas, facts, knowledge shared and exchanged through human interaction), physical (paper-based information - e.g. printed reports, paper forms, board papers) relating to OutThink, its employees and its customers (current, past and potential), irrespective of the medium or device on which it is stored or of its location; and

B. **OutThink Systems** referring to any supporting IT infrastructure, IT systems, hardware, or software, belonging to or under the control of OutThink or its contracted third parties, that are used to store, process, or transmit OutThink Information.

Using a risk-based approach, OutThink is committed to having appropriate measures in place to protect its Information Assets, reduce the likelihood and impact of information security incidents and to meet applicable legal and regulatory requirements.

Failure to comply with this Policy will be regarded as a significant breach of OutThink's risk and control management environment and may lead to disciplinary action, up to and including dismissal.

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

2. Executive Summary

This Policy supported by appropriate standards and guidance, is in place to ensure we protect the confidentiality, integrity, and availability of all OutThink information and information systems from threats which include unauthorised / accidental disclosure, corruption, unauthorised modification, loss, theft, deletion, or unavailability of Information Assets for legitimate business use. This policy is aligned to ISO/IEC 27001 requirements for an Information Security Management System (ISMS) and its effectiveness will be monitored via periodic ISMS Management reviews. These threats affect information in all formats and the supporting information systems (containers) such as infrastructure, networks, hardware, software, filing cabinets and data storage devices.

The purpose of this Policy is to set out the principles for the effective management of information security risk within OutThink. The objectives of the Policy are to:

- Ensure the protection of the confidentiality, integrity, and availability of all OutThink's Information Assets, during all stages of the information lifecycle - creation, storage, processing, transmission, and destruction. Ensure that OutThink has adequate People, Process and Technology controls in place to mitigate information security and cyber risk originating from both internal and external threats.
- Clearly outline Employee and third-party roles and responsibilities for information security and cyber risk management.
- Ensure that OutThink has appropriate mechanisms for addressing information security incidents.

In support of these objectives, this Policy;

- Defines the minimum set of actions to be taken by all Employees throughout OutThink and relevant third parties to identify and manage information security risks to which OutThink may be exposed.
- Defines key roles and responsibilities, including those related to the governance of information security risk.
- Defines who is accountable for the management of information security risk and security incident management within OutThink.

3. Risks addressed by this Policy

OutThink is exposed to risk arising from a failure to manage information safely and securely.
The Information Security Risk, from OutThink's perspective, is: "The risk of financial loss, operational and reputational damage resulting from the inability to ensure the confidentiality, integrity and availability of our Information Assets".

The risk could materialise because of internal or external threats affecting:

- *Confidentiality of Information Assets: Unauthorised disclosure, loss, or theft of information, whether* deliberate or accidental, related to internal or external threats (e.g., emailing information to the wrong recipient, leaving/losing OutThink information in a public place, a security breach resulting in the theft of personal or confidential information).
- *Integrity of Information Assets: Inaccurate information,* unauthorised amendments, or

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

corruption of information (e.g., updating the incorrect information on a system, failing to update information in all relevant systems or an attacker inflating account balances).

- *Availability of Information Assets: Unavailability of information,* unauthorised deletion of information, loss or theft of equipment, downtime due to loss of power, technical failure, human error, or distributed denial of service attacks on OutThink's Systems; Information cannot be accessed for necessary business activity, when it would normally be available.

4. To whom does this Policy apply?

This Policy applies to all employees and agents of OutThink, and to all providers of services to OutThink that process, control or access OutThink data and to the employees and agents of such providers, collectively referred to as "Employees". The Policy applies in all districts in which OutThink operates.

These roles involved in OutThink's information lifecycle include (but are not limited to):

- Data owners: is the individual who is responsible and accountable for a specific data set. This role is responsible for classification, protection and compliance of the data sets she/he owns.
- Control owners: is the individual who is responsible and accountable for the adequate design and operation of a security control.
- Control operators: responsible for implementation and operation of security controls as instructed by the control owner.

5. Control Objectives

5.1. Risk Identification, Assessment and Management

Department managers are required to assess information security controls in terms of below control objectives in a manner that is commensurate with the value and potential impact of the Information Assets held.

5.2. Information Security and Cyber Risk Management

Each Manager must assess the compliance of their department, with Control Objectives by ensuring a Risk Assessment review was completed, to confirm that there are sufficient controls in place in respect of information and cyber security, which satisfy the control objectives.

To provide assurance that information security and cyber risk are being adequately addressed, the risk appetite of the organisation must be determined and documented at the governing body level. The risk appetite must be communicated to, and understood by, all individuals throughout OutThink who are responsible for making decisions about information security and cyber risk treatment.

Critical information assets must be subject to formal information security and cyber risk assessments on a regular basis (at least annually or whenever significant change takes place) and formal action taken to address any significant risks identified, as mandated by the OutThink Information Security Risk Management Framework.

The Control Owner must ensure that processes are in place to effectively identify and manage information security risks within their areas of responsibility, in compliance with all the Control

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

Objectives stipulated within this Policy and supporting standards and guidance.

5.3. Governance and Assurance

Each Manager is responsible for every element of Information Asset management within their remit. Each Manager must assess their compliance with the Control Objectives.

To demonstrate commitment by OutThink and to enable a risk-based approach to information security to be taken, information security activities throughout the organisation must be coordinated in line with OutThink Information Security Risk Management Framework. An information security policy and control framework must be maintained. This must reflect OutThink's risk appetite, be closely aligned to industry best practice and help ensure business security requirements, legal, regulatory, and contractual obligations are being met.

Monitoring and measurement of effectiveness of implementation of requirements of this policy will be performed via a periodic and at least annual Management Information Security Management System review.

5.4. Staff Controls

Information Security controls must be embedded into each stage of the employment life cycle. Pre-screening of all applicants for employment must be completed prior to commencing their employment with OutThink. This includes background checks (such as criminal and credit record checks, within the limits of the local law) for employees handling sensitive information.

Employment terms and conditions which include adherence to OutThink's Code of Conduct (and therefore policies and guidance materials that relate to Information Security) must be accepted in writing prior to commencement of employment.

Ongoing information security awareness and role-based security training must be delivered during the term of employment.

Upon termination of employment, OutThink's information assets must be returned by the employee. Access to all OutThink systems and services will be *immediately* revoked, including all access to cloud development platforms and, where relevant, any privileged access to production systems, services, or backup datasets. All systems housing production data must be accessed with corporate federated identities (and 2-factor authentication enabled) and therefore access will be automatically revoked.

5.5. Information Handling Controls

Information Security controls must be embedded into all processes that involve the handling of information assets:

All information must be classified in line with OutThink's Information Classification Standard. Appropriate protection must be put in place in accordance with the level of classification assigned.

Ownership of critical information assets must be assigned to individuals and clearly documented as acknowledged and accepted.

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

An information asset register must be maintained and regularly updated with asset ownership, business impact, information classification and clearly documented. This asset register must be refreshed and re-certified on an annual basis.

Handling of information assets and OutThink's devices by business unit staff must be conducted in line with OutThink Information Security Acceptable Use Policy.

Information assets must be retained in line with Information Retention Guidelines.

5.6. File Sharing Controls

All sharing of files, either internal to the organisation or externally, must follow a principle of least privilege and must be in accordance with Information Handling Controls. This is especially important when sharing corporate confidential data, client confidential data or personal identifiable information outside the organisation.

It is vital that sharing of any information outside of the organisation is undertaken in accordance with OutThink's External File Sharing Procedure.

5.7. Access and Systems Controls

Information Security controls must be embedded into all processes that involve the granting of ongoing access to information assets.
Access to information assets must be controlled based on "need to know", "relevant to role" and "least privilege" principles as maintained under OutThink's Access Control Policy.
Access to information systems must be restricted to ensure the integrity of sensitive information.
Identity and access management processes must provide effective and consistent identification, authentication, and access control mechanisms throughout OutThink.

Physical access to any locations where OutThink Information Assets are housed must be controlled via appropriate physical access control mechanisms. This includes access to office areas and electronic equipment.

Physical access to information assets and information systems must be restricted by the implementation of Clean Desk, Locked Screens, and appropriate physical access controls.

To address vulnerabilities in OutThink systems, and reduce the likelihood and frequency of data breaches, system and software patches must be applied within the appropriate time window, as mandated by OutThink's Vulnerability & Patch Management Policy.

To defend against malware attacks, systems throughout the organisation must be safeguarded against malware by maintaining up-to-date malware protection software, which is supported by effective procedures for managing malware-related security incidents.

To ensure that, in the event of an emergency, essential information can be restored within critical timescales, regular backups must be performed according to a defined cycle.

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

5.8. System Development and Modification Controls

Information Security controls must be embedded into all processes that involve the development and modification of information systems:
All systems and applications acquired by OutThink must be subject to appropriate due diligence.

All cloud-based solutions that are being or have been deployed by OutThink must be subject to annual security review.

An appropriate level of security testing must be conducted on any system or application under development to identify security weakness and to determine how systems and applications will behave when under attack conditions.

Any changes to information assets must be tested and applied under a fully reviewed and documented change management process. All changes must be made securely and competently by authorised individuals only to ensure no unauthorised changes can be made.

It is vital that system development is undertaken in accordance with OutThink's Secure Software Development Policy.

5.9. Device Controls

Information Security controls must be applied to all devices that are used as information systems or to store information assets.
OutThink will acquire robust and reliable hardware that has been subject to appropriate security testing to ensure that the required functionality is provided and that OutThink's security is not compromised.

OutThink will apply appropriate secure configurations to all hardware devices (standard, where devices are similar, and it is appropriate to do so) and will deploy robust endpoint security software and mobile device management (MDM) systems where it deems necessary to protect against information loss and theft and to mitigate against external attack.

5.10. Communications Controls

Information Security controls must be applied to all communication mechanisms deployed by OutThink.

OutThink's electronic communications mechanisms such as email, conferencing and instant messaging must be protected by a combination of appropriate technical safeguards and user enforced processes to protect OutThink from risk of abuse, interception, and malicious usage.

Access to OutThink's production cloud platform will be enabled only for senior named administrators, IT/DevOps resources and Application Support Team personnel, and include additional controls such as enforced MFA (Multi Factor Authentication), VPN (Virtual Private Network), IP (Internet Protocol) access restriction and/or sign-in risk analysis and detection policies.

5.11. Third Parties Controls

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

The information security and cyber risk must be assessed before onboarding and managed throughout all stages of the relationship with external suppliers and sign-off from Information Security must be obtained.

All third parties who access our Information Assets must be supported by agreed upon and approved contracts that specify security arrangements.

5.12. Internal audit

An internal audit program will be operated to provide assurance that organization's information security and data protection policies are effectively implemented and there is adequate information security governance in place.

5.13. Incident / Breach Response Controls

OutThink's VP of People and CTO are provided with a documented set of actions to perform in the event of a disaster affecting our information assets to enable key business processes to be resumed within critical timescales.

Information security incident response plans, procedures, and templates for key breach scenarios, linked to Disaster Recovery and Business Continuity (where appropriate) must be developed documented and tested throughout OutThink. Refer to OutThink's Business Continuity Plan.

Employees who suspect an information security incident and / or actual breach of security must report the incident as per the Information Security Incident Management Process immediately.

Information security incidents must be reported immediately as per OutThink Standard Notification Process by OutThink's Privacy Officer to the affected Customer and where personal information was affected - to appropriate regulators (in cases GDPR (General Data Protection Regulation) reporting conditions were met).

6. Roles and Responsibilities

6.1. Department Management

- Primary and overarching responsibility for information security and cyber risk management within their area or responsibility and ensuring the appropriateness and effectiveness of their risk-based information security controls.
- Accountability for effectively conducting information security and cyber risk assessments within their areas of responsibility in compliance with the Control Objectives stipulated within this Policy.
- Ensuring all relevant staff are aware of and comply with the security policies and standards that apply to their duties and have sufficient training to do so.

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

6.2. Engineering Department

- Responsible for providing security operations and engineering services to the company.
- Ensuring that control objectives are developed to support the Policy and outline how Information should be stored, processed, or transmitted securely on OutThink's Systems.
- Identification of information and cyber security threats and vulnerabilities, monitoring for and responding to security incidents.
- Identifying and managing information security issues, events, and incidents.
- Ensuring that the technical security policies and control objectives set by OutThink are adhered to.

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK

7. Version Control

Version	Date	Description of Change	Approved by
1.0	10 January 2019	The first full version of the policy was issued.	Flavius Plesu, OutThink CEO
1.1	27 September 2019	Review	Vadim Gordas (CISA, CRISC, CISSP, CIPP/E, 27001 LA)
1.2	22 June 2020	Reformatted and insertion of customer data sharing policy and new staff controls, by M.Slater (Head of Engineering)	Brit Pedaja, Privacy Officer
1.3	18 September 2020	Scheduled Review	Vadim Gordas (CISA, CRISC, CISSP, CIPP/E, 27001 LA)
1.4	12 July 2021	Scheduled review	Vadim Gordas (CISA, CRISC, CISSP, CIPP/E, 27001 LA)
1.5	28 July 2022	Added requirement for periodic ISMS Management Review	Vadim Gordas (CISA, CRISC, CISSP, CIPP/E, 27001 LA)
1.6	12 February 2023	Role review and update	Matt Slater, CTO
1.7	7 July 2023	Scheduled review	Vadim Gordas (CISA, CRISC, CISSP, CIPP/E, 27001 LA)

hello@outthink.io

OutThink Ltd,
35 New Broad Street,
London EC2M 1NH, UK