**Active Cyber *Written Information Security Program (WISP)***

### OBJECTIVE:

The objective of Active Cyber, LLC (“ACTIVE CYBER”) in the development and implementation of this comprehensive written information security program (“WISP”), is to create effective administrative, technical and physical safeguards for the protection of personal information, including that of our employees. The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

For purposes of this WISP, “personal information” is defined as per the following regulations: first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account, credit card, or debit card number, with or without any required security code, access code, personal identification number, or password, that would permit access to a resident’s financial account; provided, however, that “personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

### PURPOSE:

The purpose of the WISP is to better: (a) ensure the confidentiality, integrity and availability of personal information and any other relevant sensitive data; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against the unauthorized access or purposeful/accidental destruction of such information, including the prevention of it being used in a manner that creates a substantial risk of identity theft or fraud; and (d) ensure that ACTIVE CYBER is compliant under any relevant local, state or federal security dictates.



### SCOPE:

In formulating and implementing the WISP, ACTIVE CYBER has addressed and incorporated the following protocols:

1. Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
2. Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Designed and implemented a WISP that puts safeguards in place to minimize those risks.
5. Implemented regular monitoring of the effectiveness of those safeguards and a communications plan that mandates the issuance of periodic security threat and awareness updates.
6. Implemented a comprehensive security training program to maintain employee awareness and compliance to applicable policies and procedures.

### DATA SECURITY COORDINATOR AND DATA SECURITY COMMITTEE:

ACTIVE CYBER has designated **Shawn Mathew** as the Data Security Coordinator to implement, supervise and maintain the WISP. The Data Security Coordinator will also facilitate the formation of a two-person Data Security Committee made of cross-functional ACTIVE CYBER employees and management. The Committee will meet periodically to review current security practices and any pertinent violations during the preceding period.

### INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the following mandatory measures are effective immediately:

* ACTIVE CYBER will only collect personal information of clients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations.
* Access to ACTIVE CYBER systems and applicable third party support applications shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose. Employee level access will be periodically reviewed and updated to reflect new or changing job responsibilities and employee status (terminated, etc).
* Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.
* A copy of the WISP is made available to all employees.
* All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP.



* Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any other device owned directly by the terminated employee.
* A terminated employee’s physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, access devices, company IDs, business cards, and the like shall be surrendered at the time of termination.
* Disciplinary action will be applicable in all cases of violation of the WISP, irrespective of whether personal data was actually accessed or used without authorization.
* All security measures, including the WISP, shall be reviewed on, at a minimum, an annually basis to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations.
* Should ACTIVE CYBER business practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information, the WISP will be reviewed to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations.
* The Data Security Coordinator or his/her designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise management of all reviews, including any recommendations for improved security arising from the review.
* The Data Security Coordinator shall maintain a secured and confidential master list of devices and passwords containing personal data.
* Current employees’ user IDs and passwords shall conform to accepted security standards. All passwords shall be changed on at least an annually basis, and more often if deemed necessary (e.g. seasonally).
* Employees are required to report any suspicious or unauthorized use of personal information to a supervisor or the Data Security Coordinator.
* ACTIVE CYBER shall maintain monitoring and auditing capabilities for all internal ACTIVE CYBER systems. Specific audit procedures shall be established for each relevant system and dictated by the criticality of the system and its associated data store.
* ACTIVE CYBER will routinely test the key controls and practices dictated by the WISP, with any violations or deficiencies being reported to ACTIVE CYBER senior management.



### EXTERNAL RISK MITIGATION POLICIES:

* Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
* Personal information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy.
* All system security software, including, anti-virus, anti-malware, and internet security, shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
* There shall be secure user authentication protocols in place that:
  1. Control user IDs and other identifiers;
  2. Assign passwords in a manner that conforms to accepted security standards, or applies

use of unique identifier technologies;

* 1. Control passwords to ensure that password information is secure.

### DAILY OPERATIONAL PROTOCOL

This section of our WISP outlines our daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured, and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees.

The Daily Operational Protocol shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and personnel responsible and/or authorized for the

security of personal information.

### Storage and Transmission Practices

All ACTIVE CYBER employees must guard against unauthorized access to sensitive data that is being transmitted over a public electronic communications network or stored

electronically. Such measures include encryption of any customer or partner data stored on desktops, laptops or other removable storage devices. Employees must never store sensitive data on an unencrypted medium or transmit sensitive data over an unencrypted channel. Use of SFTP, HTTPS, and PGP are the preferred methods of communication.

When disposing or scrubbing tangible devices used to store sensitive data, the device must be physically destroyed as to make it unreadable or fully overwritten a minimum of three times.

### Recordkeeping Protocol:

We will only collect personal information of clients and customers and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

Within 30 days of the publication of or any update to the WISP, the Data Security Coordinator or his/her designee shall perform an audit of all relevant company records to determine which records contain personal information, assign those files to the appropriate secured storage location, and redact, expunge or otherwise eliminate all unnecessary personal information in a manner consistent with the WISP.

Any personal information stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISP.

No personal information will ever be transferred to paper or any media other than ACTIVE CYBER secured electronic devices.

All electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without first being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the personal information or it is technologically not feasible to encrypt the data as and where transmitted.

### Access Control Protocol:

All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator.

Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique log- in ID assigned by the Data Security Coordinator.

To the extent applicable to each device type, all laptop and other computing: (i) will be equipped with a minimum of AES 128 bit full hard disk drive encryption and will have pre-boot pin based authentication; (ii) will have industry standard up to date virus and malware detection and prevention software installed with virus definitions updated no less than every three (3) calendar days; and iii) shall maintain software so as to remain on a supported release. This shall include, but not be limited to, the obligation to promptly implement any applicable security-related enhancement or fix made available by supplier of such software.

### Breach of Data Security Protocol:

Should an employee come to be aware that a security breach has taken place at any one of our facilities, that any amount of unencrypted personal information has been lost, stolen, or accessed without authorization, or that encrypted personal information, along with the access code or security key, has been acquired by an unauthorized person or for unauthorized purposes, the following protocol is to be followed:

Employees are to notify the Data Security Coordinator or department head in the event of a known or suspected security breach or unauthorized use of personal information.

In the event the security breach involves the potential exposure of partner customer data (Cloud , etc) or the compromise of partner systems, the Data Security Coordinator will immediately notify any relevant partner security organization. All subsequent steps shall be coordinated in agreement with the partner security organization.

The Data Security Coordinator shall also be responsible for drafting and logging a security breach notification. The security breach notification shall include the following:

* A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
* The steps already taken relative to the incident;
* Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
* Information regarding whether law enforcement officials are engaged in investigating the incident.
* Any corresponding notifications made to partner entities (Cloud , etc) that might be impacted by the breach.

Active Cyber already has a consistent level of data protection and security across our organization, but we have introduced new measures to ensure compliancy.

* Information Audit — We carried out audit to make sure we continue to not store any personal data on our computers.
* Policies and Procedures — we have revised data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:
  + Data Protection - our main policy and procedure document for data protection has been revised to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy and the rights of individuals.
  + Data Retention and Erasure – our policy is not to store any personal data on our computers.
  + Data Breaches - our procedures ensure that we have safeguards in place to identify, assess, investigate and report any personal data breach as early as possible. Our procedures have been explained to all employees.
  + International Data Transfers and Third-Party Disclosures - where Active Cyber stores or transfers personal information outside the EU, we have robust procedures in place to secure the integrity of the data.
  + Subject Access Request (SAR) - we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge
* Privacy Notice/Policy - our Privacy Notice complies with the GDPR, ensuring that all individuals whose personal information we may need to process and retain will be informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
* Obtaining Consent - we will seek consent before obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information
* Direct Marketing – we will not use any personal data for direct marketing.
* Data Protection Impact Assessments (DPIA) - where we process personal information that is considered high risk, we have developed stringent procedures for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subjects.
* Processor Agreements – we will not engage third parties to process personal data.

## Data Subject Rights

If we hold any personal data, we would provide easy-to-access information via our website of an individual’s right to access any personal information that Active Cyber processes about them and to request information about:

* what personal data we hold about them
* the purposes of the processing
* the categories of personal data concerned
* the recipients to whom the personal data has/will be disclosed
* how long we intend to store your personal data for
* if we did not collect the data directly from them, information about the source
* the right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
* the right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
* the right to lodge a complaint or seek judicial remedy and who to contact in such instances.

## Information Security and Technical and Organizational Measures

Active Cyber takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction.

# Legal basis for processing personal information (EEA visitors only)

If you are a visitor from the European Economic Area, our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it.

However, we will normally collect personal information from you only (i) where we need the personal information to perform a contract with you (including to provide Services), (ii) where the processing is in our legitimate interests and not overridden by your rights, or (iii) where we have your consent to do so. In some cases, we may also have a legal obligation to collect personal information from you or may otherwise need the personal information to protect your vital interests or those of another person.

If we ask you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information).

If we collect and use your personal information in reliance on our legitimate interests (or those of any third party), this interest will normally be to operate our Sites and Services and to communicate with you as necessary to provide our Sites and Services to you and for our legitimate commercial interest, for instance, when responding to your queries, improving our Sites and Services, undertaking marketing, or for the purposes of detecting or preventing illegal activities. We may have other legitimate interests, and if appropriate we will make clear to you at the relevant time what those legitimate interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided under the “How to contact us” heading below.

# How does Active Cyber keep my personal information secure?

We use appropriate technical and organizational measures to protect the personal information that we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information. When you enter sensitive information (such as login credentials), we encrypt the transmission of that information using secure socket layer technology (SSL).

We follow generally accepted standards to protect the personal information submitted to us, both during transmission and once we receive it. No method of transmission over the internet or method of electronic storage is 100% secure, however. Therefore, we cannot guarantee its absolute secrecy. If you have any questions about security on our Sites, you can contact us at [shawn.matthew@activecyber.com.](mailto:shawn.matthew@activecyber.com)

# International data transfers

Your personal information may be transferred to, and processed in, countries other than the country in which you are a resident. These countries may have data protection laws that are different from the laws of your country and, in some cases, may not provide the same level of protection.

Specifically, our Sites and Services are hosted in the USA, and our group companies and third- party service providers and partners operate around the world. The data we collect from you may be transferred to, and stored at, a destination outside the EEA. It may also be processed by staff operating outside the EEA who work for us or for one of our service providers.

However, we have taken appropriate safeguards to require that your personal information will remain protected in accordance with this Privacy Notice. These include EU-US and Swiss-US Privacy Shield, as well as APEC participation.

EU-U.S. and Swiss-U.S. Privacy Shield

Active Cyber participates in and has certified their compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. Active Cyber is committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Framework’s applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce’s Privacy Shield

List: [https://www.privacyshield.gov](https://www.privacyshield.gov/).

Active Cyber is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Active Cyber complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Framework, Active Cyber is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Active Cyber may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge)

at <https://feedback-form.truste.com/watchdog/request>.

Under certain conditions, more fully described on the Privacy Shield [website](https://www.privacyshield.gov/), you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

# Data retention

We retain personal information we collect from you where we have an ongoing legitimate business need to do so (for example, to provide you with a Service you have requested, for as long as your account remains active, or to comply with applicable legal, tax, or accounting requirements).

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

# Your data protection rights

Depending on the country in which you reside, you may have the following data protection rights:

* If you wish to **access, correct, update, or request deletion** of your personal information. These rights can be exercised by contacting us at the contact details provided under the “How to contact us” heading below.
* In addition, you can **object to processing** of your personal information, ask us to **restrict processing** of your personal information, or **request portability** of your personal information. Again, you can exercise these rights by contacting us using the contact details provided under the “How to contact us” heading below.
* You have the right to **opt out of marketing communications** we send you at any time. You can exercise this right by sending us an email at [shawn.matthew@activecyber.com,](mailto:shawn.matthew@activecyber.com) or you can unsubscribe by following instructions contained in the message you received. We do reserve the right to send you certain communications relating to the Services, such as service announcements and administrative messages, that are considered part of your account membership, and we do not offer you the opportunity to opt out of receiving those messages.
* Similarly, if we have collected and processed your personal information with your consent, then you can **withdraw your consent** at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.
* You have the **right to complain to a data protection authority** about our collection and use of your personal information. For more information, please contact your local data protection authority. Contact details for data protection authorities in the European Economic Area, Switzerland, and certain non-European countries (including the U.S. and Canada) are available [here.](http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm)

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. The data controller of your personal information is Active Cyber Inc.

If you have any questions about our GDPR compliance policies, please contact Shawn Mathew at 214-646-3353 or [shawn.mathew@activecyber.com](mailto:shawn.mathew@activecyber.com) via email.

|  |  |
| --- | --- |
| Signature:  \_ | Date:  30/04/2021 \_ \_ |

### APPENDIX A

**Partner Specific Security Directives**

### Cloud Application

In addition to the policies and procedures outlined above, all ACTIVE CYBER Cloud Application consultants are required to adhere to the following security practices and directives.

* 1. Only authorized ACTIVE CYBER consultants are permitted access to Cloud Application tenants, Projector and any other third-party applications used to support Cloud implementations or development activities.
  2. ACTIVE CYBER consultants will be diligent in ensuring the confidentiality, availability and integrity of Cloud client data. Specific requirements for ensuring the security of Cloud client personal data (any information related to client practices, client financial data and client users) are:
     1. No client personal data shall be resident on a consultant laptop unless that laptop is physically secured. No personal data should be resident on a laptop while it is in transit, whether in a consultant’s car, an airport or any other mode of transportation.
     2. No client personal data shall be resident on a consultant laptop unless that laptop is logically secured. All consultant laptops must maintain a valid anti-virus application that is running in auto-update mode to ensure maintaining the most recent virus and malware protection files.
     3. All consultants must utilize encrypted mechanisms for the storage and transmission of Cloud client personal data. Any files stored on laptops, desktops or any sort of removable storage must be secured via encryption (password protected zip files, etc). File transmission protocols must be encrypted (SFTP, PGP, HTTPS, etc).
  3. Any indication of any potential threat to, or exposure of, Cloud client personal data must be reported to the ACTIVE CYBER Data Security Coordinator (Shawn Mathew).