PIPELINESIGNALS
Follow Your Fans

Overview of The Information Security Management System (ISMS)

Introduction

This document serves as a questionnaire and FAQ to the many information security systems, data and privacy questions you may have about our products & services.

Like you, we take this part of our offerings very seriously and encourage you to provide this document to internal parties that may request such documentation. Alongside other Data & Privacy artifacts, it forms the basis of how we will receive, view, modify, store and deliver data to you.

If you have any questions or concerns, please let us know.

Section 1 - Overview of The Information Security Management System (ISMS) of Pipeline Signals

1. Have you documented the internal and external factors affecting your Information Security Management System (ISMS)?
    a. Yes. All people, process and technology used and included in the service is documented.
2. Have you documented the needs and expectations (including requirements) of all interested parties relevant to the ISMS?
    a. Yes. All needs, expectations and requirements of internal and external parties are documented. This includes all people, processes and related technology that enables this.
3. Have you determined the scope (i.e., the boundaries and applicability) of your ISMS?
    a. Yes. Our ISMS is bounded by the technology set that we use.
4. Have you formally established the ISMS and ensure its continual improvement?

    a. Yes. We ensure that continual improvement is at the core of our strategy. As technology we leverage evolves, our processes evolve also.
5. Have you assessed your security practices against the NIST CyberSecurity Framework, ISF Standard of Good Practice or ISO 27001/2, SSAE16, PCI DSS, HIPAA?
    a. As we use readily available third party cloud based technology, they abide by and use many of these frameworks. We provide a service using this technology.
6. Is any Risk Management Framework based on the industry standard (e.g. ISO27005) implemented within your organization?
    a. Our risk management processes are in place and are within the boundaries of open cloud and technology service providers that we use to execute our managed service.
7. Is the Information Security Management System (ISMS) implemented within your organization (e.g. ISO27001)?
    a. Please, provide a detailed scope of implemented ISMS and confirm whether its scope covers all areas where a customer's data is/will be transmitted, stored or processed.
    b. Here is the process we use.
        i. Step 1a: during onboarding, we require your organization to complete a confidential survey using Zoho Survey. This tool is compliant across all technology and cybersecurity data & privacy frameworks.
        ii. Step 1b: during onboarding, we use a secured Google Sheets instance to request your customer, prospect and competitor accounts information. This is transmitted only between: (a) the people in your organization listed as "program managers" (b) the people in our organization listed as "customer success managers" and/or "analysts". This shared information does not leave this Google Sheets instance and is not shared with anyone outside of the parties listed above. This tool is compliant across all technology and cybersecurity data & privacy frameworks.
        iii. Step 2a: in our organization, only the key analysts and customer success managers are responsible for monitoring the accounts for sales intelligence data. Once found, we enter this data into a proprietary database hosted on Digital Ocean. All client information is divided into their own instances and never cross-promoted or cross-checked.

iv. Step 2b: the sales intelligence data we discover for your accounts is placed in the secured shared Google Sheets instance with your organization and key listed members only.
v. Step 3: once the data is in the organization's possession, you may use the data in aiding sales account development and marketing activities.
vi. In summary, we provide a monitoring service that provides sales intelligence data to your organization. In the execution of this service, we utilize openly available, yet well-known and secure technologies. In the entire process, the following technologies are used: Zoho Surveys (powered by Zoho Cloud), Google business applications (such as Sheets, Docs, etc., powered by Google Cloud), Digital Ocean (where our basic client database is housed).

8. Has your organization experienced any reportable breaches of sensitive/confidential information within the last two years?
    a. If yes, provide a summary of the breach and corrective actions.
    b. No, there have been no breaches of sensitive or confidential information within the last two years.
9. Has your organization experienced a significant cybersecurity incident within the last two years?
    a. If yes, provide a general summary of the cybersecurity incident and corrective actions.
    b. No, we have not experienced any cybersecurity incident within the last two years.

Section 2 - Leadership

1. Has top management demonstrated leadership and commitment to information security?
    a. Yes, absolutely. We are committed and hold regular meetings to review and better our approach to information security.
2. Has top management communicated a documented information security policy throughout the organization?
    a. Yes. Our team comprises information analysts who are trained on and abide by our information security policies.

3. Has top management assigned and communicated defined information security roles and responsibilities throughout the organization?
    a. Yes. There is protocol that is followed with key personnel such as Head of Analysts and Chief Privacy Officer. Roles and responsibilities are understood and adhered to.

Section 3 - Planning

1. Do you have a well-defined and documented procedure for identifying information security risks and opportunities for improvement that are relevant to the context of the organization (4.1) and needs and expectations of interested parties (4.2)?
    a. Yes. We are constantly monitoring for improvements. However we've kept our service low-friction in terms of process and we use openly available tools and platforms to reduce friction.
2. Do you have a well-defined and documented procedure for assessing information security risks and opportunities for improvement?
    a. Yes. We are constantly monitoring for improvements. However we've kept our service low-friction in terms of process and we use openly available tools and platforms to reduce friction.
3. Do you have a well-defined and documented procedure for treating information security risks and opportunities for improvement?
    a. Yes. We are constantly monitoring for improvements. However we've kept our service low-friction in terms of process and we use openly available tools and platforms to reduce friction.
4. Do you have a well-defined and documented procedure for identifying information security objectives and creating "S.M.A.R.T." plans for achieving them.
    a. ISMS objectives should be "S.M.A.R.T."—i.e., Specific, Measurable, Achievable, Relevant, and Time bound.
        i. Yes, this is in place.
        ii. Specific Goals to ensure security: we never share credentials with any person or entity outside the core working group. This includes (a) the program manager(s) in your organization (b) the Head Analyst on our team (c) the customer success manager on our team and (d) key analysts on our team responsible for data analysis to find the sales intelligence data.

iii. Measurable: because we have rules on who should access the data, its access points are measured by default.
iv. Achievable: as we use third-party and commonly available data platforms, achieving our goals is doable.
v. Relevant: we achieve relevancy by adhering to the process and thereby ensuring information/data privacy and security.
vi. Time Bound: our terms and conditions in the contract dictate how long we keep providing access to your organization. Once our contract is complete with your organization, we simply remove your access. The data stays secure in our end for a period of 3 years and then is discarded.

5. Have you created a "statement of applicability" that documents the ISO 27001 Annex A controls that have been deemed applicable to the ISMS as a result of a risk assessment?
    a. Not applicable.

Section 4 - Support

1. Have you allocated the resources necessary for achieving your objectives and to ensure continual improvement of your ISMS?
    a. Have you determined and provided the resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS?
    b. Yes. We do this regularly in the onboarding of new analysts and also in quarterly meetings to review our existing processes for further improvement.
2. Have you ensured that in-scope personnel have the necessary levels of information security education, training and experience?
    a. Are individuals within ISMS roles competent and is the competence documented appropriately?
    b. Yes. There is an official document pertaining to policy and procedure with respect to information collection, viewing, analysis, delivery and feedback.
3. Do you ensure organization-wide awareness of information security policies and procedures, and individual roles and responsibilities with respect to security?

    a. Yes. There is an official document pertaining to policy and procedure with respect to information collection, viewing, analysis, delivery and feedback.
4. Do you have well-defined and documented policies and procedures for handling both internal and external communications about the ISMS?
    a. Yes. There is an official document pertaining to policy and procedure with respect to information collection, viewing, analysis, delivery and feedback.
5. Do you have an official documentation structure or hierarchy, whereby you include documentation that is directly required by ISO 27001, as well as documentation that is deemed necessary for an effective information security program?
    a. Yes. There is an official document pertaining to policy and procedure with respect to information collection, viewing, analysis, delivery and feedback.
6. Do you have well-defined and documented policies and procedures for ensuring the proper review and approval of new or updated ISMS documentation?
    a. Yes. There is an official document pertaining to policy and procedure with respect to information collection, viewing, analysis, delivery and feedback. It's reviewed in team and management meetings quarterly.
7. Do you have well-defined and documented policies and procedures for ensuring proper control and handling of ISMS documentation?
    a. Yes. There is an official document pertaining to policy and procedure with respect to information collection, viewing, analysis, delivery and feedback. The actual policy is reviewed quarterly and can only be changed and approved by management.

Section 5 - Operation

1. Do you have a process by which you plan, implement, control and review ISMS operations, and keep evidence of that process being followed?
    a. Yes. All quarterly meetings where the process is reviewed are documented.
2. Does your organization undergo risk assessments at planned intervals or whenever significant changes are planned or occur, and document the results?

    a. Yes, we do this quarterly. All ideas, feedback and improvement and results are documented.
3. Do you create and carry out documented risk treatment plans following risk assessments, and document the results?
    a. Yes. Our Head Analyst and Chief Privacy Officer are responsible for implementation.

Section 6 - Performance & Evaluation

1. Do you use metrics for evaluating the performance and effectiveness of your information security program?
    a. Every quarter we assess and measure that all customer data is secure and tabulate this for documentation.
2. Do you carry out internal audits of the ISMS against the ISO 27001 standard, at defined intervals?
    a. We review our processes every quarter and during this time we ensure that we are continuing to follow industry best practices.
3. Do you conduct management reviews of the ISMS at defined intervals?
    a. As we are a small team, we review our processes every quarter and during this time we ensure that we are continuing to follow industry best practices.

Section 7 - Improvement

1. Do you have a well-defined and documented corrective procedure for addressing 'nonconformities' with the ISO 27001 standard?
    a. Nonconformities are typically identified during audits. Nonconformities identified during an external certification or surveillance audit are typically accompanied by deadlines for completing corrective actions, and in some cases a failure to correct an unconformity can result in loss of certification.
    b. Yes. Since our processes are simple and adhere to SMART, implementation is not challenging for us. Typically feedback and

improvements (or even irregularities) are corrected within 10-15 business days of discovery.

2. Do you ensure, and document evidence of, the continual improvement of your information security program?
    a. Yes, all quarterly improvement review meetings are documented. All ideas that are agreed upon are implemented fairly quickly, within 10-15 business days of alignment.

Section 8 - Information Security Policies

1. Do you have a set of well-defined and documented information security policies and procedures that have been communicated to all relevant parties?
    a. Yes. All parties within our organization have been trained on formal information receipt, viewing, handling, delivery and feedback best practices.
2. Do you formally review your information security policies and procedures at defined intervals?
    a. Yes. We review information security policies every quarter.

Section 9 - Organization of Information Security

1. Have information security roles and responsibilities throughout the organization been defined and communicated to all relevant parties?
    a. Yes. All information security processes, policies and procedures have been defined and communicated with all key personnel working in and with Pipeline Signals.
2. Do you segregate duties, roles and responsibilities where applicable?
    a. Yes. Only key individuals of our team can manage and be responsible for customer information and its security.
3. Do you maintain a list of contact details for relevant authorities, and documented procedures on when and how to communicate with them?

    a. Yes. We are a small team so we know who these people are. We can assure they've been trained in appropriate information security procedures and communicate with them regularly.
4. Do you maintain contact/membership with relevant special interest groups, security forums and/or professional associations?
    a. Not applicable.
5. Have you integrated information security into your project management methodologies?
    a. Yes. Each customer engagement is a project. Following agile methodologies, we handle customer data with care.
6. Do you have a well-defined and documented mobile device policy, combined with technical and organizational measures designed for mitigating risks associated with mobile devices?
    a. Not applicable. Our data is not available on any mobile device by default.
7. Do you have a well-defined and documented teleworking policy, combined with technical and organizational measures designed to mitigate the risks associated with teleworking?
    a. Yes. Since we use third-party and well-known teleworking applications, our data adheres to industry standards and best practices by default.

Section 10 - Human Resource Security

1. Do you conduct appropriate background screenings on all job candidates, while ensuring compliance with all relevant legal and ethical requirements?
    a. Yes. We check character and professional references of all key job candidates, hires and personnel.
2. Do your written terms and conditions of employment define the information security responsibilities of both workforce personnel and the organization?
    a. Yes. We have official politics and procedures in place that must be signed, adhered to and is checked regularly for compliance.
3. Are all workforce personnel required by management to follow all applicable information security policies and procedures?
    a. Yes, absolutely.
4. Do you ensure that all workforce personnel receive an appropriate level of information security awareness, education and training?

    a. Yes, this starts right at the beginning of their employment or contract with us, during onboarding, and continues regularly throughout their tenure in quarterly information security meetings.
5. Do you have a formal disciplinary process that has been communicated throughout the organization?
    a. Yes. This is outlined in the policies and procedures documentation pertaining to information security.
6. Do you have a process for ensuring that information security responsibilities and duties that remain valid after termination or change of employment are communicated to all workforce personnel and enforced?
    a. Yes. All data is secure when an employee or contractor is terminated or leaves. This is by the terms of their contract with us which is enforceable under Canadian law (as we are a Canadian company, registered in the Province of Ontario).

Section 11 - Asset Management

1. Do you maintain an inventory of all information-related assets?
    a. Yes, all data we collect on behalf of customers is inventoried and kept secure on behalf of the customer. It is also shared securely with the customer and can be referred to on a real-time basis.
2. Do all assets have clearly defined owners who are aware of their responsibilities for the lifecycle of those assets?
    a. Yes. The same policies and procedures document outlined above governs the lifecycle of all data and information assets.
3. Do you have a documented acceptable use policy that has been communicated throughout the organization?
    a. Yes. We have an official policies and procedures document.
4. Does your formal termination process include the return of any information-related assets that had been issued to workforce personnel?
    a. There should be a role in charge of implementing any procedure that supports this.
    b. At no time is any information ever in the possession of employees or contractors who may work on a customer engagement/project. All data and information is kept secure and confidential in the shared client Google Sheet. Upon leaving the job and/or termination of employment

or contract, access is simply turned off. That person cannot access the data. Also they are legally bound by the terms and conditions of their contract which is enforceable and highly premised on information security.

5. Do you have a process (or scheme) for classifying information, based on legal requirements, value, criticality and sensitivity?
    a. Not applicable for the data and information we provide.
6. Do you have procedures for labeling information based on classification?
    a. Not applicable.
7. Do you have procedures for handling assets based on classification?
    a. Not applicable.
8. Do you have procedures for managing removable media based on classification?
    a. Not applicable.
9. Do you have procedures for secure disposal of media?
    a. Yes. If a customer ever wants their data disposed of, they can notify us by writing to our Chief Privacy Officer by email (dataprivacy@pipelinesignals.com). Within 30 business days, we will permanently delete all instances of data from our database and Google Sheets.
10. Do you protect media that contains information during transportation?
    a. Not applicable.

Section 12 - Access Control

1. Do you have a well-defined and documented access control policy?
    a. Yes. Access control is defined and documented and only key internal stakeholders can get access to customer data for the sole purpose of analyzing it and storing it securely for the customer.
2. Do you ensure that users only have access to network and network services that they have been specifically authorized to use?
    a. Yes. Our employees and contractors only have access to the appropriate applications and/or platforms relevant to performing their work. No other access points are granted.
3. Do you have a well-defined process for user registration and de-registration?

    a. Yes. Upon registration, the customer follows our secure onboarding process. Upon deregistration they can write to us at dataprivacy@pipelinesignals.com or their customer success manager and within 30 business days all customer information provided to us shall be removed.
4. Do you have a well-defined process for provisioning (assigning or revoking) user access for all systems and services?
    a. Yes. Because we use commonly available third-party cloud provider software and platforms, provisioning, assigning and revoking access is straightforward and easy to perform.
5. Do you restrict and control privileged access rights?
    a. Yes, absolutely. Even with a customer's Google Folder, various files are only shared with various members of the team. For example, customer success managers retain view access while analysts retain full view and edit access. This ensures that minimal friction with data and information is achieved, thereby minimizing chances of data disruption.
6. Do you have a well-defined process for allocating secret authentication information?
    a. Yes. We rely on the authentication of our commonly used third party cloud based software applications. Here, authentication is native and built in and assures strict best in class industry compliance.
7. Do you regularly review user access rights with asset owners?
    a. Yes, absolutely. When a new user from the customer or an internal employee or contractor is added, the entire access rights of each member is reviewed. It confirms that the right people have the appropriate level of access.
8. Do you ensure the removal of access rights of users upon termination?
    a. Yes. For internal employees or contractors, we have a specific and documented process to ensure that all access is revoked. For customer contacts, we rely on our customer contact person (whom we refer to as "the program manager") to inform us so we can revoke access immediately.
9. Do you require users to follow policies and procedures on the appropriate use of secret authentication information?
    a. Not applicable as we allow users to follow the best practices and policies and procedures of third party commonly available software applications and platforms.
10. Do you restrict access in accordance with your access control policy?

    a. Yes, absolutely. Even with a customer's Google Folder, various files are only shared with various members of the team. For example, customer success managers retain view access while analysts retain full view and edit access. This ensures that minimal friction with data and information is achieved, thereby minimizing chances of data disruption.
11. Do you have a secure log-on procedure for controlling access to systems and applications, in accordance with the access control policy?
    a. Yes. We require secure passwords and 2FA (two factor authentication).
12. Do you use a password management system?
    a. Not applicable.
13. Do you restrict and control the use of utility programs that have the ability to override system and application controls?
    a. Yes. There is master-level access that enables the overriding of system and application controls.
14. Do you restrict access to program source code?
    a. Yes. Only our Head of Product and Head of DevOps and key senior executives have access to program source code.

Section 13 - Cryptography

1. Do you have a well-defined and documented policy on the use of cryptographic controls?
    a. Not applicable.
2. Do you have a well-defined and documented policy on cryptographic key management?
    a. Not applicable.

Section 14 - Physical & Environmental Security

1. Do you have defined security perimeters around areas with sensitive or critical information?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.

2. Do you ensure that only authorized personnel are allowed access to secure areas?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
3. Do you ensure the physical security of offices, rooms and facilities?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
4. Have you put physical protection measures in place to limit the impact of natural disasters, malicious attacks or accidents?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
5. Do you have well-defined and documented procedures for working in secure areas?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
6. Do you control access to delivery and loading areas?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
7. If there are designated delivery/loading areas, is access from those areas isolated from information processing systems/facilities?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
8. Do you consider environmental threats and hazards, as well as opportunities for unauthorized access, when choosing locations and physical controls for protecting equipment?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our

application providers and platforms to ensure physical security and information access controls using industry best practices.

9. Do you ensure the protection of equipment from power failures or other disruptions?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
10. Do you ensure the protection of cables from interception, interference or damage?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
11. Do you have a process for maintaining equipment?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
12. Are controls in place to ensure that assets are not taken off-site without prior authorisation?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
13. Do you ensure the security of assets that have been taken off-site?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
14. Do you ensure the secure disposal or reuse of equipment containing any sensitive, confidential or copyrighted information?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.
15. Are users made aware of how to properly protect unattended equipment?
    a. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our

application providers and platforms to ensure physical security and information access controls using industry best practices.

16. Do you have a well-defined and documented clear desk and clear screen policy?
    a. This should be distributed and monitored.
    b. Our services are performed in and provided in the cloud. Physical security controls are not applicable. We trust and rely on our application providers and platforms to ensure physical security and information access controls using industry best practices.

Section 15 - Operations Security

1. Do you have well-defined and documented operating procedures?
    a. Yes. Our entire service process is mapped out and delivered step-by-step according to said process. Every key stakeholder is aware of how to operate within the process, what tools or technology to use, when and how.
2. Do you have proper change management controls in place?
    a. Yes. Our entire service process is mapped out and this includes change management controls clearly defined.
3. Do you manage the use of resources to ensure proper system performance?
    a. Yes. We have a dedicated team that monitors and ensures proper system performance.
4. Do you ensure the separation of development, testing and operational environments?
    a. Yes. All development, testing and operations are conducted in different environments.
5. Do you have controls in place to detect, prevent and recover from malware?
    a. Yes. All data is segregated into different environments. Additionally, even within the live environment, all data is segregated by customer. If we ever have a malware incident, to find and correct it will be done without jeopardizing actual customer data. Also note that our work is delivered in the cloud via Google Sheets, so a chance of a malware incident occurring is extremely low.
6. Do you have a well-defined and documented backup policy?
    a. Yes. We have a documented backup policy.
7. Do you maintain, and regularly review, event logs?

    a. Yes. Per our process, if there are issues we refer to event logs as a part of the overall investigative process.
8. Are controls in place to protect event logs?
    a. Yes. These are backed up in the cloud.
9. Do you maintain logs of system administrator and operator activities?
    a. Yes for system administrators. Additionally, our third party cloud applications (such as Google apps) regularly capture and record this information on a real time basis.
10. Do you ensure clock synchronization for relevant information processing systems?
    a. Not applicable.
11. Do you have well-defined and documented procedures for controlling the installation of software on operational systems?
    a. Not applicable.
12. Are controls in place to ensure that technical vulnerabilities are quickly identified, evaluated and addressed?
    a. Yes, absolutely. Any technical difficulties are discovered quickly and must be resolved within up to 4 business hours. Note that this does not affect the actual deliverable data as that is always available via a private and secure Google Sheet instance.
13. Do you have a well-defined and documented policy restricting the installation of software on company-issued devices?
    a. Not applicable.
14. Are audits of information systems planned in a way that minimizes disruptions to business processes?
    a. Not applicable.

Section 16 - Communications Security

1. Are network security controls in place?
    a. Yes. Our network security controls fall under our cloud provider, Digital Ocean, and we abide by their adhered-to industry standards and best practices.
2. Do network services agreements include details on security mechanisms, service levels and management requirements?
    a. Not applicable.
3. Do your networks segregate different groups of information services, users and systems?

    a. Yes. We have different information access types, including for users and company program managers.
4. Are controls in place to protect the transfer of information?
    a. Yes. We only provide access to information to a few key internal stakeholders who are assigned to the project.
5. Do your contracts with external parties address the secure transfer of business information?
    a. Yes. Our contracts and agreements address the handling of all business related information.
6. Are controls in place to protect electronic messaging?
    a. Yes, all electronic communications are secure with our provider (either Zoom or Google Suite).
7. Do you have a well-defined and documented policy containing the requirements for confidentiality or non-disclosure agreements?
    a. Yes. This is in place.

Section 17 - System Acquisition, Development & Maintenance

1. Are information security related requirements considered when on-boarding new information systems or enhancements to existing information systems?
    a. Yes. When new applications or technologies are considered, we review the entire existing systems holistically.
2. Are controls in place for securing application services on public networks?
    a. Yes. All levels of access are available using secure methods of access (including two factor authentication).
3. Are controls in place for securing application services transactions?
    a. Yes.
4. Is there a procedure mandating the implementation and assessment of security controls for any software or system development?
    a. Yes. When we develop new software, security controls are always considered holistically as a part of the overall offering.
5. Is there a formal change control procedure?
    a. Yes. We have change control procedures standard in all development cycles.

6. Is there a procedure to ensure a review is carried out when operating platforms are changed?
    a. Yes, but this is not fully applicable as we use popular third party and commonly available software applications and platforms. We abide by and adhere to their industry standards and best practices.
7. Is there a procedure in place which requires when and how software packages can be changed or modified?
    a. Not applicable. Our usage of software applications (like Zoho applications or Google's Business Suite applications) means we're always using the latest versions.
8. Is there a procedure on detailing required security for systems?
    a. Yes.
9. Is there a secure development environment utilized by all projects during the system development life cycle?
    a. Yes.
10. Is externally developed code supervised and subject to a security review?
    a. Yes.
11. Is security tested as part of the development process for any system or applications?
    a. Yes. All features are tested for security implications.
12. Is there a procedure to accept new systems, applications, or upgrades, into the production environment?
    a. Yes. Nothing is introduced randomly. Every feature, application, upgrade or system is tested rigorously before entering into the production environment.
13. Is there a procedure for utilizing test data and making sure the data is suitable for the test?
    a. Yes. We always test new features with test data as required.

Section 18 - Supplier Relations

1. Do you have well-defined and documented policies and procedures for addressing supplier access to the organization's information?
    a. Yes. This is included in supplier contracts and during onboarding.
2. Are information security requirements addressed in vendor/supplier contracts?
    a. Yes. This is included during onboarding.

3. Do vendor/supplier contracts address information security risks associated with the use of subcontractors?
    a. Yes. This is included in supplier contracts and during onboarding.
4. Do you have a process for monitoring and reviewing vendor/supplier services?
    a. Yes. All work is securely done in accordance with our procedures in prescribed and secure Google Folders. We can see the end product and work in progress as well.
5. Do you have a process for managing changes made to vendor/supplier services?
    a. Yes. Our overall process has change request probabilities built in.

Section 19 - Information Security Incident Management

1. Do you have well-defined policies and procedures for managing information security incidents?
    a. Yes. We have the ability to catalog all instances.
2. Has a process for reporting information security events been communicated to workforce personnel?
    a. Yes. This is already a part of our quarterly meetings to review information security, related instances, ideas, feature updates and more.
3. Has a process for reporting information security weaknesses been communicated to workforce personnel?
    a. Yes. This is already a part of our quarterly meetings to review information security, related instances, ideas, feature updates and more.
4. Do you have a process for assessing information security events and whether they should be classified as incidents?
    a. Yes. We have a process for classifying what should be classified as a security event or incident.
5. Do you have a process for responding to information security incidents?
    a. Yes. This is already a part of our quarterly meetings to review information security, related instances, ideas, feature updates, solutions and more.

6. Do you evaluate information security incidents in order to learn from them and reduce the likelihood of similar future incidents?
    a. Yes. This is already a part of our quarterly meetings to review information security, related instances, ideas, feature updates, solutions and more.
7. Do you have well-defined and documented procedures for collecting evidence from information security incidents?
    a. Yes. This is already a part of our quarterly meetings to review information security, related instances, ideas, feature updates, solutions and more.

Section 20 - Information Security Aspects of Business Continuity Management

1. Have you identified and documented your organization's requirements for information security continuity during adverse situations?
    a. Yes. We have a continuity plan in place with stipulations on how we'll be able to service our customers in a secure way and deliver sales intelligence data in a secure manner.
2. Do you have well-defined and documented policies and procedures for information security continuity?
    a. Yes. We have a continuity plan in place with stipulations on how we'll be able to service our customers in a secure way and deliver sales intelligence data in a secure manner.
3. Do you have a process for regularly verifying, reviewing and evaluating your information security continuity controls?
    a. Yes. We do this quarterly as a part of a bigger information security meeting.
4. Do you have sufficient redundancies in place to ensure the availability of information processing facilities?
    a. Yes. We have multiple ways to ensure continuity of our service.

Section 21 - Compliance

1. Do you maintain a list of all legal and contractual requirements, along with well-defined and documented policies and procedures on how to meet those requirements?
    a. Yes. We abide by the terms and conditions of all commonly available third party cloud applications and platforms.
2. Do you have well-defined and documented procedures for ensuring compliance with legal and contractual requirements regarding intellectual property?
    a. Yes. Our policies and procedures are straightforward in the enablement of our service delivery and we do not in contravention of any intellectual property.
3. Are controls in place for the protection of records in accordance with legal, contractual and business requirements?
    a. Yes. Full controls are in place to ensure protection of records in a legal and contractual manner.
4. Are measures in place for ensuring privacy and data protection in accordance with legal and contractual requirements?
    a. Yes. Full controls are in place to ensure protection of data and privacy in a legal and contractual manner.
5. Are measures in place to ensure legal and contractual compliance with respect to the use of cryptographic controls?
    a. Not applicable.
6. Does the ISMS undergo independent reviews?
    a. Yes. We do have independent and trusted partners review our ISMS.
7. Does the ISMS undergo regular management review, to ensure organizational compliance with information security policies and procedures?
    a. Yes, this is done quarterly.
8. Do information systems undergo regular review for compliance with information security policies and procedures?
    a. Yes. No new system or application is onboarded or integrated into the work stack before confirmation of it complying with our existing policies and procedures.

Section 22 - Additional Information

1. Additional Information
    a. Please provide us with any additional information and/or documentation e.g. ISO 27001 Certificate / most updated SOC2 report, SIG Questionnaires or any other attestation you may have. In addition - if possible - provide us with a list of policies you have in place with a table of content.
        i. Not applicable. As our service is delivered using Google Business applications, we rely on these applications and Google to be in compliance with all ISO standards, SOC2 standards more.
    b. If you are PCI, FedRAMP regulated, please provide us with relevant certification as well.
        i. Not applicable.