Information Security Policies and Procedures

Prepared for

Revised: July 2024

Introduction

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately secured.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

The objectives identified in this plan represent commonly accepted goals of information security management as identified by the ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management*.

Terms and Definitions

asset	anything that has value to the firm
control	means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
information security	preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
policy	overall intention and direction as formally expressed by management
risk	the likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact
risk assessment	overall process of risk analysis and risk evaluation
risk evaluation	process of comparing the estimated risk against given risk criteria to determine the significance of the risk

risk management	coordinated activities to direct and control the firm with regard to risk
threat	a potential cause of an unwanted incident, which may result in harm to a system or the firm
vulnerability	a weakness of an asset or group of assets that can be exploited by one or more threats

Roles and Responsibilities

Chief Technology Officer (CTO)	Responsible for information security in the firm, for reducing risk exposure, and for ensuring the firm's activities do not introduce undue risk to the enterprise. The vice president also is responsible for ensuring compliance with client security policies, standards, and security initiatives. Responsible for coordinating actions in response to an information security incident. Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.
User	Responsible for complying with the provisions of policies, procedures and practices.

Security Program

Information security is a business issue. The objective is to identify, assess and take steps to avoid or mitigate risk to the firm's information assets. Governance is an essential component for the long-term strategy and direction of an organization with respect to the security policies and risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that provides an appropriate venue to inform and advise executive, business and information technology management on security issues and acceptable risk levels.

The Chief Technology Officer shall be responsible for advising OutSolve Principals on changes to the information security policy, as well as coordinating with the users what the risk issues are and how to avoid any security threats or vulnerabilities.

In order to implement and properly maintain a robust information security function, OutSolve recognizes the importance of:

- Understanding OutSolve's information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage OutSolve's information security risks in the context of overall business risks;
- Ensuring all users of the firm's information assets are aware of their responsibilities in protecting those assets;
- Monitoring and reviewing the performance and effectiveness of information security policies and controls; and
- Continual improvement based on assessment, measurement, and changes that affect risk.

Security Components

Risk Management and Risk Assessment

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risk management is critical for OutSolve to successfully implement and maintain a secure environment. Risk assessments will identify, quantify, and prioritize risks against the firm's criteria for risk acceptance and objectives. The results will guide and determine appropriate action and priorities for managing information security risks and for implementing controls needed to protect information assets.

Risk management will include the following steps as part of a risk assessment:

1. Identify the risks
    a. Identify assets and the associated information owners
    b. Identify the threats to those assets
    c. Identify the vulnerabilities that might be exploited by the threats
    d. Identify the impacts that losses of confidentiality, integrity and availability may have on the assets

2. Analyze and evaluate the risks
    a. Assess the business impacts on the firm that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of those assets

   b. Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented
   c. Estimate the level of risks
   d. Determine whether the risks are acceptable

3. Identify and evaluate options for the treatment of risk
   a. Apply appropriate controls
   b. Accept the risks
   c. Avoid the risks
   d. Transfer the associated business risks to other parties

4. Select control objectives and controls for the treatment of risks

It is recognized no set of controls will achieve complete security. Additional management action will be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support goals and objectives.

As part of OutSolve's formalized Risk Assessment program, and to help identify, evaluate, and eliminate observed risks, OutSolve has contracted VikingCloud (formerly SecureTrust) to provide quarterly vulnerability scans of external endpoints and reporting of its systems and networks to determine if any risks exist and if so, to recommend appropriate action to resolve said risk. Likewise, OutSolve is contracted with Restech to provide quarterly vulnerability scans and penetration testing for both authenticated internal and external endpoints, and remediate any risks identified.

OutSolve has also completed a Business Impact Analysis (BIA), which is reviewed annually, to determine what impact these identified risks may cause to the operations of OutSolve, and what recovery time is involved to bring OutSolve's operations back online.

Security Policy

The objective of information security policy is to provide management direction and support for information security in accordance with OutSolve's business requirements and governing laws and regulations. Information security policies will be approved by management, and published and communicated to all employees and relevant external parties. These policies will set out OutSolve's approach to managing information security and will align with relevant industry policies.

Information security policies will be reviewed at annually, on or around January 1st, or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. Each policy will have an owner who has approved management

responsibility for the development, review, and evaluation of the policy. Reviews will include assessing opportunities for improvement of OutSolve's information security policies and approach to managing information security in response to changes to OutSolve's environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Organization of Information Security

Information security will be managed within OutSolve. Management will approve information security policies, assign security roles, and coordinate and review the implementation of security across the firm. Information security will be coordinated across different parts of the firm with relevant roles and job functions. Information security responsibilities will be clearly defined and communicated. Security of OutSolve's information assets and information technology that are accessed, processed, communicated to, or managed by external parties will be maintained.

Asset Management

The objective of asset management is to achieve and maintain appropriate protection of OutSolve's assets. All assets will be identified. Owners of information assets will be identified and will have responsibility for identifying the classification of those assets and maintenance of appropriate controls. To ensure information receives an appropriate level of protection, information will be classified to indicate the sensitivity and expected degree of protection for handling. Rules for acceptable use of information and information assets will be identified, documented, and implemented. By default, the CTO will be the custodian of all information and data assets, and will be the owner of the delegation process to determine who will have access to these assets. Each client's data assets are assigned to a team and lead consultant who will be responsible for day-to-day interactions with that client's data.

Once an asset has been identified (such as a data file, electronic report, etc), it will be filed appropriately on our file server with the appropriate security permissions given to only the users who require access to said asset. This asset is logged and managed in-house using custom proprietary software. In the event of a system failure, OutSolve can easily review the logs and determine what assets are missing and retrieve those assets from our off-site backup provider.

All physical assets, such as workstations, laptops, and removable media, will be logged and monitored. When a physical asset is no longer needed and will be decommissioned, it will be removed from the inventory log. An inventory audit will be performed quarterly to determine if the inventory log matches the physical inventory.

Human Resources Security

All new hires will undergo criminal background checks as well as E-Verify verification. All employees and third party users of OutSolve's information and information assets will understand their responsibilities and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse. Security responsibilities will be addressed prior to employment in position descriptions and any associated terms and conditions of employment. Where appropriate, all candidates for employment and third party users will be adequately screened, especially for roles that require access to sensitive information. Management is responsible to ensure security is applied through an individual's employment with OutSolve.

All employees and, where relevant, third party users will receive appropriate awareness training and regular updates on policies and procedures as relevant for their job function on an annual basis. All employees will be asked to sign an acknowledgement form that they understand the policies and procedures set forth.

Procedures will be implemented to ensure an employee's or third party's exit from OutSolve is managed and the return of all equipment and removal of all access rights are completed.

Physical and Environmental Security

The objective of physical and environment security is to prevent unauthorized physical access, damage, theft, compromise, and interference to OutSolve's information and facilities. Locations housing critical or sensitive information or information assets will be secured with appropriate security barriers and entry controls, including locked doors and monitored burglar and fire alarms. They will be physically protected from unauthorized access, damage and interference. Secure areas will be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with company policies.

Software Development Security

All software development performed by OutSolve's developers or commissioned on behalf of OutSolve shall adhere to secure software development practices, including, but not limited to, accounting for OWASP Top 10 vulnerabilities. All development is completed in segregated environments, where development,

testing and production are separated. No production data will be used for development or testing purposes. Only authorized personnel will have access to code repositories and all access will be secured by IP restrictions and VPN access. All code changes must be tested before being pushed into the production environment, and code will be periodically scanned and reviewed for security vulnerabilities. For more details, please see OutSolve's Software Development Life Cycle policy.

Firewall and Network Security

To prevent malicious and fraudulent access to the internal network, OutSolve has the WatchGuard Firewall appliance installed. The WatchGuard firewall provides Application Control, Intrusion Prevention Services, WebBlocker, Gateway Antivirus, and Reputation Enabled Defense. The device is constantly searching for and updating its database for threats such as buffer overflows, SQL injections, cross-site script attacks, DOS attacks, virus/malware, and URL phishing before it reaches the end users. This appliance also provides extensive logging and early warning capabilities to keep the internal network safe from known and emerging threats.

In addition to the firewall and monitoring capabilities, OutSolve also requires remote employees to only access the internal network via secure network connections. Employees are discouraged from accessing the internal network from public wireless networks, publicly accessible hotspots, and other non-secure locations, unless explicitly approved by management and using secure encrypted connection methods, such as a VPN with Two Factor authentication.

In regards to network management and system administration, Microsoft Baseline Hardening standards are used to secure the network. Windows Group Policy Objects (GPOs) are used to apply consistent hardening to domain computers. IISCrypto is used to set Best Practice standards across the network. SSH is set to the higher ciphers on network equipment. Office365 Data Loss Prevention (DLP) is set to monitor emails for sensitive information with alerting. Perch / Connectwise SIEM is in place to monitor and alert of any suspicious network activity. Huntress is used on endpoint machines for file system integrity and to alert if any changes occur to test files on the machines to warn of an attempted ransomware attack. Writing to removable media is blocked except for a few authorized users and encryption is enforced. Administrator credentials are stored in password vaults and alerts are sent if any domain or Entra ID admin accounts are created or removed.

Data Security

OutSolve values client data and treats data security threats seriously. All OutSolve servers, desktops, and laptops utilize Webroot for anti-virus scanning, as well as Zero-day protection against emerging threats. While employees are restricted from visiting suspect sites, such as file-sharing or other illicit websites via firewall rules, Webroot also provides for network intrusion scans to prevent a hacked website from infecting an OutSolve computer. All computers are auto-updated to keep up with the latest anti-virus updates, and are checked on a monthly basis to determine that updates are being applied properly. Systems are scanned weekly for viruses and malware. Operating system updates are applied on a bi-weekly basis, and all external endpoints are fully scanned quarterly for vulnerabilities using VikingCloud (formerly SecureTrust) PCI service. Annual vulnerability scanning and penetration testing is performed by Restech.

Media or equipment that can be removed from the OutSolve offices (laptops, disks, flash memory, etc.) are encrypted to prevent being intercepted by a third-party. All mobile devices containing stored data owned by OutSolve must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, PDAs, tablets, and cell phones.

Users are expressly forbidden from storing company or client data on devices that are not issued by OutSolve. Any OutSolve data stored on a cell phone or PDA must be saved to an encrypted file system using OutSolve approved software. OutSolve shall also employ remote wipe technology to remotely disable and delete any data stored on a OutSolve PDA or cell phone which is reported lost or stolen.

OutSolve uses PGP Desktop to perform media or device encryption and utilizes 256 bit encryption.

Document and Data Retention

OutSolve follows the following rules when it comes to document and data retention:

a. All paper documents (including, but not limited to, sample reports, employee forms, policy statements, etc.) will be destroyed after three years, unless otherwise stated in the initial client contract;

b. All other electronic documents/data will be deleted from all individual computers, databases, networks, and back-up storage after three years, upon client request;

c. No paper or electronic documents or client data will be destroyed or deleted if pertinent to any ongoing or anticipated OFCCP audit.

At any time, and within the above mentioned three year period, a client may request OutSolve to remove specific employee data in adherence with the client's

or OutSolve's Data Privacy Policy. Also, as part of this policy, all data removal requests will also be enacted upon any backups that are restored.

Hardware Destruction

Periodically, OutSolve will determine if workstation hardware is still usable. If a hardware asset is no longer working or usable, and cannot be repaired, the hardware will be taken out of inventory, and will be made ready to be destroyed or recycled. A local third party vendor services provider will provide or facilitate any hardware destruction needed, including sanitizing hard drives or removable memory before destruction, as well as providing documentation that said hardware was destroyed properly.

Communications and Operations Management

Responsibilities and procedures for the management and operation of all information processing will be established. As a matter of policy, segregation of duties will be implemented, where appropriate, to reduce the risk of negligent of deliberate system or information misuse. Precautions will be used to prevent and detect the introduction of malicious code and unauthorized mobile code to protect the integrity of software and information. To prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities, media will be controlled and physically protected. Procedures for handling and storing information will be established and communicated to protect information from unauthorized disclosure or misuse.

To detect unauthorized access to information and information systems, systems will be monitored and information security events will be recorded. OutSolve will employ monitoring techniques to comply with applicable industry policies related to acceptable use.

OutSolve uses a WatchGuard security appliance to harden, monitor, and maintain a secure network. Also, all networking events are logged and inspected using Azure, O365, Perch SIEM and Webroot's monitoring logs.

Clear Desk and Screen Policy

All employees are advised to have only a specific client's data on their desk or screen at one time. Upon completion of the client service, employees are instructed to close or remove the data or copy from the desk or screen before opening another client's data. Employees are also instructed to close out of all files and lock their workstations when they leave for break, lunch, or the end of the day.

Security Awareness Training

Security awareness training is provided to all staff at time of hire and on an annual basis. Training is performed by the CTO or a representative from the OutSolve Training committee and covers a range of topics including, but not limited to: password security, email security, data encryption and disposal, data confidentiality, and other policy overviews. Upon completion, all staff are required to sign a document stating they understand the security policies set forth. OutSolve also utilizes KnowBe4 phishing campaigns to continuously test and train employees.

Information Classification

All client data received is classified as sensitive and confidential, regardless of the data contents. It is treated in such a way that adheres to all mentioned secure policies related to encryption, clear desk, and disposal.

Privacy Policy

To complete Affirmative Action Plan reporting and consulting, Compensation Analyses, and other compliance related services, OutSolve requires specific data elements, defined by OutSolve's Requested Data Elements forms. OutSolve will not disclose this data to any subcontractor or other third party, without the written permission of the client. All data is secured per the description of this document, and OutSolve will take all reasonably necessary steps to protect this data. As mentioned above, all client data is classified as sensitive and confidential, and treated as such. All OutSolve staff are bound by a confidentially and non-disclosure agreement, which further protects client data.

Internet Usage

To prevent unauthorized access and security breaches, all staff are restricted from visiting obscene, explicit or restricted internet sites, downloading music or movies, using chat/messenger services, and other non-work related internet functions. OutSolve has implemented the WatchGuard firewall with filtering to help prevent this activity from occurring. This policy is reinforced to staff during the annual security awareness training as well.

Access Control

Access to information, information systems, information processing facilities, and business processes will be controlled on the basis of business and security

requirements. Formal procedures will be developed and implemented to control access rights to information, information systems, and services to prevent unauthorized access. Windows Active Directory\Microsoft Entra is used to manage user and privileged account access. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords. Users will be made aware of their responsibilities to ensure unattended equipment has appropriate protection. Steps will be taken to restrict access to operating systems to authorized users. Protection will be required commensurate with the risks when using mobile computing and teleworking facilities.

All network user passwords are changed on a 90 day basis, and must meet a minimum set of requirements. These requirements are:

- Must be at least 8 characters long
- Must contain a combination of at least three of the following characters: uppercase letters, lowercase letters, numbers, symbols (punctuation marks).
- Must not contain a portion of the user's name.
- Must not be the same password as the last 20 passwords used
- Minimum Password age of 1

All desktop sessions feature an inactivity timeout, where after 15 minutes, the session will logoff. Finally, only authorized users have access to the secure OutSolve network, as well as the client website. There is a five login attempt limit on network user accounts before the account is locked for 30 minutes. All network accounts require multi-factor authentication (MFA) to access the network. Also, all user accounts are reviewed quarterly to determine if they are still needed and active, and do not compromise the integrity of the network.

All website users who request access to the client website must go through a manual authorization process before they can be granted access to the site. Once authorized, the website user will only have access to the assets they are permitted to view. User accounts are reviewed annually to determine if the user account is still valid. If it is determined the user is no longer with the client company, their user access is revoked.

All client portal user passwords are required to reset their password on a 90 day basis, and must meet a minimum set of requirements. These requirements are:

- Must be at least 8 characters long
- Must contain a combination of at least three of the following characters: uppercase letters, lowercase letters, numbers, symbols (punctuation marks).
- Must not contain a portion of the user's name.

After five failed attempts to login to the client portal, the account is locked for 15 minutes.

Information Systems Acquisition, Development and Maintenance

Policies and procedures will be employed to ensure the security of information systems. Encryption will be used, where appropriate, to protect sensitive information at rest and in transit. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner. Technical vulnerability management will be implemented with measurements taken to confirm effectiveness.

OutSolve utilizes AES 256-bit encryption for data at rest. TLS 1.2 or higher is used for transmitting data on its client website, as well as in transmission of data to and from its FTP site. Clients also have the ability to encrypt all sent data files using PGP encryption. OutSolve keeps a record of all clients who are issued keys. The keys issued to clients are only used for the client to send data to OutSolve and are set to never expire. The sent client data is placed on an FTP server by the client, which is then removed promptly (within a 2 hour window) by OutSolve. Only known IP addresses are allowed through the FTP server firewall. All software source code is maintained by the CTO and is only accessible by him. All software passwords are encrypted using the AES encryption algorithm.

Information Security Incident Management

Information security incidents will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures will be established and communicated to all users, as well as affected clients. Responsibilities and procedures will be established to handle information security incidents once they have been reported.

Anonymous reporting of incidents has been established via an anonymous reporting portal. The portal will be checked on a periodic basis by management to determine if any incidents have been reported. These incidents will be logged, and the Incident Response Plan will be put into effect.

It is OutSolve's goal to notify users and affected clients within 24 hours of a discovered incident. OutSolve will immediately begin work on corrective action, including, but not limited to, closing the breach, determining the extent of the breach, and, if applicable, reversing the effects of the breach. A more detailed plan of this action can be found in OutSolve's Incident Response Plan document.

In the event of a compromise involving encrypted client data, immediate reissuance of the encryption keys is performed and all clients with keys will be reissued a new key.

Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process will be established to minimize the impact on OutSolve and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls. A managed process will be developed and maintained for business continuity throughout the firm that addresses the information security requirements needed for OutSolve's business continuity.

OutSolve's Business Continuity and Disaster Recovery Plan establishes this in further detail, and is available upon request.

Compliance

The design, operation, use, and management of information and information assets are subject to contractual security requirements. Compliance with requirements is necessary to avoid breaches of any contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.

Controls will be established to maximize the effectiveness of the information systems audit process. During the audit process, controls will safeguard operational systems and tools to protect the integrity of the information and prevent misuse.